电子政务电子认证服务业务规则

Electronic Certification Services Rules for E-Government

V2.1

生效日期：2026 年 1 月 12 日

上海市数字证书认证中心有限公司

Shanghai Electronic Certification Authority Co.,Ltd

修订历史

版本	状态	发布日期	发布者
V1.0	历史版本	2012 年 9 月 6 日	SHECA 安全认证委员会
V1.1	现行有效	2023 年 11 月 23 日	SHECA 安全认证委员会
V2.0	现行有效	2024 年 11 月 1 日	SHECA 安全认证委员会
V2.0	现行有效	2026 年 1 月 12 日	SHECA 安全认证委员会

变更摘要

版本	变更描述
V1.0	--
V1.1	更新声明; 披露目录服务地址; 措辞调整
V2.0	根据国家密码管理局《电子政务电子认证服务管理办法》和《电子政务电子认证服务质量评估要求》，对本电子认证服务业务规则进行了整体修改，包括严格遵循规范的格式和内容的要求。
V2.1	更新机房物理环境的分区划分; 调整措辞

声明

电子政务电子认证服务业务规则（以下简称 E-Gov CPS，本 CPS），是上海市数字证书认证中心有限公司开展电子政务电子认证服务时提供的服务内容、遵循的操作流程、系统的管理规范、相应技术规范以及相关法律责任与关系。

本 CPS 支持下列标准:

● 《电子政务电子认证服务管理办法》	国家密码管理局	2024 年
● 《电子政务电子认证服务业务规则规范》	国家密码管理局	2019 年
● 《电子认证服务密码管理办法》	国家密码管理局	2017 年
● 《证书认证系统密码及其相关安全技术规范》	国家密码管理局	2005 年
● 《电子政务数字证书格式规范》	国家密码管理局	2010 年
● 《电子政务数字证书应用接口规范》	国家密码管理局	2010 年
● 《中华人民共和国电子签名法》	中华人民共和国主席令第十八号	2004 年
● 《中华人民共和国密码法》	中华人民共和国主席令第三十五号	2020 年

本 CPS 根据服务范围和用户需要，在适当范围内进行公布。

本 CPS 符合国家密码管理局相关规定和规范的要求，并向国家密码管理局进行备案。

版权说明

对任何复制本文件的其他请求，请和上海市数字证书认证中心有限公司联系。

地址：中华人民共和国上海市四川北路 1717 号嘉杰国际广场 18 楼（200080），电话：8621-36393100，传真：8621-36393200 。电子邮件：CPS@sheca.com。

本 CPS 的最新版本请参见本公司网站 https://www.sheca.com/repository,对具体的个人、企业、政府和其他社会组织等不再另行通知。

SHECA 安全认证委员会负责本 CPS 的解释。

关于E-GovCPS中主要权利及义务的概要

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

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

2、证书申请者须知:

（1）申请者在申请证书之前，已被建议接受适当的数字认证相关方面的培训。

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

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

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

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

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

7、意见与建议

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

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

目　　录

1 概括性描述

1.1 概述

电子政务电子认证服务业务规则（以下简称 E-Gov CPS，本 CPS），是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）按照《电子签名法》、《电子政务电子认证服务管理办法》的要求，根据《电子政务电子认证业务规则规范》编写制定。E-Gov CPS 主要用来规范上海CA采用密码技术通过数字证书提供电子政务电子认证服务的主要内容及要求，阐述和规定了面向电子政务领域提供电子认证服务时所必须遵循的关键环节、操作规范、服务要求、技术要求、运营管理和以及相应的法律责任与关系等。通过实施和执行本 CPS，可以保障电子政务电子认证的权威性、可靠性，有效的防范安全风险。

上海 CA 是依法设立的第三方电子认证服务机构，获得电子认证服务许可证、电子政务电子认证服务许可等资质，严格按照《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》、《电子政务电子认证业务规则规范》以及本 CPS 的规定向电子政务用户提供电子认证服务。上海 CA 提供的电子政务电子认证服务，包括上海市公众网（上海市政务外网）上面向政务部门及相关工作人员的电子政务电子认证服务，和互联网上面向企事业单位、社会团体、社会公众的电子政务电子认证服务。针对互联网电子认证服务，上海 CA 已经制定和发布了《电子认证业务规则》，其中面向各级政务部门开展社会管理、公众服务等政务活动提供的电子认证服务，应同时遵循本 CPS 的规定，如有和本 CPS 规定不一致的，应以本 CPS 为准。

1.2 文档名称与标识

本文档的名称为《电子政务电子认证服务业务规则)》，简称 E-Gov CPS。本 CPS 的版本信息应在电子认证业务规则（CPS）后注明版本号（如 “1.0”或 “CPS1.0”）。

本 CPS 的注册对象标识符（OID）为 1.2.156.112570.150；其中 1.2.156.112570 为上海 CA 向国家 OID 管理机构正式注册的 OID。

1.3 电子政务电子认证活动参与者

1.3.1 电子认证服务机构

上海 CA 是依照《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》等规定设立的电子认证服务机构（简称 CA），建设和运营协卡认证体系。作为被信任的第三方，为电子政务领域的各类参与方（以下称主体或实体，组织、个人、设备及其它任何有明确身份标识的主体都可以成为本 CPS 声称的主体或实体）发放数字证书，并提供数字证书更新、撤销、恢复等一系列管理和服务。

上海 CA 建立了完善的 CA 运行机制和严密的安全控制机制，签发的证书与每一个证书申领实体的公钥绑定。上海 CA 承诺，已签发的、在有效期内的证书，将采用证书目录服务器和证书吊销列表（Certificate Revocation Lists）服务器，公布该证书可以公开的信息和状态。

1.3.2 证书注册机构

证书注册机构（简称 RA），作为电子认证服务机构（CA）设立或授权委托设立，接收公钥证书的申请、注销和查验申请材料的机构，负责对证书申请者进行身份标识和鉴别，初始化或拒绝证书申请和吊销请求，代表 CA 批准更新证书或更新密钥的申请。本 CPS 所述注册机构包括证书注册中心（RA）及受理点（RAT）。

证书注册机构的业务范围包括受理用户的证书申请、审核用户身份、批准证书申请、制作证书、发放证书，接受和处理证书更新、证书撤销、密钥恢复、证书介质解锁以及其它直接面向用户提供的服务。证书注册机构根据上海 CA 的授权并按照上海 CA 制定和发布的 CPS 及相应管理规程从事上述业务，有责任妥善保存客户的数据，不允许将客户的数据透露给与证书申请无关的任何单位或个人。

1.3.3 订户

订户，即证书用户，指证书的持有人，是从 SHECA 接受证书的实体。包括已经申请并拥有 SHECA 签发的数字证书的个人、机构等各类主体或实体。订户符合以下情形:

- 是证书中指明或识别的证书持有主体
- 已接受其证书
- 遵守本 CPS 及相关协议规定
- 拥有与已接受的证书内公钥所对应的私钥

SHECA提供不同类型的证书，订户应决定何种证书适合于自己的需要。订户同意如遇危及私钥安全的状况时及时通知发证机构。

1.3.4 依赖方

依赖方，是指依赖于证书真实性的实体。依赖方可以是也可以不是一个证书持有者，包括任何使用上海CA发放的证书进行网上作业的证书持有者和按照E-Gov CPS合理信任证书真实性的任何实体。

依赖方应合理的信任证书以及相关的数字签名。如果信任数字签名时需要额外保证，依赖方必须在得到这些保证后才能合理的信任该数字签名。

1.3.5 其他参与者

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

1.4 证书应用

1.4.1 数字证书类型

上海 CA 面向电子政务活动中的政务部门及其工作人员和企事业单位、社会团体、社会公众等电子政务用户提供的证书申请、证书签发、证书更新、证书撤销以及密钥生成、备份和恢复等服务。上海 CA 提供以下类型的数字证书:

1、机构证书

用以代表政务机关和参与电子政务业务的企事业单位的身份，如：某部委、某局或参加政府招投标业务的投标企业等，适用于机构身份认证和电子签名，以及数据加密等服务。

2、个人证书

为各级政务部门的工作人员和参与电子政务业务的社会公众颁发的证书，用以代表个体的身份，如：某局局长、某局职员或参加纳税申报的个人等，适用于个人身份认证和电子签名，以及数据加密等服务。

3、设备证书

为电子政务系统中的服务器或设备颁发的数字证书，用以代表服务器或设备身份的真实性，如：服务器身份证书、SSL 服务器证书、IPSec VPN 设备证书等，实现设备身份认

证以及交互数据的加解密，保证传输数据的完整性和安全性等。

4、其他类型证书

为满足电子政务相关应用的特殊需求而提供的其他应用类型的证书，如：代码签名证书等。

以上各类数字证书格式符合《电子政务数字证书格式规范》的要求，在标识实体名称时，应保证实体身份的唯一性，且名称类型应支持 X.500、RFC-822、X.400 等标准协议格式。

1.4.2 正式证书和测试证书

上海 CA 提供上述证书类型相对应的正式证书和测试证书。

正式证书的申请者必须通过规定的物理身份认证和 SHECA 需要的鉴别程序。

测试证书申请者不需要经过身份鉴别，有效期一般不超过 3 个月。测试证书只能用于测试证书对于应用系统的适应性，以及实现证书应用目的的技术可行性，不能用于任何正式的用途。

无论是正式证书还是申请测试证书，凡是涉及证书签发、申请、受理、操作、管理、使用的单位和个人，应熟悉 SHECA 证书政策中的术语、条件、需求、建议以及权益等内容。

1.4.3 适合的证书应用

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

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

SHECA 签发的证书是通用证书，没有针对特定用途和范围进行限制，可以应用在电子政务领域的各类网上活动中，以实现身份认证、电子签名等目的，法律法规和国家政策对此有限制的除外。证书申请者、订户和依赖方等各类主体可以根据实际需要，自主判断和决定采用相应合适的证书类型，以及了解证书的应用类型、应用范围，选择自己的应用方式。任何超出本 CPS 的规定使用证书的行为，都不会受到本 CPS 的保护。

1.4.4 限制的证书应用

每一类型的证书，都只能应用于证书所代表的主体身份适合的用途。例如，个人证书不能作为机构证书和设备证书来使用，机构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机构证书来使用。任何不符合的应用，不受本 CPS 的保护。

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

1.5 策略管理

1.5.1 策略文档管理机构

上海 CA 成立 SHECA 安全认证委员会，作为本机构电子政务电子认证服务业务规则（CPS）的管理机构，对电子政务电子认证服务业务规则（CPS）进行维护与管理，包括:

- 确定《电子政务电子认证服务业务规则》的维护职责，并建立合理、有效的修订和批准流程
- 定期对存在的业务风险进行评估，并及时对《电子政务电子认证服务业务规则》进行修订
- 按照《电子政务电子认证服务管理办法》规定，将修订后的《电子政务电子认证服务业务规则》及时报国家密码管理局进行备案，并在服务范围公开发布。

SHECA 安全认证委员会由上海 CA 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。

1.5.2 联系方式

上海 CA 公布以下对外的相关联系方式，任何有关本 CPS 的问题、建议、疑问等，

均可按照下述方式联系上海 CA:

1、 按照服务范围公布《电子政务电子认证服务业务规则》的发布地址

2、 网站地址: www.sheca.com

3、 电子邮箱地址: cps@sheca.com

4、 联系地址: 中华人民共和国上海市四川北路 1717 号嘉杰国际广场 18 楼

5、 邮政编码: 200080

6、 电话号码: 86-21-36393195

7、 传真号码: 86-21-36393200

1.5.3 批准程序

上海 CA 按照以下方式处理本 CPS 的起草制定、审批、发布、变更、备案等流程:

1、 起草小组成立和 CPS 制定

SHECA 安全认证委员会召集会议，指定相关部门和人员成立起草小组。

CPS 起草小组根据《电子政务电子认证服务业务规则规范》编写 CPS，在编写过程中应及时向 SHECA 安全认证委员会汇报制定进展,并就有关问题召集相关人员进行讨论。

2、 审批

本 CPS 由起草小组编写制定后，提交 SHECA 安全认证委员会审核。SHECA 安全认证委员会一致通过后，即作为正式版本。

3、 发布

根据服务范围和服务对象要求，上海 CA 采取以下方式发布本 CPS:

- 以电子的方式，在相应网站的资料库中发布，网站地址:

  https://www.sheca.com/repository
- 以电子的方式，通过指定电子邮件定向发布，电子邮箱地址:

  cps@sheca.com
- 以书面的方式，由公司战略发展部对外发布

4、 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 CPS 进行修改，由起草小组编写修改建议报告，提交 SHECA 安全认证委员会审核。经过该委员会批准通过后，按照前述方式按照服务范围对外进行发布。

5、 备案

根据《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》的规定，SHECA 安全认证委员会在批准本 CPS 的制定或修订后，上海 CA 将及时向国家密码管理局备案。

1.6 术语和定义

1、 数字证书 digital certificate

由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

2、 数字签名 digital signature

采用密码技术对数据进行运算得到的附加在数据上的签名数据，或是对数据所作的密码变换，用以确认数据来源及其完整性，防止被人（例如接收者）进行篡改或伪造。

3、 鉴别 identification

辨别认定证书申请者提交材料真伪的过程。

4、 实体鉴别 entity authentication

确认一个实体所声称的身份。

5、 验证 authentication

对证书申请材料和申请者之间的关联性进行确定的活动。

6、 密码算法 crypto-algorithm/cryptographic algorithm

描述密码处理过程的一组运算规则或规程。

7、 电子认证服务 electronic certification service

是指为电子签名相关各方提供真实性、可靠性验证的活动。

8、 电子认证服务机构 electronic certification service provider

提供电子认证服务的机构。

9、 证书注册机构 certificate register center

接收公钥证书的申请、注销和查验申请材料的机构。本规范所述注册机构包括证书注册中心及受理点。

10、 证书撤销列表 certificate revocation list

一个已标识的列表，它指定了一套证书发布者认为无效的证书。除了普通 CRL 外，还定义了一些特殊的 CRL 类型用于覆盖特殊领域的 CRL。

11、 证书持有者 certificate holder

拥有电子认证服务机构签发的有效证书的实体。

12、 证书申请者 certificate applicant

申请从电子认证服务机构获得证书的实体。

13、 证书依赖方 certification relying party

依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是也可以不是一个证书持有者。

1.7 符号和缩略语

下列缩略语适用于本规范:

CA 认证机构(Certification Authority)

RA 注册机构(Registration Authority)

CRL 证书撤销列表(Certificate Revocation List)

FAQ 经常问到的问题(Frequently Asked Questions)

USB KEY 采用 USB 接口的证书存储介质(Universal Serial Bus Key)

LDAP 轻量级目录访问协议(Lightweight Directory Access Protocol)

2 信息发布与信息管理

2.1 认证信息的发布

2.1.1 信息库

上海 CA 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。信息库内容包括但不限于以下内容： E-Gov CPS 等文档的现行和历史版本、证书、CRL，以及其它不定期发布的信息。信息库不会改变任何从发证机构发出的证书和任何证书吊销的通知，而是准确描述上述内容。

SHECA 信息库将及时发布包括证书、CPS 修订和撤销的通知和其它资料等内容，这些内容必须保持与 CPS 和有关法律法规一致。SHECA 信息库可以通过网址：https://www.sheca.com/repository/ 访问，或由 SHECA 随时指定的其它通讯方法获得。SHECA 可在 SHECA 信息库外颁布订户证书和相关 CRL 资料。

除 SHECA 授权者外，通常禁止访问资料库（或其它由发证机构维护的数据）中任何被 CPS 和/或 SHECA 信息库宣布为机密信息的资料。

2.1.2 CPS 发布

本 CPS 通过信息库发布，并向国家密码管理局进行备案。

本 CPS 发布根据服务范围和用户需求，确定发布方式和发布范围。

2.1.3 证书和 CRL 发布

证书签发成功后，上海 CA 同时会通过 LDAP 方式发布一份该证书的副本。

上海 CA 定期以 CRL 方式公布有效期内被撤销的证书。用户可以通过访问目录服务器获取这些信息。

此外，上海 CA 还提供接口方式进行在线证书状态查询、证书吊销查询服务等。

根据电子政务应用需求，上海 CA 提供证书和 CRL 数据同步功能，可将证书信息同步到电子政务信息系统中。

2.2 发布的时间和频率

2.2.1 CPS 的发布时间和频率

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

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

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

2.2.2 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。

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

2.2.3 CRL 的发布时间和频率

上海 CA 在撤销证书后，立即签发最新的 CRL，并发布到 LDAP 服务器中。

上海 CA 将公布一项或多项以下内容：发布撤销证书的清单，该清单可通过安全通道索取。

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

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

对于订户证书应至少每 5 天一次或在订户证书被撤销后的 24 小时内公布 CRL。订户证书 CRL 的下次更新时间（nextUpdate）字段与本次更新时间（thisUpdate）字段的差

必须小于等于 7 天。

对于根/中级根证书应至少每 7 个月一次或在根/中级根证书被撤销后的 24 小时内公布 ARL。根/中级根证书 ARL 的下次更新时间（nextUpdate）字段与本次更新时间（thisUpdate）字段的差必须小于等于 10 个月。如根/中级根证书被撤销，上海 CA 将在网站公布相关撤销信息。

2.3 信息访问控制

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 身份标识与鉴别

3.1 命名

3.1.1 名称类型

上海 CA 签发的电子政务数字证书，命名符合《电子政务数字证书格式规范》要求。数字证书包含的主题名称，采用采用 X.501 的甄别名 Distinguished Name(DN)方式，用以标识证书持有者的身份。

上海 CA 针对每一个实体的甄别名是唯一的，同一个实体以相同的甄别名可以签发多张证书。

3.1.2 匿名或伪名

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

但是，在某些具有特殊要求的电子政务应用中， SHECA 可以按照一定的规则为用户指定特殊的名称，并且能够把该类特殊的名称与一个确定的实体（个人、单位或者设备）唯一的联系起来。任何这一类特殊的命名，都必须经过 SHECA 安全认证委员会的批准。

3.1.3 名称形式规则

证书甄别名 DN 的内容格式符合 X.500 的命名规则:

甄别名（DN）	说明
Country(C)	国家名称
State（S）	所在省、自治区、直辖市
Locality（L）	地址
Organization(O)	组织
Organization Unit（OU）	部门名称
Common Name（CN）	主体通用名
Email（E）	电子邮件地址

3.2 初始身份确认

上海 CA 需要对证书申请者的身份进行程序性的鉴别，包括但不限于验证用户提供的

身份证明材料、通过公共数据库调查、邮政地址调查等等。

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

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

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

3.2.1 证明持有私钥的方法

上海 CA 基于两个条件来确认证书持有者对私钥的持有：

1、通过证书请求中所包含的数字签名来证明证书持有者持有与注册公钥对应的私钥。

1)证书持有者的签名密钥对在客户端生成，加密密钥对在 CA 端的密钥管理中心生成、存储，并通过安全方式传递给证书持有者；

2)证书持有者使用私钥对证书请求信息签名，并连同公钥一同提交 CA 系统；

2、CA 使用证书持有者公钥验证证书持有者签名。

证书持有者能够妥善保管自己的私钥，即只有证书持有者可以持有私钥。如以上条件满足，则证书持有者可以被视作其私钥的唯一持有者。

3.2.2 组织机构身份的鉴别

在申请组织机构证书时，申请者应指定证书申请代表，并对其合法授权，证书申请代表在证书的申请表上签字表示接受证书申请的有关条款，并承担相应的责任。上海 CA 及其证书服务机构审核单位证书申请者的代表人是否符合要求。对组织机构的身份鉴别包括如下内容：

1、确认组织机构是确实存在的、合法的实体。确认的方式可以是，政府签发的组织机构成立的有效文件，如营业执照、事业单位法人证书等，或通过权威的第三方数据库确

认。

2、确认该组织机构知晓并授权证书申请，即代表组织机构提交证书申请的人是经过授权的。确认的方式可以是，由该机构提供加盖公章的信函或其电子版扫描件确认，通过第三方数据库等辅助手段验证进行授权事宜的确认。

（a）线下证书申请者需要提供交下列材料:

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

（b）机构快捷证书仅支持在线申请。在受理证书申请之前，SHECA 应以合理的方式向申请人告知与电子认证服务有关的事项。主要验证方式有以下两种:

（1）持有可靠机构身份证书

- CA 机构在线验证申请机构的身份证书的可靠性，验证通过后，申请机构需在线确认证书申请信息并同意订户协议。
- CA 机构根据证书请求签发证书。
- 申请者接受并下载证书。

（2）未持有可靠机构身份证书

- CA 机构要求机构授权的申请人在线提供真实个人信息，并通过人脸识别对代理人进行实名认证。代理人实名认证通过后，在线上提供机构的真实身份信息，如机构法定名称、统一社会信用代码等。
- CA 机构将验证相关信息的可靠性，验证通过后，代理人在线确认机构证书申请信息并同意订户协议。
- CA 机构根据证书请求签发证书。
- 申请者接受并下载证书。

（c）申请应用服务器/设备证书，需要递交以下资料:

- 申请者填写并签字（或盖章）的书面申请表

- 申请者（个人或组织机构）的身份证明材料原件和符合条件的复印件（具体要求同前述组织机构证书的要求）。

- 申请者必须书面填写关于该应用服务器/设备的归属性声明文件，以表明该应用服务器/设备属于申请者所有。

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

证书申请机构及相关申请经办人员有义务保证申请材料的真实有效，并承担与此相关的法律责任。

上海 CA 或证书注册机构必须检查申请者所递交的文件，可以通过查询第三方数据库或咨询相应的政府机构等方式，来对申请材料进行鉴别。如果需要，可以通过从第三方得到的电话号码等其他联络方式，用某种方式与申请机构进行联络以确认某个信息（例如，验证代理人的职位或者验证申请表中的某个人是否是申请人）。如果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。

上海 CA 或注册机构根据对上述材料进行审核和鉴证的结果，作出批准申请或拒绝申请的操作。

如批准申请，将按照相关法律法规的要求妥善保管订户申请材料，订户申请材料可以是纸质或电子数据形式。

3.2.3 个人身份的鉴别

上海 CA 在把证书签发给个人时，对证书申请者进行身份鉴别。对个人的身份鉴证应该包括如下两个内容:

- 确认个人的身份是确实存在的、合法的实体。确认的方式为:采用上海 CA 认可的、提供身份核实服务的数据库中的信息，如公安部门提供的个人身份数据库或其他可靠的信息源;对于承担注册机构职能的机构向与其相关的人员(如其员工、客户、合作伙伴)颁发证书的情形，可通过采用包含在该机构业务记录或有效电子信息来完成鉴别。

- 确认证书持有者知晓并授权证书申请。确认的方式为:面对面进行确认;或通过签字的授权书确认;或通过证书申请表上的联系电话，联系证书持有者进行确认;或通过短信验证码、银行卡信息等其他安全可靠的方式进行确认。

- 如果是委托申请的，需要提交授权书以确认该委托是获得充分授权的，被委托的

申请经办人同样需要提交上述合法有效的证明文件。

证书申请人有义务保证申请材料的真实有效，并承担与此相关的法律责任。

上海 CA 或证书注册机构必须检查申请者所递交的文件，可以通过查询第三方数据库或咨询相应的政府机构等方式，来对申请材料进行鉴别。如果需要，可以通过从第三方得到的电话号码等其他联络方式，用某种方式与申请机构进行联络以确认某个信息（例如，验证代理人的职位或者验证申请表中的某个人是否是申请人）。如果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。

上海 CA 或注册机构根据对上述材料进行审核和鉴证的结果，作出批准申请或拒绝申请的操作。

如批准申请，将按照相关法律法规的要求妥善保管订户申请材料，订户申请材料可以是纸质或电子数据形式。

3.2.4 政府部门个人身份鉴别

上海 CA 在把证书签发给政府部门中的个人时，还应确认以下内容:

- 申请人提交由所属政府部门签章的证明文件;
- 通过可靠的方式确保证书持有者所在的组织、部门与证书中所列的组织、部门一致，证书中通用名就是证书持有者的真实姓名或者被所在组织、部门确认的其它标识;
- 需确认证书持有者属于该组织机构，证书持有者确实被雇佣。

上海 CA 或注册机构根据对上述材料进行审核和鉴证的结果，作出批准申请或拒绝申请的操作。如批准申请，将按照相关法律法规的要求妥善保管订户申请材料，订户申请材料可以是纸质或电子数据形式。

3.2.5 密钥更新请求的识别与鉴别

1、常规密钥更新请求的识别与鉴别

对于一般正常情况下的密钥更新申请，证书持有者应提交能够识别原证书的足够信息，并使用更新前的私钥对包含新公钥的申请信息签名。对申请的鉴别应满足以下条件:

- 申请对应的原证书存在并且由上海 CA 签发。
- 用原证书上的证书持有者公钥对申请的签名进行验证。

- 基于原注册信息进行身份鉴别
- 对申请的身份鉴别，需要根据不同情况采取不同方式:
- 密钥更新请求中，应确保更新请求与申请者身份的关联和申请行为的有效性，应采取现场受理点和远程在线等方式对用户身份进行实体鉴别。
- 当用户证书已过期时，应重新进行与初始身份确认相同的实体鉴别流程;
- 当用户证书未过期时，用户采取在线更新方式的，应由用户在线提交更新申请并进行数字签名，以实现对用户身份的实体鉴别。

2、撤销之后的密钥更新请求的识别与鉴别

证书撤销后不能进行密钥更新。

订户如果需要申请证书的，必须重新进行身份鉴别和注册，并生成新的密钥对，向上海 CA 重新申请签发证书。

3.2.6 撤销请求的身份标识与鉴别

证书撤销请求可以来自证书持有者，也可以来自上海 CA、注册机构或其他法律法规规定的部门。

证书持有者通过认证机构、注册机构申请撤销证书时，认证机构、注册机构应对证书持有者进行身份鉴证。申请撤销证书应包括以下流程:

- 证书持有者通过一定的方式向认证机构、注册机构提交撤销请求;
- 认证机构、注册机构按照本 CPS 规定的方式与证书持有者联系，并对申请人进行身份鉴证，确认要撤销证书的人或组织确实是证书持有者本人或被授权人;
- 证书持有者本人申请撤销证书时的身份标识和鉴别使用原始身份验证相同的流程，如果由于条件的限制无法进行现场审核时，上海 CA 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

如果是因为证书持有者没有履行本 CPS 所规定的义务，由上海 CA、注册机构申请撤销证书持有者的证书时，不需要对证书持有者身份进行标识和鉴别。

如果是司法机关依法提出吊销，上海 CA 将直接以司法机关书面的相关文件作为鉴别依据，不再进行身份鉴别和标识。

4 证书生命周期操作要求

4.1 证书申请

4.1.1 信息告知

上海 CA 在本 CPS 中阐述和说明了受理证书申请的所有流程及要求，并通过网站、书面告知、现场咨询、电话、电子邮件等方式告知证书申请者及证书持有者所必须提交的材料和办理流程。

4.1.2 申请的提交

- 证书申请应由证书申请者或相应的授权人提交;
- 非证书持有者代表组织机构进行批量证书申请的还须获得该组织的授权;
- 上海 CA 提供线下、线上多种方式的证书受理申请

4.1.3 注册过程及责任

在处理每一个证书申请中，必须确定以下条件得到满足:

- 保留对最终实体身份的证明和确认信息。
- 保证证书申请者和持有者信息不被篡改、私密信息不被泄漏。
- 注册过程必须保证所有证书申请者明确同意相关的证书申请者协议。
- 按规定产生一个密钥对，并将公钥传给认证机构、注册机构。

证书申请者提交证书申请时，应按照初始身份鉴别的要求，填写申请表，提交身份证明材料。

上海 CA 或注册机构在接到证书申请时，需要按照以下要求进行操作:

- 对接收到申请材料进行通知;
- 核查材料是否充分;
- 验证证书申请信息的完整性;
- 对申请材料保密;
- 确认用户接受服务协议。

4.2 证书申请处理

4.2.1 执行身份识别与鉴别功能

当上海 CA、注册机构接收到证书申请者的证书申请后，应按照要求对证书申请者的身份进行鉴别。包括:

- 按照初始身份鉴别的要求，对证书申请者的身份进行识别和鉴别;
- 对证书申请者申请行为的合法性进行鉴别;
- 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;
- 依据鉴别结果，作出接受或拒绝证书申请的决定。在 48 小时内，告知证书申请者结果及相应的原因;
- 如接受申请，应妥善保管证书申请者申请时提交的所有材料。

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。

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

4.2.2 证书申请批准和拒绝

上海 CA、注册机构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。上海 CA 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:

- 该申请完全满足前述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
- 批准申请的，应为证书申请者办理证书签发服务。

上海 CA、注册机构在进行鉴别程序时，如果申请者未能成功通过鉴别，将拒绝申请者的证书申请，并通过适当的方式，在 24 小时内通知证书申请者。对于鉴别失败的原因，上海 CA 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,上海 CA 将向申请者提供第三方的联系方式，以便申请者查询。上海 CA 采用申请者向上海 CA 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。

上海 CA 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，上海 CA 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:

- 该申请不符合前述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;
- 如果批准该申请将会对上海 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

上海 CA 处理证书请求的最长响应时间应不超过 48 小时。

4.3 证书签发

4.3.1 证书签发中 RA 和 CA 的行为

在证书的签发过程中，RA 相关操作员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发往 CA 的证书签发请求信息须有 RA 的身份鉴别与信息保密措施，并确保请求发到正确的 CA 的证书签发系统

CA 的证书签发系统在获得 RA 的证书签发请求后，对来自 RA 的信息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发证书。

在签发证书时必须满足:

- 证书签发请求中，RA 和 CA 应相互进行身份认证并确保申请信息传输的机密性。
- CA 应验证 RA 的签发请求，无误后方可签发证书。

4.3.2 CA 和 RA 通知证书申请者证书的签发

无论是拒绝还是批准证书申请者的证书申请，RA 应通过适当的方式通知证书申请者。

如果证书申请获得批准，证书签发系统签发证书后，应通过适当的方式告诉证书申请

者如何获取证书。

一般的获取方式包括:

- 面对面交付的方式;
- 邮政信函结合电子邮件的方式;
- 经过已经确认安全的通道通知;
- 其他安全方式。

上海 CA、注册机构没有上门为用户安装证书的义务。如果申请人需要，可以上门安装，但需要收取相应的服务费用。上海 CA 提供热线支持服务，对外公布热线支持电话和服务信箱。

4.4 证书接受

4.4.1 构成接受证书的行为

上海 CA 提供多种接受证书的方式，只要满足任何一个约定方式的条件，应当视为证书持有者接受证书。包括:

- 通过面对面的提交，证书持有者接受载有证书和私钥的介质;
- 按 CA 或 RA 的提示，通过网络将证书下载到本地存放介质，如智能 USB KEY 或智能 IC 卡;
- 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。
- 完成以上行为表明证书持有者接受证书。

在证书持有者接受到证书后，证书持有者应立即对证书进行检查和测试。

4.4.2 CA 对证书的发布

对于证书申请者明确表示拒绝发布证书信息的，CA 应不发布该证书申请者证书信息。没有明确表示拒绝的，认证机构应将证书信息发布到目录系统。

4.4.3 CA 通知其他实体证书的签发

CA 没有义务将证书签发信息通知除证书持有者、证书申请者和 RA 以外的实体。

4.5 密钥对和证书使用

4.5.1 证书持有者私钥和证书使用

认证机构应明确证书持有者私钥和证书的用途，证书持有者应按约定的方式使用其私钥和证书。未按规定用途使用造成的损失由证书持有者自行承担责任。

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。在证书到期或被吊销之后，证书持有者必须停止使用该证书对应的私钥。

该证书只能根据本 CPS 及相关规定，用于其规定的、批准的用途。签名密钥对用于签名与签名验证，加密密钥对用于加密解密。如果密钥对允许用于身份鉴别，则可以用于身份鉴别。订户只能在正当的应用范围内使用私钥和证书，并且与证书内容相一致（如果证书中的某些字段明确了证书的使用范围和用途，那么该证书将在也只被允许在这一范围内进行使用，例如密钥用途）。所有的使用行为必须符合订户协议的要求。

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

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

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

如果证书中的某些字段明确了证书的使用范围和用途，那么该证书将在也只被允许在这一范围内进行使用。任何超出证书所标明的适用范围内的行为，都将由行为人独立承担责任。上海 CA 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。

电子签名只限于以下几种情况下才能被创建:

- 在证书的使用有效期内被创建

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

4.5.2 依赖方对公钥和证书使用

依赖方应按约定的方式对签名信息进行验证。未按规定用途使用造成损失的由依赖方自行承担责任。

当依赖方接受到签名的信息后，应该:

- 获得对应的证书及信任链;
- 验证证书的有效性;
- 确认该签名对应的证书是依赖方信任的证书;
- 证书的用途适用于相应的签名;
- 使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

在下列条件下，接收到被订户签名过的信息的接收方，可以信任与订户捆绑的签名:

签名是在合法证书的使用有效期内被创建，并且通过确认有效的证书链，该签名可以被验证。

信赖方是合理地信任该数字签名。如果信任签名时需要额外保证，信赖方必须在得到这些保证后才能合理地信任该签名。

当然，是否信赖经过验证的签名的最终决定，将由验证者独立地做出。

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密

依赖方应使用接收方的公钥进行信息加密，加密证书应同加密信息一同发送给接受方。

4.6 证书更新

4.6.1 证书更新的情形

证书的更新包括证书的补发和换发。

- 证书的补发:

补发是指在证书有效期内，证书持有者出现证书载体丢失和证书载体损坏并进行更新证书（密钥）的操作。补发操作成功时，旧证书将被吊销，新证书有效期从补发成功之日起到旧证书失效日止。

- 证书的换发:

每个证书都有其有效期，在认证机构规定的期限内，（如证书到期前 30 天内或已到期后 30 天内），如果证书持有者的注册信息没有改变，证书持有者可以申请证书更新。换发操作成功时，旧证书将被吊销，新证书有效期将从证书换发之日起加一个证书有效周期（已经过期的证书换证，其有效期仅为证书有效期）。

证书更新期限也可根据实际的业务要求，由认证机构自行确定并发布。但被撤销的证书不能进行证书更新。

4.6.2 更新申请的提交

证书持有者、证书持有者的授权代表(如: 机构证书等)或证书对应实体的拥有者(如设备证书等）可以要求更新证书。

证书持有者、证书持有者的授权代表（如机构证书等）或证书对应实体的拥有者（如设备证书等）在证书满足更新条件时，应按要求向注册机构提出更新申请。可采取当面提交更新申请表或在线提交带有证书持有者数字签名的更新申请。

4.6.3 处理证书更新请求

处理证书更新请求应对原证书、申请的签名信息、及身份信息进行验证和鉴别，无误后方可进行。

处理证书更新请求的过程，包括申请验证、鉴别、签发证书。对申请的验证和鉴别须基于以下几个方面:

- 申请对应的原证书存在并且由认证机构签发;
- 用原证书上的证书持有者公钥对申请的签名进行验证;
- 基于原注册信息，按照密钥更新时的要求，进行身份鉴别。

在以上验证和鉴别通过后才可进行证书更新。

证书更新可以通过以下方式进行:

- 面对面的更新方式;

- 在线的自动更新方式。

4.6.4 通知证书持有者新证书的签发

上海 CA、注册机构应明确通知证书持有者新证书签发的方式及时间。

证书更新的通知和证书初次签发处理的方式相同。

4.6.5 构成接受更新证书的行为

接受更新证书的行为和证书初次申请时的接受规则相同。

4.6.6 CA 对更新证书的发布

更新证书的发布条件、方式及途径和证书初次申请时的发布规则相同。

4.6.7 CA 通知其他实体证书的签发

证书更新后是否需要通知其他实体和证书初次申请时的通知方式相同。

4.7 证书撤销

4.7.1 证书撤销的条件

认证机构、注册机构及证书持有者应在发生下列情形之一时，申请撤销数字证书:

- 政务机构的证书持有者工作性质发生变化;
- 政务机构的证书持有者受到国家法律法规制裁;
- 证书持有者提供的信息不真实;
- 证书持有者没有或无法履行有关规定和义务;
- 认证机构、注册机构或最终证书持有者有理由相信或强烈的怀疑一个证书持有者的私钥安全已经受到损害;
- 政务机构有理由相信或强烈怀疑其下属雇员的私钥安全已经受到损害;
- 和证书持有者达成的证书持有者协议已经终止;
- 证书持有者请求撤销其证书;
- 证书仅用于依赖方主导的系统并由依赖方提出撤销申请的;
- 法律、行政法规规定的其他情形。

4.7.2 证书撤销的发起

证书持有者、认证机构、注册机构、证书持有者所属的组织机构或证书使用唯一依赖方有权发起证书撤销申请。

当出现符合证书撤销条件中的情形时，应在认证机构发布的撤销请求期限内通过可靠方式要求撤销证书。

以下实体可以请求撤销一个证书持有者证书:

- 批准证书持有者证书申请的认证机构、注册机构、电子政务机构或依赖方在满足证书撤销条件的前提下，可以要求撤销一个证书持有者证书;
- 对于个人证书，证书持有者可以请求撤销他们自己的个人证书;
- 对于机构证书，只有机构授权的代表有资格请求撤销已经签发给该机构的证书;
- 对于设备证书，只有拥有该设备的机构授权的代表有资格请求撤销已经签发给该设备的证书。

4.7.3 证书撤销的处理

- 认证机构、注册机构在接到证书持有者的撤销请求后，应通过核实身份证明材料、验证预留信息等方式，确认请求确实来自证书持有者。
- 对于验证通过的请求，在CA系统中执行撤销证书操作，并在24小时内将撤销证书发布到证书撤销列表中。
- 认证机构、注册机构在确信出现证书撤销条件中的情况而需要立即撤销证书时，可以立即撤销证书。
- 证书撤销后，应通过电话、短信、网站等方式告知用户或依赖方证书撤销结果

4.7.4 依赖方检查证书撤销的要求

对于安全保障要求比较高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在信赖一个证书前必须查询证书撤销列表确认该证书的状态:

- 应根据证书标明的发布地址获取证书撤销列表;
- 应验证撤销列表的签名，确认其来自于该证书对应的签发机构;
- 应验证证书撤销信息，确认证书是否被注销。

4.7.5 CRL 发布频率

上海 CA 定时发布最新的证书撤销列表，最长时间间隔不得超过 24 小时。

4.7.6 CRL 发布的最大滞后时间

证书从撤销到发布到 CRL 上的滞后时间不得超过 24 小时。

4.7.7 在线状态查询的可用性

上海 CA 提供证书状态的在线查询服务（OCSP），并提供 7*24 小时查询服务。

4.7.8 在线状态查询要求

对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在信赖一个证书前必须通过证书状态在线查询检查该证书的状态:

- 应按照查询协议要求，向证书中标明的 OCSP 服务地址提交状态查询请求;
- 查询过程应确保信息传输的机密性和完整性;
- 应获得证书状态信息。

4.7.9 撤销信息发布的其他形式

除了 CRL、OCSP 外，目前不提供其它的吊销信息发布方式。

4.8 密钥生成、备份和恢复

证书加密密钥对的生成、备份和恢复应由国家密码管理局规划建设的密钥管理基础设施提供密钥管理服务。密钥恢复应按照国家密码管理局的规定开展。

证书持有者的签名密钥对由证书持有者的密码设备（如智能密码钥匙或智能 IC 卡）生成，加密密钥对由国家密码管理局规划建设的密钥管理基础设施提供密钥管理服务。

签名密钥对由证书持有者的密码设备保管。

密钥恢复是指加密密钥的恢复，密钥管理基础设施不负责签名密钥的恢复。密钥恢复分为两类:

- 证书持有者密钥恢复和问责取证密钥恢复。
- 证书持有者密钥恢复：当证书持有者的密钥损坏或丢失后，某些密文数据将无法还原，此时证书持有者可申请密钥恢复。证书持有者向认证机构提交申请，经审核后，通过认证机构向密钥管理基础设施发送请求；密钥恢复模块接受证书持有

者的恢复请求，恢复证书持有者的密钥并下载于证书持有者证书载体中。

- 问责取证密钥恢复：问责取证人员向密钥管理基础设施提交申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

5 数字证书支持服务

5.1 应用集成支持服务

5.1.1 服务策略和流程

为更好的满足应用对证书的需求，上海 CA 提供的服务内容有:

- 制定应用集成服务的相应的管理策略和流程，对业务系统进行充分调研，指导或参与业务系统证书应用部分的开发和实施;
- 制定项目管理制度，规范系统和程序开发行为;
- 制定安全控制流程，明确人员职责;
- 实施证书软件发布版本管理，并进行证书应用环境控制;
- 项目开发程序和文档等资料应妥善归档保存。

5.1.2 证书应用接口程序

上海CA提供证书应用接口程序供应用系统集成和调用。

证书应用接口程序为上层提供简洁、易用的调用接口，其主要包括密码设备接口和通用密码服务接口。接口符合《电子政务数字证书应用接口规范》，提供证书环境设置、证书解析、随机数生成、签名验证、加解密、时间戳以及数据服务接口等功能。

- 密码设备调用接口

密码设备调用接口包括服务器端密码设备的底层应用接口和客户端证书介质的底层应用接口。服务器端密码设备的底层应用接口在符合国际标准 PKCS#11 技术规范的基础上，符合《公钥密码基础设施应用技术体系密码设备应用接口规范》;客户端证书介质的底层应用接口符合《智能 IC 卡及智能密码钥匙密码应用接口规范》。

- 通用密码服务接口

通用密码服务接口是屏蔽了底层不同密码设备类型和底层接口的通用中间件，该接口符合《电子政务数字证书应用接口规范》。

其主要包括服务器端组件接口和客户端控件接口。服务器端组件和客户端控件支持不同认证机构所签发的符合《电子政务数字证书格式规范》的数字证书。

证书应用接口程序应支持Windows、AIX、Solaris、linux等多种系统平台，并提供C、C#、Java等多种接口形态，可通过com组件、java组件、ActiveX控件、Applet插件等多种形态提供服务。

5.1.3 证书应用方案支持

上海CA具备针对电子政务信息系统的电子认证安全需求分析的能力、电子认证法律法规、技术体系的咨询能力以及设计满足业务要求的电子认证及电子签名服务方案设计能力。

数字证书应用方案设计可包括：证书格式设计、证书交付、支持服务、信息服务、集成方案、建设方案、介质选型等。

5.1.4 证书应用接口集成

上海CA具备面向各类应用的证书应用接口集成能力，并达到以下要求：

- 应具备在多种应用环境下进行系统集成的技术能力，包括基于 Java、.NET 等 B/S 应用模式和基于 C、VC 等 C/S 应用模式的系统集成能力。
- 应提供满足不同应用系统平台的证书应用接口组件包，包括 com 组件、java 组件、ActiveX 控件、Applet 插件等。
- 应提供集成辅助服务，包括接口说明、集成手册、测试证书、集成示例、演示 DEMO 等。

5.1.5 集成内容

上海CA为电子政务应用单位提供证书应用接口程序集成工作。集成工作应提供以下服务：

- 证书应用接口的开发包（包括客户端和服务器端）；
- 接口说明文档；
- 集成演示 Demo；
- 集成手册；
- 证书应用接口开发培训和集成技术支持；
- 协助应用系统开发商完成联调测试工作。

5.2 信息服务

5.2.1 服务内容

信息服务是面向证书应用单位提供证书发放和应用情况信息汇总及统计分析的信息管理服务。根据政务部门对证书应用信息的管理及决策需求，上海CA可以并且能够为证书应用单位提供相应的信息服务，为其实现科学管理和领导决策提供可靠依据。

信息服务应包括:

1、 证书信息服务

CA 系统中签发、更新、重签发的数字证书，可实时或定时与电子政务信息系统进行数据同步，实现将证书信息同步到电子政务信息系统中。认证机构提交的数据应包括业务类型、认证机构身份标识、用户基本信息、用户证书信息等。

2、 CRL信息服务

CRL 在 CA 系统中发布后，可实现将 CRL 实时发布到指定的电子政务信息系统中。上海 CA 提交的数据包括业务类型、认证机构身份标识、CRL 文件、同步时间等。

3、 服务支持信息服务

上海 CA 面向电子政务用户、应用系统集成商、应用系统发布与之相关的服务信息，包括 CPS、常见问题解答、证书应用接口软件包等。

4、 决策支持信息服务等

上海 CA 面向电子政务应用单位、政府监管机构提供决策支持信息，包括用户档案信息、投诉处理信息、客户满意度信息、服务效率信息等。

5.2.2 服务管理规则

认证机构在提供信息服务时，应确保做好相关信息的隐私保障机制，实现信息保护对用户的承诺。包括:

- 对 CA 机构内的工作人员按其工作角色设定与之相应的信息访问权限，并对其所有访问操作进行详细记录;
- 对证书应用单位的管理员设定信息访问权限，限定其仅能访问本应用所签发证书信息。
- 应用单位管理员对非授权信息的访问，须依照政策管理规定，须经上级主管部门

批准后方可进行。

- 对问责程序需要进行的信息访问，应严格审核相应的问责人员身份及授权文件，无误后方可进行问责举证。
- 对监管部门应管理需求进行的信息访问，应按照相关的管理规定和调取程序，为其提供信息访问权限

1、 私有信息类型的敏感度

以下信息应属于私有信息:

- 个人隐私信息;
- 商业机密;
- 政府部门的敏感信息和工作秘密。

证书发行过程中涉及的用户申请信息是敏感信息，而发布的证书和CRL信息不是敏感信息。

2、 允许的私有信息采集

认证机构仅允许在进行证书发行和管理时才能收集私有信息。除了有特殊要求外，认证机构不应收集更多私有信息。

3、 允许的私有信息使用

认证机构应只使用CA或者RA收集的私有信息。

因在某项业务中开展证书应用而获得的私有信息，在使用时，必须首先得到该业务应用单位的许可。

4、 允许信息的安全存储

认证机构采取安全手段对用户私有信息进行安全存储，确保用户私有信息不发生泄露、未授权访问等安全事件。

5、 允许的个人信息发布

认证机构和注册机构仅能面向证书应用单位发布与之相关的私有信息，以协助证书应用单位进行证书业务管理；对证书应用单位的管理员设定信息访问权限，限定其仅能访问本应用所签发证书信息。

任何特定的私有信息发布应遵照相关法律和政策实行。

6、 所有者纠正私有信息的机会

认证机构应允许用户在其证书生命周期内对其私有信息进行更正。

7、 对司法及监管机构发布私有信息

对监管部门应管理需求进行的信息访问，认证机构按照相关的管理规定和调取程序，为其提供信息访问权限。在以下情况下，可以执行将私有信息发给获得相应授权的人员：

- 司法程序;
- 经私有信息所有者同意;
- 按照明确的法定权限的要求或许可。

5.2.3 服务方式

信息服务应以页面或接口的形式面向应用系统或证书用户提供服务。以接口形式提供服务的应符合《电子政务数字证书应用接口规范》的要求。

1、 证书信息同步服务

证书信息同步服务通过采用webservice技术实现CA系统与电子政务信息系统的证书应用同步。电子政务信息系统通过部署统一的webservice接口，认证机构的CA系统通过调用统一的webservice同步接口，实现CA系统向电子政务信息系统进行证书信息的自动同步功能。同时，为了保证数据传输的安全性，可通过对webservice通信数据添加数字签名，以防止数据在传输中被篡改或数据损坏。

2、 CRL信息同步服务

CRL信息同步服务通过采用webservice技术实现CA系统与电子政务信息系统的CRL同步。CA系统主动调用该接口，实时将最新的CRL文件同步到电子政务信息系统中。

为了提高CRL文件传输的安全性，应对发送的CRL数据进行数字签名，电子政务信息系统只需要根据认证机构身份标识找到对应的根证书链，验证CRL签名的有效性即可确定CRL的有效性。

CRL发布周期不得超过24小时。

3、 服务支持信息服务

认证机构通过WEB网站面向电子政务用户发布如下信息：

- 电子政务电子认证服务业务规则
- 证书生命周期服务流程及相关费用
- 证书用户操作手册
- 证书常见问题解答（FAQ）

- 获得证书帮助联系方式（客户服务热线电话、办公地址、邮政编码、投诉电话等）
- 其他应该发布的相关信息。

认证机构通过 WEB 网站面向电子政务应用系统集成商发布如下信息:

- 数字证书应用接口软件包
- 数字证书应用接口实施指南
- 证书常见问题解答（FAQ）
- 获得证书帮助联系方式（客户服务热线电话、办公地址、邮政编码、投诉电话等）
- 其他应该发布的相关信息。

认证机构通过 WEB 网站面向电子政务应用系统发布如下信息:

- 时间戳服务数据接口
- http 协议的 CRL 发布服务接口
- LDAP 协议的 CRL 发布接口
- LDAP 协议的证书发布接口
- OCSP 服务接口（可选）

4、 决策支持信息服务

认证机构应面向应用提供方以 Web 或 WebService 方式提供如下信息服务:

- 用户档案信息: 分业务、地域、时段等要素提供用户信息的统计分析服务;
- 投诉处理信息: 提供特定业务、时间、特定用户群、问题类型等的投诉处理汇总信息及分析;
- 客户满意度信息: 提供面向业务的客户满意度调查信息;
- 服务效率信息: 提供面向业务的服务效率分析信息，如处理时间、服务接通率等

5.3 使用支持服务

5.3.1 服务内容

使用支持服务是认证机构面向证书使用用户（即证书申请者、证书持用者）及证书应用单位提供的一系列售后服务及技术支持工作。

服务内容应包括: 数字证书管理、数字证书使用、证书存储介质硬件设备使用、电子认证软件系统使用、电子认证服务支撑平台使用以及各类数字证书应用（如证书登录、证书加密、数字签名）等贯穿证书使用和应用过程中的所有问题。

1、 面向证书持有者的服务支持

- 数字证书管理

包括数字证书的导入、导出，以及客户端证书管理工具的安装、使用、卸载等。

- 数字证书应用

基于数字证书的身份认证、电子签名、加解密等应用过程中出现的各种异常问题，如：证书无法读取、签名失败、证书验证失败等。

- 证书存储介质硬件设备使用

包括证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。

- 电子认证服务支撑平台使用

为用户提供在认证机构的数字证书在线服务平台中使用的各类问题，如：证书更新失败、下载异常、无法提交注销申请等。

2、 面向应用提供方的服务支持

- 电子认证软件系统使用

提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

- 电子签名服务中间件的应用

解决服务中间件在集成时出现的各种情况，如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等

5.3.2 服务能力

认证机构应提供多种服务方式，包括坐席服务、在线服务、现场服务等，并公布相应的服务获取方式。

认证机构应建立服务保障体系，包括建立专业的服务队伍、服务规范、知识库、服务跟踪系统、满意度调查、投诉受理等。服务保障体系应根据服务业务的变化及时更新。

认证机构应提供全面的培训服务，包括电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答（FAQ）、操作手册等。

1、 座席服务

用户拨打认证机构的服务热线，通过语音系统咨询证书应用问题，热线坐席根据用户的问题请求，查询系统知识库清单，协助用户处理。

2、 在线服务

在线服务通过提供自助信息查询系统、网络实时通讯系统、远程终端协助系统，以及在线帮助与传统模式的结合，满足用户多种服务帮助的需求。

- 自助信息查询系统

将知识库信息按照不同的类型、属性、层次等方式、结构进行分类存储，用户可以按照咨询问题或者已知条件在信息系统上进行启发式的检索，查找目标问题的答案。

- 网络实时通讯系统

用户通过在线帮助网站远程发起支持请求，网站客服人员能够第一时间同登陆网站的访客取的联系，进行交流。

- 远程终端协助系统

用户通过安装远程终端软件，可以通过互联网或者局域网向客户服务人员发起协助请求。由服务人员通过远程终端控制功能，实时检测用户的软硬件环境，通过同屏显示指导、帮助用户解决应用故障。

- 在线帮助与传统模式的结合

将在线服务系统与电话服务结合，方便客户既可以打电话、也可以自助上网，随时查询自己的服务记录、请求处理状态、产品配置信息等等。

3、 现场服务

根据用户的实际需求，由技术支持工程师上门现场为用户处理数字证书应用中存在的问题。

4、 满意度调查

通过多种用户可接受的调查方式进行客户回访，包括电话、WEB网站、邮件系统、短信、传真等。

向用户提供调查表格以供用户填写，调查表格应清晰载明此次回访的目的及内容。并将用户回访中产生的相关文档进行归档、保存。

5、 投诉受理

应向用户公布电子政务电子认证服务监管部门的投诉受理方式。

可通过电话、网站平台、电子邮件、即时通讯工具等方式及时接受客户投诉，投诉受理过程中应记录投诉问题，并将结果及时反馈给用户。

将投诉受理中产生的相关文档进行归档、保存。

6、 培训

培训方式可以由认证机构与客户双方约定的形式开展。

培训内容主要包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答（FAQ）、操作手册等

5.3.3 服务质量

服务质量应明确以下内容:

- 服务的获取方式;
- 座席服务、在线服务、现场服务的服务时间，响应效率;
- 投诉处理承诺;
- 培训效果的评估及处理;
- 服务响应机制及流程。

座席服务、在线服务、现场服务时间应充分满足各类用户的需要，至少为5*8小时工作时间。在有应急服务需求的特殊情况下，服务时间应根据具体业务需求确定，甚至是7*24小时不间断服务。

应对技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，并制定响应处理流程和机制，以确保服务的及时性和连续性。技术支持响应时间应以最大程度不影响客户使用为准则

6 认证机构设施、管理和操作控制

6.1 物理控制

物理环境按照《证书认证系统密码及其相关安全技术规范》的要求严格实施，具有相关屏蔽、消防、物理访问控制、入侵检测报警等相关措施。上海CA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。上海CA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。

6.1.1 场所区域和建筑

上海CA电子政务电子认证服务的运营场地物理环境按照《证书认证系统密码及其相关安全技术规范》建设，通过了国家密码管理局组织的安全性审查。

公司机房具备独立的防震、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。机房采用高安全性的监控技术，包括视频、身份鉴别、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。

所有机房的建设和管理严格按照SHECA的规定要求，机房区域划分为：公共区、服务区、管理区、核心区，具体如下：

1.公共区：机房入口处、办公区域、辅助和支持区域属于公共区，采用访问控制措施，只有经过SHECA 授权的人员才能出入。

2.服务区：服务区是RA操作人员、管理人员的工作区，需要同时经过相关权限检验和人脸鉴别才可以进入，人员进出服务区有日志记录。

3.管理区：管理区是CA运营管理区域，系统监控室、安全监控室、配电室等均属于该区域。此区域必须通过相关权限检验和人脸鉴别才可以进入。

核心区：证书认证系统、加密设备等相关密码物品存放在该区域，其中CA服务器、数据库系统、以及加密设备等相关密码物品位于核心区内的屏蔽机房内。核心区通过相关权限检验和人脸鉴别才可以进入；屏蔽机房两名可信人员同时经过相关权限检验和人脸鉴别才可以进入。

6.1.2 物理访问

上海CA的服务区、管理区、和核心区的门禁系统可实现对人员进出的控制，操作人员进入工作区域进行操作，必须通过人脸验证和权限检验。进出每一道门都有日志记录。

服务区、管理区、和核心区的门都设有强开报警和超时报警；整套门禁系统连接UPS，在市电中断时由UPS提供紧急供电。

操作人员进入机房，必须通过IC卡门禁系统和人脸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。

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。

6.1.3 电力和空调

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

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。

上海CA参照电信设施管理的规定进行维护和保养。

6.1.4 水患防治

上海CA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。

6.1.5 火灾预防和保护

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。上海CA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。

6.1.6 介质存储

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

6.1.7 废物处理

上海CA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。

6.1.8 异地备份

1、系统备份

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

2、数据备份

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

6.1.9 入侵侦测报警系统

在机房场所建筑区域内安装入侵侦测报警系统，进行安全布防。安全区域窗户上应安装玻璃破碎报警器，建筑内天花板上应安装活动侦测器，发生非法入侵应立即报警。

6.2 操作过程控制

应确定可以执行重要操作的可信角色，定义可信角色的要求，并建立职责分割的机制避免单方操作错误对业务的影响。

可信角色包括系统管理员、安全管理员和系统审计员等。

应对执行操作的主体执行可靠的识别与鉴别机制。定义对每个角色的身份标识和鉴别要求，并完整地记录其所有的操作行为。

需要职责分割的角色。按照角色而定义的责任分离，这些角色不能由相同的人承担。

6.3 人员控制

认证机构应根据本机构具体情况，按照技术系统的要求，设置相应的具体岗位和制定技能要求。电子认证系统软件开发商应提供系统管理员、操作员、审计员、安全员等系统管理和操作人员的角色定义和要求。认证机构应定期或当业务、操作和工作环境发生重大变更时，重新评估人员需求，以确保拥有足够数量的、能胜任工作的人员。具体要求包括:

- 建立可信人员策略，包括岗位定义、背景调查内容和程序;

- 在正式聘任员工授权接触公司重要资料前，证明其可信性，并签署员工保密协议;
- 建立每个职位的工作范围及其责任，并确定每个重要职位的可信性要求;
- 建立培训制度及培训档案;
- 建立人员异动管理制度、员工离职后应立即删除其接触公司资料的权限;
- 建立可信雇员清单及所有职员清单。

6.3.1 资格、经历和无过失要求

对于充当可信角色或其他重要角色的人员，其需要具备资格、经历和无过失要求，例如对这些职位的候选者所需具备的信任证明、工作经历和官方凭证。

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。

6.3.2 背景审查程序

在招聘充当可信角色或其他重要角色的人员时所需背景审查程序，这些角色可能要求调查其犯罪记录、档案。

充当可信角色的人员需要经过严格的背景调查程序。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。

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

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。上海CA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。

6.3.3 培训要求

招聘人员后对每个角色的培训要求和过程。培训内容包括:

- 安全管理策略
- 工作岗位职责
- 认证系统使用的软件介绍
- 认证系统管理控制体系
- 电子政务电子认证相关规范和标准
- 本CPS政策及相关标准和程序
- 电子政务电子认证相关法律法规
- 其他需要进行的培训

6.3.4 再培训周期和要求

在完成原始培训后对每个角色的再培训周期和过程。

对于安全管理策略，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。

对于电子政务电子认证相关规定和标准学习，每年至少进行一次。

对认证系统的升级、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。

6.3.5 工作轮换周期和顺序

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，可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。

6.3.6 对下列行为的处罚

当员工被怀疑，或者已进行了未授权的操作，例如未经授权滥用权利或超出权限使用认证系统或进行越权操作，上海CA在得到信息后立即中止该员工进入敏感区域内工作。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，将立即吊销或终止该人员的安全令牌。

6.3.7 独立合约人的要求

上海CA因为人力资源不足或者特殊需要，聘请专业的第三方服务人员参与系统维护、设备维护等，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，使其能够严格遵守上海CA的规范。

6.3.8 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
- 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

6.4 审计日志程序

认证机构需要建立明确的审计日志程序:

- 确定CA中心的业务符合对CPS等文档中的定义;
- CA中心的管理人员需要定期对安全策略和操作流程的执行情况进行检查确认，进行运营风险评估;
- 必须准确完整地记录CA机构涉及运营条件和环境、密钥和证书生命周期管理的日志和事件;
- 各类日志、安全事件的记录应在机密和公正的情况下以自动或手动方式产生，并定期归档；授权安全管理人员定期检阅记录和跟进有关事项;
- 建立检测CA系统访问的检测系统，保证非授权的访问能够被发现;

6.5 记录归档

6.5.1 归档记录的类型

上海CA对下列记录（包括但不限于）进行归档保存:

- 系统建设和升级文档
- 证书申请信息、证书服务批准和拒绝的信息、与证书订户的协议、证书和CRL等
- 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
- 电子认证服务规则、各类服务规范和运作协议、管理制度等
- 系统数据库数据
- 人员进出记录和第三方人员服务记录
- 监控录像
- 员工资料，包括背景调查、录用、培训等资料
- 各类外部、内部审查评估文档

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

6.5.2 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,上海CA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为电子签名认证证书失效后5年。

6.5.3 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。

上海CA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，上海CA会采取异地备份的方式予以保存。

上海CA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。

6.5.4 归档文件的备份程序

所有存档的文件和数据，通常保存在上海CA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。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，按照恢复策略，利用这些归档保存的数据进行系统的恢复。

6.5.5 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。

6.5.6 归档收集系统

认证系统的相关运营信息，由上海 CA 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。

6.5.7 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。如由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较

6.6 认证机构密钥更替

认证机构进行密钥更替时应采用与初始化根密钥相同的方式进行。

应确保新旧密钥更替期间，认证机构根密钥及信任链验证的有效性，避免对现有应用造成影响。新旧根证书过渡时，必须采用新私钥为旧公钥签名证书、旧私钥为新公钥签名证书、新私钥为新公钥签名的证书方式，保证用户和依赖方能够可靠地验证CA机构根证书以及确保证书信任链的有效性

6.7 数据备份

上海CA建立数据备份管理制度，定期开展数据备份。

数据备份采取同城数据备份方式，具备快速恢复能力，减少对业务运营的影响。

6.8 损害和灾难恢复

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，上海CA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，包括:

- 建立CA中心的业务可持续性计划，并进行经常检查和更新，确保其持续有效;
- 对CA系统中的重要部件制订完善的灾难恢复流程，并经常进行演练，确保流程操作的有效性;
- 建立重要系统、数据、软件的备份，并存放在符合CPS要求的安全环境中，确保只有合理授权人员才可接触备份;
- 定期测试备份设备、设施、后备电源等，确保其可用性;
- 建立当CA签名密钥可信性受威胁时的应变计划;
- 制订相关流程，对CA中心终止服务时的告知及业务承接作出计划。

6.8.1 事故和损害处理程序

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，上海CA将按照灾难恢复计划实施恢复。具体由上海CA灾难恢复计划决定。

6.8.2 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。

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。

6.8.3 私钥损害处理程序

当认证系统的私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，应该:

- 立即向主管部门汇报，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。同时立即生成新的密钥对，并自签发新的机构证书;
- 新的机构证书签发以后，按照本CPS关于证书签发的规定，重新签发用户证书;
- 新证书签发以后，将会立即通过信息库、目录服务器、HTTP等方式进行发布。

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

6.8.4 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，上海CA制订了一套完整的业务连续性计划，并建立了相应的同城异地灾难备份系统，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，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。

业务连续性能力包括:

- 建立CA中心的业务可持续性计划，并进行经常检查和更新，确保其持续有效。
- 对CA系统中的重要部件制订完善的灾难恢复流程，并经常进行演练，确保流程操作的有效性
- 建立重要系统、数据、软件的备份，并存放在符合CPS要求的安全环境中，确保只有合理授权人员才可接触备份。
- 定期测试备份设备、设施、后备电源等，确保其可用性。
- 建立当CA签名密钥可信性受威胁时的应变计划。

制订相关流程，对CA中心终止服务时的告知及业务承接作出计划。

6.9 认证机构或注册机构终止

与认证机构或注册机构终止和终止通告相关的过程，应按照《电子政务电子认证服务管理办法》的要求，处理好相关承接事项，包括认证机构或注册机构档案记录管理者的身份问题。

- 认证机构拟暂停或者终止认证服务的，应当在暂停或者终止认证服务六十个工作日前，选定业务承接认证机构，就业务承接有关事项作出妥善安排，并在暂停或者终止认证服务四十五个工作日前向国家密码管理局报告。
- 不能就业务承接事项作出妥善安排的，应当在暂停或者终止认证服务六十个工作日前，向国家密码管理局提出安排其他认证机构承接业务的申请。

7 认证系统技术安全控制

7.1 密钥对的生成和安装

7.1.1 密钥对的生成

CA 密钥对的产生，必须由若干名接受过相关培训的认证机构人员在特定安全区域内按照严格的安全规程，在能够生成有足够安全强度密钥的认证系统上操作完成。

用于此类密钥生成的密码模块需通过国家密码主管部门鉴定、认证。

对于CA 密钥对的产生，认证机构应该有严格的密钥生成流程。

7.1.2 私钥传送给订户

可能的方法包括实体自己生成因而自动拥有、用物理的方式将私钥传递给实体、邮寄保存私钥的令牌、或是通过SSL会话传递。

7.1.3 公钥传送给证书签发机构

实体公钥安全地提供给证书认证服务机构的方式。可能通过在线SSL会话或经注册机构签署的消息。

证书订户以公钥向上海CA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。

7.1.4 电子认证服务机构公钥传送给依赖方

将认证机构公钥安全地提供给潜在的依赖方的方式。可能的方式包括用人工将公钥发送给依赖方、用物理方式邮寄一份拷贝给依赖方、或通过SSL会话传递

上海CA的公钥包含在上海CA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。

7.1.5 密钥的长度

SM2密钥长度为256位，保留支持更长位数的密钥长度。

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，上海CA将会完全遵从。

7.1.6 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。

7.1.7 密钥使用目的

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

所有密钥的使用，都必须遵循本CPS的规范。

7.2 私钥保护和密码模块工程控制

认证机构必须通过物理、逻辑和过程控制的综合实现来确保CA 私钥的安全。

证书持有者应按照订户协议要求。采取必要的预防措施防止私钥的丢失、泄露、更改或未经授权的使用。

7.2.1 用来产生密钥的模块标准

上海CA使用的主机加密服务器具有国家密码管理局批准的产品型号证书。密码模块的标准、使用和控制都符合国家的有关规定。

7.2.2 私钥是否由 M 选 N 多人控制

认证机构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。上海CA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。

7.2.3 私钥是否被托管

1、订户自己生成并保管签名密钥：建议订户采用安全的密码模块生成、保存签名私钥，并采取安全方式进行备份、恢复，SHECA不负责密钥的备份、恢复和归档。

2、SHECA代订户生成签名密钥后交由订户自己保存：订户私钥须在符合国家密码管理相关规定的密码模块内生成（通常是智能密码钥匙、智能IC卡等形式），订户应妥善保存密码模块及其个人识别码（PIN），SHECA不负责密钥的备份、恢复和归档。

3、SHECA代订户生成并保管签名私钥：需取得订户单独同意，并明确托管的风险、双方权利义务与法律责任。

1）订户私钥须在符合国家密码管理相关规定的密码模块内生成，以密文的形式存放在密钥库，SHECA应采用技术手段和管理措施妥善保护私钥安全;

2）订户使用私钥时SHECA必须验证订户身份，以保障私钥由订户专控，只有订户可以使用;

3）订户每次使用私钥，SHECA需记录私钥使用的记录并可供订户查阅。

4）因非SHECA管理原因而导致托管签名私钥遗失或冒用，损失由订户自己承担，SHECA对此不承担责任。

4.SHECA不建议订户将签名私钥委托第三方主体管理;若因订户委托第三方管理签名私钥而引发争议，SHECA不承担相关责任。

7.2.4 私钥是否备份

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前述要求。CA私钥复制到备份硬件密码模块中要符合规定要求。

7.2.5 私钥是否归档

不支持私钥归档。

7.2.6 私钥可以被导入或导出密码模块的条件

认证机构私钥严格的按照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。

7.2.7 激活（使用）私钥的实体

为激活私钥必须执行登录、上电、提供PIN、插入令牌/钥匙等等。

7.2.8 解除私钥激活状态的实体以及方式

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，自动冻结或者有效期届满。

7.2.9 销毁私钥以及方式

销毁密钥的方式包括交出令牌、销毁令牌或者重写密钥。

7.3 密钥对管理的其他方面

认证机构必须归档CA 和证书持有者证书，归档的证书可存放在第三方数据库中。

不同用途的证书必须按照规定的有效期用于指定的应用。

证书操作期和密钥对使用期限:

- 公钥和私钥的使用期限与证书的有效期相关但却有所不同;
- 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。

7.4 激活数据

1. 私钥激活数据的产生必须安全可靠，并具有日志记录。
2. 激活数据应具有足够的复杂度。
3. 认证机构、证书持有者应妥善保管激活数据，CA私钥还应进行分割保护。
4. 激活数据在传输中应确保机密性，并在不需要时，妥善销毁。

7.4.1 激活数据的产生和安装

用于保护存放有认证机构CA 私钥的加密卡激活信息（秘密分割）的产生过程必须安全可靠，符合相应的安全要求。秘密分割的创建和分发记录有相应的日志。

CA 私钥和证书持有者证书私钥的激活数据一般是口令，这些口令必须具有足够的复杂度:

- 由用户产生;
- 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;
- 不能包含用户名信息中的较长的子字符串。

7.4.2 激活数据的保护

对于CA 私钥的激活数据，认证机构必须通过秘密分割将分割后的激活数据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，签署协议确认他们知悉秘密分割掌管者责任。

如果证书持有者使用口令或PIN 码保护私钥，证书持有者应妥善保管好其口令或PIN码，防止泄露或窃取。如果证书持有者使用生物特征保护私钥，证书持有者也应注意防止其生物特征被人非法获取。

7.4.3 激活数据的其他方面

- 激活数据的传送

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。还有，Windows 或网络的登录用户的用户名/密码（用于证书持有者激活数据），经过网络传送时注意非法用户的窃取。

- 激活数据的销毁

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢失、偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或全部，比如记录有口令的纸页必须粉碎

7.5 计算机安全控制

CA 软件和数据文件应运行和保存在安全可信的系统中。认证机构应确保包含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人员访问认证系统服务器，一般的应用用户在认证系统服务器上没有账户。

应为CA系统划定独立的安全域并确保系统访问授权信息的安全性。认证机构的生产系统网络应与其它部分逻辑分离。这种分离可以阻止除指定的应用程序外对网络的安全访问。认证机构应使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。只有认证机构系统操作与管理组中的、有必要工作需要、访问系统的可信人员可以直接访问认证系统数据库。

系统口令必须符合口令安全管理要求。

7.6 生命周期技术控制

7.6.1 CA 系统运行管理

应制定CA系统运行的安全保障机制，确保在系统运行、维护过程中的安全。

应建立监控和检查机制，确保系统网络运行环境的安全性。

- CA 系统的操作流程需要文档化并进行维护
- CA 系统（包括软件、网络等方面）的变更需经管理层批准，经批准的变更实行前必须通过测试，并进行记录
- 可能对系统的安全性有影响的改动必须事先得进行风险评估，改动前应进行备份并得到管理层的明确批准
- CA 中心的测试系统、运营系统、网络设施等，具有专门的操作维护人员，并有相应明确的授权
- 操作维护人员需要定期检查系统及网络的稳定性、安全性及容量，确定符合服务水平

- 建立检测和防护控制来防止病毒和恶意软件，并能提供适当的报警信息
- 建立监控流程，确保记录并报告发现的或怀疑的、对系统或服务有威胁的安全缺陷。建立并执行系统故障报告、处理流程
- 建立制度，对CA系统相关的媒介（包括设备、证书介质、文档等）进行妥善保管，避免非授权的访问

7.6.2 CA系统的访问管理

应制定对CA系统的安全访问策略，并确保访问身份、访问角色、访问授权的安全可靠。

- 制定CA系统的访问策略，内容包括：访问角色及相关权限，认证及鉴别的方法，分权机制，特殊CA操作的人数（密钥生成时m/n规则）等
- 制定CA系统访问人员角色职能定义，确保合理的职责分割和权限控制，并明确授权及取消授权的操作流程和策略
- 制定网络安全策略，并制定访问网络的控制策略
- 制定操作系统及CA软件的安全访问的策略
- 建立对各种对CA系统访问的审计措施

7.6.3 CA系统的开发和维护

应建立有效地保障机制，确保对CA系统资源的使用、修改、添加等操作的可靠性：

- 建立CA系统软件修订控制流程，对系统新增或修改进行管理。
- 严格控制对CA系统的源代码及测试数据的访问。
- 操作系统升级变更时，应用系统软件需要重新测试。
- 在CA系统中，购买、使用或修改的软件，需要进行严格检查，避免“特洛伊木马”等攻击

7.7 网络安全控制

CA系统的运行网络环境应满足安全运营的要求，避免网络攻击、漏洞带来的运营风险。

认证机构应通过防火墙、入侵检测、防病毒、安全身份认证等安全技术，确保认证系统的安全运营。对于认证系统的网络安全，认证机构应制定专门的网络安全策略与实施方

案，有关方案应符合安全和审计要求指南。说明与网络安全相关的控制，如防火墙、防病毒、入侵检测等。

7.8 时间戳

认证系统的各种系统日志、操作日志应该有可靠的记录时间。

认证机构应部署时间戳系统，在系统关键业务运行日志、操作日志等日志中，使用时间戳服务。

8 证书、证书吊销列表和在线证书状态协议

8.1 证书

上海 CA 使用的证书详细格式，符合《电子政务数字证书格式规范》的要求。

8.1.1 版本号

证书符合 X.509 V3，这一版本信息存放在证书版本属性栏内。

8.1.2 证书扩展项

上海 CA 使用的证书标准项、标准扩展项和自定义扩展项符合《电子政务数字证书格式规范》的要求。 包括:

- 密钥用途
- 证书策略
- 基本限制
- 扩展密钥用途
- CRL 发布点
- 主题密钥标识

8.1.3 算法对象标识符

上海CA使用的算法对象标识符，如下:

SM2算法，OID：1.2.156.10197.1.301

基于SM2算法和SM3算法的签名的OID为：1.2.156.10197.1.501

8.1.4 名称形式

名称形式见前述规定，符合X.501的甄别名格式。

8.1.5 证书策略对象标识符

证书策略对象标识符，存放在证书内证书策略的相关栏目。

本CPS的注册对象标识符（OID）为1.2.156.112570.150。

8.1.6 策略限制扩展项的用法

无规定。

8.1.7 策略限定符的语法和语义

无规定。

8.1.8 关键证书策略扩展项的处理规则

无规定。

8.2 证书吊销列表

上海 CA 定期签发 CRL，供用户查询使用。

8.2.1 版本号

X.509 V3，此版本号存放在 CRL 版本格式栏目内。

8.2.2 CRL 和 CRL 条目扩展项

无规定。

8.2.3 CRL 下载

可以通过证书中签发的 CRL 扩展项标明的 URL 下载 CRL。

8.3 在线证书状态协议

上海 CA 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。

8.3.1 版本号

RFC2560 定义的 OCSP V1。

8.3.2 OCSP 扩展项

无规定。

8.3.3 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上海 CA 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，这些错误信息没有上海 CA 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)

9 认证机构审计和其他评估

上海 CA 在提供电子政务电子认证服务时，接受国家密码管理局的电子政务电子认证服务能力评估。同时，为了保证服务的可靠开展，上海 CA 还定期开展内部审计和评估。

9.1 评估的频率和情形

1、 根据《电子政务电子认证服务管理办法》的要求，接受国家密码管理局组织的年度评估和检查。

2、 接受上海市密码管理局定期或不定期的评估和检查。

3、按照国家主管部门的要求、每年至少定期执行一次内部的评估审核。

9.2 评估者的资质

上海 CA 无条件接受国家密码管理局、上海市密码管理局的评估和检查。

在进行内部评估审计时，上海 CA 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，并且熟悉电子政务电子认证法规和政策、相关标准规范、本 CPS，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。内部评估由政策法务部组织实施。

9.3 评估者与被评估者之间的关系

国家密码管理局、上海市密码管理局是上海 CA 的主管机构。

在开展内部评估时，评估者与被评估的对象之间，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。

9.4 评估内容

1、上海 CA 按照国家密码管理局、上海市密码管理局提出的评估要求和规范，接受其任何内容的评估。

2、上海 CA 内部评估审核的内容包括:

- 是否符合电子政务电子认证相关法规政策和规范的要求

- 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
- 服务质量评估

9.5 对问题与不足采取的措施

1、国家主管部门评估完成后，上海 CA 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，提交修改措施以及整改计划书，并接受其对整改计划的检查，以及对整改情况的复审。

2、完成内部评估后，评估人员需要列出所有问题项目的清单，由评估人员和被评估对象共同讨论有关问题，并将结果书面报告上海 CA 安全认证委员会，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。

10 电子政务电子认证服务中的法律责任相关要求

10.1 要求

上海 CA 在开展电子政务电子认证服务时，严格按照《电子签名法》、《电子政务电子认证服务管理办法》等法律法规的要求，对涉及保密、隐私、知识产权、担保以及服务运营等各方面承担相关的责任与义务。

10.2 内容

10.2.1 费用

上海 CA 按照物价部门规定的收费内容、收费标准收取服务涉及的费用，并根据实际

情况向下调整。

上海 CA 通过网站、现场张贴告示等方式公布相关收费标准。

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，上海 CA 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，上海 CA 遵守严格的操作程序和策略。如果上海 CA 违背了本 CPS 所规定的责任或其它重大义务，订户可以要求撤销证书并退款。订户需要填写退款申请表以要求退款。

10.2.2 财务责任

上海 CA 保持足够的资金以维持业务运作和履行相应的责任，介绍主管部门对财务状况的检查。

当因为违反国家相关规定、本 CPS 规定而造成订户或依赖方损失时，上海 CA 将根据国家法律规定予以赔付。

10.2.3 业务信息保密

上海 CA 对开展业务过程中所接收的属于私有信息的业务信息负有保密责任。

上海 CA 对属于私有信息的业务信息的使用和发布应符合法律、法规的要求。

对违法、违规使用、发布属于私有信息的业务信息的，上海 CA 承担由此造成的证书持有者、依赖方的损失，并负担相应的经济、行政责任。

10.2.4 个人隐私保密

上海 CA 对开展业务过程中所接收的属于私有信息的个人隐私信息负有保密责任。

上海 CA 对属于私有信息的个人隐私的使用和发布应符合法律、法规的要求。

对违法、违规使用、发布属于私有信息的个人隐私信息的，上海 CA 承担由此造成的证书持有者、依赖方的损失，并负担相应的经济、行政责任。

10.2.5 知识产权

上海 CA 享有并保留对证书以及提供的全部软件、系统的一切知识产权，包括所有权、名称权和利益分享权等。

所有上海 CA 发行的证书和提供的软件、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上海 CA，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。

订户自己产生的密钥的知识产权归其所有，但是公钥经过上海 CA 签发成证书后，上海 CA 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。

在没有上海 CA 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，使用或接受任何上海 CA 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。

10.2.6 陈述和担保

1、电子认证服务机构的陈述与担保

- 建立电子政务电子认证业务规则（E-Gov CPS）和其他认证服务所必需的规范、制度体系
- 在本 CPS 相关条款规定的范围内，提供认证服务，遵守本 CPS 的各项规定
- 保证其私钥得到安全的存放和保护，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
- 和证书订户、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上海 CA 承担信托责任。上海 CA 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
- 在证书中没有发证机构所知的或源自于发证机构的错误陈述
- 在生成证书时，不会因发证机构的失误而导致数据转换错误，即不会因发证机构的失误而使证书中的信息与发证机构所收到的信息不一致
- 发证机构签发给订户的证书符合本 CPS 的所有实质性要求
- 发证机构将按本 CPS 的规定，及时吊销证书
- 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
- 证书中的所有信息都是准确的
- 发证机构完全遵照本 CPS 的规定签发证书

2、注册机构的陈述与担保

- 遵循本CPS 接受并处理申请者的证书服务请求
- 严格执行证书申请者的身份鉴别和验证
- 必须遵循上海CA 制订的服务受理规范、系统运作和管理要求，根据本CPS 决定是否给申请者提供相应的证书服务
- 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。必须能够提供证书服务全部的数据资料及备份
- 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
- 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、的陈述与担保

- 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，通知上海CA 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）
- 未经授权的人员从未访问过订户私钥
- 订户向发证机构陈述的所有包含在证书中的有关信息是真实的。如果订户发现了证书中信息存在某些错误 ，但订户还没有及时通知给发证机构，那么，发证机构视为：订户承诺上述信息都是真实的
- 订户将按本CPS 的规定，只将证书用于经过授权的或其它合法的使用目的
- 一经接受证书，既表示订户知悉和接受本CPS 中的所有条款和条件，并知悉和接受相应的订户协议
- 一经接受证书，订户就应承当如下责任：始终保持对其私钥的控制，使用可信的系统，和采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用
- 一经接受证书，即表示订户同意使上海CA 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上海CA

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。如果因此给上海 CA 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

- 不得拒绝任何来自上海 CA 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

4、依赖方的陈述与担保

- 熟悉本 CPS 的条款，了解证书的使用目的
- 依赖方在信赖上海 CA 签发的证书前，已经对证书进行过合理的检查和审核，包括：检查上海 CA 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上海 CA 带来的损失进行补偿，并且承担因此造成的自身或他人的损失
- 对证书的信赖行为就表明依赖方已经接受本 CPS 的所有规定，尤其是其中有关免责、拒绝和限制义务的条款
- 不得拒绝任何来自上海 CA 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

10.2.7 担保免责

上海 CA 在下列情况下免于承担责任:

- 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。
- 如果由于非认证机构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，上海 CA 不负任何赔偿责任
- 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，由此得到了上海 CA 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，上海 CA 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

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

10.2.8 偿付责任限制

上海 CA 对所有当事人（包括但不限于订户、申请者、接受者或信赖方）的合计赔偿责任，不可能超过如下所述对这些证书的封顶赔偿金额:

对于有关一张特定证书的所有签名和交易处理的总计，上海 CA 及其授权的证书服务机构对于任何人（或者其它实体）有关该特定证书的合计赔偿责任应该限制在一个不超出下述数额的范围内（单位: 人民币元）:

1、个人类证书，不超过 2，000 元

2、机构类证书，不超过 50，000 元

3、设备类证书，不超过 80，000 元

法律法规或国家主管部门另有规定的，上海 CA 将严格遵照执行。

10.2.9 赔付责任

根据《电子政务电子认证服务管理办法》的规定，当认证机构暂停或者终止认证服务时，未就业务承接有关事项作出妥善安排，而给证书用户造成损失的，应承担所产生的赔偿及行政责任。

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《电子政务电子认证服务管理办法》及其他法律法规的规定，上海 CA 应承担的赔偿责任。

10.2.10 有效期和终止

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

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

本CPS将持续有效，直到有新的版本取代。

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

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

10.2.11 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，上海CA将以网站、电子邮件等合理的方式与相关各方进行沟通，通常不会采取个别的方式进行。。

10.2.12 修订

经上海CA安全认证委员会授权，政策法务部每年至少审查一次本CPS，确保其符合国家法律法规和电子政务电子认证相关规定的要求，符合认证业务开展的实际需要。

本CPS的修订，由政策法务部提出修订报告后，必须经过上海CA安全认证委员会审核并批准后才能开始修订。

修订后的CPS应送交国家密码管理局备案。

10.2.13 争议处理

由于本CPS引发争端的，上海CA首先采取协商方式予以解决。如果无法协商解决的，可以请求国家电子政务电子认证服务监管部门、仲裁部门或司法机构予以解决处理。

10.2.14 管辖法律

本CPS接受《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》

等的管辖和解释。

10.2.15 与适用法律的符合性

电子认证服务活动参与者，均需遵守《中国人民共和国电子签名法》、《电子政务电子认证服务管理办法》、《电子认证服务密码管理办法》以及国家密码管理局相关密码技术、产品标准规范的规定。

10.2.16 一般条款

本 CPS 直接影响上海 CA 权利、义务的条款和规定，除非通过受到影响的当事人发出经过鉴定的信息或文件，或者在此另有其他规定，否则不能进行口头上的修正、放弃、补充、修改或终止。

在本 CPS 与其他规则、规范或协议发生冲突时，所有认证活动的参与方都将受本 CPS 规定的约束

包括完整协议条款、转让条款、分割性条款、强制执行条款、不可抗力条款等。

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。

本 CPS 的任何条款或其应用，如果因为任何原因或在任何范围内发现无效或不能执行，那么本 CPS 其余的部分仍将有效。相关当事人了解并同意，本 CPS 所规定的责任限制、保证或其它免责条款或限制、或损害赔偿的排除等，均是可独立于其它条款的个别条款，并可加以执行。

在法律法规许可的范围内， 上海 CA 将不对以下超越其控制能力的不可抗力事件，所造成本 CPS 规定的担保责任的违反、延误或无法履行负责：构成不可抗力的事件包括战争、恐怖袭击、罢工、瘟疫、自然灾害、火灾、地震、供应商或卖方执行失败、互联网或其他基础设施的瘫痪和其它天灾等。

10.2.17 其他条款

无。