

# 协卡网络信任服务体系证书策略

UniTrust Network Trust Service Hierarchy Certificate Policies

(UNTSH CP)

1.0 版本

生效日期：2009 年 3 月 26 日



上海市数字证书认证中心有限公司

上海市北京西路 1318 号



## 《协卡网络信任服务体系证书策略》

### UniTrust Network Trust Service Hierarchy Certificate Policies

本文档由上海市数字证书认证中心有限公司（SHECA）编写和发布，SHECA 拥有全部版权。

任何需要本文的单位或者个人，可以与上海市数字证书认证中心有限公司政策法规部联系：

地址：上海市北京西路 1318 号 200040

电话：86-21-62077146

电子邮件：policy@sheca.com

#### 商标说明

UniTrust 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
V1.0	2009年3月26日	崔久强	SHECA 安全认证委员会	初次发布

版权所有@上海市数字证书认证中心有限公司

本文件所有版权归上海市数字证书认证中心有限公司所有。未经书面授权，本文件中所有的文字、图表不得以任何形式进行出版。



## 声明

本 CP 全部或者部分支持下列标准：

- RFC3647：互联网 X.509 共钥基础设施-证书策略和证书业务声明框架
- RFC2459：互联网 X.509 共钥基础设施-证书和 CRL 属性
- RFC2560：互联网 X.509 共钥基础设施-在线证书状态协议-OCSP
- ITU-T X.509 V3（1997）：信息技术—开放系统互连—目录：认证框架
- RFC 3280：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，按照 AICPA/CICA WebTrust for Certification Authority 进行评估，本 CP 符合上述审计标准的情况，将在 [www.sheca.com](http://www.sheca.com) 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.....	10
1.3 PKI 参与者.....	10
1.4 证书使用.....	11
1.5 策略管理.....	13
1.6 定义与缩写.....	14
2. 发布和信息库责任.....	15
2.1 信息库.....	15
2.2 认证信息发布.....	15
2.3 发布时间或频率.....	15
2.4 信息库访问控制.....	15
3. 身份标识与鉴别.....	16
3.1 命名.....	16
3.2 初始身份的确认.....	17
3.3 密钥更新请求的标识与鉴别.....	18
3.4 吊销请求的标识与鉴别.....	19
4. 证书生命周期操作要求.....	20
4.1 证书申请.....	20
4.2 证书申请处理.....	21
4.3 证书签发.....	21
4.4 证书接受.....	22
4.5 密钥对和证书使用.....	22
4.6 证书更新.....	23
4.7 证书密钥更新.....	25
4.8 证书变更.....	26
4.9 证书吊销和挂起.....	27
4.10 证书状态服务.....	30
4.11 订购的结束（终止服务）.....	31
4.12 密钥托管和恢复.....	31
5. 设施、管理和运作控制.....	32
5.1 物理控制.....	32
5.2 程序控制（流程控制、过程控制）.....	33
5.3 人员控制.....	35
5.4 审计记录程序.....	36
5.5 记录归档.....	38
5.6 密钥变更.....	39
5.7 损害灾难恢复.....	40

5.8 CA 或 RA 的终止.....	41
6. 技术安全控制.....	42
6.1 密钥对生成和安装.....	42
6.2 私钥保护和密码模块工程控制.....	43
6.3 密钥对管理的其他方面.....	46
6.4 激活数据.....	47
6.5 计算机安全控制.....	48
6.6 生命周期技术控制.....	48
6.7 网络安全控制.....	49
6.8 时间戳.....	49
7. 证书、CRL 和 OCSP 描述（轮廓）.....	50
7.1 证书描述（轮廓）.....	50
7.2 CRL 描述.....	53
7.3 OCSP 描述.....	53
8. 一致性审计和其它评估.....	54
8.1 评估的频率或情形.....	54
8.2 评估者的资质.....	54
8.3 评估者和被评估者的关系.....	54
8.4 评估包含的主题（评估内容）.....	55
8.5 对不足采取的行动.....	55
8.6 评估结果沟通.....	55
9. 其它事项和法律事务.....	57
9.1 费用.....	57
9.2 财务责任.....	58
9.3 业务信息保密.....	58
9.4 个人信息隐私保护.....	60
9.5 知识产权.....	61
9.6 陈述与担保.....	62
9.7 担保免责.....	64
9.8 有限责任.....	64
9.9 赔偿.....	64
9.10 有效期和终止.....	65
9.11 对各参与方的个别通知和沟通.....	65
9.12 修订.....	65
9.13 争议解决条款.....	66
9.14 管辖法律.....	66
9.15 与适用法律的符合性.....	66
9.16 其它条款.....	67
9.17 其它条款.....	67
附录 A 定义和缩写.....	68
附录 B 证书格式.....	71
附录 C CRL 格式.....	74

# 1. 导言

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证书策略 (UniTrust Network Trust Service Hierarchy Certificate Policies, 缩写为 UNTSH CP), 是协卡认证数字证书服务的策略声明, 适用于所有由 UNTSH 签发和管理的数字证书及相关参与主体。证书策略是一套命名的规则集, 用以指明证书对一个特定团体和 (或者) 具有相同安全需求的应用类型的适用性。依赖方利用证书策略来帮助其决定一个证书 (以及其中的绑定) 是否足够可信, 或者是否适用于某特定应用。本 CP 为 UNTSH 架构内的证书申请、签发、管理、使用、吊销、更新以及为 UNTSH 架构内所有的参与方提供相关信任服务方面制定了业务、法律和技术上的要求和规范。这些规范保护 UNTSH 证书服务的安全性和完整性, 包含一整套在 UNTSH 范围内一致适用的单一规则集, 因此在整个 UNTSH 架构内能够提供同样的信任担保。本 CP 并不是 SHECA 和 UNTSH 各参与方之间的法律性协议, SHECA 和 UNTSH 各参与方之间的权利义务依靠他们之间签署的各类协议构成。

本 CP 的对象包括:

- UNTSH 内的认证服务机构, 遵循本 CP 的规范制定电子认证业务规则 (CPS), 并按照其 CPS 运营
- UNTSH 内的订户, 需要了解身份鉴别要求, 作为订户权利义务, 以及 UNTSH 对其提供的保护
- 依赖方, 需要了解在多大程度上信任一张 UNTSH 证书或该证书的电子签名

本 CP 不适用于任何非 UNTSH 内的任何服务, 例如 SHECA 为某些企业或组织建立的那些自行运营的内部 CA。

本 CP 满足互联网工程工作组 (The Internet Engineering Task Force, IETF) RFC 3647 《证书策略和证书业务声明框架 (Certificate Policy and Certificate Practice Statement Construction)》的结构和内容要求, 并根据中国的法律规定和 SHECA 的运营要求进行了适当的改变。

## 1.1 概述

本 CP 作为最高策略, 为整个 UNTSH 内的证书提供管理、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。本 CP 设定了 UNTSH 根证书的架构、生命周期、使用、依赖和管理的角色、责任、流程, 以及各相关主体的职责。作为根证书的运营方, SHECA 管理 UNTSH 根证书的层次机构。本 CP 制定了 UNTSH 所有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。

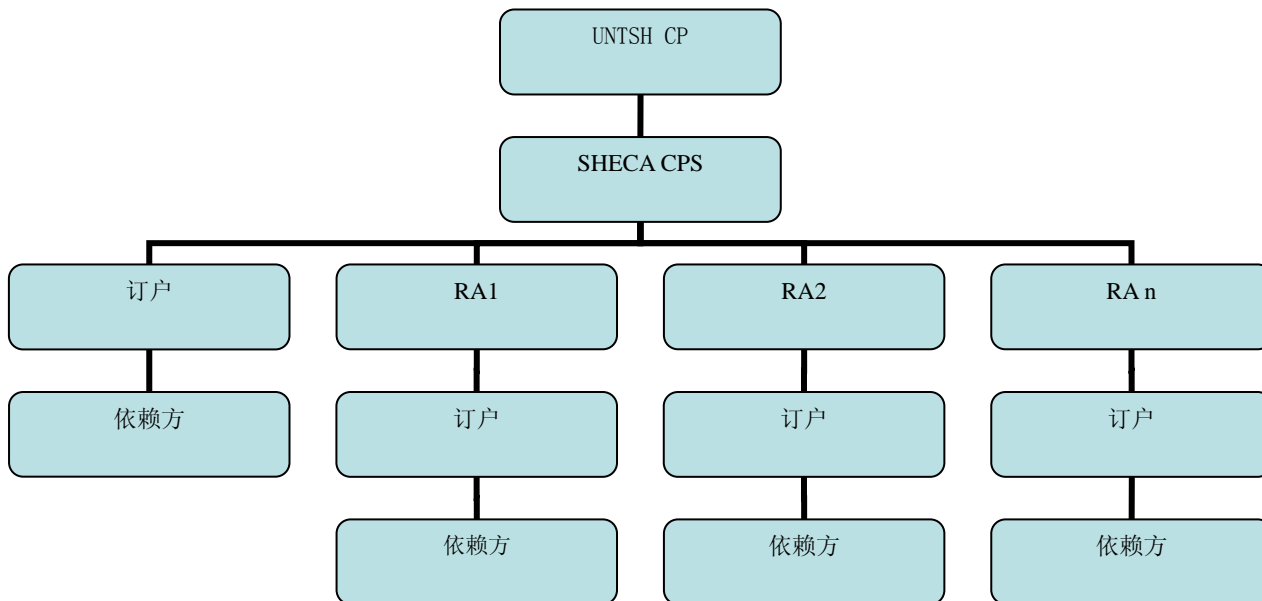
SHECA 作为一个证书服务机构 (CA), 在本 CP 的约束下生成根证书和子 CA 证书, 签发订户证书。证书注册机构 (RA) 是 UNTSH 内鉴别证书请求的实体, SHECA 本身同时也是一个

RA, 其他组织、企业等通过与 SHECA 签署协议, 也可以作为 UNTSH 的 RA, 鉴别其相关用户的证书请求。基于不同的类型和应用范围, 作为证书持有人的订户可以使用证书进行网络站点安全保护、代码签名、邮件签名、文档签名、身份认证等不同的应用。依赖方依照本 CP 中关于依赖方的义务要求, 决定是否信任一张证书。SHECA 的电子认证业务规则 (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](http://www.sheca.com) 上公布被审查的结果。

## 1.1. 1 UNTSH 架构

本 CP 是 UNTSH 最高的策略, UNTSH 的证书服务机构 (CA) 按照本 CP 制定 CPS, RA 按照本 CP 及相关 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 及相关 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、各相关注册机构 (RA 中心)、服务分理中心 (RAB)、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 CP 以及相应 CPS 的要求。

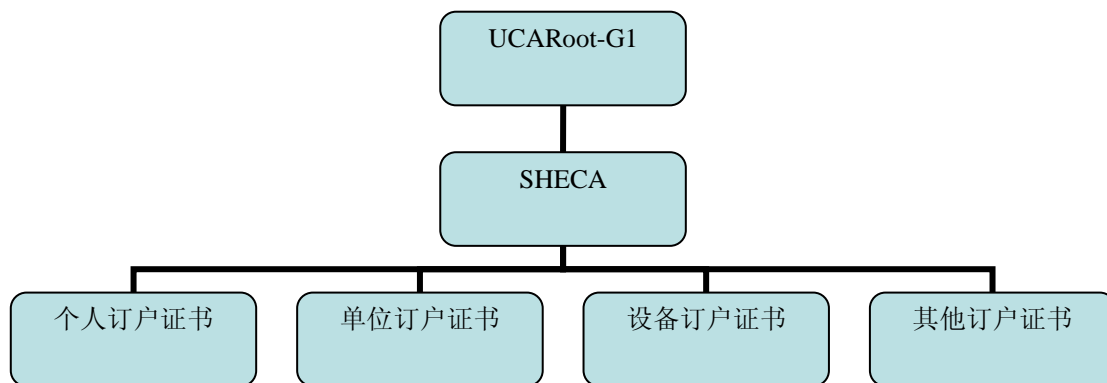


## 1.1.2 UNTSH 证书层次架构

UNTSH 目前有 3 个根 CA 证书, 分别为 UCA Global Root、UCA Root G1 和 UCA Root G2, 均为自签发根证书, 由 SHECA 管理和运营。每个根 CA 下设子 CA, 以签发用户证书。

协卡认证体系的 PKI 层次架构如下:

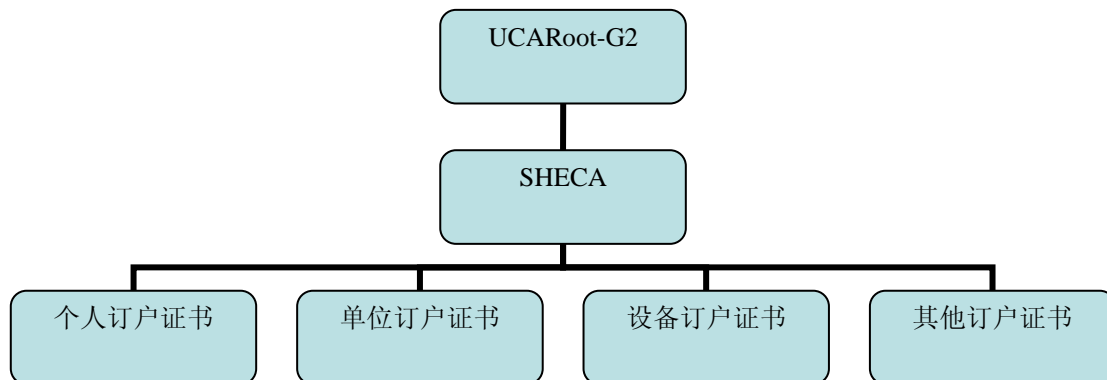
- UCA Root-G1 (1024-bit)



UCA Root-G1 根密钥长度为 1024-bit，下设 SHECA 子 CA 证书，签发个人订户证书、单位订户证书、设备订户证书和其他订户证书。

UCA Root-G1 将于 2013 年 1 月 1 日到期，2009 年 1 月 1 日起不再签发下级证书。

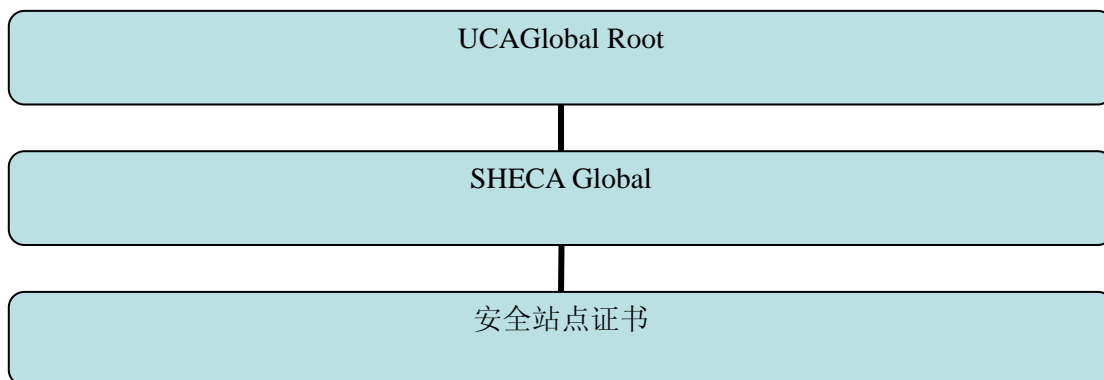
- UCA Root-G2 (2048-bit)



UCA Root-G2 根密钥长度为 2048-bit，下设 SHECA 子 CA 证书，签发密钥长度为 1024-bit 或者 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。

UCA Root-G1 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 Global Root (4096-bit)



UCA global Root 根密钥长度为 4096-bit，下设 SHECA 子 CA 证书，只签发密钥长度为

2048-bit 位安全站点证书。

UCA Root-G1 有效期将于 2037 年 12 月 31 日到期，2033 年 1 月 1 日起不再签发下级证书。

### 1.1.3 UNTSH 证书信任等级

UNTSH 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，UNTSH 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。

## 1.2 文档名称和标识

本文档的名称为《协卡网络信任服务体系证书策略》(UniTrust Network Trust Service Hierarchy Certificate Policies，缩写为 UNTSH CP)，简称为协卡认证体系证书策略。SHECA 没有为其分配对象标号符。

## 1.3 PKI 参与者

### 1.3.1 电子认证服务机构 (CA)

电子认证服务机构是颁发证书的实体。SHECA 是依法设立电子认证服务机构，建设和运营 UNTSH。UNTSH 是多层次的 CA 结构模式，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。通常，根 CA 只签发子 CA 证书，子 CA 签发可签发最终用户证书或其它 CA 的证书。协卡认证体系内的 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示的主体都可以成为本 CP 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 作为运营主体，负责制定和发布 UNTSH 的证书策略，发布证书吊销列表，发布证书信任链，并负责证书生命周期的全面管理，包括证书的签发、吊销、更新、状态查询和炎症、目录服务等。同时，SHECA 还要管理下属的所有证书注册机构 (RA)。

### 1.3.2 注册机构 (RA)

注册机构 (RA)，是为最终用户证书申请者建立注册过程的实体，对证书申请者进行身份标识和鉴别，初始化或拒绝证书吊销请求，代表 CA 批准更新证书或更新密钥的申请。UNTSH 的 RA 既可以是 CA 的下属组成部分，由 SHECA 指定的部门担任，又可以独立于 CA 之

外，由 SHECA 和相关组织签订相关协议，授权委托其担任 RA 的角色。

RA 必须在 SHECA 的批准和授权下，按照本 CP 和相应 CPS 确定的流程和规范才可以进行证书服务操作。SHECA 在发展 RA 时，必须对 RA 进行适当的评估，以确认其是否能够履行 RA 的职责。

### 1.3.3 订户

订户，即从 CA 接收证书的实体，包括所有从 UNTSH 接受证书的个人、单位。订户和申请人很多时候并不一致，如果订户和申请人不一致，则需要申请人保证获得明确、适当的授权。个人又分为自然人和从属于某一单位的个人；单位包括各类政府组织、企事业单位和其它社会团体，一般而言，单位应该具有法人资格或者组织机构代码证号码；对于设备类证书，由于证书中包含主体的特殊性，订户通常应被理解为拥有该设备的单位或者个人，并由拥有该设备的单位或者个人承担相应的义务。

在电子政务应用中，由于某些特定应用的需要，某一政府机构为某些特定群体用户申请证书，可能不方便或者无法提供详细的、完整的订户身份证明信息。对于此类用户，该政府机构需要提供订户身份的说明信息，并为其做出身份真实性的保证，以书面形式提交给 SHECA。

订户代表着证书中公钥所绑定的唯一实体，拥有对与其证书唯一对应的私钥的最终控制权。订户在本 CP 的范围内使用证书，愿意并能够承担本 CP 约定的义务。

### 1.3.4 依赖方

依赖方，是指信任证书、使用证书或者使用证书里的公钥来验证电子签名的个人或者单位。依赖方可以是证书订户，也可以不是订户。

要信任或者验证一张证书，依赖方必须验证证书的吊销信息，包括证书吊销列表(CRL)、查询、OCSP 查询以及其它的查询方式。依赖方必须经过合理的审核后才能够信任一张证书。

### 1.3.5 其他参与方

在提供证书服务时，提供单位或个人身份信息查询和验证或者其它额外需要提供信息的组织，可以作为 UNTSH 的合作方协助完成对证书申请信息的鉴别。

一些不是 SHECA 批准的 RA，但是为某一特定群体申请证书、验证证书信息并支付证书费用的组织，被称为证书垫付商。SHECA 通过与垫付商签署协议，为其涉及的特定用户群体提供所需的证书服务。该类垫付商及其特定的证书订户群体同样需要遵循本 CP 的规定。

## 1.4 证书使用

在 CP 或 CPS 描述不同保证等级的情况下，该子项能够描述对不同保证等级适用或不适用的应用或应用类别。

## 1.4.1 合式（适当）的使用

UNTSH 的订户证书是通用证书，按照证书类型的不同，都有适用的应用。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。除了因为证书标识的主体身份的不同而导致的证书应用差异外，UNTSH 订户证书可以广泛应用在电子政务、电子商务或者其它社会化活动中，以实现身份认证、电子签名等目的。法律法规和国家政策有限制的除外。

UNTSH 订户证书，从功能上可以满足下列安全需要：

- 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。
- 信息传输机密性-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。

证书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。

### 1.4.1.1 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。

### 1.4.1.2 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。

### 1.4.1.3 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。

### 1.4.1.4 安全站点证书的使用

安全站点证书标识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。

## 1.4.2 禁止的使用

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CP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

SHECA 作为 UNTSH 的运营方,成立 SHECA 安全认证委员会,作为策略管理机构,负责制定、维护和解释本 CP。SHECA 安全认证委员会至少应包含一名 SHECA 的管理层成员,两名 UNTSH 运营服务主管、一名直接参与策略编写的成员。SHECA 安全认证委员会的主任由管理层成员担任。

SHECA 安全认证委员会的所有成员在就证书策略进行管理和批准时,均享有一票决定权,如果选票相同,认证委员会主任可拥有双票决定权。

SHECA 政策法务部作为认证委员会的日常工作机构,负责起草本 CP 并根据要求提出修改报告,负责此方面的对外咨询服务。

### 1.5.2 联系人

SHECA 指定政策法务部作为本 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 政策法务部联系。

联系人:上海市数字证书认证中心有限公司政策法务部。

电话:86-21-62077146

传真:86-21-62077101

地址:中华人民共和国上海市北京西路1318号

邮政编码:200040

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。SHECA 安全认证委员会作为最高策略管理机构，是批准和决定 SHECA 或者其它某个 CA 的 CPS 是否符合本 CP 的机构。

政策法务部作为 SHECA 安全认证委员会指定的策略工作部门，负责 CPS 实施的日常监督检查，保证 CA 依据其 CPS 进行的运营服务符合本 CP 的要求。

### 1.5.4 CP 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。

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本 CP 进行修改，由政策法务部提交修改建议报告，提交 SHECA 安全认证委员会审核。经过该委员会批准后，SHECA 通过 [www.sheca.com](http://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 后向信息产业部备案。

## 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 建立和维护一个可公开访问的在线信息库，用于发布本证书策略（CP）、电子认证业务规则（CPS）、相关协议、证书、证书吊销列表（CRL）、证书在线状态查询（OCSP）等。SHECA 的信息库，应包括作为证书服务一部分的证书和证书状态查询等信息，以及作为证书策略及相关文档等信息，这两类信息可以通过不同的方式进行发布。

SHECA 在其 CPS 以及其它文档中公布其信息库的位置和方式，以方便有关方能够访问并获取所需信息。

### 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、证书吊销列表、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、证书吊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](http://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 及时发布证书策略、电子认证业务规则、证书服务和使用的协议等文档以及文档的修订信息。

SHECA 应至少在 24 小时以内发布一次订户证书的证书吊销列表（CRL），应至少每三个月发布一次子 CA 证书（Sub-CA Certificate）的证书吊销列表（ARL），每年发布一次根证书（Root-CA Certificate）列表，如果根证书被吊销，应及时在网站公布吊销信息。

SHECA 应在本 CP 或相应 CPS 规定的时间内，及时发布证书，以供下载、查询和使用。

### 2.4 信息库访问控制

SHECA 不对包括 CP、CPS、证书、证书状态信息和 CRL 的访问进行限制，但任何对证书、证书状态信息和证书吊销列表有访问需求的相关方应该遵循本 CP 和相关 CPS 的要求，SHECA 并保留设置访问控制措施的权利。

SHECA 采取措施限制对信息库进行任何未经授权的增加、删除、修改等操作。

## 3. 身份标识与鉴别

此项描述在颁发证书之前对最终用户证书申请者的身份和（或）其它属性进行鉴别的过  
程。对于期望成为 CA、RA 或其它 PKI 运营机构的实体，此项设置鉴别其身份的过程和接  
受准则。此项还描述如何鉴别密钥更新请求者和吊销请求者。另外，此项还说明命名规则，  
包括在某些名称中对商标的承认问题。

### 3.1 命名

除非在本 CP、相关 CPS 中特别指出，UNTSH 的证书命名都应是被鉴别和证实的。

#### 3.1.1 命名类型

命名应符合 X. 500 的规定。订户证书应在主题中包含一个 X. 501 甄别名。

#### 3.1.2 对命名有意义的要求

订户的命名一定要有意义，应具有通常能够被理解的语义，可以明确确定证书主题中  
的个人、单位或者设备的身份。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

订户证书不被允许使用匿名或假名，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 解释不同 命名的规则

UNTSH 订户证书按照 X. 500 规则解释不同命名。

#### 3.1.5 命名的唯一性

UNTSH 订户证书的命名，在整个 CA 信任域内必须是唯一的。命名的唯一性意味着可以  
将名称与唯一的实体（个人、单位或者设备）对应起来。当出现相同的名称时，以先申请者

优先使用。

### 3.1.6 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。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。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。

在证书申请者提交的命名中包含商标信息时，申请者应被要求提交商标注册文件（众所周知的驰名商标可以不被要求），但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。

## 3.2 初始身份的确认

### 3.2.1 证明拥有私钥的方法

证书申请者必须证明持有与所要注册公钥相对应的私钥，证明的方法包括在证书请求消息中包含数字签名（PKCS#10）、其它与此相当的密钥标识方法，或者 SHECA 要求的其它证明方式，包括提交 SHECA 发放的初始化信息（被分配的密钥存储介质和与其相对应的密码信封中包含的口令）等。

### 3.2.2 组织机构身份的鉴别

任何组织（政府机构、企事业单位等），在以组织名义申请单位证书、设备证书、邮件证书等各类型证书时，其身份应当被进行严格的身份，包括：

- 任何由第三方提供的证明该组织确实存在的资料，例如由政府机构发放的合法性证明（组织机构代码证、工商营业执照等信息），以及其它被认可的权威组织提供的证明资料。
- 通过电话、邮政信函、被要求的证明文件或者与此类似的其它方式确认该组织资料信息的真实性，申请人是否得到足够的授权一起其它需要验证的信息。

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、归属权证明文件等。

SHECA 还可以为 UNTSH 订户证书的组织身份鉴别设定其它所需要的鉴别方式和资料。

### 3.2.3 个人身份的鉴别

对于所有类型的个人身份证书，包括身份证书、邮件证书、代码签名证书、域名证书等，在申请时都必须确认个人申请者的真实身份。包括：

- 个人应当提交其法定的身份证明文件，包括身份证、军官证或者其它相当的身份证

明资料。

- 面对面审核，或者以其他电话、邮政信函等方式确认身份资料等信息的真实性。
- 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。
- 对于委托他人进行申请的，要提交被充分授权的书面证明文件。

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，可委托第三方进行调查，或要求申请者提供额外的信息和证明材料。

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、归属权证明文件等。

SHECA 还可以为 UNTSH 订户证书的个人身份鉴别设定其它所需要的鉴别方式和资料。

### 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

### 3.2.5 授权的确认

对授权的确认包括如下两个方面：

- 委托申请的授权确认，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，需要确认委托人的授权证明、被委托人的身份资料
- 当个人申请者的申请信息总包含组织信息（政府机构、企事业单位）时，需要确认该组织是否存在，以及该申请人是否属于该组织的成员

如果 SHECA 无法得到所有需要的信息，可委托第三方进行调查，或要求证书申请者提供额外的信息和证明材料。

### 3.2.6 互操作原则

SHECA 允许非 UNTSH 的认证机构（CA）能够和 UNTSH 进行互操作，但是该 CA 必须满足以下条件：

- 与 SHECA 签署相关的协议
- 其 CPS 符合本 CP 的要求
- 接受 SHECA 对其进行的评估和年度审查

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

为此，SHECA 要求订户生成一对新的密钥对取代到期证书的密钥对，为之生成新的证书，这称之为证书密钥更新（re-key）。但是，很多时候，订户往往要求在获得新的证书时继续

使用到期证书所对应的密钥对，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。

### 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。

### 3.3.2 吊销后密钥更替的识别与鉴别

发证机构不提供证书被吊销后的密钥更新。订户使用原始身份验证相同的流程进行申请，包括必须重新进行身份鉴别和注册，并生成新的密钥对，申请签发新的证书。

## 3.4 吊销请求的标识与鉴别

证书吊销请求可以来自订户，也可以来自 CA 或者 RA。在申请吊销时，订户需要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，CA 或者 RA 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吊销，CA 或者 RA 将直接以司法机关书面的吊销请求文件作为鉴别依据，不再进行其他方式的鉴别。

在紧急情况或者特殊情况下，订户可以自己吊销证书。在此情形下，订户需要使用证书私钥保护口令激活私钥对吊销请求进行签名，并由 CA 进行签名验证。CA 或者 RA 可以采用电话、传真、邮政信函的方式对订户的吊销进行验证。

SHECA 保证对于吊销请求的鉴别，予以合理的进行。

CA 机构的证书吊销请求，必须经过其管理机构或者监督机构进行确定才可以进行。

## 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

下列人员可以提交证书申请：

- 个人申请者，其身份必须所申请的证书主题相对应，委托他人代为申请的，必须出具可靠的授权证明文件
- 政府机构、企事业单位或其它社会组织的授权代表
- 经过授权的 CA 机构的代表
- 经过授权的 RA 机构的代表

#### 4.1.2 注册过程和责任

##### 4.1.2.1 申请者的责任

对于终端来说用户来收，所有申请者在申请证书时，必须了解订户协议的内容，特别是其中关于义务和担保的内容。在证书申请注册的过程中，还需要做到：

- 填写证书申请表，根据申请的证书类型提供真实、可靠、完整的身份资料
- 产生密钥对，或者提交委托生成密钥对的书面文件
- 将公钥上送给 CA
- 证明对私钥的拥有权

对于申请 RA 及 CA 机构证书的申请者，必须与 SHECA 签署协议后，递交相应的申请证明资料，才能进行申请。其证书的命名和证书内容由 SHECA 决定。

##### 4.1.2.1 申请注册过程

申请者将证书请求发送到 RA，RA 验证该请求，并对其签名，然后将其发送给 CA。CA 接收到该请求后，验证 RA 的签名，签发订户证书。在整个注册过程中，必须采取措施保证：

- RA 必须对申请信息和申请者的资料进行鉴别
- 在 RA 向 CA 发送证书请求时，保证传输信息过程安全、保密、完整

## 4.2 证书申请处理

### 4.2.1 执行识别与鉴别

作为证书注册机构，RA 需要根据前面 3.2 条款的要求，对证书申请进行标识和鉴别。在鉴别时，RA 应该采取足够合理的方式进行。

### 4.2.2 批准或拒绝证书申请

如果符合下述条件，RA 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

如果发生下列情形，RA 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

### 4.2.3 处理证书申请的时间

CA 和 RA 将在合理的时间内处理证书申请，无论是批准还是拒绝。虽然 SHECA 对于证书处理并没有明确的时间限定，但这种处理通常应该在 7 个工作日内完成，除非在相关的订户协议、CPS 或者其它的协议对此有专门的约定。

## 4.3 证书签发

### 4.3.1 证书签发期间 CA 的行为

在证书申请被批准后，CA 将验证 RA 上送的证书请求中该 RA 的签名，并根据证书请求签发订户证书。CA 签发证书时，该证书包含的内容基于被批准的证书请求中的订户身份信息。

### 4.3.2 CA 通知订户证书签发

CA 签发证书时，将直接或者通过 RA 通知订户证书已被签发，并向订户提供可以获得证书的方式，包括通过网络下载、通过邮件发放等方式，或者通过其它与订户约定的方式告

知订户如何获得证书。

## 4.4 证书接受

### 4.4.1 构成证书接受的行为

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、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 CA 发布证书

CA 将已经签发的证书发布到可以被公开访问的信息库中，包括 LDAP 目录发布、HTTP 方式发布等。

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 CA 通知其他实体证书的签发

CA 在签发证书时，可能会将证书发送给批准该证书的 RA。但是通常情况下，CA 不专门对包括 RA、受理点、主管部门等在内的其它实体进行专门的通知，这些实体可以通过目录服务或者查询信息库来获得订户证书及相关信息。

如果法律法规另有要求，CA 将会按照其规定进行通知操作。

## 4.5 密钥对和证书使用

### 4.5.1 订户私钥和证书使用

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 CP 及相关 CPS 的规定的法的被使用。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。

在证书到期或被吊销之后，订户必须停止使用私钥。

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。

SHECA 签发的各类证书，仅用于表明订户在申请证书时所标识的身份，以及验证订户

用于该证书内包含的公钥相对应的私钥做出的签名。任何超出本 CP 及相关 CPS、订户协议的规定使用证书及其对应的私钥的，SHECA 将不承担由此带来的任何后果。

## 4.5.2 依赖方公钥和证书使用

依赖方只能在接受本 CP 的要求的情况下，在正当的应用范围内依赖 UNTSH 订户证书。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。如果某些应用要求在使用证书时需要额外的保证，依赖方必须独立、合理的对这种保证进行判断并作出决定。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，依赖方必须据此来建立对该证书的依赖。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。

在依赖方对 UNTSH 订户证书采取任何依赖行为前，必须独立的评估和判断：

- 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，是否已经被吊销。如果订户证书或者其证书链内的任何证书已经被吊销，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吊销前做出的。

除非本 CP 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 CP 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。任何关于对证书的依赖所造成的风险均由依赖方独立承担，除非能够证明是 CA 或者 RA 的错误所致。

在对证书是否被适当的应用作出判断后，依赖方应该利用适当的软件或者硬件去验证签名或者其它所需要的操作。

## 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。

### 4.6.1 证书更新的情形

每张证书都有其有效期，在证书到期时，订户需要获得一张更新的证书，以继续使用证书。

如果证书已经到期，订户依然可以进行通过证书更新来获取新的证书，除非该证书的安全性能够出现问题。

## 4.6.2 要求更新的实体

只有下列人员可以要求证书更新：

- 个人证书订户，如果委托他人办理，需要提供明确的授权文件
- 单位证书订户被明确授权的代表
- 拥有设备证书的个人，拥有设备证书的单位被明确授权的代表

## 4.6.3 处理证书更新请求

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

订户也可以选择一般的初始证书申请流程进行证书更新，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证书更新时的鉴别处理手段。

## 4.6.4 通知订户新证书签发

同 4.3.2。

## 4.6.5 构成更新证书接受的行为

同 4.4.1。

## 4.6.6 CA 对更新证书的发布

同 4.4.2。

## 4.6.7 CA 通知其他实体证书的签发

同 4.4.3。

## 4.7 证书密钥更新

证书密钥更新是指在在不改变证书中包含的信息的情况下，订户生成新的密钥对，CA 用其中新的公钥为订户签发一张新证书。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。

### 4.7.1 证书密钥更新的情形

每个证书都有其有效期，在证书到期时，订户需要获得一张包含新公钥的新证书，以继续使用证书。

如果证书已经到期，订户依然可以进行通过证书密钥更新来获取新的证书。被吊销后的证书，不能申请证书密钥更新，只能按照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

只有下列人员可以要求证书密钥更新：

- 个人证书订户，如果委托他人办理，需要提供明确的授权文件
- 单位证书订户被明确授权的代表
- 拥有设备证书的个人，拥有设备证书的单位被明确授权的代表

### 4.7.3 处理证书密钥更新请求

对于证书密钥更新，其处理过程需要确保提出证书密钥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足以识别订户身份的信息，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

订户也可以选择一般的初始证书申请流程进行证书密钥更新，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证书密钥更新时的鉴别处理手段。

### 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 4.4.1。

## 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生成新的证书。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。

### 4.8.1 证书变更的情形

在证书有效期内，如果订户证书内所包含的信息发生下列变更，而这种变更不会影响订户权利义务的变化，则可以申请证书变更。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，只能吊销该证书，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 要求证书变更

同 4.1.1。

### 4.8.3 处理证书变更请求

同 3.2。

## 4.8.4 通知订户新证书的签发

同 4.3.2。

## 4.8.5 构成变更证书接受的行为

同 4.4.1。

## 4.8.6 CA 对变更证书的发布

同 4.4.2。

## 4.8.7 CA 通知其他实体证书的签发

同 4.4.3。

## 4.9 证书吊销和挂起

证书吊销包括申请吊销和强制吊销。证书吊销后，订户可以重新向 CA 申请签发新的证书，与初始申请时的流程和要求相同。

目前，SHECA 不提供证书挂起服务。

### 4.9.1 证书吊销的情形

发生下列情形，订户证书可以被吊销：

- 订户提出吊销要求
- 订户、CA、RA 或其它相关方有理由相信或怀疑一个订户的私钥安全已经受到损害
- CA 或 RA 或其它相关方有理由相信订户违背了订户协议下的义务、陈述或担保，或者订户无法履行协议规定的义务
- 和订户达成的协议已经终止
- CA 或 RA 有理由相信证书签发时没有依据本 CP 或相关 CPS 的规定，证书签发给非证书主题所标识的人员，证书签发时进行合理或者可靠的鉴别
- CA 或 RA 有理由相信证书申请中的信息和订户的真实信息不相一致或者有违背事实的错误或失误
- CA 或 RA 确定证书签发的一个必要前提条件既没有满足又没有豁免
- 订户的名称或者甄别名发生了改变
- 证书内包含的信息（包括证书中包含的未经鉴别的信息）发生了改变或者错误
- 证书继续使用将会对 UNTSH 造成损害
- 由于证书系统发生改变会导致订户的信任和担保程度

- 证书机构、企事业单位或其它社会性团体等组织为其员工申请的证书，该员工已经不再隶属于该组织
- CA 的密钥发生改变
- 法律法规的相关规定或要求

对于 UNTSH 证书服务系统中使用的证书，例如 CA、RA、受理点或其它服务主体（包括服务系统中的设备使用的证书）使用的证书发生下列情形，可以吊销其证书：

- CA 与 RA、受理点等签订的协议终止或者发生改变
- 证书私钥发生安全性损害或者被怀疑发生安全性损害
- 出于管理的需要

证书订户如果发现或者怀疑证书私钥安全发生损害，应立即通知 CA 进行吊销。

## 4.9.2 要求证书吊销的实体

下列实体能够要求吊销证书：

- 证书订户或其委托代表
- CA、RA、受理点或者证书垫付商
- 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 证书吊销请求的处理程序

在申请证书吊销时，CA 将对吊销请求进行验证和鉴别，以确保该证书是被合理、可靠的吊销。具体的处理流程包括：

- 证书订户（或者其授权的委托代理人）书面填写申请表并签名，并提交了合法的身份证明材料
- 非面对面的方式提出吊销要求，必须经过电话、传真等方式进行确认
- 除证书订户（或者其授权的委托代理人）外的其他实体，如 CA、RA、受理点、法院、政府主管部门及其他公权力部门，以及为订户申请证书的组织，提出吊销时也必须按照规定填写申请表并签字或盖章，并提交相应的证明材料。
- 所有非经订户本人提出的吊销请求，必须经过 SHECA 安全认证委员会认可。由于证书制作过程中的失误（例如证书下载错误、密钥对不匹配）导致的证书吊销，由客户服务部门主管批准，并定期报 SHECA 安全认证委员会。
- CA 收到吊销请求后，应验证申请者的身份、权限和吊销理由的正当性，确认无误后进行吊销
- 证书被吊销后，应被及时公开发布到证书吊销列表
- CA 必须对吊销进行记录，包括批准吊销人员的其姓名、签名、验证程序和结果、吊销理由及吊销的日期等

认证机构、注册机构在确信出现 4.9.1 中的情况而需要立即吊销证书时，可以立即吊销证书。

## 4.9.4 吊销请求的宽限期

证书吊销请求应该在一个合理的期限内提出。通常，自发现需要吊销到提出吊销请求之间间隔的期限，不得超过 8 个小时。

## 4.9.5 CA 必须处理吊销请求的时间

CA 在收到吊销请求后应采取合理的步骤进行处理，不得进行拖延。通常，自接到吊销请求到完成吊销之间的间隔期限，不得超过 4 个小时，并且应该在吊销后不超过 24 小时内把吊销信息发布到证书吊销列表。

## 4.9.6 依赖方检查吊销的规定

依赖方在信任 UNTSH 证书前，需要检查该证书的状态信息，包括查询证书吊销列表、通过 [www.sheca.com](http://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。

## 4.9.7 CRL 签发频率

CA 必须定时签发证书吊销列表（CRL），对于订户证书，至少每 24 小时签发和公布一次，对于子 CA 证书，至少每 3 个月签发和公布一次，对于根 CA 证书，必须每年公布一次。

SHECA 安全认证委员会可根据情况，自主决定缩短产生和更新 CRL 的时间，法律法规另有规定的除外。

## 4.9.8 CRL 最大滞后时间

证书被吊销后，应该在一个合理的期限内发布到 CRL，通常这取决于系统的处理速度。UNTSH 保证在证书被吊销后，最晚也将在吊销行为发生的 24 小时内将其发布到 CRL。

## 4.9.9 在线吊销/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）或者基于网站方式（http）的证书状态信息查询、。

## 4.9.10 在线吊销检查的要求

依赖方在信赖一张证书前必须检查该证书的状态。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 吊销公告可获得的其他方式

无规定。

### 4.9.12 密钥损害的特殊要求

UNTSH 各参与方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吊销。如果 CA 的密钥（根 CA 或子 CA 密钥）安全被损害或者怀疑被损害，应该在合理的时间内用合适的方式及时通知订户和依赖方。

### 4.9.13 证书挂起的情形

无规定。

### 4.9.14 谁能要求挂起

无规定。

### 4.9.15 挂起请求的程序

无规定。

### 4.9.16 挂起的期限

无规定。

## 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，或者通过 CA 发布的网络地址（URL）以 Http 方式进行查询。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。

### 4.10.3 可选功能

OCSP 是一项可选的服务，在很多情形下，并不是所有的应用系统或者产品都能支持此项服务。

## 4.11 订购的结束（终止服务）

订户出现下列情形时意味着该订户的证书服务已经终止：

- 证书到期后没有进行更新
- 证书到期前被吊销
- 证书到期前提出终止服务

## 4.12 密钥托管和恢复

UNTSH 不托管任何订户的私钥，因此也就不提供密钥恢复服务。

### 4.12.1 密钥托管和恢复的策略与实施

无规定。

### 4.12.2 会话密钥封装和恢复的策略与实施

无规定。

## 5. 设施、管理和运作控制

### 5.1 物理控制

UNTSH 有详细的文件，描述 CA 和 RA 需要遵守的物理控制和安全策略。对这些策略的符合性要求，在第 8 章中的 UNTSH 审计要求中做出了规定。由于这些文件包含敏感信息，需要与 SHECA 签署保密协议后才可以获得。下面只描述一下相关要求的大概内容。

#### 5.1.1 场所位置与建筑

所有 UNTSH 内的 CA、RA 都在受到物理保护的的环境下进行运营和操作。所有采取的物理保护手段能够防止、检测并阻止未经授权的使用、访问或者披露敏感的信息和系统。对于所有的 CA 和 RA，都应严格遵循 SHECA 关于物理环境的要求。

环境安全控制基于多级物理安全层的建立。每一级物理安全层就是一道安全防护屏障，通过上锁的门等方式来提供可控的物理访问管理，可以控制每一个人进入每一个区域，并且能够保证这些控制手段要有主动防护功能，例如能够对门的开启和关闭进行不同模式的提醒。物理安全层的安全控制手段是递进的，由外到里的每一级物理安全层都必须提供更加严格的访问控制和更加可靠的物理安全措施。同时，每一级物理安全层都必须完全包含下一级物理安全层，最外一级的物理安全层应该是整个建筑物的外墙。

CA 的 CPS 应该对物理安全层进行比较详细的规定。

#### 5.1.2 物理访问

对物理安全层每一级的访问都必须是可审计和可控的，从而保证对每一级物理安全层的访问都只有经过授权的人才可以进行。

#### 5.1.3 电力和空调

CA 和 RA 的物理安全设施需要配置主、备电力供应系统，以确保持续不间断的电力供应。同时，也需要有空调系统来控制温度和湿度。

#### 5.1.4 防水措施

CA 和 RA 的物理设施应该采取措施并进行相应的设备配置，制定相应的处理程序，以防止水灾或者水泄漏对系统造成损害或不利影响。

## 5.1.5 火灾预防与保护

CA 和 RA 的物理设施应该采取措施并进行相应的设备配置，制定相应的处理程序，以防止火灾或者烟雾对系统造成损害或不利影响。

火灾防护措施应当符合当地消防管理部门的要求。

## 5.1.6 介质存储

CA 和 RA 需要严格保护备份系统数据或者其它任何敏感信息的存储介质，避免这些介质受到水灾、火灾、电磁损害以及其它环境要素造成的损坏，并且需要建立严格的保护手段以防止对介质未经授权的使用、访问或者披露。

## 5.1.7 废物处理

CA 和 RA 需要建立严格的废物处理流程，特别是包含隐私或者敏感信息的纸张、电子介质或者其他任何废弃物，保证对此类废弃物进行彻底的物理销毁或者信息清除，避免对这类废物中包含的隐私或者敏感信息的非授权使用、访问或披露。

## 5.1.8 异地备份

CA 和 RA 需要建立关键系统数据或者包括审计数据在内的任何其它敏感信息的备份措施，对于关键系统和数据应该采取异地备份手段，确保其处于安全的设施内。

## 5.2 程序控制（流程控制、过程控制）

### 5.2.1 可信角色

证书服务具有高可靠性和高安全性的要求。为了保证可靠的人员管理，员工、第三方服务人员、顾问等应该被认定为可信的人员，才可在可信的岗位进行工作。成为可信人员必须符合本 CP 中关于人员背景的要求。

可信人员是指能够访问、进入或者控制认证或者密钥操作的角色，包括员工、第三方服务人员和顾问等，他们可能会对以下几个方面产生重要影响：

- 证书申请中的信息验证和确认
- 对证书申请、吊销进行批准、拒绝或者其他操作
- 证书签发和吊销
- 对严格控制访问的信息库进行访问
- 处理订户信息或请求

可信人员包括但不限于以下角色：

- 客户服务人员

- 系统管理和操作人员
- 系统设计和研发人员
- 安全管理人员
- 设备管理人员
- 机房管理人员
- 人力资源管理人员

## 5.2.2 每项任务所需的人数

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整敏感操作。

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 的密钥设备的使用寿命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分割权力，反之亦然。

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。

## 5.2.3 每个角色的识别和鉴别

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 CP 的要求严格进行。

## 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、吊销、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、吊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

## 5.3 人员控制

### 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，必须能够提交相应的证明文件。

### 5.3.2 背景调查程序

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。

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

### 5.3.3 培训要求

为了使员工能够胜任工作，需要对员工进行必要的岗前培训和工作中的再培训，以更好的满足工作岗位对人员的要求。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
- PKI 基本知识
- 电子签名法和相关法律法规
- 工作职责和岗位说明
- 安全管理策略和要求

- 相应的业务知识

### 5.3.4 再培训的频率和要求

CA 和 RA 应定期对重要岗位的员工安排定期培训，使其更加符合岗位需求。对于公司安全管理策略，应该每年至少进行一次培训。重要岗位应每年进行一次业务技能培训。

### 5.3.5 工作轮换的频率和顺序

无规定。

### 5.3.6 未授权行为的处罚

CA 应建立、维护和实施一套惩戒管理办法，对未授权行为或其他造成 CA 损害的行为进行适当的处罚，包括解除或终止劳动合同、调离工作岗位、罚款、批评教育等方式。这些处罚行为应当符合法律法规的要求。

### 5.3.7 独立合约人的要求

对于提供第三方服务的独立合约人员，包括顾问、系统和设备维护人员、外部技术支持人员等，如果其参与的工作属于可信角色范畴，那么其所需的安全要求和 CA 机构内的员工是一致的。除了必须就工作内容签署保密协议以外，该服务人员必须在 CA 专人全程监督和陪同下从事相关工作。同时还需要对其进行必要的知识培训和安全规范培训，使其能够严格遵守相关规范。

### 5.3.8 提供给人员的文件

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

- 岗位说明
- 相关业务操作说明
- 相关安全管理规范
- 相关培训材料

## 5.4 审计记录程序

### 5.4.1 事件记录的类型

CA 和 RA 必须记录与运行系统相关的事件。这些记录，无论是手动生成或者是系统自动生成，都应该包含以下信息：

- 事件发生的日期和时间
- 事件的内容
- 记录时间的实体
- 记录的类型等

应该记录的内容包括但不限于：

- CA 密钥生命周期内的管理事件，包括密钥生成、备份、存储、恢复、归档和销毁
- 密码设备生命周期的管理事件，例如接收、使用、卸载和弃用
- 证书生命周期内的管理事件，包括：证书的申请、批准、更新、吊销等
- 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
- 防火墙和路由器记录的安全事件
- 系统操作事件，包括系统启动和关闭，系统权限的创建、删除，设置或修改密码
- 认证机构设施的访问，包括授权人员进出认证机构设施、非授权人员进出认证机构设施及陪同人和安全存储设施的访问
- 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

## 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。

## 5.4.3 审计日志的保留期限

所有审计日志的记录，在按照 5.5.2 的要求进行归档后，至少还应保存一个月。

## 5.4.4 审计日志的保护

所有的审计日志，应当采取与严格的物理和逻辑访问控制措施，防止未经授权的浏览、修改、读取、删除等。

## 5.4.5 审计日志的备份程序

对审计日志的备份应该建立和执行可靠的制度，定期进行备份。

## 5.4.6 审计收集系统（内部和外部）

无规定。

## 5.4.7 事件引发主体的通知

在事件被审计收集记录时，不要求或者不需要通知引起事件的相关个人、单位、设备、应用程序等实体。但是 SHECA 可根据日志审计的结果，决定是否需要（例如时间的严重程度）通知有关实体。

## 5.4.8 脆弱性评估

根据对事件进行的审计处理，应当定期进行安全脆弱性评估，并根据评估报告采取相应的补救措施。根据不同的事件记录，这种评估的执行可能每天、每周或者每年进行。SHECA 每年至少会进行一次评估，作为整个证书运营服务年度评估的一部分。

## 5.5 记录归档

### 5.5.1 记录归档的类型

需要归档的记录，除了 5.4.1 规定的外，还需要对如下记录进行归档，包括：SHECA 对下列记录（包括但不限于）进行归档保存：

- 证书系统建设和升级文档
- 证书和 CRL 等
- 证书申请支持文档，证书服务批准和拒绝的信息，与证书订户的协议
- 审计记录
- 证书策略文档
- 员工资料，包括背景调查、录用、培训等资料
- 各类外部、内部评估文档

### 5.5.2 归档的保留期限

不同归档记录的保留期限是不同的。根据法律法规的要求、业务需要和运营服务的实际情况，不同归档记录的保留期限如下：

- 订户证书和相关申请资料，自证书到期或吊销后保留不少于 5 年
- CA、子 CA 证书和密钥，及相关生成记录，自证书到期或吊销后保留不少于 10 年
- 物理访问记录，保留不少于 2 年
- 系统操作和管理记录，保留不少于 2 两年
- 外部评估记录和内部年度评估审计记录，保留不少于 5 年
- 业务管理类记录，保留不少于 2 年

### 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。

被保护的归档记录应防止未经授权的浏览、修改、删除等非法操作，应保存在可靠的系统或者场所内。

归档记录应能保证在本 CP 规定的保留期内，可以被有效的访问。

### 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。

对于书面的归档资料，不需要进行备份，但需要采取严格的措施保证其安全性。

### 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（内部或外部）

UNTSH 内 CA、RA 等各实体的归档，由内部收集。

### 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

在 CA 机构的证书到期时，SHECA 将对 CA 证书进行更新。只要 CA 密钥对的累计寿命没有超过 6.3.2 中规定的最大生命期，那么 CA 证书可以使用原密钥进行更新。否则将需要产生新的密钥对，替换已经过期的 CA 密钥对。即时在密钥对生命期内，SHECA 也可以通过生成新密钥对的方式产生新的 CA 证书。在一个上级 CA 证书过期之前，密钥变更过程被启动，以保障这个上级 CA 体系中的实体从 CA 旧密钥对到新密钥对的平稳过渡。

在生成新的 CA 密钥对时，必须严格遵守 SHECA 关于密钥管理的规范。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。

CA 密钥更替时，必须保证整个证书链的顺利过渡。

## 5.7 损害灾难恢复

CA 应制定、维持可靠的损害和灾难恢复计划，通过实施物理、逻辑和过程控制等有效的综合方案将密钥损害或其他灾难造成的风险和潜在影响降到最小，在合理的期限内恢复业务运作。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

CA 应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 UNTSH 的根 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，SHECA 应该：

- 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。
- 立即吊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。
- 新的根证书签发以后，按照本 CP 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。
- 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。

当 UNTSH 的子 CA 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：

- 立即向 SHECA 安全认证委员会进行汇报并生成新的密钥对和证书请求，申请签发新的证书。
- 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。
- 立即吊销所有由该子 CA 签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。
- 新的子 CA 证书签发以后，按照本 CP 关于证书签发的规定，重新签发订户证书。
- 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。

当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 CP 的规定，立即申请证书吊销，并尽可能地通知信赖方。认证机构应及时吊销订户证书并按发布证书吊销信息。证书订户需要重新申请证书才能继续使用。

## 5.7.4 灾难后的业务存续能力

为了避免由于突发灾难造成认证业务停顿，CA 应制订一套完整的业务连续性计划，并建立相应的异地灾难备份系统。在出现异常灾难时，能够尽快恢复系统运行和服务提供，从而将风险减到最小。并且保证：

- 在尽可能短的时间内恢复业务系统，最多不超过 24 小时
- 能够恢复客户信息
- 能够保证恢复后的运营场地符合安全要求
- 能够恢复对老客户、新客户的服务
- 有足够的人员能够继续开展业务并且不违反职责分割的要求

## 5.8 CA 或 RA 的终止

CA 或 RA 需要停止运行时，在停止运作之前，有关实体要在合理的时间内尽快通知订户、信赖方和其他受到影响的实体。

如果认证机构要终止运行，认证机构应制定业务承接计划，以使订户和信赖方的损失降到最低。这种终止计划包括下列适用内容：

- 通知政府主管机构
- 通告由于 CA 运行停止而受到影响的各方，如订户和信赖方，通知他们该 CA 的状态
- 处理通知费用问题
- 吊销认证机构签发的 CA 证书
- 保存 CA 归档文件和记录到规定的期限
- 证书吊销服务的继续，如 CRL 的签发或在线证书状态检查服务的维护。如果必要，吊销最终订户和下级 CA 的未过期和未被吊销的证书
- 如果需要，对证书未到期、未吊销而根据 CA 中止计划被吊销订户的赔偿支付，或者由继任 CA 签发替换证书给订户
- CA 私钥和保存该私钥的硬件模块的处理
- 将终止的 CA 服务传给继任 CA 的条款

当 RA 因故终止服务时，认证机构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。

## 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

##### 1、CA 密钥的产生

CA 密钥对由国家密码主管部门批准和许可的设备生成的。密钥的生成、管理、储存、备份和恢复等应遵循 FIPS140-2 标准的相关规定。由于 FIPS140-2 标准并非是国家密码主管部门认可和标准，国家对于密码产品有严格的管理要求，因此，FIPS140-2 标准仅是参照执行，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。

为保证 CA 密钥对的绝对安全，需要制定严格的密钥管理流程对其进行控制。至少应包括电磁屏蔽环境、人员监督、密钥分割、视频监控等条件。

##### 2、订户签名密钥对的生成

签名证书订户使用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、USB Key、IC 卡等生成。用户在选择这些设备前，应事先向 CA 咨询有关的系统兼容和接受事宜。CA 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。

CA 一般不提供代为生成签名密钥对，如果用户书面申请并经 CA 批准，CA 可以为申请者代为生成密钥对，并且承诺不保留私钥的副本，采取足够的措施保证密钥对的安全性、可靠性和唯一性，但是由于此密钥对的遗失、泄漏等原因造成损失的，SHECA 不承担任何责任与义务。

证书订户签名密钥对的产生，必须遵循国家的法律政策规定。CA 支持多种模式的签名密钥对产生方式，除了硬件密码模块生成密钥对外，服务器证书订户可以利用 Web 服务器软件提供的密钥生成功能生成密钥对，电子邮件证书可以使用浏览器自带的密码模块生成密钥对，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。

##### 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。

4、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。

#### 6.1.2 私钥分发给订户

在订户生成自己的密钥对的情况下，不需要将私钥传给订户。如果 CA 为订户生成密钥对，那么应该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 公钥分发给证书签发者

证书订户以公钥向 CA 提交证书请求时（例如 PKCS # 10 格式），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 CA 公钥分发给依赖方

CA 的公钥应主要通过网站下载方式发布给依赖方。在订户证书签发时，CA 可通过 PKCS#7 格式将包含 CA 公钥的证书链传递给最终订户。CA 也需要通过 LDAP 目录发布其公钥。

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 密钥长度

CA 和订户的 RSA 密钥长度，至少应该是 1024 位。

### 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。

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。

### 6.1.7 密钥使用目的

CA 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 CA 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。

所有密钥的使用，都必须遵循本 CP 及相关 CPS 的规范。

参见 7.1.2。

## 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

CA 密钥对由国家密码主管部门批准和许可的设备生成的。密钥的生成、管理、储存、备份和恢复等应遵循 FIPS140-2 标准的相关规定。由于 FIPS140-2 标准并非是国家密码主管部门认可和标准，国家对于密码产品有严格的管理要求，因此，FIPS140-2 标准仅

是参照执行，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。

## 6.2.2 私钥多人控制 (m 选 n)

CA 的私钥操作采用多人控制的策略 (即  $n$  out of  $m$  策略,  $m > n$ ,  $n \geq 3$ ), 使用“秘密分割”技术, 将使用和操作 CA 私钥时所需的激活数据分成若干个部分, 由受过 SHECA 安全认证委员会批准的可信人员持有。在对私钥进行操作时, 需要至少三个或三个以上的可信人员共同完成生成和分割程序。

## 6.2.3 私钥托管

无规定。

## 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, 由相应的国家密码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码管理部门进行联系。

## 6.2.5 私钥归档

CA 的私钥经过加密后按照严格的安全措施保存。在私钥生命期结束后, 仍将采取同样的安全保密机制进行保存, 并遵从 5.5.2 关于归档的规定。归档期限结束后, 对 CA 私钥的销毁应符合 6.2.10 的规定。

## 6.2.6 私钥导入或导出密码模块

CA 的私钥, 严格的按照密码管理办法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 私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 私钥在密码模块中的存储

CA 必须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 CA 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 of 特定软件密码模块。

## 6.2.8 激活私钥的方法

UNTSH 的所有私钥，都被建议至少采用输入保护口令的方式激活私钥。除非订户自己进行变更，并愿意承担变更后的责任。

CA 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，并且保存在 IC 卡等硬件介质中，必须由 m 选 n 的方式分别输入激活数据才能激活私钥。

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。

解除私钥激活状态的方式包括退出登陆状态、切断电源、将硬件密码模块移开、注销用户或系统等。

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。

对于 CA 私钥，当存放私钥的加密设备断电，私钥进入非激活状态。

## 6.2.10 销毁私钥的方法

CA 的私钥不再被使用，或者与私钥相对应的公钥到期或者被吊销后，根据需要可将私钥进行归档，除归档外的私钥必须被按照从加密设备中彻底删除、加密设备初始化或者物理销毁加密设备等方式销毁。销毁。归档的 CA 私钥在其归档期限结束时需在多名可信人员参与的情况下安全销毁，必须通过将 CA 私钥从加密设备中彻底删除、加密设备初始化、物理销毁加密设备的方式销毁。所有用于激活私钥的 PIN 码、IC 卡、动态令牌等也必须同私钥一起被销毁或者收回。

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吊销后，由订户决定其销毁方法，包括通过私钥的删除、系统或密码模块的初始化、物理销毁私钥存储模块等方式。订户必须保证有效销毁其私钥，并承担有关的责任。

### 6.2.11 加密模块评估（规格、参量）

CA 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条件，选择所需要的模块。

## 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，归档的具体要求参照 5.5 的规定。

### 6.3.2 证书操作期和密钥对使用期

公钥和私钥的使用期限与证书的有效期限相关，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 50 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。对于不同的证书，其密钥对允许通过证书更新的最长使用期限如下：

- 对于 4096 位根 CA 证书，其密钥对的最长允许使用年限是 50 年
- 对于 2048 位根 CA 证书，其密钥对的最长允许使用年限是 30 年
- 对于 1024 位根 CA 证书，其密钥对的最长允许使用年限是 15 年
- 对于 1024 位其他 CA 证书，其密钥对的最长允许使用年限是 15 年
- 对于 2048 位最终订户证书，其密钥对的最长允许使用年限是 8 年
- 对于 1024 位最终订户证书，其密钥对的最长允许使用年限是 4 年

## 6.4 激活数据

### 6.4.1 激活数据的生成和安装

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。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。

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 激活数据的其它方面

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。

## 6.5 计算机安全控制

### 6.5.1 特殊的计算机安全技术要求

UNTSH 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、逻辑访问控制、物理访问控制、人员职责分权管理、网络访问控制等。

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访问产品服务器，一般的应用用户在产品服务器上没有账户。核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。

### 6.5.2 计算机安全评估

UNTSH 系统，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第三方机构的有关评估、审查和认证。

## 6.6 生命周期技术控制

### 6.6.1 系统开发控制

UNTSH 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、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

UNTSH 系统的信息安全管理，严格遵循信息产业部、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。

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 and 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。

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 生命周期安全控制

无规定。

## 6.7 网络安全控制

UNTSH 系统采用多级防火墙、入侵检测、安全审计、病毒防范系统，并且及时更新防火墙、入侵检测、安全审计、病毒防范系统的版本，定期进行策略审计和评估，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、CRL 和 OCSP 描述（轮廓）

### 7.1 证书描述（轮廓）

UNTSH 证书遵循 ITU-T X.509 V3 (1997): 信息技术—开放系统互连—目录: 认证框架 (1997 年 6 月) 标准和 RFC 3280:Internet X.509 公钥基础设施证书和 CRL 结构 (2002 年 4 月)。

#### 7.1.1 版本号

UNTSH 订户证书, 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, 只签名。

	CA 证书	身份证书 I	身份证书 II(签名)	身份证书 II(加密)	电子邮件证书	代码签名证书	安全站点证书
关键	×	×	×	×	×	×	×
0 digitalSignature	×	√	√	×	√	√	√
1 nonRepudiation	×	√	√	×	√	√	√
2 keyEncipherment	×	√	×	√	√	×	√
3 dataEncipherment	×	√	×	√	√	×	√
4 keyAgreement	×	√	×	√	√	×	√
5 keyCertSign	√	×	×	×	×	×	×
6 cRLSign	√	×	×	×	×	×	×
7 encipherOnly	×	×	×	×	×	×	×
8 decipherOnly	×	×	×	×	×	×	×

- netscape 证书类型

该扩展项用来向使用网景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。

- 扩展密钥用途

	身份证书 I, 身份证书 II	电子邮件证书	代码签名证书	安全站点证书
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	×	×	×	×

- 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。

## 2、自定义扩展项

有关自定义扩展项的内容,请参考本 CP 附录中的说明。

## 7.1.3 密钥算法对象标识符

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:

- SHA1withRSAEncryption 对象标识符为: {iso(1) ISO Identified Organization (3) OIW(14) secsig(3) algorithm(2) 29}

- MD5withRSAEncryption 对象标识符为: {iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 4}

### 2. 摘要算法:

- md5 的对象标识符为: {iso(1) member-body(2) US(840) rsadsi(113549)

digestAlgorithm(2) 5 }

- sha1 的对象标识符为：{iso(1) ISO Identified Organization (3) 0IW(14) secsig(3) algorithm(2) 26}

### 3. 非对称算法：

- rsaEncryption 对象标识符为：{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 1}

### 4. 对称算法

- 本 CP 建议使用国家密码管理部门认可的对称算法。

## 7.1.4 命名形式

UNTSH 证书，其命名形式的格式和内容符合 X. 501 的甄别名格式。

## 7.1.5 命名限制

订户的命名一定要有意义，应具有通常能够被理解的语义，可以明确确定证书主题中的个人、单位或者设备的身份，订户证书不被允许使用匿名或假名。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。具体请参考附录中的证书格式规范。

## 7.1.7 策略限制扩展项的使用

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语义

无规定。

## 7.2 CRL 描述

UNTSH 签发的 CRL 符合 RC3280 标准。

### 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 OCSP 描述

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

### 7.3.1 版本号

RFC2560 定义的 OCSP V1 版本。

### 7.3.2 OCSP 扩展项

无规定。

## 8. 一致性审计和其它评估

SHECA 作为 UNTSH 的运营主体，定期进行一致性审计和运营评估，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 评估的频率或情形

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 CP 的规定运营和服务，按照内部评估和审计规范，每年至少定期执行一次内部的评估审核，包括对 UNTSH 内其它实体（RA、受理点等）的评估审核。

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。

### 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 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。内部评估由政策法规部组织实施。

3、对于聘请的外部审计机构，应该具备以下的资质：

- 必须是经许可的、有执业资格的评估机构，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
- 具备独立审计的精神

### 8.3 评估者和被评估者的关系

1、外部评估者（信息产业主管部门、独立审计师事务所以及其他机构）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。

## 8.4 评估包含的主题（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、证书吊销的操作、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 对不足采取的行动

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 评估结果沟通

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 [www.sheca.com](http://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 [www.sheca.com](http://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. 其它事项和法律事务

本 CP 作为订户协议的一部分，对 UNTSH 各参与方都有约束作用。特别是在本节中涉及的费用、法律、财务、担保等权利义务，需要证书订户、依赖方、CA、RA 等予以充分的了解和遵循。

### 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 [www.sheca.com](http://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 [www.sheca.com](http://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 [www.sheca.com](http://www.sheca.com) 上予以公布。

#### 9.1.3 吊销和状态信息查询费用

SHECA 对证书吊销和状态查询，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 [www.sheca.com](http://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、SHECA 将向用户提供证书存储介质及相关服务，SHECA 在与订户或者其他实体签署的协议中指明该项价格。

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 CP 所规定的责任或其它重大义务，订户可以要求 SHECA 吊销证书并退款。在 SHECA 吊销了订户的证书后，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。

此退款策略不限制订户得到其它的赔偿。

完成退款后，订户如果继续使用该证书，SHECA 将追究其法律责任。

## 9.2 财务责任

### 9.2.1 保险范围（覆盖）

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 CP 签发的订户证书。

目前，SHECA 运营的 UNSH 认证体系没有提供第三方保险服务。

### 9.2.2 其他财产

无规定。

### 9.2.3 对终端实体的保险或担保范围

SHECA 运营的 UNTSH 认证体系没有提供第三方保险服务。

证书订户一旦接受 UNTSH 的证书，或者通过协议完成对证书服务的接受，那么就意味着该订户已经接受了本 CP 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 CP 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、UNTSH 体系的系统结构、配置，包括系统、网络、数据库等；各类服务系统安全配置和方案；系统操作、维护记录；各类系统操作口令。

6、UNSTH 关于运营管理的文档和记录，包括物理安全策略与实施方案，逻辑安全策略和实施方案；密钥管理策略与操作记录；可信人员名单；内部安全管理策略与制度；CA 或 RA 批准或拒绝的申请纪录等

7、UNTSH 所有证书订户的身份信息，订户或者其应用系统访问 CRL、OCSP 的记录（时间、频度）等

8、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 不在保密范围的信息

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、证书被吊销的信息，属于公开信息，SHECA 在目录服务器中公布这些信息。

5、证书策略（CP）、电子认证业务规则（CPS）、订户协议等

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 CP 的规定，承担相应的保护保密信息责任，必须通过有效的技术手段和管理程序对其进行保护。

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 CP 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，并制定相应的管理办法对隐私信息进行保护。

### 9.4.2 被视为隐私的信息

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，包括联系电话、地址等都将作为隐私处理，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，都有义务承担相应的保护隐私信息责任，不得将订户隐私信息透露随意给第三方。

### 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，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

## 9.4.7 其它信息披露情形

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。

## 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。

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、CP、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、吊销的期间或之后，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

### 9.6.1 CA 的陈述和担保

#### 1、CA 的一般陈述

- 在本 CP 及相关 CPS 条款规定的范围内，提供基础设施和认证服务
- 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、CA 对订户的陈述

除非本 CP 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 CP 的所有实质性要求
  - 发证机构将按本 CP 的规定，及时吊销证书
  - 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 CP 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、CA 对依赖方的陈述

发证机构就其所发证书向所有按照本 CP 及相关 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 CP 及相关 CPS 的规定签发证书

#### 4、CA 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 CP 中的规定接受了该证书。

### 9.6.2 RA 的陈述和担保

#### 1、注册机构 RA 按照程序取得了 SHECA 的授权后，将保证：

- 遵循本 CP、相关 CPS、与 SHECA 签订的协议以及其它 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 RAB、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，有权决定是否给申请者提供相应的证书服务

- 依确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
  - 接受 SHECA 进行的管理，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。
- 2、分理中心 RAB 的陈述
- 作为具备可管理 RAT 的证书服务机构，遵循本 CP 及相关 CPS 的规定，接受 CA、RA 的授权和管理，并按照 CA 和 RA 的授权对 RAT 进行管理
  - 承诺对所有证书服务申请者的隐私信息予以保密，并承担与此相关的法律责任
  - 接受授权机构对其进行的资格审核和管理评估
  - 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
- 3、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 CP 及相关 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
  - 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。

### 9.6.3 订户的陈述和担保

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，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、吊销）
- 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）或证书吊销列表
- 一经接受证书，既表示订户知悉和接受本 CP 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，订户就应承担如下责任：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
- 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

## 9.6.4 依赖方的陈述和担保

依赖方在信赖任何 SHECA 签发的证书时，就意味着保证：

- 熟悉本 CP 及相关 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，确认该证书没有被吊销；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 CP 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。

## 9.6.5 其他参与方的陈述和担保

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 规定的方式支付
- 垫付商的垫付行为，就表明其愿意并且能够承担本 CP 及相关 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

在法律允许的范围内，认证机构认证业务声明、订户协议、信赖方协议和其他订户协议应包含条款免除认证机构的某些可能担保，这包括为了某个特定目的的任何适用性和合适性担保。

## 9.8 有限责任

在法律允许的范围内，CA 在承担任何责任和义务时，只承担法律范围内的有限责任。

## 9.9 赔偿

CA 对自身原因造成的订户损失，应对订户进行赔偿，或信赖方在履行了信赖方协议的情况下，由于认证机构的原因造成的信赖方损失，认证机构对信赖方的赔偿。

订户对自身原因造成的认证机构、信赖方损失, 应对认证机构进行赔偿。

信赖方对自身原因造成的认证机构损失, 应对认证机构进行赔偿。

在根据本 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、免赔等进行具体的描述。

## 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, 且在认证机构中止业务前一直有效, 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, 涉及审计、保密信息、隐私保护、归档、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。

## 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, UNTSH 内的 CA、RA 等实体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。

## 9.12 修订

SHECA 有权修订本 CP。SHECA 有权把修订结果以 CP 的修订版的形式通过网站 [www.sheca.com](http://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, 政策法务部每年至少审查一次本 CP, 确保其符合国家法律法规和主管部门的要求, 符合认证业务开展的实际需要。

本 CP 的修订, 由政策法务部提出修订报告后, 必须经过 SHECA 策略最高管理部门——SHECA 安全认证委员会审核并批准后才能开始修订。修订后的 CP 经过 SHECA 安全认证委员会批准后正式对外发布。

## 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](http://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](http://www.sheca.com))，它等同于修改本 CP。这些修改将取代原有版本中的任何冲突和指定条款。

如果在修订发布 7 天内，证书申请者和订户没有决定请求吊销其证书，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
- 证书策略的对象标识符进行修改

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

无论合同或其他法律条款的选择及无论是否在中华人民共和国建立商业关系，本 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

所有 SHECA、UNTSH 个实体的认证服务活动，都必须符合《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》以及其它中华人民共和国法律法规的规定。

## 9.16 其它条款

### 9.16.1 完整协议

CP、CPS、订户协议及信赖方协议及其补充协议将构成 PKI 参入者之间的完整协议。本 CP 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 CP 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 CP 规定的约束，但以下所示协议除外：

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

### 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 可分割性

本 CP 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 CP 其余的部分仍将有效。

### 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

无规定。

## 附录 A 定义和缩写

### 激活数据 Activation Data

用于操作密码模块所必需的、并且需要被保护的数据值（例如 PIN、口令、或人工控制的密钥共享部分），而不是密钥。

### 鉴别 Authentication

确定个人、组织或事物如其所声称的人或事物的过程。在 PKI 上下文中，鉴别指的是确定以某个特定名称申请或试图访问某事物的个人或组织确实为正确的个人或组织的过程。

### 认证机构（CA） Certification Authority

受用户信任,负责创建和分配公钥证书的权威机构。有时，认证机构也可为用户创建密钥。

### CA 证书 CA-certificate

由其它 CA 为一个 CA 的公钥签发的证书。

### 证书策略（CP） Certificate Policy

一套命名的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。例如，一个特定的 CP 可以指明某类证书适用于鉴别从事企业到企业（B-to-B）交易活动的参与方，针对给定价格范围内的产品和服务。

### 认证路径 Certification Path

一个有序的证书序列（包含路径中起始对象的公钥），通过处理该序列可获得末端对象的公钥。

### 认证业务声明（CPS） Certification Practice Statement

关于认证机构在签发、管理、吊销或更新证书（或更新证书中的密钥）过程中所采纳的业务实践的声明。

### 身份标识 Identification

建立个人或组织的身份的过程，如指明某个人或组织是特定的个人或组织。在 PKI 上下文中，身份标识指代两个过程：

确定某个人或组织的给定名称与真实世界中该个人或组织的身份相联系；

确定在那个名称之下申请或试图访问某事物的个人或组织确实为被命名的个人或组织。寻求标识的人可能是证书申请者，或者是 PKI 中可信职位的申请者，或者是试图访问网络或应用软件的人（如 CA 管理员试图访问 CA 系统）。

### 签发认证机构（签发 CA） Issuing Certification Authority

在特定的 CA 证书上下文中，签发 CA 是签发证书的 CA（参见主体 CA）。

### 参与者 Participant

在一个给定 PKI 中扮演某一角色的个人或组织，如订户、依赖方、CA、RA、证书制作机构、证书库服务提供者、或类似实体。

### **策略限定符 Policy qualifier**

依赖于策略的信息，可能与 CP 标识符共同出现在 X.509 证书中。该信息中可能包含可用 CPS 或依赖方协议的 URL 地址，也可能包含证书使用条款的文字(或引起文字出现的数字)。

### **注册机构 (RA) Registration Authority**

具有下列一项或多项功能的实体：标识和鉴别证书申请者，同意或拒绝证书申请，在某些环境下初始化证书吊销或挂起，处理订户吊销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书（即 RA 代表 CA 承担某些任务）。[注：在其它文档中可能使用本地注册机构（LRA），是相同的概念。]

### **依赖方 Relying party**

证书的接收者，他依赖于该证书和（或）该证书所验证的数字签名。在本标准中，术语“证书使用者”与“依赖方”可互换使用。

### **依赖方协议 Relying party agreement**

认证机构与依赖方所签署的协议，通常规定了在验证数字签名或以其他方式适用证书时双方所拥有的权利和义务。

### **主体认证机构 (主体 CA) Subject Certification Authority**

在特定的 CA 证书上下文中，主体 CA 指的是在证书中其公钥被认证的 CA。（参见签发 CA）

### **订户 Subscriber**

被颁发给一个证书的证书主体。

### **订户协议 Subscriber Agreement**

CA 与订户之间签署的协议，规定了双方在颁发和管理证书的过程中所承担的责任和义务。

### **协卡网络信任服务体系 UniTrust Network Trust Service Hierarchy**

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，缩写为 UNTSH，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。

### **验证 Validation**

对证书申请者进行身份标识的过程。验证是身份标识的子集，并且在建立证书申请者身份的过程中指的就是身份标识。



## 附录 B 证书格式

### SHECA 证书格式

SHECA 证书格式符合 X.509 的规范定义，其编码方式采用 ASN.1 distinguished encoding rules (DER) [X.208]，SHECA 证书格式其本表达如下：

```
Certificate ::= SEQUENCE {
    tbsCertificate      TBSCertificate,
    signatureAlgorithm  AlgorithmIdentifier,
    signatureValue      BIT STRING }
TBSCertificate ::= SEQUENCE {
    version             [0] EXPLICIT Version DEFAULT v1,
    serialNumber        CertificateSerialNumber,
    signature            AlgorithmIdentifier,
    issuer               Name,
    validity             Validity,
    subject              Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID      [1] IMPLICIT UniqueIdentifier OPTIONAL,
                        -- 该项 SHECA 目前未采用
    subjectUniqueID     [2] IMPLICIT UniqueIdentifier OPTIONAL,
                        --该项 SHECA 目前未采用
    extensions          [3] EXPLICIT Extensions OPTIONAL
}
}
```

其中：

版本(version)	采用 V3，根证书采用 V1
序列号(serialNumber)	采用大整型十六进制数
签名算法(signature)	sha1WithRSAEncryption 或 md5WithRSAEncryption
颁发者 (issuer)	目前为：

CN = SHECA

O = SHECA

主题(subject) 根据证书类型，SHECA 有选择性的使用如下信息项目：

countryName 国家名  
organizationName 组织名  
organizationalUnitname 组织单位名  
stateOrProvinceName 省份名  
commonName 通用名  
localityName 城市名  
title 职务



surname 别名  
 givenName 常用名  
 email 电子邮箱  
 postalAddress 邮政地址  
 postalCode 邮政编码  
 postalOfficeBox 信箱号  
 telephoneNumber 电话号码  
 telexNumber 电传号码

在标准扩展项中主要采用了：

- 证书政策发布点   OID: id-ce 32
- 基本限制           OID: id-ce 19
- CRL 发布点        OID: id-ce 31
- netscape 证书类型   OID: 2.16.840.1.113730.1.1

## 证书自定义扩展项说明

自定义扩展项：

```

id-sheca OBJECT IDENTIFIER ::= { 1, 2, 156, 1, 8888}
ShecaDefineExtention ::= SEQUENCE {
    ShecaDefineExtentionIdentifier ShecaDefineExtentionID,
    ShecaExtentions SEQUENCE SIZE (1..MAX) OF ShecaExtention}
ShecaDefineExtentionID ::= OBJECT IDENTIFIER (id-sheca 0)
ShecaExtention ::= SEQUENCE {
    ShecaextentionId OBJECT IDENTIFIER,
    Shecaextention GeneralName}
  
```

目前已使用的自定义扩展项：

```

证书链发布地址: {id-sheca 0x90}
证书服务 URL: {id-sheca 0x91}
OCSP URL: {id-sheca 0x92}
证书级别: {id-sheca 0x93}
证书级别定义:
    个人身份证书        0x00000103
    个人 EMAIL 证书     0x00000102
    个人代码签名证书    0x00000105
    单位身份证书        0x00000203
    单位 EAIL 证书      0x00000202
    单位代码签名证书    0x00000204
    服务器身份证书     0x00000304
    WEB 服务器证书     0x00000301
    唯一标识: {id-sheca 0x94}
        个人证书使用身份证号(SF)
        护照(HZ)
        军官证(JG)
        士兵证(SB)
  
```

单位证书使用企事业代码号(JJ)



Web 服务器使用域名  
服务器证书使用 ip 地址：端口  
证书策略 URL: {id-sheca 0x95}

## 附录 C CRL 格式

### CRL 格式

SHECA CRL 格式符合 X.509 的规范定义，其编码方式采用 ASN.1 distinguished encoding rules (DER) [X.208]，SHECA CRL 格式其本表达如下：

```
CertificateList ::= SEQUENCE {
    tbsCertList          TBSCertList,
    signatureAlgorithm  AlgorithmIdentifier,
    signatureValue      BIT STRING }

TBSCertList ::= SEQUENCE {
    version              Version OPTIONAL,
                        -- 目前版本为 2
    signature            AlgorithmIdentifier,
    issuer               Name,
    thisUpdate          Time,
    nextUpdate          Time OPTIONAL,
    revokedCertificates SEQUENCE OF SEQUENCE {
        userCertificate  CertificateSerialNumber,
        revocationDate  Time,
        crlEntryExtensions Extensions OPTIONAL
                        --未选
    } OPTIONAL,
    crlExtensions       [0] EXPLICIT Extensions OPTIONAL
                        -- 未选
}
```