协卡网络信任服务体系

事件证书证书策略/电子认证业务规则

UniTrust Network Trust Service Hierarchy Certificate Policy/Certificate Practice Statement for Event Certificate

Version 1.0

2019 年 12 月 13 日

♥ 中国
上海市虹口区
四川北路 1717 号 18 楼
Tel: 86-21-36393100
Fax: 86-21-36393200
https://www.sheca.com

《协卡网络信任服务体系事件证书证书策略/电子认证业务规则》

UniTrust Network Trust Service Hierarchy Certificate Policy/Certificate Practice Statement for Event Certificate

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中心联系：

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

版本控制

版本	生效日	作 者	发布者	说明
V1.0	2019年12月13日	陈晓曈	SHECA安全认证委员会	修订发布

变更摘要

版本	变更描述
V1.0	--

声明

本文档全部或者部分支持下列标准：

- RFC3647：互联网X.509 公钥基础设施-证书策略和证书业务声明框架
- RFC2459：互联网X.509 公钥基础设施-证书和CRL属性
- RFC2560：互联网X.509 公钥基础设施-在线证书状态协议-OCSP
- ITU-T X.509 V3（1997）：信息技术—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

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

版权说明

关于SHECA CP/CPS中主要权利及义务的概要

此概要仅是本文档重要部分的简单描述，有关条款的完整论述以及其他重要条款和细节请看本文档全文。

1、本文档文件规定了SHECA数字证书认证服务的实施及使用，数字证书认证服务包括SHECA数字证书发放、管理和验证，涵盖了数字证书整个生命周期内的操作流程、运行管理、运营环境、管理政策等。

2、证书申请者须知：

（1）申请者在申请证书之前，已被建议接受适当的数字认证相关方面的培训。

（2）从SHECA网站及其他渠道可以得到有关数字签名、证书及CPS的文件，证书申请者可以参加相关的培训和学习。

3、SHECA提供不同类型的证书，申请者应自行或向SHECA咨询决定何种证书适合于自己的需要。

4、申请者必须在接受证书后方可使用证书与其他人建立通讯或引导他人使用证书。申请者在接受证书的同时，就已表明其接受了本文档规定的权利和义务，并承担相应的责任。

5、如果你是数字签名或数字证书的接受者或者依赖方，你必须决定是否信赖它。在此之前，SHECA建议你应检查SHECA的证书目录服务，以确保该证书是正确和有效的，并使用证书检验数字签名是在证书有效期内由该证书的持有者生成的，而且有关信息并未改动。

6、证书持有人同意，如果发生危及私钥安全的状况时，及时通知SHECA及其授权的证书服务机构。

7、如果使用者对以后CPS 版本的编辑工作有任何意见与建议，请Email 至：cps@sheca.com；或请邮寄至：中华人民共和国上海市四川北路1717号嘉杰国际广场18楼（200080 ）。

8、更多的信息请看SHECA网站（http:// www.sheca.com）。

目录

1. 引言

1.1 概述

上海市数字证书认证中心有限公司(Shanghai Electronic Certification Authority Co.,Ltd.，缩写为 SHECA)是中国领先的第三方电子认证服务机构，首批获得电子认证服务许可证，以专业的管理、运营和技术保障能力向用户提供各类数字证书服务，为建设一个和谐、信任的网络环境而努力。

本文档所称事件数字证书是一类面向事项运用一次性私钥的特殊的数字证书。事件数字证书一般用于一次性事件数字签名，签名过后私钥销毁，保证各签名参与主体的身份真实性、信息的完整性以及签名行为的不可抵赖性。

证书策略/电子认证业务规则（Certification Policy/ Certificate Practice Statement，以下简称本文档）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。本《协卡网络信任服务体系事件证书证书策略/电子认证业务规则》(以下简称本文档）试用于 UNTSH 架构内的事件证书，为 UNTSH 事件证书申请、签发、管理、使用、吊销、更新以及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。本文档并不是 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。

本文档满足互联网标准组织制定的 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》，以及国内标准 GB/T 26855-2011《信息安全技术公钥基础设施证书策略与认证业务声明框架》的框架和内容要求。

1.1.1 上海市数字证书认证中心有限公司（SHECA）

上海市数字证书认证中心有限公司(Shanghai Electronic Certification Authority Co.,Ltd.，缩写为 SHECA，简称上海 CA)成立于 1998 年，是中国第一家专业的第三方电子认证服务机构，全国运行经验最丰富、应用领域最广、用户群体最大的认证机构之一。

2005 年 4 月，获得国家密码管理局“电子认证服务密码使用许可证”；2005 年 9 月，获得信息产业部“电子认证服务许可证”，成为《中华人民共和国电子签名法》实施后首批获得国家运营资质的电子认证服务机构；2008 年 6 月，通过国际 WebTrust 认证；2008 年 12 月，实现根证书内置于微软操作系统，是全国第一家实现全球化电子认证服务的机构。

SHECA 拥有一支专业、强大的技术研发队伍，专注于研发构建网络信任体系建设所需要的技术、产品和服务，拥有多项自主研发、自主产权的核心技术与产品以及解决方案。

SHECA 作为依法设立的第三方电子认证服务机构，建设和运营的协卡认证体系（UniTrust NTSH）。协卡认证体系（UniTrust NTSH）是中国最有影响的数字证书发放和管理机构，发放和管理的数字证书得到广泛的应用。

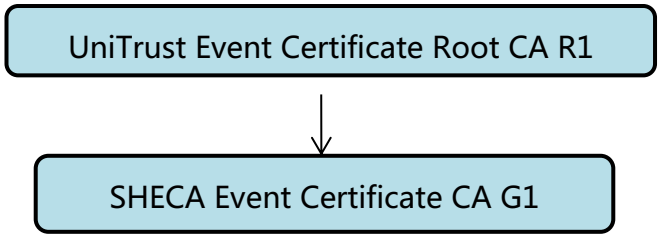
1.1.2 协卡认证网络信任服务事件证书体系

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

协卡认证体系拥有清晰、完整的 PKI 层次架构，以实现不同应用对证书服务的不同需求。每个根 CA 下设子 CA，以签发用户证书。因此，协卡认证体系包含了根 CA、子 CA、各相关注册机构（RA 中心）、服务受理点（RAT）以及其他授权的服务关联实体，这些实体都是协卡认证体系内不同层次的服务主体。协卡认证体系所有和证书相关的服务和管理，都完整、正确、全面的贯彻和实施本文档以及相应证书策略的要求。

其中，事件证书认证体系如下:

UniTrust Event Certificate Root CA R1



UniTrust Event Certificate Root CA R1 根密钥长度为 4096-bit，目前下设一个子 CA 证书，SHECA Event Certificate CA G1 子 CA 签发密钥长度为 RSA 2048-bit 的中级证书。

UniTrust Event Certificate Root CA R1 有效期将于 2044 年 11 月 10 日到期，2039 年 11 月 1 日起不再签发下级证书。

1.2 文档名称与标识

本文档的名称为《协卡网络信任服务体系事件证书证书策略/电子认证业务规则》（UniTrust Network Trust Service Hierarchy Certificate Policy/Certificate Practice Statement for Event Certificate），简称《事件证书证书策略/认证业务规则》，本文档的对象标识符（OID）为：1.2.156.112570.1.0.5。

SHECA 所设置的对象表号符及对应对象如下表所示：

OID	对象	
1.2.156.112570	万维信	UniTrust
1.2.156.112570.1	上海市数字证书认证中心	SHECA
1.2.156.112570.1.0	策略	Policies
1.2.156.112570.1.0.5	协卡网络信任服务体系 事件证书证书策略	UniTrust Network Trust Service Hierarchy Event Certificate Practice Statement (UNTSH Rapid CP)
1.2.156.112570.1.0.6	协卡网络信任服务体系 时间证书认证业务规则	UniTrust Network Trust Service Hierarchy TimestaMp Certificate Practice Statement (UNTSH Rapid CPS)
1.2.156.112570.1.2.4	Adobe签名策略	Adobe Signing Policy
1.2.156.112570.1.2.5	文件签名策略	Document Signing
1.2.156.112570.1.3	客户端证书策略	Client Certificates Policy
1.2.156.112570.1.4	时间戳策略	TimeStamping Policy
1.2.156.112570.1.4.1	时间戳AATL策略	TimeStamping AATL Policy
1.2.156.112570.1.5	OCSP策略	OCSP Policy

1.3 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 是依法设立的电子认证服务机构，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 可签发最终用户证书或其它 CA 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文档

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、状态查询和验证、目录服务等。同时，SHECA 还要管理下属的所有证书注册机构（RA）以及所有的授权服务机构（子 CA）。

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，按照本文档和相应 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 接收事件证书的实体，包括所有从 UNTSH 接受证书的个人、单位或设备。订户代表着证书中公钥所绑定的唯一实体，拥有对与其证书中公钥唯一对应的私钥的最终控制权。订户在本文档的范围内使用证书，愿意并能够承担本文档约定的义务。

在电子签名应用中，订户即为电子签名人。

1.3.4 依赖方

依赖方，是指在 SHECA 认证服务体系范围内，任何使用证书进行网上作业的证书持有者和按照本文档合理信任证书真实性的任何实体。依赖方可以是证书订户，也可以不是订户。在本业务中，是信任上海 CA 签发的事件证书，按照事件证书机制进行电子签名验证的实体。

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，经过合理的审核后才能够信任一张证书。

1.3.5 其他参与者

其他参与者指为 CA 证书服务体系提供相关服务的其他实体。

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文档的规定。

1.4 证书应用

1.4.1 适合的证书应用

SHECA 机构签发的事件证书广泛适用于企业信息化、电子政务和电子商务等领域，用于证明电子化环境进行的电子签名主体的身份、所签名文档数据的完整性及电子签名的不可篡改性。

1.4.2 限制的证书应用

事件证书仅能用于证书订户的电子签名及身份验证，任何不符合的应用，不受本文档的保护。

SHECA 机构发放的数字证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，由此造成的法律后果由订户负责。

1.5 策略管理

1.5.1 策略文档管理机构

根据中华人民共和国电子签名法、信息产业部电子认证服务管理办法和电子认证业务规则规范的要求，SHECA 制定本文档，并指定专门的机构——SHECA 安全认证委员会作为策略的管理机构。

SHECA 安全认证委员会，作为 SHECA 认证服务体系所有策略的制订管理机构，由 SHECA 的管理层主要成员、各相关部门主管（服务部门、运营部门、技术部门等）及相应的 CPS 编写人员组成，负责审核批准 CPS，并作为 CPS 实施检查监督的最高决定机构。

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

1.5.2 联系人

SHECA 将对电子认证业务规则进行严格的版本控制，并由 SHECA 指定专门的机构和人员负责相关的事宜。 任何有关 CPS 的问题、建议、疑问等，都可以与此联系人进行联系。

联系人：上海市数字证书认证中心有限公司战略发展中心。

电话：86-21-36393197

传真：86-21-36393200

地址：中华人民共和国上海市四川北路 1717 号嘉杰国际广场 18 楼

邮政编码：200080

电子邮件：policy@sheca.com

1.5.3 决定CPS 符合策略的机构

作为电子认证业务的主管部门，信息产业部发布了《电子认证业务规则规范》，SHECA 根据规范的要求，制定本文档，并提交信息产业部备案。SHECA 安全认证委员会作为最高策略管理机构，是本文档符合策略的决定机构，负责批准和决定本文档是否符合相应 CP/CPS 的规定。

SHECA 保证其制订和发布的文档，其执行、解释、翻译和有效性均符合和适用中华人民共和国的法律规定。

战略发展中心作为认证服务策略的工作部门，负责本文档实施的日常监督检查，保证 SHECA 认证服务体系内的运行符合本文档的要求。

1.5.4 CP /CPS批准程序

本文档由上海 CA 安全认证委员会审批通过后，在上海 CA 的网站上对外公布。

本文档经上海 CA 安全认证委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

1.6 定义和缩写

1.6.1 SHECA

上海市数字证书认证中心有限公司的缩写。

1.6.2 协卡网络信任服务体系

由上海市数字证书认证中心有限公司（Shanghai Electronic Certification Authority Co.,ltd，缩写为 SHECA）建设、运营的一个公开密钥基础设施，简称协卡认证，提供基于数字证书的电子认证服务。SHECA 是依照《中华人民共和国电子签名法》设立的第三方电子认证服务机构，致力于创建和谐的网络信任环境，向互联网用户提供安全、可靠、可信的数字证书服务。

1.6.3 SHECA安全认证委员会

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

1.6.4 电子认证服务机构

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

1.6.5 注册机构

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

1.6.6 受理点

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

1.6.7 系统管理员

负责安装、配置和维护 CA 系统的软硬件系统，负责 CA 服务器的启动和中止，管理 CA 的操作员。

1.6.8 录入员

负责录入证书申请者提交的信息，协助用户办理数字证书申请、撤销、更新等手续。

1.6.9 审核员

负责审核证书申请信息，协助用户办理数字证书申请、撤销、更新等手续。

1.6.10 证书制作员

负责为证书申请者下载制作证书，并提交给用户。

1.6.11 证书

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

1.6.12 数字证书

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

1.6.13 事件数字证书

事件数字证书是面向即时业务或者特定业务场景，上海 CA 所设计的一类基于事件证书专利技术的特殊数字证书。在业务过程中，自动将业务场景中相关信息（电子文档、签名行为特征信息、手写笔迹或其他签名行为证据信息等）关联至数字证书的扩展域，签发出事件数字证书，实现业务过程中的可靠电子签名。事件数字证书所对应的私钥一般为一次性使用，其在使用一次后即被销毁。

在本文档中，如无特殊定义，所述的数字证书，均指事件数字证书。

1.6.14 可靠数字证书

符合《电子签名法》及相关法规规定的个人或单位身份证书。

1.6.15 电子签名

简称为签名，具有识别签名人身份和表明签名人认可签名数据的功能的技术手段。

1.6.16 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。本文档中提及的签名为数字签名。

1.6.17 电子签名人

是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的人。

1.6.18 电子签名依赖方

是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的人。

1.6.19 私钥（电子签名制作数据）

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

1.6.20 公钥（电子签名验证数据）

是指订户验证电子签名的数据。

1.6.21 订户

被颁发给一个证书的证书主体。

1.6.22 依赖方

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。

1.6.23 证书垫付商

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

2 信息发布与信息管理

2.1 认证信息的发布

SHECA 在 http://www.sheca.com 上公布与其相关的信息；该网站是 SHECA 发布所有信息最首要、最及时、最权威的渠道。SHECA 将及时公布新的信息。只有 SHECA 有权处理网站上的旧信息。

2.1.1 SHECA信息库

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

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

SHECA 信息库将及时发布包括证书、CP/CPS 修订和撤销的通知和其它资料等内容，这些内容必须保持与 CP/CPS 和有关法律法规一致。SHECA 信息库可以通过网址： http://www.sheca.com/repository/ 访问，或

由 SHECA 随时指定的其它通讯方法获得。SHECA 可在 SHECA 信息库外颁布订户证书和相关 CRL 资料。除 SHECA 授权者外，禁止访问资料库（或其它由发证机构维护的数据）中任何被 CP/CPS 和（或）SHECA 信息库宣布为机密信息的资料。

2.1.2 公告和通知的发布

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

SHECA 根据新的技术发展，会公布保护证书持有者私钥可能的有效措施。

2.2 发布的时间和频率

2.2.1 电子认证业务规则的发布时间和频率

SHECA 将及时发布 CP/CPS 的最新版本，一旦对规则的修改、补充、调整等获得批准，SHECA 将在 http://www.sheca.com 上发布，并将最新的 CP/CPS 发布在 SHECA 信息库内，并与原有 CP/CPS 共同列出，以便检索。本文档至少每年更新一次。

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

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

2.2.2 证书的发布时间和频率

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

证书通过目录服务器发布时，SHECA 将在成功签发证书的同时进行实时发布。用户还可以通过 http 的方式，在 http://www.sheca.com 查询获得证书。

2.2.3 CRL的发布时间和频率

事件证书的订户证书在进行一次签名后私钥即时销毁，因此实际不进行证书撤销操作。

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

SHECA 不提供针对事件证书的订户证书 CRL 服务；针对中级根，SHECA 至少每三个月发布一次子 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。

2.2.4 公告、通知等信息的发布时间及频率

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

这类信息的发布是不定期的，SHECA 将保证会在第一时间发布信息。

2.2.5 用户服务、业务架构、市场发展等信息的发布时间及频率

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

2.3 信息库访问控制

2.3.1 SSL通道

敏感信息访问采用带安全套接层协议（SSL）的超文本传输协议（HTTPS），以实现访问记录的安全模式（此时

必须使用支持 SSL 的浏览器）。

2.3.2 权限管理和安全审计通道

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

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

3 标识与鉴别

3.1 命名

3.1.1 名称类型

认证机构依照特定的签发程序，保存与证书注册过程有关的特定记录，对特定对象的身份进行鉴别，以区别于其他的申请者。这一命名过程中出现的名称，包括甄别名和证书扩展项中包含的用户唯一识别项，是一组能辨别真实世界中实体的数据。

SHECA生成或者签发的证书的主要识别名称（SubjectName），采用X.500 Distinguish Name（DN）的方式。

每个证书订户按照X.509的规定，将对应一个可分辨的名称，该名称由甄别名和用户唯一标识项组成。甄别名包含于每张证书的主题中，用户唯一标识项包含于证书扩展项中。该名称唯一标识证书订户的身份。

作为可信第三方的认证机构负责确认公钥与已命名实体之间的联系。这种确认关系通过证书明白无误地表示出来。命名可以由SHECA和申请者协商解决，也可以由申请者独立完成。

3.1.2 对名称意义化的要求

标识名称所采用的用户识别信息，必须具有明确的、可追溯的、肯定的代表意义，不允许匿名或者伪名等出现。

3.1.3 订户的匿名或伪名

SHECA不接受或者允许任何匿名或者伪名，仅接受有明确意义的名称作为唯一标识符。

3.1.4 理解不同名称形式的规则

SHECA认证服务体系签发的证书，其甄别名DN的内容格式都符合X.500的命名规则。下面是一般识别名称的命名规则：

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

甄别名的命名规则由SHECA定义。

3.1.5 名称的唯一性

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

3.1.6 名称纠纷的处理

当订户或者申请者使用的名称相同时，SHECA以首先申请注册的用户优先使用。SHECA没有权利和义务处理因

此产生的相关纠纷，相关用户可以向有关主管部门申请解决。

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

3.1.7 命名机构

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

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

3.1.8 商标的承认、鉴别和角色

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

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

3.2 初始身份确认

3.2.1 证明持有私钥的方法

事件证书申请人在签名行为发生时产生证书请求，包括申请人的身份信息，以及证书申请人在进行签名行为时的记录信息（包括证书申请人的签名场景、签名动作、签名内容对象或签名内容特征值，从而可以事后有效还原签名行为）。签名行为的记录信息与证书申请人的身份信息在证书申请时进行绑定。因此，在签名行为发生时证书申请人视作其私钥的唯一持有者。

3.2.2 组织身份的鉴别

事件证书订户身份的鉴别参照机构身份鉴别方法，订户在为电子签名行为申请事件证书前，应通过身份鉴别，有效证明订户身份，接受事件证书申请的有关条款，同意承担相应的责任。

在事件证书鉴别过程中，由 CA 机构或授权的注册机构，接受订户的证书申请，对订户的身份真实性进行审核，并采集和记录订户的身份信息和电子签名行为的记录信息。

如果订户拒绝SHECA的身份鉴别要求，那么就被视作放弃对证书的申请。同时SHECA声明，SHECA可以拒绝任何申请要求，没有对此说明原因的义务。

3.2.3 个人身份的鉴别

事件证书订户身份的鉴别参照UniTrust个人身份证书鉴别方法，订户在为电子签名行为申请事件证书前，应通过身份鉴别，有效证明订户身份，接受事件证书申请的有关条款，同意承担相应的责任。

在事件证书鉴别过程中，由 CA 机构或授权的注册机构，接受订户的证书申请，对订户的身份真实性进行审核，并采集和记录订户的身份信息和电子签名行为的记录信息。

如果订户拒绝SHECA的身份鉴别要求，那么就被视作放弃对证书的申请。同时SHECA声明，SHECA可以拒绝任何申请要求，没有对此说明原因的义务。

3.2.4 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：

- 所提供的信息的年限；
- 该数据源更新的频率，确保数据保持更新；
- 数据的供应方，以及数据收集的目的；
- 数据的公开可用性及可访问性；
- 伪造或更改数据的难度。

3.2.5 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，订户提交的其他信息为没有验证的订户信息。

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

3.2.6 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事件证书时，SHECA和其授权的证书服务机构还需审核申请人的身份和资格，包括必需的身份资料和授权证明，并且通过电话、信函或其他方式与其代表的实体进行核实确认，以审核其是否有权代表那个实体。SHECA和其授权的证书服务机构有责任确认该授权信息，并将授权信息妥善保存。

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

3.2.7 互操作准则

对于非UNTSH认证服务体系内的其他证书服务机构，可以与SHECA进行交叉认证、单身交叉认证或其他形式的互操作，但是该证书服务机构的CP/CPS必须符合本文档要求，并且与SHECA签署相应的协议。SHECA将依据协议的内容，接受非SHECA的发证机构鉴别过的信息，并为之签发相应的证书。如果双方之间没有任何类似的协议，SHECA会根据情况决定是否接受这些被鉴别审核过的资料，并做出是否进行受理的决定。但交叉认证并不表示SHECA批准了或赋予了其他CA中心或电子认证服务机构的权利。

如果国家法律法规对此有规定，SHECA将严格予以执行。

3.3 密钥更新请求的身份标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

事件证书的密钥只适用于一次性签名事件，没有证书密钥更新服务。

3.3.2 吊销后密钥更新的标识与鉴别

事件证书的密钥只适用于一次性签名事件，不涉及吊销后密钥更新服务。

3.3.3 证书变更的标识与鉴别

事件证书的密钥只适用于一次性签名事件，没有证书变更服务。

3.4 吊销请求的标识与鉴别

事件证书只针对即时性签名事件，证书使用后即时失效，没有证书吊销服务。

3.5 授权服务机构的标示和鉴别

在外部证书服务机构满足SHECA相关授权服务协议的情况下，同意授权给该机构办理SHECA事件证书业务，该机构也将同意接受SHECA运营监督和审核评估。

1.该机构在申请成为SHECA授权后机构时需提供以下材料：

- 企业营业执照及加盖公章的复印件，组织机构代码证及加盖公章的复印件或事业单位法人证书及加盖公章的复印件
- 办理人身份证及加盖公章的复印件
- 按照要求填写并加盖公章的授权服务机构申请表

2.机构申请成为SHECA授权服务机构的流程：

- 申请机构填写、签署《SHECA 授权服务机构申请表》、《SHECA 证书受理点操作员登记表》、《SHECA 授权机构（CA 分中心）服务协议》并加盖公章后提交给 SHECA，并提交已加盖公章的营业执照、已签字的操作员身份证复印件。
- SHECA 会根据实际情况，填写《SHECA 授权服务机构评估表》。
- 若评估通过，申请机构填写《SHECA分中心（子CA）证书受理表》、《SHECA服务器（RA）证书受理表》、《SHECA授权服务机构证书管理员登记表》。

4 证书生命周期操作要求

4.1 证书申请

SHECA 仅接受在线申请方式，订户应遵守证书申请操作所规定的步骤。

4.1.1 正式证书

正式证书是指申请者按照本文档的规定和流程，递交真实的申请信息后经过认证机构批准获得证书，SHECA 对此类证书承担本文档规定的义务和责任。证书申请者根据事件证书的要求，提交内容完整的带个人手写签名或者加盖公章的申请表格。该申请表可以从 SHECA 的网站下载或到 SHECA 和其授权的证书服务机构领取。

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

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

事件证书分为以下两类：

1. 个人事件证书，以个人身份申请的事件证书，用于对特定时间，人员，任务，内容进行签名，以有效的证明事件的可靠性。

申请个人事件证书，需要递交以下材料：

- 申请者按照要求填写并签字的申请表
- 申请者按照要求填写并签字的订户协议

2. 机构事件证书，以机构身份申请的事件证书，用于对特定时间，人员，任务，内容进行签名，以有效的证明事件的可靠性。

   申请机构事件证书，需要递交以下材料：

- 按照要求填写并加盖公章的申请表

- 按照要求填写并加盖公章的经办人委托书
- 加盖公章的营业执照
- 按照要求填写并加盖公章的订户协议
- 若机构申请人持有可靠单位身份证书，仅需提供按照要求填写并加盖公章的订户协议

4.1.2 证书申请实体

在证书申请的过程中，参与整个申请过程的实体主要包含：

1. 证书申请者，包含个人、企业单位、事业单位、政府机构、社会团体、人民团体等各类组织机构。任何合法的组织、个人和有明确身份归属的其他网络主体均可申请事件证书，以保证网上交易和网上行政作业的安全和可靠。
2. SHECA 授权服务受理机构，以及相应的系统、系统管理员、操作员等。
3. 电子认证服务机构，包括 SHECA 以及 SHECA 授权的下级操作子 CA 等。
4. 订户，发证机构已经为其签发证书，并不依赖于其是否已经接受证书。
5. 密钥生成器，包括电子认证服务机构和用户自己选择的密钥生成器，包括但不限于只能密码钥匙（USB Key）、IC 卡、加密卡、加密机等硬件提供者和 IE 等。
6. 主管部门，包括《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》等规定的各类主管部门。

4.1.3 申请过程与责任

4.1.3.1 申请过程

SHECA对于事件证书仅支持在线申请。

1. 个人申请者
   a. CA 机构会通过人脸识别、银行卡验证、手机短信验证或可靠个人身份认证对申请人进行实名认证。如果实名认证未通过，CA 机构将拒绝为申请人发放证书，并将未通过的信息存档。
   b. 如果实名认证通过后，CA 机构会要求申请人在线录入证书申请信息。
   c. CA 机构会要求申请人在线确认并签署订户协议。
   d. CA 机构根据证书请求签发证书。
   e. 申请者接受并下载证书。
2. 机构申请者

（1）持有可靠机构身份证书

   a. 在线验证申请机构的身份证书的可靠性，如果验证未通过，CA 机构将拒绝为用户发放证书，并将未通过的信息存档。
   b. 验证通过后，申请机构需在线填写并同意订户协议。
   c. CA 机构根据证书请求签发证书。
   d. 申请者接受并下载证书。

（2）未持有可靠机构身份证书

   a. CA 机构会通过人脸识别对代理人进行实名认证。如果实名认证未通过，CA 机构将拒绝为申请人发放证书，并将未通过的信息存档。
   b. 如果实名认证通过后，CA 机构会要求代理人将加盖过公章的各项申请文件上传提交。
   c. CA 机构会人工验证相关信息的可靠性，如果验证不通过，则拒绝进行下一步操作，直接返回失败信息。
   d. 验证通过后，申请机构需在线填写并同意订户协议。
   e. CA 机构根据证书请求签发证书。

f. 申请者接受并下载证书。

4.1.3.2 各参与实体的责任

1. 电子认证服务机构的责任

电子认证服务机构应承担的责任是：保证电子认证服务机构本身的签名私钥在SHECA内部得到安全的存放和保护，SHECA建立和执行的安全机制符合国家相关政策的规定。

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

电子认证服务机构保证整个CA系统安全可靠的运行。SHECA不对由于客观以外或其他不可抗力事件造成的操作失败或延迟承担赔偿责任。为了表达明确，这些事件包括罢工或其他劳动纠纷、暴动、国内骚动、供应商故意或无意的行为、不可抗力、战争、火灾、爆炸、地震、洪水或其他灾难等。

2．证书申请者的责任

证书申请者必须严格遵守与证书申请以及私钥的所有权和安全保存相关的要求：

证书申请者承诺，在证书服务申请表上填列的所有声明和信息必须是完整、精确、真实和正确的，可供发证机构检查和核实；并且，证书申请者愿意承担任何因提供虚假信息、伪造信息等行为引起的法律责任。由于证书申请者自身原因导致发证机构无法正确为其签发证书的，由申请者自行承担有关损失和责任。

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

3．订户的责任

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

订户必须确保本身持有的证书用于申请时预定的目的。

SHECA只是告知，但并不要求证书申请者一定遵从 SHECA 提出的安全措施；订户可以选择任何自己认为可以保密的所有措施。

4．依赖方的责任

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

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

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

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

5.密钥生成器提供者的责任

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

6、主管部门

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

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

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

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

- 确认证书申请者接受订户协议中的各项条款。

- 按照事件证书的要求对证书申请者的身份进行验证。
- 确认证书申请者合法的拥有与证书中所含公钥配对的私钥（如要求订户作出保证等方式）。
- 确认证书中包含的信息，除了未经验证的订户信息外，都是准确的。
- 确认任何受托人在代表其组织机构申请证书时，该受托人已得到了所代表的组织机构的合法授权。
- 确认任何委托办理的各方之间的授权合法性和委托方、受托方的身份。

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

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

中华人民共和国上海市四川北路 1717 号 嘉杰国际广场 18 楼（200080）

上海市数字证书认证中心有限公司 SHECA 客户服务中心

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

4.2.2 证书申请批准和拒绝

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

如果符合下述条件，可以批准证书申请：

- 该申请完全满足前面 3.2 条款关于订户信息的标识和鉴别规定
- 申请者接受或者没有反对订户协议的内容和要求
- 申请者已经按照规定支付了相应的费用，另有协议规定的情况除外

当SHECA及其授权的证书服务机构在进行鉴别程序时，如果申请者未能成功通过鉴别，SHECA将拒绝申请者的证书申请，并立即通知申请者鉴别失败。对于鉴别失败的原因，SHECA有权拒绝解释，并且不需要通知申请者。法律法规对此有明确要求的除外。如果是由于第三方信息而导致身份鉴别失败,SHECA将向申请者提供第三方的联系方式，以便申请者查询。SHECA采用申请者向SHECA提交证书申请时使用的相同方法来通知证书申请者其证书申请失败。

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

如果发生下列情形，可以拒绝证书申请：

- 该申请不符合前面 3.2 条款关于订户信息的标识和鉴别规定
- 申请者不能提供所需要的身份证明材料或其他需要提供的支持文件
- 申请者反对或者不能接受订户协议的有关内容和要求
- 申请者没有或者不能够按照规定支付相应的费用
- RA 或者 CA 认为批准该申请将会对 CA 带来争议、法律纠纷或者损失

被拒绝的证书申请者可随后再次提出申请。

4.2.3 处理证书申请的时间

事件证书申请为即时处理。

4.3 证书签发

4.3.1 证书签发过程中电子认证服务机构的行为

证书申请者一旦提交了证书申请，尽管事实上还没有接受证书，但仍被视为该订户已同意发证机构为其签发证

书。

发证机构在批准证书申请之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

4.3.2 电子认证服务机构和注册机构对订户的通告

事件证书用于标识和证明订户的电子签名行为，发证机构在批准了证书申请之后，将为订户签发证书并直接应用于对应的电子签名。订户成功完成电子签名，即视为SHECA证书签发成功，SHECA不再就证书签发向订户进行其他方式的通告。

4.4 证书接受

4.4.1 构成接受证书的行为

事件证书签发完成后，并将证书应用于对应的电子签名时起，就被视为同意接受证书。

4.4.2 电子认证服务机构对证书的发布

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

订户、依赖方可以通过 HTTP 的方式查询自己或他人的证书。

如果订户书面提出申请，CA可以不把该订户的证书发布到任何公开的信息库中。

4.4.3 电子认证服务机构在颁发证书时对其他实体的通告

对于SHECA签发事件证书，SHECA不对其他实体进行通告。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在提交了证书申请并接受了CA机构所签发的证书后，均视为已经同意遵守与CA机构和依赖方有关的权利和义务的条款。订户才可以使用其证书以及与该证书相对应的私钥。该证书只能根据本文档及相关CP/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。

事件证书仅应用于订户对应的电子签名行为，订户只能在该次电子签名中使用私钥和证书，订户只有在接受了相关证书之后，才能使用对应的私钥执行电子签名运算。私钥将在完成本次电子签名数学运算后进行销毁，之后订户须停止使用该证书对应的私钥。

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

如果证书中的某些字段明确了证书的使用范围和用途，那么该证书将在也只被允许在这一范围内进行使用。任何超出证书所标明的适用范围内的行为，都将由行为人独立承担责任。SHECA 对超出适用范围的任何使用行为，不承担任何由此产生的责任和义务。

4.5.2 依赖方对公钥和证书的使用

在信任证书和签名前，依赖方要独立地做出应有的努力和合理的判断：

- 该证书是否由可信任的 CA 所签发

- 对于任何给定的目的，证书被适当的使用；并且判断该证书没有被用于任何本文档或者法律法规禁止的或者限制的使用范围。订户接受证书后，由订户负责保证证书被适当的使用。
- 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）

除非本文档另有规定，证书并不是来自发证机构的对任何权力或特权的承诺。依赖方只能在本文档规定的范围内信赖证书和证书中包含的公钥，并对此做出决定。

如果证书中的某些字段明确了证书的使用范围和用途，那么该证书将在也只被允许在这一范围内进行使用。依赖方必须对此做出合理的判断，任何对超出证书所标明的适用范围的行为的信赖，都将由依赖人独立承担责任，SHECA 对此不承担任何责任和义务。

4.6 证书更新

事件证书仅用于订户特定一次的电子签名行为，不提供证书更新服务。

4.7 证书密钥更新

事件证书密钥在使用过一次后即销毁，不提供证书密钥更新服务。

4.8 证书变更

事件证书仅用于订户特定一次的电子签名行为，不提供证书变更服务。

4.9 证书吊销和挂起

事件证书仅用于订户特定一次的电子签名行为，密钥在使用过一次后即销毁，不提供证书吊销和挂起服务。

4.10 证书状态服务

事件证书仅用于订户特定一次的电子签名行为，证书使用一次后即失效， 根据依赖方约定，可向依赖方提供状态查询服务。

4.11 订购结束

事件证书订购结束是指当订户使用数字证书完成电子签名后，该证书的服务时间结束。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略和行为

订户的签名密钥对由签名设备生成密钥并执行签名后，即时销毁，签名密钥不进行保管。

5 电子认证服务机构设施、管理和操作控制

5.1 物理控制

SHECA 及其下属授权服务机构遵守的物理控制和安全策略，认证服务系统位于安全稳固的建筑物内，具备独立的软硬件操作环境。只有经过授权的操作人员，才可以根据有关的安全操作规范进入相应的区域进行操作。SHECA 的根密钥位于最高安全强度的环境内，避免被破坏或者被未经授权的操作。

5.1.1 场地位置与建筑

SHECA 认证系统的主机房位于上海市电信大楼，备份机房位于上海市大数据中心灾备中心，均有四道物理的保护层，以监控和管理 SHECA 机房的物理通道。鉴于上海市所处的地理环境，发生地震等自然灾害的概率较小，

SHECA 的主备机房均具备独立的防震、防火、防水、温控、门禁系统、视频监控系统和警报系统等，以保证认证服务的连续性和可靠性。所有机房的建设和管理严格按照 SHECA 的规定要求。机房内部一律禁止参观。只有经过SHECA 授权的人员才能进入授权的部位和区域。机房采用高安全性的监控技术，包括视频、指纹、门禁等安全管理手段，以确保物理通道的安全。进入 SHECA 机房时，有可控时间限制的门禁系统。机房实行全天候自动监控。

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

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

5.1.2 物理访问

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

操作人员进入工作区域进行操作，必须通过指纹验证和权限检验。

5.1.3 电力与空调

CA 系统供电得到充分保障，使用不间断电源（UPS），避免电源波动。采用双电源，在单路电源损坏时，可以自动切换，维持系统正常运转。

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

SHECA 参照电信设施管理的规定进行维护和保养。

5.1.4 水患防治

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

5.1.5 火灾防护

机房采用防火材料建设，具备中央防火监控设备和自动喷淋系统，避免火灾的威胁。SHECA 还通过与专业防火部门协调，建立了消防灭火等应急响应措施，机房通过了国家权威部门的消防测试。

5.1.6 介质储存

系统使用的存储介质，处在防磁、防静电干扰的环境中，得到了安全可靠的保护，避免诸如温度、湿度、和磁力等环境变化可能产生的危害和破坏。

5.1.7 废物处理

SHECA 使用的硬件设备、存储设备、加密设备等，当废弃不用时，涉及敏感性和机密性的信息都被安全、彻底的消除。

文件和存储介质包含有敏感性和机密性信息时，在处理时都经过了特殊的销毁措施，保证其信息无法被恢复和读取。

所有处理行为将记录在案，以满足审查的需要，所有的销毁行为都遵循有关的法律法规。

5.1.8 异地备份

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

- 数据备份，SHECA 同时进行异地的数据备份。异地备份的操作在 SHECA 灾难恢复计划中进行规定。SHECA 异地数据备份介质安全要求都符合 SHECA 备份标准和程序。

5.2 程序控制

5.2.1 可信角色

证书服务具有高可靠性和高安全性的要求。为了保证可靠的人员管理，员工、第三方服务人员、顾问等应该是被认定为可信的人员，才可在可信的岗位进行工作。SHECA 所有有权使用或控制那些可能影响证书的签发、使用、管理和撤销等操作（包括对 SHECA 信息库限制性操作）的员工、第三方服务人员等（统称“人员”），在本文档 中均视为可信角色。

SHECA 明确规定 CA 关键职能的职位，他们包括：

1、应用系统管理员

2、操作系统管理员

3、数据库系统管理员

4、网络系统管理员

5、录入员

6、审核员

7、密钥控制小组

8、安全执行小组

9、其他人员等。

安排上述职位是为了确保责任能够明确分担，建立有效的安全机制，保证内部管理和操作的安全。

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

5.2.2 每项任务需要的人数

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

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

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

对于证书申请的鉴别和签发，也需要至少两个可信人员操作才能完成。 对于重要的系统数据操作和重要系统维护，需要安排至少一人进行操作，一人进行监督记录。

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

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

5.2.3 每个角色的识别与鉴别

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

- 根据实际需要确定不同的角色，为其划分权限和要求，并设定不同角色的背景要求
- 对人员进行背景调查，使其符合相应角色的可信要求

- 赋予可信角色在系统中的权限，并为其发放令牌

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

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

所有 SHECA 人员必须确保：

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

5.2.4 需要职责分割的角色

需要进行职责分割的角色，包括但不限于下列人员：

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

对于证书服务的受理，必须通过录入员、审核员两个角色进行才能完成。对于根密钥的操作，必须有 3 名以上的根密钥的管理员人员同时到场，才能进行有关的操作。

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

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

5.3 人员控制

5.3.1 资格、经历和无过失要求

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

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

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

根据不同可信岗位的工作特点，背景审查应该包括但不限于以下内容：

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

- 无犯罪证明材料

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

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

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

- 验证先前工作记录的真实性
- 验证身份证明的真实性
- 验证学历、学位及其他资格证书的真实性
- 检验无犯罪证明材料并确认无犯罪记录
- 通过适当途径了解是否有工作中的严重不诚实行为

在背景调查中，如果发现下列情形，可以拒绝其获得可信人员的资格：

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

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

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

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

5.3.3 培训要求

SHECA 对员工进行以下内容的培训：

- SHECA 安全管理策略
- 工作岗位职责
- PKI 基础知识
- SHECA 认证系统使用的软件介绍
- SHECA 认证系统管理控制体系
- 身份验证、审核策略和程序
- 灾难恢复和业务连续性程序
- 认证策略、本文档政策及相关标准和程序
- 针对验证程序存在的一般威胁，包括钓鱼和其他社会工程学行为
- 电子认证相关法律法规等
- 其他需要进行的培训

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

5.3.4 再培训周期和要求

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

对于公司安全管理策略，应该每年至少进行一次培训。

认证系统运营相关的人员，每年至少进行一次相关技能和知识培训。

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

5.3.5 工作岗位轮换周期和顺序

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

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

5.3.6 未授权行为的处罚

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

一旦发现上述情况，SHECA 立即撤销或终止该人员的安全令牌。

5.3.7 独立合约人的要求

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

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

否则，独立承包人或顾问只能在可信人员陪同和直接监督下有权访问相关安全设施。

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

5.3.8 提供给员工的文档

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

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

5.4 审计日志控制

5.4.1 记录事件的类型

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

1. 证书订户服务申请和撤销的信息，如申请表、协议、身份资料和其他相关信息等。
2. CA 密钥的生成、存储、恢复、归档、销毁、运输和迁移等。
3. 认证系统各类服务系统密钥对的生成、内置、变更等成功和失败的纪录。
4. 认证系统日常运作产生的日志记录文件。

5. 进出SHECA及其授权机构控制区域内的表格、安全令牌进出敏感区域的纪录、机房工作日志、系统日常维护记录、监控录像等。
6. 系统软硬件设备上线、更换、下线等的纪录。
7. 认证机构、注册机构和受理点之间的协议、规范和相关工作记录。
8. SHECA 还要记录与系统不直接相关的事件，例如：物理通道参观记录、人事变动。
9. 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。
10. 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。
11. 防火墙和入侵检测系统记录的安全事件。

5.4.2 处理日志的周期

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

5.4.3 审计日志的保存期限

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

5.4.4 审计日志的保护

SHECA 执行严格的物理和逻辑访问控制措施，以确保只有 SHECA 授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，严格禁止未授权的访问、阅读、修改和删除等操作。

5.4.5 审计日志备份程序

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

5.4.6 审计收集系统

SHECA 的审计收集系统涉及的对象包括：

- □证书管理系统
- □证书签发系统
- □证书审批受理系统
- □备份恢复系统
- □访问控制系统（包括防火墙）
- □用户服务系统
- □网站、数据库安全保障系统
- □其他 SHECA 认为有必要审查的系统

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

5.4.7 对异常事件的通告

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

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

门处理等措施。是否通知攻击者或肇事者，由 SHECA 决定。

5.4.8 脆弱性评估

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

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

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

5.5 记录归档

5.5.1 归档记录的类型

SHECA 对下列记录（包括但不限于）进行归档保存：

1. SHECA 的系统建设和升级文档
2. 证书申请信息、证书服务批准和拒绝的信息、与证书订户的协议等
3. 系统运行和认证服务产生的日志数据、认证系统证书密钥升级和更新信息等
4. 电子认证服务规则、各类服务规范和运作协议、管理制度等
5. 系统数据库数据
6. 人员进出记录和第三方人员服务记录
7. 监控录像
8. 员工资料，包括背景调查、录用、培训等资料
9. 各类外部、内部审查评估文档

5.5.2 归档记录的保存期限

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

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

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

3、订户证书和密钥的相关变动信息，至少保存 7 年。

4、认证机构的证书和密钥，以及相关的变动信息，至少保存 20 年。

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

6、其他信息保留期限至少 5 年。

7、业务管理类记录，保留不少于 2 年。

8、与法律政策的规定不一致的，选择两者中较长的期限予以保存。

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

5.5.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证，以保证归档文件能够得以长期有效的保存。只有经过授权的工作人员按照特定的安全方式才能接近和存取。除了法律的需要和认证操作规范的需要，任何人不得随意获得。

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

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

5.5.4 归档文件的备份程序

所有存档的文件和数据，通常保存在 SHECA 的主要存储场所。确有必要的，还将在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有授权的工作人员才能在监督的情况下，对档案进行读取操作。SHECA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

对于需要持续保存、归档的文件和数据，将根据 SHECA 的备份策略进行归档和整理。

当认证系统因为异常情况导致无法正常运营时，按照 SHECA 的恢复策略，利用这些归档保存的数据进行系统的恢复。

5.5.5 记录时间戳要求

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

5.5.6 归档收集系统

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

5.5.7 获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。归档记录的一致性在归档时进行验证。归档期间，所有被访问的记录在归还时必须验证其一致性。

5.6 电子认证服务机构根证书有效期限

SHECA 的根证书有效期最长不超过 25 年，任何由其签发的证书，包括子 CA 证书和订户证书，其有效期都短于根证书的有效期，任何由子 CA 其签发的订户证书，其有效期都短于子 CA 证书的有效期。

根证书及子 CA 证书的有效期，在证书内有明确的表示。

5.7 电子认证服务机构密钥更替

在证书到期以前，SHECA 将按照 本文档 的规定对根密钥进行更换，生成新的证书。在进行密钥的生成时，严格按照 SHECA 关于密钥管理的规范。CA 密钥更替必须遵循以下原则：

1. 在下级证书生命周期结束前停止签发新的下级证书，确保在 CA 的证书到期时所有下级证书也全部到期。
2. 在停止签发新的下级证书后至证书到期时，继续使用 CA 私钥起起案发CRL，直到最后一张下级证书过期。
3. 生成和管理 CA 密钥对时，严格遵守密钥规范。
4. 及时发布新的 CA 证书。
5. 确保整个过渡过程安全、顺利，不出现信任真空期。
6. 针对外部认证机构（子CA）的CA密钥，不提供密钥更替服务。CA证书更新按照外部子CA证书的申请流程

进行。

5.8 损害与灾难恢复

为了在出现异常或灾难情况时，能够在最短的时间内重新恢复认证系统的运行，SHECA 制订了可靠的损害和灾难恢复计划，以应对突发事故导致的系统问题。

5.8.1 事故和损害处理程序

SHECA 遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，SHECA 将按照灾难恢复计划实施恢复。具体由 SHECA 灾难恢复计划决定。

5.8.2 计算资源、软件和/或数据的损坏

当认证系统运营使用的软件、数据或者其他信息出现异常损毁时，可以依照SHECA 的系统备份与恢复操作手册，根据系统内部备份的资料，或者异地备份的资料，执行系统恢复操作，使认证系统能够重新正常运营。

当认证系统使用的硬件设备出现损毁时，可以依照 SHECA 的系统备份与恢复操作手册，启动备份硬件设备以及相关的备份操作系统和认证系统，重新恢复系统运行。

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

5.8.3 SHECA私钥损害处理程序

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

1. 立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其它公共媒体对订户进行通告，采取措施保证用户利益不受损失。
2. 立即撤销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。同时 SHECA 立即生成新的密钥对，并自签发新的根证书。
3. 新的根证书签发以后，按照本文档 关于证书签发的规定，重新签发下级证书和下级操作子 CA 证书。
4. SHECA 新的根证书签发以后，将会立即通过 SHECA 信息库、目录服务器、HTTP 等方式进行发布。

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

1. 立即向 SHECA 进行汇报并生成新的密钥对和证书请求，向 SHECA 申请签发新的证书。
2. SHECA 立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其它公共媒体对订户进行通告，采取措施保证用户利益不受损失。
3. 立即撤销所有由该子 CA 签发的证书，更新OCSP 信息，供证书订户和依赖方查询。
4. 新的子 CA 证书签发以后，按照本文档 关于证书签发的规定，重新签发订户证书。
5. 新的证书签发以后，将会立即通过 SHECA 信息库、目录服务器、HTTP 等方式进行发布。

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

5.8.4 灾难后的业务连续性能力

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

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

5.9 电子认证服务机构或注册机构的终止

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

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

2. 安排业务承接。

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

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

6 认证系统技术安全控制

6.1 密钥对的生成和安装

密钥对是电子签名安全机制的关键，本文档制订了相应的规定，确保密钥对的产生、传送、安装等具备保密性、完整性和不可否认性。

6.1.1 密钥对的生成

1、SHECA 事件证书根密钥的产生

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

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

2、事件证书子 CA 密钥对的生成

事件证书的子 CA 密钥对指的是 SHECA 自营或与 SHECA 签订授权机构协议的外部 CA 分中心控制的，由 SHECA 事件证书根密钥签发的中级根密钥。事件证书子 CA 密钥同样符合 FIPS140-2 标准，密钥对的生成要求与 SHECA 根密钥一致。必须有超过 3 位的具备权限的密钥管理和操作人员同时操作。

3、订户签名密钥对的生成

订户证书的签名密钥对由符合国家密钥管理标准的硬件安全模块（Hardware Security Module,以下简称 HSM）生成，确保其密钥生成过程安全可靠。SHECA 在技术、业务流程和管理上，已经实施了安全保密的措施。

4、订户加密密钥对的生成

加密密钥对由相应的国家密钥管理机构生成，并以安全的方式传送。

6.1.2 私钥传送给订户

订户的签名密钥对由硬件安全模块（HSM）生成并保管。

6.1.3 公钥传送给证书签发机构

证书订户以公钥向 SHECA 申请签发证书时，该请求信息内的公钥，得到订户私钥签名、用户身份验证和信息

完整性的保护，并且通过安全可靠的方式进行传输。

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

6.1.4 电子认证服务机构公钥传送给依赖方

SHECA 的公钥包含在 SHECA 自签发的根 CA 证书中，通过网站 http://www.sheca.com 进行发布。SHECA 支持在线传递公钥或从 SHECA 的网站下载的方式传递公钥，以供证书订户和依赖方查询使用。

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

6.1.5 密钥的长度

SHECA 事件证书的订户证书的 RSA 密钥长度应为 RSA2048 位或以上，采用 SM2 算法的密钥对应为 256 位。

SHECA 事件证书根密钥长度为 RSA4096 位或 SM2 算法的 256 位。

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

6.1.6 公钥参数的生成和质量检查

公钥参数必须使用国家密码主管部门批准许可的加密设备生成并遵从这些设备的生成规范和标准。SHECA 当然的认为这些设备内置的协议、算法等已经具备了足够的安全等级要求。

对于参数质量的检查，同样由通过国家密码主管部门批准许可的加密设备进行，例如加密机、加密卡、USB Key、IC 卡等。SHECA 当然的认为这些设备内置的协议、算法等已经具备了足够的安全等级要求。

6.1.7 密钥使用目的

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

所有密钥的使用，都必须遵循本文档的规范。

事件证书订户的签名密钥可以用于提供安全服务，实现身份认证、不可抵赖性和信息的完整性等，用于签署具备法律效力的电子文档和电子交易数据。

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 机构所用的密码设备都是经国家相关部门认可的产品，其接口、协议、密钥和物理安全要符合国家相关规范要求。

所采用的主机加密服务器均取得国家商用密码产品型号证书。其主要功能包括：

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

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

3、权限管理：可以初始化管理员和操作员，负责管理员、操作员权限的判断。 管理员口令采用分割权限的密钥管理机制。

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

5、生成输出密钥：生成可以输出加密设备的RSA密钥对时，该密钥对已加密。

6、采用硬件的物理噪声源随机数发生器芯片产生随机数。

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

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

兼容性。

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

6.2.2 私钥的多人控制

1、SHECA采用多人控制策略来激活、使用、停止其私钥（m选n）。

SHECA的私钥采用多人控制的策略（即n out of m策略，m>n, n>=3 ）。目前采用五人控制，需要至少三个或三个以上的密钥控制人员来共同完成生成和分割程序。SHECA系统在技术上已经建立了相应安全机制，对生成操作进行限制。具有权限的密钥管理人员，分别持有分割后的一段密码。所有和私钥相关的信息，例如控制IC卡、保护PIN码等，分别由不同的管理人员来控制。

2、订户证书的私钥应存储在硬件安全模块

订户证书的私钥应存储在硬件安全模块中，由订户通过访问控制使用操作。子CA管理硬件安全模块并负责私钥的安全，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，子CA在第一时间告知SHECA。

6.2.3 私钥托管

加密私钥的保护、管理、存档、备份、托管等，由上海密钥管理中心（KM）部门进行规范和决定。由于事件证书的订户证书私钥在使用后即销毁，订户证书私钥存放在硬件安全模块中。

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，由于事件证书私钥在使用后即销毁，不进行备份。

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，订户私钥不进行归档。

6.2.6 私钥导入或导出密码模块

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

SHECA不提供订户私钥从硬件密码模块中导出的方法，也不允许如此操作。

6.2.7 私钥在密码模块中的存储

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

订户证书的私钥在进行签名后即失效。

6.2.8 激活私钥的方法

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

6.2.9 解除私钥激活状态的方法

一旦私钥被激活，除非这种状态被解除，私钥总是处于活动状态。在某些私钥的使用当中，私钥每次被激活，只能进行一次操作，如果需要进行第二次操作，需要再次进行激活。

SHECA解除私钥激活状态的方式包括退出、切断电源、移开令牌/钥匙，自动冻结。未经授权的任何人员，绝不可以进行相关操作。

6.2.10 销毁密钥的方法

SHECA的私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，加密设备必须被清空。同时，所有用于激活私钥的PIN码、IC卡、动态令牌等也必须被销毁或者收回。私钥归档的操作按照本文档的规定处理。

事件证书订户私钥在进行一次签名后即销毁。

具有销毁密钥权限的管理员使用含有自己的身份的加密IC卡登录，启动密钥管理程序，进行销毁密钥的操作，需要半数以上的管理员同时在场。

6.2.11 密码模块的评估

SHECA使用国家密码主管部门批准和许可的密码产品，接受其颁布的各类标准、规范、评估结果、评价证书等各类要求。根据SHECA对产品性能、工作效率、供应厂商的资质等方面的评估，选择需要的模块。

6.2.12 密钥的运输

不适用

6.2.13 密钥的传输

不适用

6.3 密钥对管理的其他方面

6.3.1 公钥归档

订户证书中的公钥包括签名证书中的公钥，由 CA 机构定期归档。

6.3.2 证书操作期和密钥对使用期限

事件证书密钥对的有效期与证书有效期不同，私钥有效期为从签发证书到第一次使用该证书进行数字签名，公钥有效期一般与证书有效期一致。

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3年。对于CA证书，最长的有效期不超过30年。

证书类型	密钥对最长使用期限	证书最长有效期
根证书（2018年之前签发）	30年	30年
根证书（2018年之后签发）	25年	25年
中级CA证书	25年	25年
订户证书	私钥用后即毁 公钥3年	3年

时间戳证书	15个月	135个月
OCSP证书	12个月	12个月

6.4 激活数据

6.4.1 激活数据的产生和安装

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。

6.4.2 激活数据的保护

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

6.4.3 激活数据的其他方面

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 特别的计算机安全技术要求

SHECA 认证系统的信息安全管理，按照国家密码管理局公布的《证书认证系统密码及其相关安全技术规范》、工业与信息化部公布的《电子认证服务管理办法》，参照 ISO17799 信息安全标准规范以及其它相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。

- 主要的安全技术和控制措施包括：
- 身份识别和验证管理
- 资源和信息存取权限控制
- 安全审计和日志
- 资料备份和保存的安全保护
- 人员职责分权，对CA工作角色进行分类，建立安全分散和牵制机制
- 内部操作程序控制
- 灾难备份恢复机制
- 个人计算机安全管理等
- 信息传递加密机制

通过严格的安全控制手段，确保 CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。此外，认证机构应只允许有工作需求的必要人员访问证书服务器，一般的应用用户在证书服务器上没有账户。核心系统必须与其它系统物理分离，生产系统与其他系统逻辑隔离。

6.5.2 计算机安全评估

SHECA 的认证业务系统，通过了国家密码管理局、中国国家信息安全测评中心、上海市信息安全测评中心等部门的有关评估、审查和认证。

6.6 生命周期技术控制

6.6.1 系统开发控制

SHECA 的开发控制包括可信人员管理、开发环境安全管理、产品设计和开发评估、使用可靠的开发工具等，设计的产系统满足冗余性、容错性、模块化的要求。软件设计和开发过程遵循以下原则：

第三方验证和审查

安全风险分析和可靠性设计

同时，SHECA 制订的的软件开发规范，参考国家相关标准，在实施中严格执行相关的规划和开发控制。

6.6.2 安全管理控制

SHECA 认证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。

SHECA 认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行使用，任何修改和升级会记录在案并进行版本控制、功能测试和记录。SHECA 还对认证系统进行定期和不定期的检查和测试。

SHECA 采用严格的管理体系来控制和监视系统的配置，以防止未授权的修改。

硬件设备从采购到上线前，会进行安全性的检查，用来识别设备是否被入侵，是否存在安全漏洞等。加密设备的采购和安装，在更加严格的安全控制机制下，进行检验、安装和验收。

SHECA 认证系统所有的软硬件设备升级以后，废旧设备在进行处理时，必须确认其是否有影响认证业务安全性的信息存在。

6.6.3 生命期的安全控制

无规定。

6.7 网络的安全控制

SHECA认证系统采用多级防火墙和网络控制系统的保护，并且实施完善的访问控制技术。

认证系统只开放与申请证书、查询证书等相关的操作功能，供用户通过网络进行操作。

为了确保网络安全，SHECA认证系统安装部署了防火墙、入侵检测、安全审计、病毒防范系统，并且及时更新防火墙、入侵监测、安全审计、病毒防范系统的版本，以尽可能的降低来自网络的风险。

6.8 时间戳

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

7 证书格式

7.1 证书

SHECA使用的证书详细格式，符合国家相关标准的要求，并遵循ITU-T X.509 V3（1997）：信息技术—开放系统互连 - 目录：认证框架（1997年6月）标准和RFC 5280: Internet X.509 公钥基础设施证书和CRL结构（2008年5月）。

7.1.1 版本号

SHECA签发的证书，符合X.509 V3证书格式，这一版本信息存放在证书版本属性栏内。

7.1.2 证书扩展项

SHECA 除了证书扩展项除使用 IETF RFC 3280 中定义的证书扩展项，还支持私有扩展项。

- 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。

	事件证书（订户证书）	CA证书
0 digitalSignature	√	√
1 nonRepudiation	×	×
2 keyEncipherment	×	×
3 dataEncipherment	×	×
4 keyAgreement	×	×
5 keyCertSign	×	√
6 cRLSign	×	√
7 encipherOnly	×	×
8 decipherOnly	×	×

- 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

事件证书应配置以下扩展密钥用途

	事件证书（订户证书）
文件签署 (1.3.6.1.4.1.311.10.3.12)	√
Adobe PDF 签署 (1.2.840.113583.1.1.5)	√

- CRL发布点

CRL 分发点扩展项包含可以获取 CRL 的 URL，用于验证证书状态。

- 序列号

SHECA 签发的证书采用随机序列号。

- 私有扩展项

事件证书支持下列私有扩展项：

签名扩展项，Signature Extension，应包含签名相关证据内容，如声音、图像等。

7.1.3 算法对象标识符

SHECA签发的证书密钥算法标识符为sha256RSA或SM3。

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

1、签名算法：

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

2、摘要算法：

- sha256的对象标识符为：{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)

csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)}

- sm3的对象标识符为：{iso(1) member-body(2) cn(156) ccstc (10197) sm-scheme(1) sm3(401)}

3、非对称算法：

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

4、对称算法

本文档建议使用国家密码管理部门认可的对称算法

7.1.4 名称形式

SHECA签发的证书，其名称形式的格式和内容符合X.501的甄别名格式，主体Subject 的X.500 DN 是C=CN命名空间下的X.500 目录唯一名字，各属性的编码一律使用 UTF8String。

主体Subject 的X.500 DN 支持多级O 和OU，其格式如下： C=CN;

O=×× OU= ××; CN=××

7.1.4.1 C（Country）应为证书主体所在国家，可选填；

7.1.4.2 O（Organization）应为证书主体或者证书主体所属单位的所在省、自治区、直辖市名称全称，可选填；

7.1.4.3 OU（Organization Unit）应为证书主体或者证书主体所属单位的名称全称，可选填；

7.1.4.4 CN（Common Name）应为证书主体的姓名；

7.1.5 名称限制

SHECA签发的证书，其识别名称不允许为匿名或者伪名，必须是有确定含义的识别名称。

7.1.6 证书策略对象标识符

SHECA按照X.509标准签发的证书，其证书策略对象标识符，存放在证书内证书策略的相关栏目。具体请参考本文档 1.2。

7.1.7 策略限制扩展项的用法

无规定。

7.1.8 策略限定符的语法和语义

无规定。

7.1.9 关键证书策略扩展项的处理规则

无规定。

7.2 证书撤销列表

事件证书不签发CRL，所有订户证书私钥在签名后即销毁；仅针对中级根证书（子CA）签发ARL。

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ARL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ARL。

7.3 在线证书状态协议

SHECA为用户提供OCSP（在线证书状态查询服务）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。

7.3.2 OCSP扩展项

无规定。

7.3.3 OCSP的请求和响应

一个OCSP请求包含以下数据：

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

在接受一个请求之后，OCSP服务端响应时进行如下检测：

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

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

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

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

- 未正确格式化的请求（malformedRequest）
- 内部错误（internalError）
- 请稍后再试（trylater）

- 需要签名（sigRequired）
- 未授权（unauthorized)

8 电子认证服务机构审计和其他评估

8.1 评估的频率或情形

审计是为了检查、确认 CA 是否按照本文档及其制度和安全策略开展业务，发现存在的可能风险。根据工作需要，定期组织开展审计评估。

8.2 评估者的资质

内部审计人员由 CA 机构内部人员组成，外部审计的审计人员的资质由第三方确定。

8.3 评估者与被评估者之间的关系

评估者与被评估者应无任何业务、财务往来或其它利害关系，足以影响评估的客观性。

8.4 评估内容

审计所涵盖的主题包括：人事、机房物理安全、安全运营管理、密钥安全和运行服务、客户服务等内容。

8.5 对问题与不足采取的措施

对审计中发现的问题，CA 机构将根据审计报告的内容准备解决方案，明确对此采取的行动。CA 机构将根据国际惯例和相关法律、法规迅速解决问题。

8.6 评估结果的传达与发布

除非法律明确要求，CA 机构一般不公开评估结果。

对 CA 关联方，CA 机构将依据签署的协议来公布评估结果。

9 法律责任和其他业务条款

9.1 费用

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

证书及其相关服务的价格，在SHECA的网站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。未公布价格的，以与订户的协议价格为准。

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对证书签发的费用，公布在SHECA的网站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http://www.sheca.com上予以公布。

9.1.3 证书撤销或状态信息的查询费用

SHECA对证书状态查询，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CP/CPS或其他相关的作业文件时，SHECA需要收取因此产生的邮递和处理工本费。

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

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

9.1.5 退款策略

SHECA对订户收取的费用，除了证书申请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违背了本文档所规定的责任或其它重大义务，订户可以要求SHECA撤销证书并退款。在SHECA撤销了订户的证书后，SHECA将立即把订户为申请该证书所支付的费用全额退还给订户。订户需要填写退款申请表，并递交给SHECA及其授权的证书服务机构，以要求退款。

此退款策略不限制订户得到其它的赔偿。

完成退款后，订户如果继续使用该证书，SHECA将追究其法律责任。

9.1.6 支付能力

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

9.2 财务责任

9.2.1 保险范围

SHECA根据业务发展情况决定其投保策略，包括但不限于：

1、建筑物与硬件设施的火灾等意外险。

2、证书责任险，保险范围涵盖所有SHECA依据本文档签发的订户证书。

目前，SHECA没有提供第三方保险服务。

9.2.2 其他资产

无规定。

9.2.3 对最终实体的保险或担保

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

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

9.3 业务信息保密

9.3.1 保密信息范围

1、保密信息包括SHECA和其授权的证书服务机构、SHECA与订户、SHECA与其他证书服务相关方、SHECA关联实体之间的协议、往来函和商务协定等。除非法律明确规定和SHECA明确进行了书面许可，一般不能在未经另一方许可的情况下擅自公开。

2、 与证书持有者证书公钥配对的私钥是机密的，证书订户应该遵照本文档的规定妥善保管，不能公布给未经授权的任意第三方。如果因证书订户泄露私钥，订户应自行承担一切责任。

3、 对SHECA或SHECA对关联实体的审计报告、审计结果等相关信息是机密信息，除了SHECA授权和信任的员工，不能泄露给其他任何人。这些信息除了审查目的或法律规定的目的，不能用于其他用途。

4、有关SHECA认证系统的运营信息只能在严格指定的情况下，才能提供给经SHECA授权的员工，这种授权并不意味着对信息公开的授权。对SHECA来讲，所有涉及系统运营的信息，都在保密范围之内。

5、除非法律明文规定，SHECA没有义务，也不会公布或透露订户证书中已经包括的信息以外的任何信息；同时，SHECA在与其授权的证书服务机构或其他形式的关联实体签署协议时，都将此作为必须满足的要求。

9.3.2 不属于保密的信息

1、与证书有关的申请流程、申请需要的手续、申请操作指南等信息是可以公开的。而且SHECA在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

2、非保密信息还包括证书中包括的相关订户信息。证书中的订户信息是可以公开的。

3、证书、证书内包括的公钥，供用户公开、自由查询和验证。

4、证书被撤销的信息，属于公开信息，SHECA在目录服务器中公布这些信息。

5、上述非保密信息，并不能够被任意不被授权的第三方使用，SHECA和信息的所有人保留所有这些信息的相关权利。

9.3.3 保护保密信息的责任

SHECA、任何订户、关联实体以及与认证业务相关的参与方等，都有义务按照本文档的规定，承担相应的保护保密信息的责任。

当SHECA在任何法律法规要求或者法院以及其它公权力部门通过合法程序的要求下，必须披露本文档中规定的保密信息时，SHECA可以按照法律、法规、或法规条令以及法院判决的要求，向执法部门公布相关的保密信息。SHECA无须承担任何责任。这种披露不能被视为违反了保密要求和义务。

当保密信息的所有者出于某种原因，要求SHECA公开或披露他所拥有的保密信息时，SHECA应满足其要求；同时，SHECA将要求该保密信息的所有者对这种申请进行书面授权，以表示其自身的公开或者披露的意愿。

如果这种披露保密信息的行为涉及任何其他方的赔偿义务，SHECA不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应承担与此相关的或由于公开保密信息引起的所有赔偿责任。

9.4 个人隐私保密

9.4.1 隐私保密原则

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

任何人选择使用SHECA的任何服务，那么就表示已经同意接受SHECA有关隐私保护的声明。

9.4.2 作为隐私处理的信息

SHECA在管理和使用订户提供的相关信息时，除了证书中已经包括的信息外，该订户的基本信息和身份认证资料，都将被作为隐私处理，非经订户同意或者法律法规及公权力部门的合法要求，不会任意对外公开。

9.4.3 不被视为隐私的信息

证书订户持有的证书内包括的信息，以及该证书的状态信息等，是可以公开的，将不被视为隐私信息。

9.4.4 保护隐私的责任

SHECA、任何订户、关联实体以及与认证业务相关的参与方等，都有义务按照本文档的规定，承担相应的保护隐私信息的责任。

当SHECA在任何法律法规或者法院以及公权力部门通过合法程序的要求下，或者信息所有者书面授权的情况下，SHECA可以向特定对象公布相关的隐私信息。SHECA无须为此承担任何责任，而且这种披露不能被视为违反了隐私保护义务。如果这种隐私披露导致了任何损失，SHECA对此不应承担任何责任。

9.4.5 使用隐私信息的告知与同意

SHECA在其认证业务范围内使用所获得的任何订户信息，只用于订户身份识别、管理、和服务订户的目的。在使用这些信息时，无论是否涉及到隐私，SHECA都没有告知订户的义务，也无需得到订户的同意。

SHECA在任何法律法规或者法院以及公权力部门通过合法程序的要求下，或者信息所有者书面授权的情况下向特定对象披露隐私信息时，也没有告知订户的义务，并且不需得到订户的同意。

认证机构、注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，事前必须告知订户并获得订户同意和授权，而且这种同意和授权是要用可归档的方式（如传真、信函、电子邮件等）。

9.4.6 依法律或行政程序的信息披露

除非符合下列条件之一，否则SHECA不会将订户的保密信息和隐私信息提供给任何对象：

- 政府法律法规的规定并且经相关部门通过合法程序提出申请
- 法院以及公权力部门处理因使用证书产生的纠纷时合法的提出申请
- 具有合法司法管辖权的仲裁机构的正式申请
- 证书订户以书面方式进行授权

9.4.7 其他信息披露情形

证书订户以书面方式进行授权，要求SHECA向特定对象提供隐私信息时，SHECA可以将信息提供给该订户指定的接受对象；非经订户本人的书面授权，SHECA将拒绝任何第三者的披露请求。

除了政府法规和相关部门的合法请求，以及信息所有人的书面授权，或者SHECA的合法用途以外，SHECA目前不存在任何其他的隐私信息披露情形。

9.5 知识产权

1、SHECA自身拥有知识产权的声明

SHECA享有并保留对证书以及SHECA提供的全部软件、系统的一切知识产权，包括所有权、名称权和利益分享权等。SHECA自行决定SHECA关联实体采用的证书服务软件系统，以便保证系统的兼容和互通。

按本文档的规定，所有SHECA发行的证书和SHECA提供的软件、系统、文档中，使用、体现和涉及到的一切版权、商标和其他知识产权均属于SHECA，这些知识产权包括所有相关的文件、CPS、规范文档和使用手册等。SHECA 认证体系内关联实体在征得SHECA的同意后，可以使用相关的文件和手册，并有责任和义务提出修改意见。

订户自己产生的密钥的知识产权归其所有，但是公钥经过SHECA签发成证书后，SHECA即拥有该证书的知识产权，只提供给证书订户和依赖方使用的权力。

在没有SHECA书面同意的情况下，使用者不能在任何证书到期、撤销的期间或之后，使用或接受任何SHECA使用的名称、商标、交易形式或可能与之相混淆的名称、商标、交易形式或商务称号。

2、SHECA使用其他方知识产权的声明

SHECA在认证业务系统中使用的软硬件设备、辅助设施和相关操作手册，其知识产权为相关供应商所有，SHECA保

证都是合法的拥有相应权利，绝对没有故意侵害第三方的权利。

SHECA尊重在证书中DN项内存放的订户的注册商标，但是并不保证该注册商标的所有权归属。证书订户的注册商标如果在证书注册时已经被前面的申请者占用，由此产生的注册商标和知识产权的纠纷处理并不在SHECA的责任范围内。

9.6 陈述与担保

除非SHECA在协议中作出特别约定，如果本文档的规定与其他SHECA制订的相关规定、指导方针相互抵触，用户必须接受本文档的约束。在SHECA与包括订户在内的其他方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本文档的规定执行；对协议中不同于本文档的约定，按双方协议中约定的内容执行。

9.6.1 电子认证服务机构的陈述与担保

1、SHECA的一般陈述

- 建立电子认证业务规则（CPS）和其他认证服务所必需的规范、制度体系。
- 在本文档 相关条款规定的范围内，提供基础设施和认证服务，遵守本文档 的各项规定。
- SHECA 保证其私钥得到安全的存放和保护，SHECA 建立和执行的安全机制符合国家相关政策的规定。
- 所有和认证业务相关的活动都符合法律法规和主管部门的规定。
- SHECA 和证书订户的关系以及 SHECA 和依赖方的关系并不是代理人和委托者的关系。证书订户和依赖方都没有权利以合同形式或其他方法让 SHECA 承担信托责任。SHECA 也不能用明示、暗示或其它方式，作出与上述规定相反的陈述。

2、SHECA对订户的陈述

除非本文档 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文档 的所有实质性要求。
- 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文档的规定，即被视为发证机构作出了符合上述描述的合理的努力。

3、发证机构对依赖方的陈述

发证机构就其所发证书向所有按照本文档 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文档 的规定签发证书。

4、SHECA有关公开发布的陈述

通过公开发布证书，发证机构向SHECA信息库和所有合理依赖证书中信息的依赖方证明：发证机构已向订户签发了证书，并且订户已经按照本文档中的规定接受了该证书。

9.6.2 注册机构的陈述与担保

外部认证机构（子CA）、注册机构RA按照程序取得了SHECA的授权后，将保证：

- 遵循本文档和 SHECA 的授权协议以及其它 SHECA 公布的规范和流程，接受并处理申请者的证书服务请求，并依据授权设置、管理各类下级证书服务机构，包括 RAT 等。
- 子 CA、RA 必须遵循 SHECA 制订的服务受理规范、系统运作和管理要求，根据本文档、SHECA 公布的规范，子 CA、RA 有权决定是否给申请者提供相应的证书服务。
- 按照 SHECA 的要求和规范，确定下属证书服务受理机构的设置方式、管理方式和审核方式，这些方式的确定必须以书面的文件形式公布，涵盖并且不得与 SHECA 公布的相关条款产生冲突、矛盾或者

不一致。

- 依据本文档的规定，确保其运营系统处在安全的物理环境中，并具备相应的安全管理和隔离措施。子 CA 必须保证 CA 系统、密钥管理中心及机房符合本文档相关章节要求，RA 必须能够提供证书服务全部的数据资料及备份，并按照 SHECA 的要求，保证其与下属证书服务机构间的信息传输安全。RA 承诺严格执行为所有证书用户提供隐私保密的义务，并愿意承担因此而带来的法律责任。
- 接受 SHECA 根据本文档和授权协议对子 CA、RA 进行管理，包括进行服务资质审核和规范执行检查。
- 承认 SHECA 对所有证书服务申请者的服务请求拥有最终处理权。
- 不得拒绝任何来自 SHECA 的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。
- 为订户提供必要的技术咨询，使订户顺利地申请和使用证书。

9.6.3 其他关联服务机构的陈述与担保

受理点RAT的陈述

- 提供认证服务和其自身的管理，必须遵守本文档、相关授权运作协议的规定。
- 作为被授权的证书服务机构，接受授权机构对其进行的资格审核和管理评估。
- 对所有证书服务申请者的隐私信息负有保密责任，无论这种申请是否被批准。
- 遵守本文档中的所有条款，履行身份鉴别和服务受理的责任。
- 不得拒绝任何来自 SHECA 的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。
- 为订户提供必要的技术咨询，使订户顺利地申请和使用证书。

9.6.4 订户的陈述与担保

一旦接受发证机构签发的证书，从接受之时起直至证书的整个使用有效期内，如果订户不另行通知，那么订户被视为向SHECA及所有合理信赖证书中所含信息的人作出如下保证：

- 在证书申请表上填列的所有声明和信息必须是完整、精确、真实和正确的，可供 SHECA 及其授权的证书服务机构检查和核实；并且，愿意承担任何提供虚假、伪造等信息的法律责任。
- 如果存在代理人，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知 SHECA 或其授权的证书服务机构。
- 用与证书中所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效证书并已被订户接受（证书没有过期、撤销）。
- 未经授权的人员从未访问过订户私钥。
- 订户向发证机构陈述的所有包含在证书中的有关信息是真实的。如果订户发现了证书中信息存在某些错误 ，但订户还没有及时通知给发证机构，那么，发证机构视为：订户承诺上述信息都是真实的。
- 订户将按本文档 的规定，只将证书用于经过授权的或其它合法的使用目的。
- 除非经订户和发证机构间的书面协议明确规定，订户保证不从事发证机构（或类似机构）所从事的业务，例如：把与证书中所含的公钥所对应的私钥用于签发任何证书（或认证其他任何形式的公钥）或证书撤销列表。
- 一经接受证书，既表示订户知悉和接受本文档中的所有条款和条件，并知悉和接受相应的订户协议。
- 一经接受证书，订户就应承当如下责任：始终保持对其私钥的控制，使用可信的系统，和采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用。
- 一经接受证书，即表示订户同意使 SHECA 免于由下列原因直接或间接造成的任何责任和损失：订户（或其授权的代理人）虚假地或错误地陈述了事实；订户未能披露重要事实，而订户的这种有意或无意的错误陈述或失职造成了对 SHECA 和任何信任其证书的依赖方的欺骗；订户没有采用必要的合理措施防止其私钥被损害、丢失、泄露、被篡改或被未经授权使用。如果因此给 SHECA 造成任何责任、损失、任何诉讼及一切相关费用，订户将予以经济赔偿。

- 不得拒绝任何来自 SHECA 的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

9.6.5 依赖方的陈述与担保

依赖方在信赖任何SHECA签发的证书时，就意味着保证：

- 熟悉本文档的条款，了解证书的使用目的。
- 依赖方在信赖 SHECA 签发的证书前，已经对证书进行过合理的检查和审核，包括：检查 SHECA 公布的最新的 CRL，确认该证书没有被撤销；检查该证书信任路径中所有出现过的证书的可靠性；检查该证书的有效期；以及检查其它能够影响证书有效性的信息。
- 一旦由于疏忽或者其他原因违背了合理检查的条款，依赖方愿意就因此而给 SHECA 带来的损失进行补偿，并且承担因此造成的自身或他人的损失。
- 对证书的信赖行为就表明依赖方已经接受本文档的所有规定，尤其是其中有关免责、拒绝和限制义务的条款。
- 不得拒绝任何来自 SHECA 的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

9.6.6 其他参与者的陈述与担保

垫付商的陈述：

- 垫付商必须承担其所有垫付的证书费用，并按 SHECA 规定的方式付清。
- 垫付商的垫付行为，就表明其愿意并且能够承担本文档规定的，对证书服务申请者的身份真实性提供担保的责任。
- 不得拒绝任何来自 SHECA 的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

9.7 担保免责

SHECA在下列情况下免于承担责任：

1、不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担任何赔偿责任。这些事件包括但不限于劳动纠纷、交易一方故意或无意的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、水灾或其他大灾难等。

2、如果由于非SHECA的原因而造成的设备故障、线路中断，导致签发数字证书错误、延误、中断或者无法签发，SHECA不负任何赔偿责任。

3、本文档的内容，没有任何信息可以暗示或解释成，SHECA必须承担其它的义务或SHECA必须对其行为作出其它的承诺。包括不承担其它任何形式的任何保证和义务，任何对特殊目的适用性的保证。

4、如果申请者故意或无意的提供不完整、不可靠或已过期的，包括但不限于伪造、篡改、虚假的信息，而其又根据正常的流程提供了必须的审核文件，由此得到了SHECA签发的数字证书。由此引起的法律问题、经济纠纷应由申请人全部承担，SHECA不承担与该证书内容相关的法律和经济责任，但可以根据受害者的请求提供协查和举证帮助。

5、SHECA不承担任何其他未经授权的人或组织以SHECA名义编撰、发表或散布不可信赖的信息所引起的法律责任。

6、对于由于证书、签名或根据本文档而提供或设计的任何其他交易或服务的使用、签发、授权、执行或拒绝执行而导致的或与之有关的任何间接性的、特别性的、附带性的、或结果性的损失，或任何利益损失、数据丢失，或其他间接性的、结果性的或惩罚性的损失，无论是否可以合理预见， SHECA将不会对此负责，即使SHECA曾经被警告过这种损害的可能性。

7、SHECA对签发的各类证书的适用范围有明确的规定，若证书订户将其证书用于其他不被允许的用途，SHECA不承担任何责任，无论这种使用是否造成损失。

8、SHECA在法律许可的范围内，根据法律、政策等以及受害者的要求，如实提供电子政务、电子商务或其它网络作业中不可抵赖的电子签名依据，但并不对此承担法律或政策规定之外的责任。

9.8 有限责任

根据《中华人民共和国公司法》、《中华人民共和国电子签名法》和其他法律法规的规定，作为依法设立的有限责任公司，SHECA在承担任何责任和义务时，只承担法律范围内的有限责任。

在本文档 和SHECA与任何一方签订的协议中，SHECA不做任何其他保证和履行任何进一步的义务。

9.9 赔偿

9.9.1 赔偿范围

在认证活动中产生的赔偿，都以本文档的规定为处理依据，法律法规另有要求的除外。

1、SHECA的赔偿责任

- 在签发证书时，如果未按照本文档的规定进行处理，或者违反法律法规的要求而造成证书订户损失的，SHECA 应承担赔偿责任。
- 因为操作人员恶意、故意或者疏忽，未按照本文档的规定办理证书的签发、撤销等请求，而造成证书订户损失的，SHECA 应赔偿订户的损失。
- 因 SHECA 的根密钥出现问题，造成订户证书出现问题的，SHECA 应赔偿相关的损失。
- 证书订户或者其它有权提出撤销证书的人提出撤销请求后，到 SHECA 将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果 SHECA 按照本文档的规范进行了有关操作，SHECA 不承担任何损害赔偿责任。
- 证书订户赔偿的追溯有效期限，按照有关法律法规的要求进行操作。

2、注册机构（包括受理点）的赔偿责任

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

3、订户的赔偿责任

- 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致造成SHECA及其授权的证书服务机构或者第三方遭受损害的，订户应赔偿一切损害责任
- 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知SHECA及其授权的证书服务机构，以及不当交付他人使用造成SHECA及其授权的证书服务机构、第三方遭受损害的，订户应承担一切损害赔偿责任。
- 订户使用证书或者依赖方信任证书的行为，有违反本文档及相关操作规范，或者将证书用于非本文档规定的业务范围的，订户或者依赖方应自行承担一切损害赔偿责任。
- 用户使用或信赖证书时，未能依照本文档等规范进行合理审核，导致SHECA及其授权的证书服务机构或第三方遭受损害的，应由该用户承担一切损害赔偿责任。
- 证书订户或者其它有权提出撤销证书的实体提出撤销请求后，到SHECA将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果SHECA按照本文档的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任。
- SHECA与之签署的协议另有赔偿规定的，参照其规定。

9.9.2 赔偿限额

SHECA及其授权的发证机构，对所有当事人（包括但不限于订户、申请者、接受者或信赖方）的合计赔偿责任，不能超过合同约定的证书单价。

对于有关一张特定证书的所有签名和交易处理的总计，SHECA及其授权的证书服务机构对于任何人（或者其它实体）有关该特定证书的合计赔偿责任应该限制在合同约定证书价格的范围内。

本条款限制适用于一定形式的损害，包括但不局限于任何人或实体（包括但不限于订户、证书申请者、接收方或信赖方）由于信任或使用SHECA签发、管理、使用或撤销的证书或已过期证书而导致的直接的、补偿性的、间接的、特别的、结果的、惩戒性的或意外的损害。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的赔偿均有限额而不考虑签名、交易处理或其它有关的索赔数量。当超过赔偿限额时，除非得到依法判决或仲裁，可用的赔偿限额将首先分配给最早得到索赔解决的一方。SHECA没有责任为每张证书支付高出赔偿限额总和的赔偿，而不管高出赔偿限额总和在索赔提出者之间是如何分配的。

9.10 有效期限与终止

9.10.1 有效期限

本文档自发布之日起正式生效，文档中将详细注明版本号及发布日期，当新版本正式发布生效时，旧版本将自动失效。

由于必要的原因，SHECA在获得国家主管部门的批准后，可以宣布提前终止CP/CPS的有效期。

9.10.2 终止

本文档将持续有效，直到有新的版本取代。

如果订户终止使用其证书，或者依赖方终止对证书的信任，订户证书已经被撤销而没有重新申请证书，那么除了本文档中有关审计、归档、保密信息、隐私保护、知识产权、赔偿和有限责任的条款外，对于该订户或者依赖方来说，本文档将不再对其有约束力。SHECA与其另有协议规定的，按照协议中的规定执行。

9.10.3 效力的终止与保留

在本文档中涉及审计、保密信息、隐私保护、归档、知识产权的条款，以及涉及SHECA的赔偿及有限责任的条款，在本文档终止以后仍然继续有效存在。

9.11 对参与者的个别通告与沟通

除非法律法规或者协议有特别的规定，SHECA将以合理的方式与相关各方进行沟通，不会采取个别的方式进行。

无论何时任何人打算或要求发布任何本文档中提及的服务、规范、操作等的通知、要求或请求，这些信息将用书面形式进行传达。

书面通信必须由提供书面单据的快递服务送达，或经由挂号邮件确认，须附回邮及回函。邮递地址如下：

中华人民共和国上海市四川北路1717号嘉杰国际广场18楼（200080 ））

上海市数字证书认证中心有限公司

如果通过电子邮件方式发送通知给SHECA，则这种通知只有在SHECA收到电子邮件通知后24小时内，收到书面确认材料，方为有效。

通过SHECA寄给其他人，地址如下:

SHECA邮递记录中的最新地址。

9.12 修订

SHECA有权修订本文档。SHECA有权把修订结果以本文档修订版的形式通过网站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，战略发展中心每年至少审查一次本文档，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。

本文档的修订，由战略发展中心提出修订报告后，必须经过SHECA策略最高管理部门——SHECA安全认证委员会审核并批准后才能开始修订。修订后的CP/CPS正式对外发布后，应送交信息产业主管部门备案。

9.12.2 通知机制和期限

SHECA有权在合适的时间修订和改变本文档中任何术语、条件和条款，而且无须预先通知任何一方。

SHECA在网站http://www.sheca.com和SHECA信息库中公布修订结果。如果关于本文档 的修改被放置在SHECA信息库中的规范更新和通知栏(查看http://www.sheca.com ），它等同于修改本文档。这些修改将取代本文档原有版本中的任何冲突和指定条款。

所有以书面形式提供给订户的CP/CPS修订，按以下规则发送：

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

9.12.3 修订同意

如果在修订发布7天内，证书申请者和订户没有决定请求撤销其证书，就被认为同意该修订，所有的修订和改变立刻生效。

9.12.4 必须修改业务规则的情形

如果出现下列情况，那么必须对本文档进行修改：

- 密码技术出现重大发展，足以影响现有 CP/CPS 的有效性
- 证书策略发生重大变化
- 有关认证业务的相关标准进行更新
- 认证系统和有关管理规范发生重大升级或改变
- 法律法规和主管部门要求
- 现有 CP/CPS 出现重要缺陷

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

尽管如此，如果SHECA发表了一项修订，而如果该修订不能及时生效，将导致对全部或部分SHECA认证服务体系的损害，那么该修订在它发布之日起立即生效。

9.13 争议处理

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

无论专家组是否完成建议报告并将建议传达，以及形成怎样的裁决决定，并不妨碍SHECA、当事人及其他关联利益方采取与法律和本文档一致的方式，寻找其它的解决措施。

9.14 管辖法律

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

无论合同或其他法律条款的选择及无论是否在中国人民共和国建立商业关系，本文档的执行、解释、翻译和有效性均适用中华人民共和国的法律。法律的选择是确保对所有订户有统一的程序和解释，而不管他们在何地居住以及在

何处使用证书。

9.15 与适用法律的符合性

所有电子认证活动的参与方，都必须遵守《中国人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》以及其它中华人民共和国法律法规的规定。

9.16 一般条款

9.16.1 完整协议

本文档直接影响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。

在本文档与其他规则、规范或协议发生冲突时，所有认证活动的参与方都将受本文档规定的约束，但以下所示协议除外：

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

9.16.2 转让

CA、订户及信赖方之间的责任、义务不能通过任何形式转让给其他方。

9.16.3 分割性

本文档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，那么本文档其余的部分仍将有效。相关当事人了解并同意，本文档所规定的责任限制、保证或其它免责条款或限制、或损害赔偿的排除等，均是可独立于其它条款的个别条款，并可加以执行。

9.16.4 强制执行

无规定。

9.16.5 不可抗力

在法律法规许可的范围内，依据相应CP/CPS、订户协议等应该包括保护不可抗力条款，以保护各方利益。SHECA将不对以下超越其控制能力的不可抗力事件，所造成本文档规定的担保责任的违反、延误或无法履行负责：

构成不可抗力的事件包括战争、恐怖袭击、罢工、瘟疫、自然灾害、火灾、地震、供应商或卖方执行失败、互联网或其他基础设施的瘫痪和其它天灾等。

9.17 安全资料的财产所有

除非另外约定，以下与安全相关的信息资料和数据被认为是以下所指示的当事人的财产：

- 证书：证书是 SHECA 的财产。除非是那些没有 SHECA 明确的书面许可就不能公开在任何信息库或目录中的证书外，证书可完整非专属的、免费的复制和分发。关于版权声明的问题，可以向 SHECA 咨询。
- CP/CPS：本文档是 SHECA 的私有财产。
- 甄别名：甄别名归命名实体所有。
- 私钥：私钥归订户私人所有(或他们代表的组织、机构或者任何其他实体)，而不管其存储和保护所使用的介质。
- 公钥：公钥归订户私人所有(或他们代表的组织、机构或者任何其他实体)，而不管其存储和保护所使用的介质。

- SHECA 的公钥: SHECA 所拥有的公钥是 SHECA 的财产，SHECA 允许使用这些公钥。
- SHECA 的私钥: SHECA 的私钥是 SHECA 的私有财产，无论是部分还是整体。