天威诚信™

电子认证业务规则

V 1.4.2

生效日期: 2020 年 11 月 1 日

版本说明：

天威诚信认证业务规则版本控制表

版本	主要修改说明	生效时间	主要修改人	批准人
1.0	根据 CA/B Forum 上 Baseline Requirements 的要求，按照 RFC3647 框架编写，形成版本。	2018.7.31	许蕾	天威诚信安委会
1.1	1) 添加处理证书申请的时间。 2) 添加针对有效时间展示格式的明确定义。 3) 修改公钥归档的描述。 4) 增加自主开发系统的描述。 5) 根据对 CP 和 CPS 一致性检查结果进行相关修改。	2018.9.28	安垠，李超，杨柳，张政，陈大鹏，杨学龙，李艳蓉，宋志敏，许蕾	天威诚信安委会
1.2	1) 增加定期跟踪 CA/B 论坛 BR 标准更新来进行 CP/CPS 更新。 2) 修改互操作准则描述。 3) 添加根 CA 签发行为描述。	2018.12.25	安垠，许蕾	天威诚信安委会

	4) 修改证书吊销情形描述。 5) 增加 CRL 有效期描述。			
1.3	1）增加了证书问题报告提交方式的说明； 2）修订了 IP 地址鉴证的细则内容； 3) 修订了鉴证操作说明； 4) 首次发布对应的英文版 CPS。	2019.5.15	安垠，杨柳，李瀚	天威诚信安委会
1.3.1	1）增加附件 B 证书信息。	2019.7.1	安垠，李瀚	天威诚信安委会
1.4	1，根据 BR 中 SC25，3.2.2.4.2 依据的 BR 域名验证方法调整为 3.2.2.4.18。 2，其他修订：一些格式错误调整。	2020.4.9	安垠，张政，郑玉恬	天威诚信安委会
1.4.1	1，5.2.2 中加密设备的管理权限由 3 选 2 改为 5 选 3。 2，6.2.2 中 CA 私钥的秘密分割由 3 选 2 改为 5 选 3。 3，证书有效期和鉴证资料有效期调整为 398 天。	2020.5.20	许蕾，张政，安垠，郑玉恬	天威诚信安委会

1.4.2	1，根据 CAB Ballot SC28 及 Ballot SC30 进行对应调整； 2，文档中一些小的编辑修改；	2020.11.1	郑玉恬，安垠	天威诚信安委会

目 录

1. 概括性描述

1.1 概述

1.1.1 公司简介

北京天威诚信电子商务服务有限公司（下称“天威诚信数字认证中心”，或简称“天威诚信”），是首批获得工业和信息化部颁发《电子认证服务许可证》的电子认证服务机构。2012 年，天威诚信电子认证服务系统通过了国家密码管理局组织的安全性审查。2018 年，天威诚信着手实施 WebTrust 国际安全审计认证工作，希望以国际标准化的运营管理和服务水平，为广大的、对通信和信息安全方面有各种各样需求的公众用户提供全球化的电子认证服务。

1.1.2 电子认证业务规则（CPS）

本《电子认证业务规则》（简称 CPS）的总体条款结构符合工业和信息化部所发布的《电子认证业务规则规范（试行）》，并在制定过程中遵循《中华人民共和国电子签名法》、《电子认证服务管理办法》、以及《电子认证服务密码管理办法》等法律法规的要求，本 CPS 同时遵循 RFC3647 的框架进行编写，阐明了天威诚信如何开展电子认证业务，包括批准、签发、管理、吊销和更新证书的业务方式和过程，以及相应的服务、法律和技术上的措施和保障，以供电子认证活动参与方了解和遵循。

本 CPS 所阐述的内容遵循天威诚信证书策略（Certificate Policy, 简称 CP）、 CA/浏览器论坛（CA/Browser Forum）发布的最新版本的 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates（简称“Baseline Requirements”）、 Guidelines for the Issuance and Management of Extended Validation Certificates（简称“EV Guidelines”）、《Network and Certificate System Security Requirements》（简称“NCSSR”）进行签发和管理公共可信任 SSL 数字证书。天威诚信定期查看其更新情况，并将持续根据其发布的最新版本进行修订 CPS。如果本 CPS 与 CA/

浏览器论坛（CA/Browser Forum）发布的相关标准规范中的条款有不一致的地方，则以CA/浏览器论坛正式发布的规范为准。

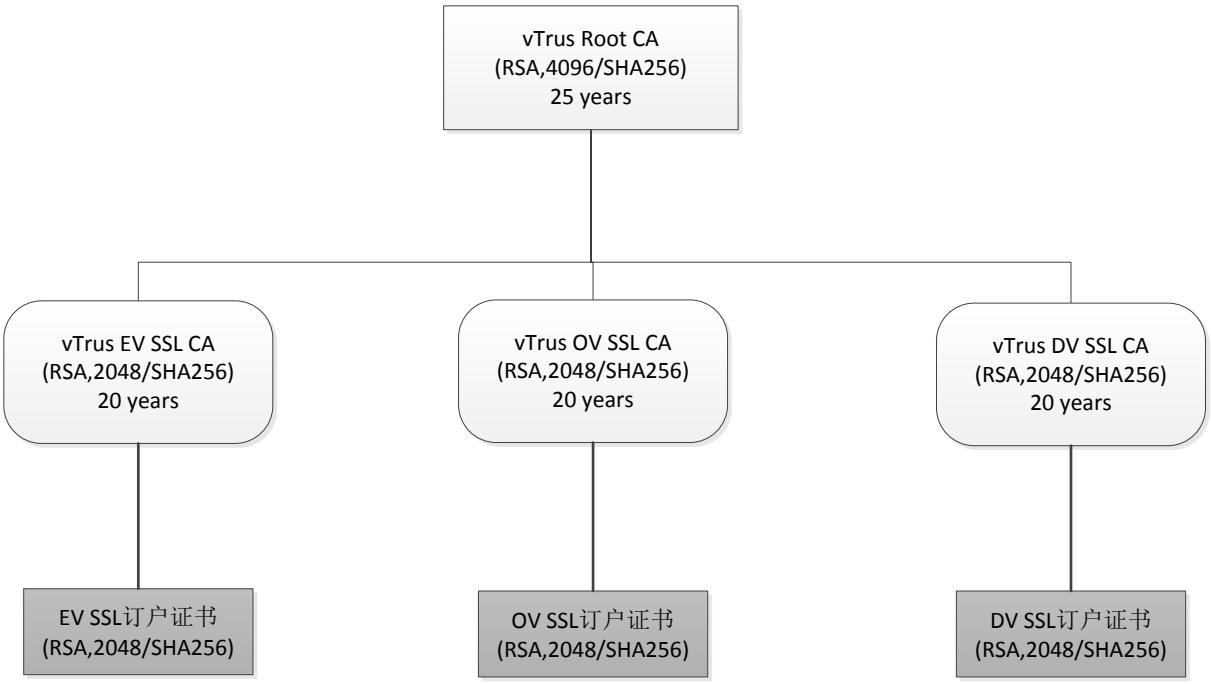
1.1.3 天威诚信证书体系架构

天威诚信目前有 2 个根证书，分别为 vTrus Root CA 证书（RSA）、vTrus ECC Root CA 证书（ECC），每个根 CA 下设中级 CA，以签发订户证书。天威诚信不签发外部中级 CA 证书。

1) vTrus Root CA

天威诚信 vTrus Root CA 证书的密码算法为 RSA，根密钥长度为 4096-bit；此根 CA 下设 3 个中级 CA 证书：

- vTrus EV SSL CA 证书，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 EV SSL 服务器类证书；
- vTrus OV SSL CA 证书，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 OV SSL 服务器类证书；
- vTrus DV SSL CA 证书，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 DV SSL 服务器类证书。

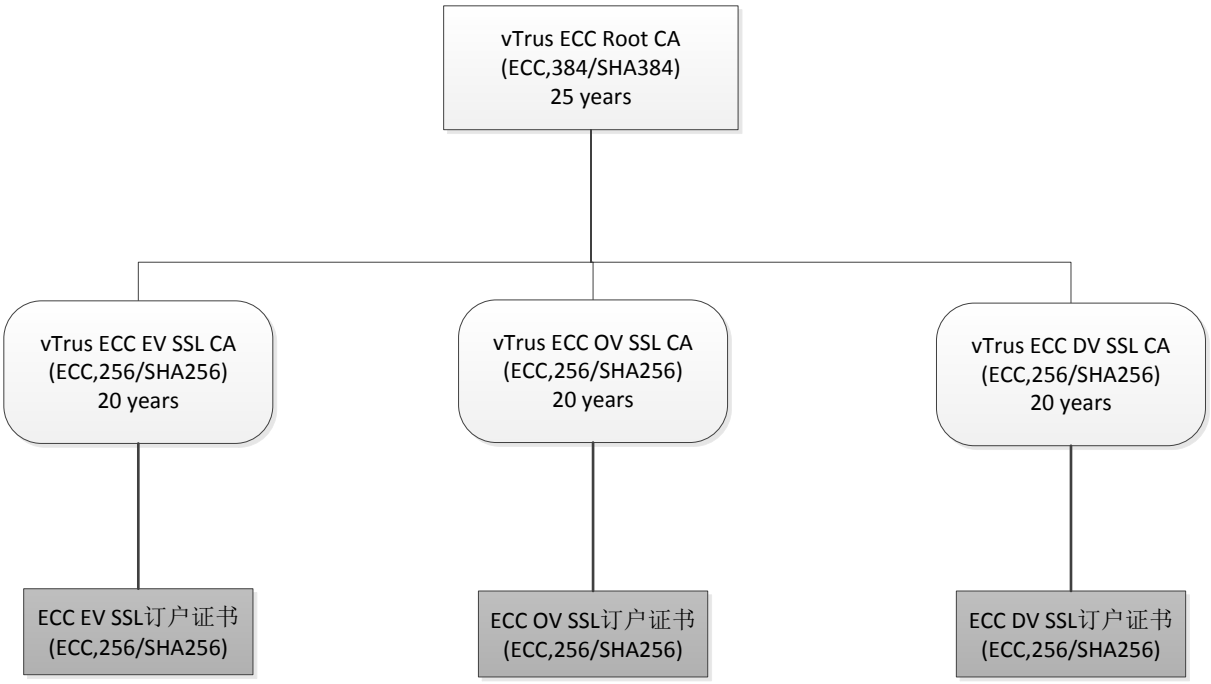


RSA 三级根体系图

2) vTrus ECC Root CA

天威诚信 vTrus ECC Root CA 证书的密码算法为 ECC，根密钥长度为 384-bit；此根 CA 下设 3 个中级 CA 证书：

- vTrus ECC EV SSL CA 证书，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 EV SSL 服务器类证书；
- vTrus ECC OV SSL CA 证书，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 OV SSL 服务器类证书；
- vTrus ECC DV SSL CA 证书，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 DV SSL 服务器类证书。



ECC 三级根体系图

1.2 文档名称与标识

本文档称为《天威诚信电子认证业务规则》（简称天威诚信 CPS、本 CPS），CPS 为“Certification Practice Statement”的缩写，在本文档中，CPS 等同于本节中定义的文档名称和适用名称。

天威诚信注册的 OID 为 1.2.156.112535，在本 CP 中为各类证书分配的 OID 如下：

1) EV SSL 证书策略对象标识符：1.2.156.112535.1.1.6.1；

2) OV SSL 证书策略对象标识符：1.2.156.112535.1.1.5.1；

3) DV SSL 证书策略对象标识符：1.2.156.112535.1.1.5.2。

天威诚信同时会使用 CA/B Forum 保留的策略对象标识符。

1）EV SSL 证书策略对象标识符 2.23.140.1.1；

2）OV SSL 证书策略对象标识符 2.23.140.1.2.2；

3）DV SSL 证书策略对象标识符 2.23.140.1.2.1。

本 CPS 另有英文版本发布，若英文版本与中文版本出现任何歧义，概以中文版本为准。

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（Certification Authority，简称 CA）指所有得到授权能够颁发公钥证书的实体。天威诚信是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》的相关规定，依法设立的第三方电子认证服务机构。天威诚信通过给从事电子交易活动的各方主体颁发数字证书、提供数字证书验证服务等手段而成为电子认证活动的参与主体。

1.3.2 注册机构（RA）

注册机构（RA）代表 CA 建立起证书注册过程，确认证书申请者（订户）的身份，批准或拒绝证书申请，批准订户的证书吊销请求或直接吊销证书，批准订户的证书更新请求。

天威诚信除了承担 CA 的角色外，将自行担任 RA，不再另行设立 RA。

1.3.3 订户

订户指从天威诚信获得证书的所有最终用户，可以是个人、机构、或设备。订户通常需要同天威诚信，或其注册机构签订合约以获得证书，并承担作为证书订户的责任。

在电子签名应用中，电子签名人、证书持有人即订户。

1.3.4 依赖方

天威诚信的依赖方是为某一应用而使用、信任天威诚信或其注册机构签发的证书的实体。依赖方可以是天威诚信的证书订户，也可以不是证书订户。

1.3.5 其他参与者

其他参与者是指为天威诚信的电子认证活动提供相关服务的其他实体。

1.4 证书应用

1.4.1 适合的证书应用

天威诚信签发的 SSL 服务器证书，主要用于标识 Web 网站或者 Web 服务器的身份，证明网站的身份或者资质，提供 SSL 加密通道。

天威诚信签发的 SSL 服务器类证书分为 DV SSL（Domain Validation SSL）证书、OV SSL（Organization Validation SSL）证书和 EV SSL（Extended Validation SSL）证书。订户可以根据实际需要，自主判断和决定采用相应合适的证书类型。

1.4.1.1 EV SSL 证书

EV SSL 证书（Extended Validation SSL Certificates），即扩展验证型服务器证。EV SSL 证书可用来验证证书中标识的域名的身份，以及持有该域名的法人机构身份。凡是经过验证后确定是由天威诚信签发的 EV 证书，均表明该证书中所包含的信息真实有效，并且已经通过了适当且可靠的身份鉴别程序。EV SSL 证书可实现网站机密信息的加密以及网站身份的验证功能。

1.4.1.2 OV SSL 证书

OV SSL 证书（Organization Validation Certificates），即需要验证网站所属机构真实身份的标准型 SSL 证书。OV SSL 证书可实现网站机密信息的加密以及网站身份的验证功能。

1.4.1.3 DV SSL 证书

DV SSL 证书（Domain Validation SSL Certificates），即只验证网站域名所有权的简易型 SSL 证书。DV SSL 证书只提供网站机密信息的加密功能。

1.4.2 限制的证书应用

天威诚信所颁发的 SSL 证书在功能上是受到限制的，只能应用于证书所代表的主体身份适合的用途。

对于证书的应用超出本 CPS 限定的应用范围，将不受本 CPS 保护。

1.4.3 受禁的使用

天威诚信所颁发的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，禁止用于中间人攻击或流量监控，否则由此造成的法律后果由订户自行承担；同时，所有证书不设计用于、不打算用于、也不授权用于危险环境中的控制设备，或用于要求防失败的场合，如核设备的操作、航天飞机的导航或通讯系统、空中交通控制系统或武器控制系统中，因为它的任何故障都可能导致死亡、人员伤害或严重的环境破坏。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的管理机构是天威诚信安全策略委员会，该委员会负责制定、批准、发布、实施、更新、废止本 CPS。天威诚信的安全策略委员会由来自于公司管理层、主管运营安全、技术安全、和人才安全的合适代表组成。

当安全策略委员会审批成员投“同意”票超过半数，且当安全策略委员会主任审批“同意”后，此版 CPS 可视为审批通过。

本策略文档的对外咨询服务等日常工作由运营管理部门负责。

1.5.2 联系人

天威诚信将对电子认证业务规则实施严格的版本控制，并指定专门的部门负责相关事宜。任何有关 CPS 的问题、建议、疑问等，都可以按以下方式进行联系。

如果需要天威诚信相关的策略文档请发邮件到信箱：itrus_cps@itrus.com.cn，或寄送至：

北京天威诚信电子商务服务有限公司

中华人民共和国北京市海淀区上地八街 7 号院 4 号楼 4 层（100085）

电话号码：0086-010-50947500

传真号码：0086-010-50947517/50947516

官方网站：https://www.itrus.com.cn

订户，依赖方，应用软件提供商和其他第三方可以向天威诚信提交包括密钥泄露，证书滥用，误签发等各种不合规的证书问题报告，请访问 https://www.itrus.com.cn/repository 并根据证书问题报告中（Certificate Problem Report）的说明填写，然后在线提交或发送至 support@itrus.com.cn。

1.5.3 决定 CPS 符合 CP 的机构

天威诚信安全策略委员会是策略制定的主要机构，也是审核批准本 CPS、决定本 CPS 是否符合天威诚信 CP 的最高权威机构。

1.5.4 CPS 批准程序

本 CPS 由天威诚信安全策略委会组织 CPS 编写小组编制，该小组完成后提交安全策略委员会审核，经该委员会批准后，正式在天威诚信官方网站上发布。

本 CPS 根据国家的政策法规、技术要求、业务发展情况以及 CA/浏览器论坛（CA/Browser Forum）发布的 Baseline Requirements、EV Guideline、NCSSR 的最新要求每年修订，由 CPS 编写小组根据相关的情况拟定 CPS 修订内容，提交安全策略委员会审核，经该委员会批准后，递增版本号、更新发布时间、生效时间及修订记录，并正式在天威诚信官网上发布。

所有正式发布的 CPS 版本将根据《电子认证服务管理办法》中规定，从对外发布之日起的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 定义

术语	定义
安全策略委员会	认证服务体系内的最高策略管理监督机构和CPS一致性决定机构
电子认证服务机构	Certificate Authority，也就是证书认证机构，是颁发证书的实体。
注册机构（RA）	负责处理证书申请者和证书订户的服务请求，并将之提交给认证服务机构，为最终证书申请者建立注册过程的实体，负责对证书申请者进行身份标识和鉴别，发起或传递证书吊销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。
证书策略（CP）	一套命名的规则集，用以指明证书对一个特定团体或者具有相同安全需求的应用类型的适用性。例如，一个特定的CP可以指明某类证书适用于鉴别从事企业到企业交易活动的参与方，针对给定价格范围内的产品和服务。
认证业务规则（CPS）	构成对证书的创建、颁发、管理和使用的治理框架的若干文档之一。
认证路径（Certification Path）	一个有序的证书序列（包含路径中起始对象的公钥），通过处理该序列可获得末端对象的公钥。
策略限定符（Policy qualifier）	依赖于策略的信息，可能与CP标识符共同出现在X.509证书中。该信息可能包含可用CPS或依赖方协议的URL地址，也可能包含证书使用条款的文字。
数字证书	指的是用作识别签名者身份的数字签名，和签名者识别签名的数字证书。
电子签名	具有识别签名人身份和表明签名人认可签名数据的功能的技术手段。

数字签名	通过使用非对称密码加密系统对电子记录进行加密、解密变换来实现的一种电子签名。
电子签名人	是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的人。
电子签名依赖方	是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的人。
私钥（电子签名制作数据）	在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。
公钥（电子签名验证数据）	是指订户验证电子签名的数据。
订户	从电子认证服务机构接收证书的实体，也被称为证书持有人。在电子签名应用中，订户即为电子签名人。
依赖方	依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。

1.6.2 缩写

缩写	全称	中文翻译
CA	Certificate Authority	电子认证服务机构，证书颁发机构
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
SSL	Secure Sockets Layer	加密套接层协议
CRL	Certificate Revocation List	证书撤消列表
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
OCSP	Online Certificate Status Protocol	在线证书状态协议
PIN	Personal Identification Number	个人身份识别码
PKCS	Public KEY Cryptography Standards	公共密钥密码标准

PKI	Public Key Infrastructure	公共密钥基础设施
RA	Registration Authority	注册审核服务机构
RFC	Request For Comments	请求评注标准（一种互联网建议标准）

2. 信息发布与管理

2.1 信息库

天威诚信的信息库包括以下内容：证书策略（CP）、电子认证业务规则（CPS）、用户协议、依赖方协议、根证书和中级 CA 证书等。

2.2 认证信息的发布

天威诚信在官方网站 https://www.itrus.com.cn/repository 发布信息库，该网站是天威诚信发布所有信息最重要、最及时、最权威的渠道。

天威诚信的认证业务规则可从天威诚信的官方网站获取；天威诚信提供证书撤销列表（CRL）和在线证书状态查询服务（OCSP），订户或依赖方可实时查询证书的状态信息。

另外，天威诚信也将会根据需要采取其他可能的形式进行信息发布。

天威诚信将“itrus.com.cn”和“itrus.cn”作为 CAA 查询标签。

2.3 发布的时间或频率

天威诚信的 CP 和 CPS 可通过信息库 7*24 获得。

天威诚信至少每年发布一次 CP 和 CPS。

天威诚信会定期跟进 CA/B 论坛 BR 标准的变化，并及时调整 CP/CPS 来符合 BR 标准的变化。

天威诚信签发的订户证书一经签发即可下载，订户可通过邮件或天威诚信提供的证书服务站点获得已签发的证书，并通过 OCSP 对证书状态进行查询。

天威诚信对于订户证书的 CRL 至少 96 小时发布一次；对于子 CA 证书的 CRL 至少 12 个月发布一次，如果有子 CA 证书吊销的情况，则天威诚信在 24 小时之内更新发布 CA 证书的 CRL。在紧急的情况下，信息库其他内容的发布时间和频率，由天威诚信独立做出决定，这种发布应该是即时的、高效的，并且是符合国家法律的要求的。

2.4 信息库访问控制

天威诚信信息库中的信息以只读的方式对外提供查询和获取。天威诚信通过网络安全防护、系统安全设计、安全管理制度确保这些信息只有授权人员才能对信息库进行操作，如增加、删除、修改和发布信息库。

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

天威诚信颁发的数字证书符合 X.509 标准、RFC 5280 标准、CA / Browser 论坛 BR 及 EV Guidelines 的要求。分配给证书持有者实体的甄别名（Distinguished Name），采用 X.500 标准命名方式。天威诚信颁发的 SSL 服务器证书，所有的域名或 IP 地址都添加到主题别名中，而通用名为主域名或 IP 地址，必须是一个出现在主题别名中的域名或 IP 地址。

3.1.2 对名称有意义的要求

订户证书所包含的名称具有一定的代表性意义，其中包含的主体识别名称，应当能够明确确定证书持有机构以及所要标识的网络主机服务器、或互联网域名，并且可以被依赖方识别。主体识别名称应当符合法律法规等相关规定的要求。

3.1.3 订户的匿名或伪名

本 CPS 所述证书的订户在进行证书申请时不能使用匿名或伪名。

3.1.4 理解不同名称形式的规则

天威诚信签发的数字证书符合 X.509 V3 标准，甄别名格式遵守 X.500 标准。

3.1.5 名称的唯一性

在天威诚信信任域内，不同订户的证书的主体甄别名不能相同，必须是唯一的。但对于同一订户，天威诚信可以用其唯一的主体甄别名为其签发多张证书。

3.1.6 商标的识别、鉴别和角色

天威诚信签发的证书不包含任何商标，不验证申请人的商标使用权。

当发生商标纠纷时，天威诚信有权拒绝证书申请和吊销已签发的证书。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

证书申请者必须证明持有与所要注册公钥相对应的私钥，证明的方法是在证书申请消息中包含数字签名（PKCS#10）。

3.2.2 机构身份和域名的鉴别

3.2.2.1 机构身份的鉴别

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

任何由第三方提供的证明该组织确实存在的资料，例如由政府机构发放的合法性证明（组织机构代码证、工商营业执照等信息），以及其它被认可的权威组织提供的证明资料。

1. 通过电话、邮政信函、被要求的证明文件或者与此类似的其它方式确认该组织资料信息的真实性，申请人是否得到足够的授权以及其它需要验证的信息。

2. 由天威诚信进行的现场访问及现场核查政府机构出具的有效文件。

天威诚信可使用上述 1-2 项文件中的内容或通信来验证组织机构的地址和申请人被授权的信息。

可通过对物业账单、银行对账单、信用卡账单、政府出具的税务文件或天威诚信认为可靠的其他形式的身份证明来核实订户的地址（但不是订户的身份）确认授权申请的真实性，即代表组织机构申请证书的人是经过授权的。确认方式可以是加盖公章的机构授权委托书及经办人身份文件；或通过第三方得到的联系电话、邮箱地址、信函地址等方式与机构取得联系，确认申请人的身份和机构授权事实。

天威诚信必须根据订户申请证书类型的不同，参考 CA/B 论坛的 BR 及 EV Guidelines 执行不同的身份鉴别方法。

3.2.2.2 DBA/商业名称的鉴别

不适用。

3.2.2.3 国家的鉴别

如果天威诚信签发的证书主题中包含国家代码，则天威诚信通过下列方法中的一种或多种方式进行验证：

(a)从 DNS 记录中获取到的 IP 地址所在国家；

(b)申请域名的 CCTLD。

(c)通过 3.2.2.1 中的方法查询政府机构或其他可信第三方数据源确认申请者的地址所在的国家。

3.2.2.4 域名的确认和鉴别

天威诚信将对在证书中列出的所有域名进行所有权的验证。根据 CABForum 上的要求，天威诚信不对申请的内部名称签发证书，并且不会将域名所有权验证委托给任何第三方进行。对于域名的验证，被验证的实体可以是订户的母公司、子公司或联营公司，天威诚信必须通过以下方式来确认域名权限：

3.2.2.4.1 通过邮件、短信或邮寄邮件方式发送随机值，然后接收一个使用该随机值的确认响应，确认申请人对 FQDN 的所有权。随机值必须发送到标识为域名联系人的电子邮件地址或'admin'，'administrator'，'webmaster'，'hostmaster'或'postmaster'，后面是（“@”）之后跟着授权域名、电话号码或邮件地址。（依据 BR 中 3.2.2.4.2 和 3.2.2.4.4 的域名验证办法）

3.2.2.4.2 通过在“/.well-known/pki-validation”目录下对约定的信息进行改动，确认订户对 FQDN 的所有权。（依据 BR 中 3.2.2.4.18 的域名验证办法）

3.2.2.4.3 通过在 DNS CNAME、TXT 或 CAA 记录中是否存在已约定的随机值，以确认订户对域名的所有权。要求：1）授权域名;或者 2）一个前缀以下划线字符开头的授权域名。（依据 BR 中 3.2.2.4.7 的域名验证颁发）

注：使用以上方法验证了对 FQDN 的所有权，CA 也可为其他相同顶级域名颁发证书。此方法适用于验证通配符域名。

3.2.2.5 IP 地址的确认和鉴别

根据 CABForum 的要求，天威诚信不为 IANA 标注的 Reserved IP 签发证书。天威诚信将对在证书中列出的所有 IP 进行所有权的验证。天威诚信必须通过以下方式来确认 IP 权限：

3.2.2.5.1 通过在“/.well-known/pki-validation”目录下对约定的信息进行改动，确认订户对 IP 的控制权（依据 BR 中 3.2.2.5.1 的 IP 验证办法）；

3.2.2.5.2 通过邮件、短信或邮寄邮件方式发送随机值，然后接收一个使用该随机值的确认响应，确认申请人对 IP 的控制权。随机值必须发送到标识为 IP 联系人的电子邮件地址、电话号码或邮件地址（依据 BR 中 3.2.2.5.2 的 IP 验证办法）；

3.2.2.5.3 通过 IP 地址上的反向 IP 查找获得与 IP 地址关联的域名，然后使用 BR 第 3.2.2.4 节允许的方法验证对 FQDN 的控制，确认申请人对 IP 地址的控制（依据 BR 中 3.2.2.5.3 的 IP 验证办法）；

3.2.2.5.4 通过拨打标识为 IP 联系人的电话号码并获得确认申请人验证 IP 地址请求的响应，确认申请人对 IP 地址的控制（依据 BR 中 3.2.2.5.5 的 IP 验证办法）；

3.2.2.5.5 天威诚信不为 IP 地址签发 DV 和 EV 证书;

3.2.2.6 通配符域名的确认和鉴别

对于通配符域名，天威诚信验证通配符右侧的域名。确保该域名是明确归属于某一商业实体、社会组织或政府机构等机构，并经过合法的注册获得的。

天威诚信拒绝通配符右侧的域名直接是顶级域名、公共后缀或由域名注册管理机构控制的域名的证书申请证书，除非订户能够证明其完全控制该域名的所有命名空间。

必要时，天威诚信需采取其他独立的审核方法，以确定域名的归属权，如需要订户提供相应的协助，订户不能以任何理由拒绝这种请求。

3.2.2.7 数据源及其准确性

3.2.2.7.1 鉴证数据源

天威诚信将鉴证数据来源（注册机构及查询方式等）在官方网站上公布，如有需要，请访问 https://www.itrus.com.cn/repository 。

天威诚信在使用新的鉴证数据来源之前，将首先在此文件中进行更新披露。

3.2.2.7.2 数据源准确性

在使用任何数据源作为可靠的数据源之前，天威诚信对该来源的可靠性、准确性，及更改或伪造可抗性进行评估，遵守 CAB 论坛 BR 第 3.2.2.7 节、EV Guidelines 第 11.11 节对数据源的要求，并考虑以下因素：

1．所提供信息的使用年限；

2．信息来源的更新频率；

3．数据提供者和数据收集的目的；

4．公众对数据可用性的可访问性；

5．伪造或改变数据的相对难度。

天威诚信将从权威第三方数据提供机构获取数据，并进行 3.2 章节的鉴证工作。

3.2.2.8 认证机构授权（CAA）

对于天威诚信颁发的公共可信任的 SSL 证书，在证书签发之前，天威诚信将对待签发证书主题别名扩展项中的每一个 dNSName 做 CAA 记录检查。天威诚信将在查询 CAA 记录的 8 小时内，向证书申请者发放证书。若超过 8 小时，天威诚信将重新进行 CAA 检查。

天威诚信根据 RFC8659 的规定处理“issue”、“issuewild”及“iodef”的属性标签：若“issue”、“issuewild”标签中不包含“itrus.com.cn”和“itrus.cn”，则天威诚信不签发对应的证书；若 CAA 记录中出现“iodef”标签，则天威诚信与申请者沟通后决定是否为其颁发证书。

天威诚信以下列 CAA 记录查找失败情况作为可签发证书的条件：

1) 在非天威诚信的基础设施中查询 CAA 记录失败；

2) 至少尝试过一次重新查找 CAA 记录；

3) 域名所在区域不存在指向 ICANNA 根区域的 DNSSEC 验证链。

3.2.3 个人身份的鉴别

在本 CPS 下，天威诚信目前只签发 SSL 证书，不签发任何个人身份证书及邮件证书。在申请 OV 和 EV 型 SSL 证书时，如需进行个人信息的核验，天威诚信使用如下鉴别方法：

1．订户应提交至少一个当前有效的政府签发的身份证件（护照、驾驶执照、国家身份证件或同等证件类型）的可辨认副本来验证申请人的姓名；天威诚信将通过政府机构或第三方可信数据源进行核验；

2．面对面审核，或者以其他电话、邮政信函等方式确认身份资料等信息的真实性。

3．对于委托他人进行申请的，要提交被充分授权的书面证明文件。

3.2.4 没有验证的订户信息

天威诚信签发的证书不包含未经验证的订户信息。

3.2.5 授权确认

如果订户申请的证书包含的主体身份信息是一个组织，天威诚信会使用第 3.2.2.1 中列出的来源来验证可靠的通讯信息，并使用这个信息与订户代表或在订户组织内的权威来源（包括但不限于订户的主要营业部、公司办公室、人力资源部门）确认证书申请的真实性。

如果订户以书面形式指定了证书申请的个人，则天威诚信将不接受任何超出本规范的证书请求。天威诚信可以请订户提供经其核实并盖章的书面授权信函。

3.2.6 互操作准则

天威诚信可以与其他电子认证服务机构进行互操作，要求该电子认证服务机构的 CP 及 CPS 必须符合天威诚信 CP 的要求，并与天威诚信签署相关协议。

如果国家法律法规对其有要求，天威诚信将严格遵守。

截止目前，天威诚信未签发任何交叉认证的证书。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规的密钥更新的标识与鉴别

天威诚信支持在有效期内的证书订户进行密钥更新请求，订户可以选择生成一个新的密钥对来替换正在使用的密钥对或即将到期的密钥对。

收到密钥更新请求后，天威诚信会使用订户提交的新请求创建一个新的证书，新证书内容与旧证书的主题信息保持一致，证书的有效期与原证书相同。

3.3.2 吊销之后的密钥更新的标识与鉴别

天威诚信对吊销后证书不进行密钥更新。

3.4 吊销请求的标识与鉴别

在天威诚信的证书业务中，证书吊销请求可以来自订户，依赖方，应用软件供应商。另外，当天威诚信认为必要的时候（参见本 CPS 第 4.9.1.1 节所述相关情形），有权发起吊销订户证书。

订户通过一定的方式，如邮件、传真、电话等，向天威诚信提交请求，天威诚信通过与证书保障级别相应的通讯方式与订户联系，确认要吊销证书的人或组织确实是订户本人，或者其授权者。依据不同的环境，通讯方式可以采用下面的一种或几种：电话、传真、e-mail、邮寄或快递服务。

4. 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

证书申请实体包括个人、组织或实体。

4.1.2 注册过程与责任

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

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

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

申请者应自行产生密钥对，产生 PKCS#10 证书请求文件并递交给天威诚信，并支付相应费用。

订户有责任向天威诚信提供真实、完整和准确的证书申请信息和资料。

天威诚信承担对订户提供的证书申请信息与身份证明资料的一致性检查工作，同时承担相应审核责任。

根据《中华人民共和国电子签名法》的规定，申请者未向天威诚信提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、天威诚信造成损失的，承担相应的法律及赔偿责任。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

当天威诚信及其注册机构接受到订户的证书申请后，应按本 CPS 第 3.2 节的要求，对订户进行身份识别与鉴别。

天威诚信会根据或之前由于怀疑网络钓鱼或其他诈骗用途或顾虑而拒绝的证书请求或吊销的证书，建立和维护 SSL 证书高风险数据库列表，在接受证书申请时将会查询该列表信息。对于列表中出现的订户，天威诚信将执行额外的验证。

天威诚信会对待签发证书主题别名扩展项中的每一个 dNSName 做 CAA 记录检查，并按照 3.2.2.8 中的检查方法和结果判定是否批准该证书申请。

天威诚信验证订户提交的申请材料后，根据验证结果决定接受、拒绝该申请或要求申请者补充递交相关材料。天威诚信在处理证书申请过程中，将通过有效手段确保证书信息与正确的申请信息相符，并将证书签发给正确的申请者。

在证书签发前，若天威诚信根据本 CPS 第 3.2 节指定来源获得的数据或证明文件不超过 398 天且该信息未发生变化，则天威诚信可重复使用该鉴证数据或证明文件，核实 OV 型和 EV 型证书中的信息。对于 DV 类型证书，天威诚信不重复使用鉴证数据。

4.2.2 证书申请批准和拒绝

完成本 CPS 第 4.2.1 节识别与鉴别的执行后，天威诚信可根据鉴证结果批准或拒绝申请。如果拒绝申请，则应该通过适当的方式、在合理的时间内通知 SSL 证书申请者。

如果天威诚信认为签发证书可能会给天威诚信带来争议、法律纠纷或者损失，天威诚信也可能拒绝证书申请。

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

4.2.2.1 证书申请的批准

如果符合下述条件，天威诚信可以批准证书申请：

1) 根据本 CPS 第 3.2 节的规定，已经成功识别和认证所有必需的订户信息；

2) 订户接受或者没有反对订户协议的内容和要求；

3) 订户已经按照规定支付了相应的费用。

4.2.2.2 证书申请的拒绝

如果发生下列情形，天威诚信有权拒绝证书申请：

1) 根据本 CPS 第 3.2 节的规定，不能完成识别和认证所有必需的订户信息；

2) 订户不能根据要求提供所需要的身份证明材料；

3) 订户反对或者不能接受订户协议的有关内容和要求；

4) 订户没有或者不能够按照规定支付相应的费用；

5) 天威诚信或者注册机构认为批准该申请将会对天威诚信带来争议、法律纠纷或者损失。

对于拒绝的证书申请，天威诚信通知申请者证书申请失败。

4.2.3 处理证书申请的时间

天威诚信在收到证书请求的合理时间内开始处理证书申请，在客户提交的申请资料齐全的情况下，天威诚信将在 5 个工作之内完成证书申请处理。

4.3 证书签发

4.3.1 证书签发中 CA 的行为

天威诚信的根 CA 在签发证书时，要求天威诚信授权的内部可信角色，经过严格的审批流程后，直接进行证书签名操作。

天威诚信在签发订户证书前，将确保注册机构已对所接收的证书申请的真实性完成验证。

使用 CA 进行证书签发时，RA 会将证书申请信息打包为数据包，在对数据包进行签名和加密后，将其发送给 CA。CA 通过验证数据包上的签名，鉴别数据包的完整性，并根据签名者的信息鉴别发送者的身份和权限。鉴别通过后，CA 将使用私钥对证书申请签名生成订户证书。

4.3.2 通知订户证书的签发

天威诚信的证书签发系统签发证书后，将直接或者通过 RA 通知订户证书已被签发，并告知订户如何获得证书。

4.4 证书接受

4.4.1 构成接受证书的行为

在订户发生以下任意一种行为后，天威诚信认为订户接受了证书：

1) 订户下载或安装了证书；
2) 天威诚信注册机构在订户的允许下，代替订户下载证书，并把证书通过邮件方式发送给订户；
3) 在天威诚信将证书获取通知发送给订户后，在 24 小时内订户未表示拒绝。

4.4.2 CA 对证书的发布

天威诚信把证书发给订户视为证书的发布，天威诚信同时会根据谷歌，苹果的要求，将证书发布在多个 Certificate Transparency Log 服务器上。。

4.4.3 CA 对其他实体的通知

对于签发的证书，天威诚信及其注册机构不通知其他实体。

4.5 密钥对和证书的使用

密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受相关法律和天威诚信 CPS 的保障。

4.5.1 订户的私钥和证书的使用

订户在提交了证书申请并接受了天威诚信所签发的证书后，均视为已经同意遵守与天威诚信、依赖方有关的权利和义务的条款。密钥对和证书不应用于其规定的、批准的用途之外的目的。

订户应保护其私钥避免未经授权的使用，并且不再使用过期或被吊销的证书。订户以外的各方不得存档订户的私钥。

4.5.2 依赖方公钥和证书使用

依赖方应在依赖证书前考虑总体情况和损失风险。

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

1) 获得数字签名对应的证书及信任链；

2) 确认该签名对应的证书是依赖方信任的证书；

3) 通过查询 CRL 或 OCSP 确认该签名对应的证书是否被吊销；

4) 证书的用途适用于对应的签名；

5) 使用证书上的公钥验证签名。

6) 考虑本 CPS 或其它地方规定的其它信息

以上条件不满足的话，依赖方有责任拒绝签名信息。

4.6 证书更新

证书更新是指在订户证书到期之前，证书的主题信息不发生改变的情况下，为订户签发一张新证书。

4.6.1 证书更新的情形

对于天威诚信签发的订户证书，证书到期前 30 天起可进行证书更新。到期前 30 天内，订户可访问天威诚信证书服务站点或到注册机构进行证书更新的申请。对于 SSL 证书，天威诚信接受订户在不更新密钥时申请更新证书。

4.6.2 请求证书更新的实体

同 4.1.1。

4.6.3 证书更新请求的处理

同本 CPS 第 4.2 节。

4.6.4 签发新证书时对订户的通知

同本 CPS 第 4.3.2 节。

4.6.5 构成接受更新证书的行为

同本 CPS 第 4.4.1 节。

4.6.6 CA 对更新证书的发布

同本 CPS 第 4.4.2 节。

4.6.7 CA 对其他实体的通知

同本 CPS 第 4.4.3 节。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

同本 CPS 第 3.3 节。

4.7.2 请求证书密钥更新的实体

同本 CPS4.1.1。

4.7.3 证书密钥更新请求的处理

天威诚信对证书密钥更新请求的处理通过证书更新请求处理流程完成，参见本 CPS 第 4.6.3 节的描述。

4.7.4 签发新证书时对订户的通知

同本 CPS 第 4.3.2 节。

4.7.5 构成接受密钥更新证书的行为

同本 CPS 第 4.4.1 节。

4.7.6 CA 对密钥更新证书的发布

同本 CPS 第 4.4.2 节。

4.7.7 CA 对其他实体的通知

同本 CPS 第 4.4.3 节。

4.8 证书变更

4.8.1 证书变更的情形

证书变更是指现有证书中的主题信息不变，证书有效期不变，其他信息发生变化而申请颁发新证书。当证书变更时，天威诚信会对证书信息进行重新验证，如果证书申请资料在可用期内（即申请资料及鉴证数据在 398 天之内），则可以直接使用申请资料，天威诚信仅对发生变化的信息进行鉴证。若上述证书申请资料超过最大有效期则天威诚信会对所有信息重新鉴证审核，通过后重新颁发新的证书。

4.8.2 请求证书变更的实体

只有在有效期内的证书订户或证书订户的授权代表可以请求证书变更。天威诚信不向所有订户提供证书修改服务。

4.8.3 证书变更请求的处理

同本 CPS 第 4.2 节。

4.8.4 签发新证书时对订户的通告

同本 CPS 第 4.3.2 节。

4.8.5 构成接受变更证书的行为

同本 CPS 第 4.4.1 节。

4.8.6 CA 对变更证书的发布

同本 CPS 第 4.4.2 节。

4.8.7 CA 对其他实体的通告

同本 CPS 第 4.4.3 节。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

4.9.1.1 订户证书吊销的原因

当发现以下情况之一时，天威诚信将在 24 小时之内将证书吊销：

1) 订户以书面形式请求吊销证书；

2) 订户通知天威诚信最初的证书请求未得到授权且不追加授权行为；

3) 天威诚信获得了证据，证明与证书公钥对应的订户私钥遭到了损害，或不再符合 Baseline Requirements 第 6.1.5 节及第 6.1.6 节的相关要求；

4) 天威诚信获得证据，证书中所包含的域名或 IP 地址的控制权验证已不再可靠；

5) 天威诚信获得了证书遭到误用的证据；

6) 天威诚信获悉订户违反了订户协议、CP/CPS 中的一项或多项重大责任；

7) 天威诚信获悉任何表明 FQDN 或 IP 地址的使用不再被法律许可（例如，某法院或仲裁员已经吊销了域名注册人使用域名的权力，域名注册人与申请人的相关许可及服务协议被终止，或域名注册人未成功更新域名）；

8) 天威诚信获悉某通配符证书被用于鉴别具有欺骗误导性的子域名；

9) 天威诚信获悉证书中所含信息出现重大变化；

10) 天威诚信获悉证书的签发未能符合 Baseline Requirements 要求，或天威诚信的 CP 或 CPS；

11) 天威诚信认为任何出现在证书中的信息不准确、不真实或具有误导性；

12) 天威诚信由于任何原因停止运营，且未与另一家 CA 达成协议以提供证书吊销服务；

13) 天威诚信依据 Baseline Requirements 签发证书的权力失效，或被吊销或被终止，除非其继续维护 CRL/OCSP 信息库；

14) 天威诚信的 CP 或 CPS 要求吊销订户证书；

15) 天威诚信发现了已经被论证的方法证明订户的私钥被泄露，该方法可以通过公钥简单的计算出私钥（如 Debian 弱密钥，参考 http://wiki.debian.org/SSLkeys），或者有明确的证据证明订户用来生成私钥的方法是有缺陷的；

16) CPS 中职责的履行被延迟或受不可抗力的阻碍；自然灾害；计算机或通信失败；法律、规章或其它法律的改变；政府行为；或其它超过个人控制的原因并且对他人信息构成威胁的；

17) 天威诚信已经履行催缴义务后，订户仍未缴纳服务费。

4.9.1.2 中级 CA 证书吊销的原因

若出现以下情况中的一种或多种，天威诚信应在 7 天之内吊销中级 CA 证书：

1) 中级 CA 正式书面申请吊销；

2) 中级 CA 发现并通知根 CA 初始提交的证书申请未经过授权且不追加授权行为；

3) 天威诚信获得了证据，证明与证书公钥对应的中级 CA 私钥遭到了损害，或不再符合 Baseline Requirements 第 6.1.5 节及第 6.1.6 节的相关要求；

4) 天威诚信获得了证书遭到误用的证据；

5) 天威诚信获悉中级证书的签发未能符合 Baseline Requirements 要求，或中级 CA 未能符合 CP/CPS；

6) 天威诚信认为任何出现在证书中的信息不准确、不真实或具有误导性；

7) 天威诚信由于任何原因停止运营，且未与另一家 CA 达成协议以提供证书吊销服务；

8) 天威诚信依据 Baseline Requirements 签发证书的权力失效，或被吊销或被终止，除非其继续维护 CRL/OCSP 信息库；

9) 本 CP 或相应的 CPS 要求吊销中级 CA 证书。

4.9.2 请求证书吊销的实体

请求证书吊销的实体可为订户、天威诚信及其注册机构、或经司法机构授权的司法人员。此外，依赖方、应用软件提供商，防病毒机构或其他的第三方可以提交证书问题报告，告知天威诚信有合理理由吊销证书。

4.9.3 吊销请求的流程

4.9.3.1 订户主动提出吊销申请

1) 订户向天威诚信提交吊销申请表和身份证明材料，同时说明吊销原因；

2) 天威诚信按照本 CPS 第 3.4 节的规定进行证书吊销请求的鉴别；如鉴证通过则进行吊销处理。

3) 天威诚信完成吊销后及时将其发布到证书吊销列表；

4) 天威诚信通过电话、邮件等适当方式，通知订户证书被吊销及被吊销的理由；若未能联络订户时，在必要的情况下，天威诚信对吊销的证书将通过网站进行公告；

5) 天威诚信提供 7*24 小时的证书吊销申请服务，订户可通过天威诚信官方网站公布的联系方式申请证书吊销。

4.9.3.2 订户被强制吊销证书

1) 当天威诚信有充分的理由确信出现本 CPS 第 4.9.1.1 节中会导致订户证书被强制吊销的情形时，天威诚信将通过内部流程申请吊销证书；

2) 在天威诚信的根证书或中级 CA 证书相对应的私钥出现安全风险时，经国家电子认证服务主管部门批准后可直接进行订户证书吊销；

当依赖方如司法机构、应用软件提供商、防病毒机构等第三方提请证书问题报告时，天威诚信应组织调查并根据调查结果来决定是否吊销证书，如果通过调查确认证书需要吊销，则从收到证书问题报告到证书吊销不超过 4.9.1 中规定的期限；

3) 在证书吊销后，天威诚信或注册机构将通过适当的方式，包括邮件、电话等，通知最终订户证书已被吊销及被吊销的理由；若未能联络订户时，在必要的情况下，天威诚信对吊销的证书将通过网站进行公告；

4.9.4 吊销请求宽限期

天威诚信不支持吊销请求宽限期。

4.9.5 CA 处理吊销请求的时限

天威诚信将在接到证书问题报告的 24 小时内，对证书问题报告内容进行调查，以决定是否吊销或采取其它适当的行动处理机制。

如果天威诚信通过调查确认证书需要吊销，则从收到证书问题报告到证书吊销不超过 4.9.1 中规定的期限。

4.9.6 依赖方检查证书吊销的要求

依赖方应当检查他们所信任的证书是否被吊销。检查方式是通过查询天威诚信提供的 OCSP 服务或 CRL 查询。

4.9.7 CRL 发布频率

对于订户证书，天威诚信的 CRL 发布周期不超过 96 小时，即在 4 天内发布最新 CRL。订户 CRL 的有效期最长不会超过 10 天。

对于中级 CA 证书，天威诚信的 CRL 发布周期不超过 12 个月。如果吊销中级 CA 证书，天威诚信在吊销后 24 小时之内更新 CRL。中级根 CRL 的有效期最长不会超过 12 个月。

4.9.8 CRL 发布的最大滞后时间

天威诚信的 CRL 发布最大滞后时间为 CRL 签发之后的 24 小时内。

4.9.9 在线状态查询的可用性

天威诚信向证书订户和依赖方提供在线证书状态查询服务。天威诚信的 OCSP 服务符合 RFC6960 的要求，并使用天威诚信专门的 OCSP 服务证书签名。

4.9.10 在线状态查询要求

用户可以自由进行在线状态查询，天威诚信没有设置任何的查询限制。

天威诚信提供 Get 和 Post 两种方式的 OCSP 查询服务。

对于订户证书，天威诚信至少每 4 天更新 OCSP 信息，OCSP 响应的最长有效期为 7 天。

对于中级 CA 证书，天威诚信至少每 12 个月更新 OCSP 信息。当吊销中级 CA 证书时，天威诚信会在 24 小时内更新 OCSP 信息。

对于未签发的证书的状态查询请求，天威诚信 CA 不返回“good”状态。

4.9.11 吊销信息的其他发布形式

除了通过 CRL 或 OCSP 服务器提供证书吊销信息查询外，天威诚信不提供吊销信息的其它发布形式。

4.9.12 密钥损害的特别要求

无论是订户还是注册机构，发现证书密钥受到安全损害时，应立即向天威诚信提出吊销证书的请求。如果 CA 的密钥（根 CA 或中级 CA 密钥）安全被损害或者怀疑被损害，天威诚信将在合理的时间内用合式的方式及时通知订户和依赖方。

4.9.13 证书挂起的情形

天威诚信不支持证书挂起。

4.9.14 请求证书挂起的实体

不适用。

4.9.15 挂起请求的流程

不适用。

4.9.16 挂起的期限限制

不适用。

4.10 证书状态服务

天威诚信通过 CRL 和 OCSP 提供证书状态查询服务，并确保对查询请求有合理的响应时间和并发处理能力。

4.10.1 操作特征

对于被吊销的证书，天威诚信在该证书到期前不删除其在 OCSP 服务器中的吊销记录；在该证书到期前不删除其在 CRL 中的吊销记录。天威诚信的证书状态查询以网络服务的形式提供：

- CRL 采用 HTTP 协议提供；
- OCSP 符合 RFC6960。

4.10.2 服务可用性

天威诚信的 CRL、OCSP 证书状态服务均为 7*24 可用，且会最大限度地减少停机时间。响应时间不超过 10 秒（EV 证书的 CRL 响应时间不超过 3 秒；此处响应时间不包括因为订户网络等原因导致的获取数据缓慢的耗时），即：在网络允许的情况下，订户和依赖方能够实时获得证书状态查询服务的响应。

4.10.3 可选特征

无。

4.11 订购结束

订购结束包含以下情况：

1) 证书到期后没有进行更新；

2) 证书到期前被吊销。

一旦用户在证书有效期内终止使用天威诚信的证书认证服务，天威诚信在批准其终止请求后，将实时把该订户的证书吊销，并按照 CRL 发布策略进行发布；天威诚信详细记录吊销证书的操作过程并定期将订购结束后的证书及相应订户数据进行归档。

4.12 密钥托管与恢复

天威诚信不托管任何 SSL 证书订户的私钥，因此也不提供密钥恢复服务。

4.12.1 密钥托管与恢复的策略与行为

不适用。

4.12.2 会话密钥的封装与恢复的策略与行为

不适用。

5. 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

天威诚信的运营场地位于北京市海淀区上地八街 7 号院 4 号楼 4 层，天威诚信的机房和系统建设按照下列标准实施：

1) GB/T 25056-2010《信息安全技术证书认证系统密码及其相关安全技术规范》
2) 国密局[2010]7 月《电子政务电子认证基础设施建设要求》
3) GB50174-2008《电子信息系统机房设计规范》
4) GB6650-86：《计算机机房活动地板的技术要求》
5) GB9361－2011《计算机站场地安全要求》
6) GB2887-2011《计算机场地通用规范》
7) GB50222-95《建筑内部装修设计防火规范》
8) GB50016—2014《建筑设计防火规范》
9) GB50116-2013《火灾自动报警系统设计规范》
10) GB50057－2010《建筑物防雷设计规范》
11) GB5054－2011《低压配电设计规范》
12) GBJ19－2003《采暖通风与空气调节设计规范》
13) YD/T754-95《通讯机房静电防护通则》

5.1.1.1 公共区

天威诚信场地的入口处、办公区域、辅助和支持区域属于公共区，采用访问控制措施，可以使用身份识别卡控制出入。

5.1.1.2 服务区

服务区是 RA 操作人员、管理人员的工作区，需要同时使用身份识别卡和指纹鉴别才可以进入，人员进出服务区要有日志记录。

5.1.1.3 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。此区域必须使用身份识别卡和指纹鉴别才可以进入。

5.1.1.4 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。

核心区使用身份识别卡和指纹鉴别才可以进入；屏蔽机房两名可信人员同时使用身份识别卡和指纹鉴别才可以进入，确保在屏蔽区内单个人员无法完成敏感操作。

5.1.2 物理访问控制

天威诚信的服务区、管理区、和核心区的门禁系统可实现对各层门进出的控制，具备以下功能：

- 采用身份识别卡和指纹鉴别的控制方式控制每道门的进入；
- 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。

整个区域还有视频监控系统，对场地内外的重要通道实行 7*24 小时不间断录像。所有录像资料至少保留 12 个月，以备查询。

5.1.3 电力与空调

天威诚信有安全、可靠的电力供电系统及电力备用系统以确保系统 7*24 小时正常供电及在出现供电系统出现供电中断是能够提供正常的服务。另外，天威诚信还具有加热/通风/空调系统控制运营设施中的温度和湿度。

天威诚信机房采用不间断供电系统 UPS，可提供至少 8 小时的电力供应。机房区域内采用了防静电措施，实现机柜、服务器、网络设备等电位连接和接地。

机房的空调采用风冷式冷凝器机组，室外风冷式冷凝器机组放置在顶楼。机房室内设计温度 23±2℃。

5.1.4 水患防治

天威诚信机房部署有漏水报警系统，一旦发生水患系统将立即报警，通知有关人员采取应急措施。

5.1.5 火灾防护

天威诚信机房内各区域均采用了烟感和温感火灾探测器，并安装了火灾自动报警系统及气体自动灭火系统，该系统具有自动和手动操作两种启动方式。

在自动状态下，当防护区发生火警时，火灾报警控制器接到防护区两独立火灾报警信号后立即发出联动信号。经过 30 秒时间延时，火灾报警控制输出信号，启动灭火系统，同时，报警控制器接收压力讯号器反馈信号，防护区内门灯显亮，避免人员误入。

当防护区经常有人工作时，可以通过防护区门外的手动/自动转换开关，使系统自动状态转换到手状态，当防护区发生火警时，报警控制器只发出报警信号，不输出动作信号。由值班人员确认火警，按下控制面板或击碎防护区外紧急启动按钮，即可立即启动系统，喷发气体灭火剂。

另外，根据国家的有关消防要求，天威诚信在管理区内设置了紧急出口，紧急出口设有消防门，门外部没有开启装置，仅能从内部打开。紧急出口有视频监控设备进行实时监控。当消防门被打开时，监控系统将报警通知值班人员。

5.1.6 介质存储

天威诚信对储存产品软件和数据、归档、审计或备份信息的介质保存在安全设施中，这些设施受到适当的物理和逻辑访问控制的保护，只允许授权人员的访问，并防止这些介质受到意外损坏（如水、火灾和电磁）。

5.1.7 废物处理

天威诚信对不再使用的敏感文件和材料在处理之前将其切成碎片，使信息无法恢复。加密设备在作废处置前根据制造商提供的方法先将其初始化再进行物理销毁。

5.1.8 异地备份

天威诚信对关键数据、审计日志数据进行异地备份，该备份地点的安全级别不低于实际生产环境。

5.2 程序控制

5.2.1 可信角色

天威诚信在提供电子认证服务过程中，将能从本质上影响证书的颁发、使用、管理和吊销等涉及密钥操作的职位都视为可信角色。这些角色包括但不限于：

1) 密钥与密码设备管理人员，负责维护 CA 密钥和证书生命周期，负责管理加密设备；

2) 鉴证和客服人员，负责订户信息录入、审核数字证书申请信息并完成鉴证和审批工作，并提供相关支持服务；

3) 系统维护人员，负责对 CA 系统的硬件和软件实施日常维护，并监控和排查故障；

4) 安全管理人员，负责场地安全、日常安全管理工作；

5) 安全审计人员，负责对业务操作行为进行审计；

6) 人力资源管理人员，负责对关键岗位人员实施可信度背景调查、安全管理等工作。

5.2.2 每项任务需要的人数

天威诚信对业务操作流程有严格的控制程序，按照本 CPS 第 5.2.4 节的职责分割策略，确保个人不能同时承担多项重要角色，且敏感操作需要多个可信赖的人共同完成，这包括：

1) 屏蔽区场地访问设置为双人进出模式；

2) 保存根密钥激活数据的保险柜设置为双人开启模式；

3) 加密设备的管理权限按照 5 选 3 方式进行分割，并由不同可信人员持有；

4) 重要系统的超级管理员密码分割成两部分由不同可信人员持有；

5) 鉴证过程至少两名可信人员参与。

5.2.3 每个角色的识别与鉴别

对于可信人员的物理访问，天威诚信通过门禁卡和指纹识别进行鉴别，并确定相应的权限。

对于进行订户证书生命周期管理的天威诚信、注册机构的可信人员，他们使用相应的数字证书访问系统，完成证书管理工作。

对于系统维护人员，他们使用各自的账户和密码通过堡垒机登录系统进行维护工作。

5.2.4 需要职责分割的角色

为保证系统安全，天威诚信对如下角色实施职责分离策略：（NO 代表不可兼任）：

	密钥与密码设备管理人员	鉴证和客服人员	系统维护人员	安全管理人员	安全审计人员	人力资源管理人员
密钥与密码设备管理人员	——	NO	NO	NO	NO	NO
鉴证和客服人员	NO	——	NO	NO	NO	NO
系统维护人员	NO	NO	——	NO	NO	NO
安全管理人员	NO	NO	NO	——	NO	NO
安全审计人员	NO	NO	NO	NO	——	NO
人力资源管理人员	NO	NO	NO	NO	NO	——

5.3 人员控制

5.3.1 资格、经历和无过失要求

天威诚信对承担可信角色的工作人员的资格要求如下：

1) 具备良好的社会和工作背景；
2) 遵守国家法律、法规，无违法犯罪记录；
3) 遵守天威诚信有关安全管理的规范、规定和制度；
4) 具有认真负责的工作态度和良好的从业经历；
5) 具备良好的团队合作精神。

5.3.2 背景审查程序

为了确保担任可信角色的人员能够胜任有关工作，天威诚信将按照《天威诚信可信雇员政策》对雇佣的人员先进行背景调查。背景调查符合法律法规的要求，尽可能地通过相关组织、部门进行人员背景信息的核实，并保护个人隐私。

所有的可信员工和申请调入的可信员工都必须书面同意对其进行背景调查。背景调查分为：基础调查和高级调查。

基础调查包括对工作经历、教育方面的调查。

高级调查除包含基础调查项目外，还包括对犯罪记录的调查。

调查程序包括：

1) 人力部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。
2) 人力部门通过电话、网络等形式对其提供的材料的真实性进行鉴定。
3) 在背景调查中，对发现以下情形的人员，可直接拒绝其成为可信人员的资格：
   - 存在捏造事实或资料的行为；
   - 借助不可靠人员的证明；
   - 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的行为。
4) 人力部门完成调查后，将结果上报主管相关工作的领导进行批准。

5) 天威诚信与员工签订保密协议，以约束员工不许泄露 CA 证书服务的所有保密和敏感信息。

5.3.3 培训要求

为了使有关人员能胜任其承担的工作，天威诚信对所有可信角色岗位的员工制定有专门的培训计划，培训内容包括：

1) 天威诚信颁布的证书策略和电子认证业务规则；
2) PKI 基本知识；
3) 天威诚信运营体系、技术体系和安全管理制度；
4) 工作职责和岗位说明。

5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受天威诚信组织的培训一次。对于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。此外，天威诚信将根据机构系统升级、策略调整等要求，不定期的要求人员进行继续培训。

5.3.5 工作岗位轮换周期和顺序

天威诚信在职人员的工作岗位轮换周期和顺序将依据内部工作安排决定。

5.3.6 未授权行为的处罚

天威诚信建立并维护一套管理办法，对未授权行为进行适当的处罚，包括解除或终止劳动合同、调离工作岗位、罚款、批评教育等方式。这些处罚行为符合法律法规的要求。

5.3.7 独立合约人的要求

天威诚信目前未聘用外部独立合约人从事认证相关的工作。

5.3.8 提供给人员的文档

提供给人员的文档通常包括证书策略、电子认证业务规则、员工手册、岗位职责说明书、工作流程和规范等。

5.4 审计日志程序

5.4.1 记录事件的类型

天威诚信对如下几类事件进行记录：

- CA 证书及密钥生命周期的管理事件，包括，
  - 密钥生命周期的管理事件，例如生成、备份、存储、恢复、和归档。
  - 证书的申请、批准、更新、吊销等。生成证书 CRL 和 OCSP。
  - 密码设备生命周期的管理事件，例如接收、使用、和销毁。
  - 更换证书配置文件。

这些记录由认证系统的系统日志和操作人员的手工记录组成。

- 订户证书生命周期的管理事件，包括，
  - 证书的申请、批准、更新、吊销等。
  - 证书的所有验证活动。
  - 成功或失败的证书操作。
  - 生成证书 CRL 和 OCSP。

  这些记录由认证系统的系统日志和操作人员的手工记录组成。
- 系统操作事件，包括，
  - 系统启动和关闭。
  - 系统权限的创建、删除、变更、和密码修改。

  这些记录由认证系统的系统日志和操作人员的手工记录组成。
- 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。

- 在证书系统上安装、更新或删除软件。
- 系统崩溃，硬件故障和其他异常。
- 防火墙记录的安全事件。

这些记录由系统的自动日志和操作人员的手工记录组成。

- 天威诚信场地的工作记录，如，
  - 授权人员进出。
  - 非授权人员进出及陪同人。
  - 场地设施的维护操作。

这些记录由系统的自动日志和操作人员的手工记录组成。

日志记录一般包括如下信息：

- 每个日志记录的日期和时间。
- 对于自动日志记录，登记的序列号或序号。
- 做日志记录的实体的身份。
- 日志记录的内容。

5.4.2 处理日志的周期

对于系统的自动日志和操作人员的手工记录，天威诚信每月进行一次检查和汇总。

对系统安全日志，每月进行一次跟踪处理，检查违反策略和规范的重大事件。

5.4.3 审计日志保存期限

天威诚信妥善保存电子认证服务的审计日志，与证书相关的审计日志，在证书失效后至少保留 2 年。

5.4.4 审计日志的保护

天威诚信的系统日志备份到日志服务器，手工电子记录备份到 SVN，手工纸质记录归档保存到管理区内。

天威诚信采取了物理和逻辑的访问控制方法，以确保只有授权人员才能接近这些审查记录，严禁未授权的访问、阅读、修改和删除等操作。

5.4.5 审计日志备份程序

天威诚信的系统日志实时同步到日志服务器，并且每天备份到异地。

5.4.6 审计收集系统

对于电子审计信息，天威诚信的日志服务器可对如下日志进行收集和归档：

1) 证书管理系统；

2) 证书签发系统；

3) 证书受理系统；

4) 访问控制系统；

5) 数据库系统；

6) 其他需要审计的系统。

对于纸质审计信息，则有专门的文件柜来实现收集归档。

5.4.7 对导致事件主体的通知

当天威诚信发现被攻击时，将记录攻击者的行为，在法律许可的范围内追溯攻击者，保留采取相应对策措施的权利。天威诚信有权决定是否对事件相关实体进行通知。

5.4.8 脆弱性评估

根据 CA/B Forum NCSSR 的要求，天威诚信每 3 个月对系统进行一次漏洞扫描，每年进行一次渗透测试，同时根据审计发现的安全事件，天威诚信将每年对系统、物理场地、运营管理等方面进行安全脆弱性评估，并根据评估报告采取措施，以降低运营风险。

5.5 记录归档

5.5.1 归档记录的类型

天威诚信对以下几类记录进行归档：

1) 证书系统建设和升级文档；

2) 证书；

3) 订户证书生命周期管理记录；

4) 审计记录；

5) CP 和 CPS；

6) 员工资料，包括但不限于背景调查、录用、培训等资料；

7) 各类外部、内部评估文档。

5.5.2 归档记录的保存期限

- 对 CA 证书及密钥生命周期管理记录，保留至 CA 证书失效后 2 年。
- 对订户证书生命周期管理记录，保留至订户证书失效后 2 年。
- 安全事件记录保留 2 年。

5.5.3 归档文件的保护

天威诚信对各种电子、纸质形式的归档文件，都有安全的物理和逻辑保护措施和严格的管理程序，确保归档了的文件不会被损坏，防止非授权的访问、修改、删除或其它的篡改行为。

5.5.4 归档文件的备份程序

对于系统生成的电子归档记录，将定期进行备份，备份文件进行异地存放；对于手工生成的电子记录，归档到 SVN 备份。

对于书面的归档资料，不需要进行备份，但需要采取严格的措施保证其安全性，防止对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳要求

天威诚信的日志未采用时间戳技术。

5.5.6 归档收集系统

对于系统生成的电子记录，实时同步到日志服务器，并且每天备份到异地。

对于手工生成的电子记录，由 SVN 服务器完成收集备份工作。

对于书面的归档资料，收集归档到管理区内。

5.5.7 获得和检验归档信息的程序

天威诚信采取了物理和逻辑的访问控制方法，以确保只有授权人员才能接近这些归档信息，严禁未授权的访问、阅读、修改和删除等操作。

5.6 CA 密钥的更替

天威诚信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 CA 证书和订户证书，其失效时间不超过根证书的失效时间，任何由 CA 证书签发的订户证书，其失效时间不超过 CA 证书的失效时间。

CA 证书对应的密钥对，当其寿命超过本 CPS 规定的最大生命期时，天威诚信将启动密钥更新流程，替换已经过期的 CA 密钥对。天威诚信密钥变更按如下方式进行：

1) 上级 CA 将在其私钥到期时间小于下级 CA 密钥的生命期之前停止签发新的下级 CA 证书（“停止签发日期”）。
2) 产生新的密钥对，签发新的上级 CA 证书。
3) 在“停止签发证书的日期”之后，对于批准的下级 CA 或订户证书请求，将采用新的 CA 密钥签发证书。
4) 上级 CA 继续利用原来的 CA 私钥签发 CRL 直到利用原私钥签发的最后的证书过期为止。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

天威诚信已规定相应的事故和损害处理程序，制定各种应急处理方案，包括但不限于：

- 电力系统应急方案；
- 消防应急方案；
- 网络与信息系统应急方案；
- 密钥应急处理方案等。

相关岗位的工作人员将按照相关制度和应急方案，定期进行应急演练。

5.7.2 计算机资源、软件和/或数据损坏处理程序

天威诚信对业务系统及其他重要系统的资源、软件和/或数据进行了备份，并制定了相应的应急处理流程，当发生网络故障、系统、软件被破坏、数据库故障等现象或因不可抗力造成灾难时，天威诚信将按照灾难恢复计划实施恢复。

5.7.3 实体私钥损害处理程序

对于实体证书私钥的损害，天威诚信将按照如下程序进行处理：

1) 当证书订户发现实体证书私钥损害时，订户必须立即停止使用其私钥，并立即访问天威诚信或向注册机构的证书服务站点吊销其证书，或者立即通过电话等方式通知天威诚信或注册机构吊销其证书，并按照相关流程重新申请新的证书。天威诚信将按本 CPS 第 4.9 节发布证书吊销信息。
2) 当天威诚信或注册机构发现证书订户的实体证书私钥受到损害时，天威诚信或注册机构将立即吊销证书，通知证书订户；订户必须立即停止使用其私钥，并按照相关流程重新申请新的证书。天威诚信将按本 CPS 第 4.9 节发布证书吊销信息。
3) 当天威诚信的根 CA 或中级 CA 出现私钥损害时，天威诚信将按照密钥应急方案进行紧急处理，并立即通过邮件方式通知依赖方及应用软件供应商如 Mozilla/Microsoft/Apple/Google/360 等。

5.7.4 灾难后的业务存续能力

一旦物理场地出现了重大灾难，天威诚信将根据业务连续性计划在 72 小时内恢复其 CA 系统的运行，使其可以向订户提供证书的查询和吊销服务；在 5 个工作日内天威诚信将恢复证书鉴证业务，允许订户申请新证书。

5.8 CA 或 RA 的终止

当天威诚信及其注册机构需要停止其业务时，将会严格按照《中华人民共和国电子签名法》及相关法规中对认证机构中止业务的规定要求进行有关工作。

在天威诚信终止前，必须：

1) 确定业务承接单位；

2) 起草终止声明；

3) 通知相关实体；

4) 处理存档文件记录；

5) 停止 CA 系统服务；

6) 存档相关系统日志；

7) 处理和存储敏感文档。

6. 技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

6.1.1.1 CA 密钥对的生成

天威诚信的密钥使用国家密码主管部门批准和许可的加密设备生成，该设备对密钥的生成、管理、存储、备份和恢复遵循 FIPS140-2 标准的相关规定。由于国家对于密码产品有严格的管理要求，而 FIPS140-2 标准并非是国家密码主管部门认可和支持的标准，因此 FIPS140-2 标准仅参照执行，是在通过国家密码主管部门鉴定、认证、并在国家密码管理政策许可前提下的选择性适用，具体参照设备制造商提供的资料。

CA 密钥对的生成过程，由天威诚信专门的密钥管理员和若干名可信雇员、以及独立第三方审计人员见证下，在天威诚信屏蔽机房按照天威诚信密钥生成规程完成。天威诚信密钥生成规程规定了 CA 密钥产生的流程控制及参加人员。

6.1.1.2 订户密钥对的生成

订户密钥对由订户自身的服务器或其它设备内置的密钥生成机制生成。如果订户申请时提交的是一个包含弱算法的 PKCS#10 申请文件，天威诚信会拒绝该申请，并建议用户生成新的密钥对。

天威诚信不替订户生成密钥对。

6.1.2 私钥传送给订户

不适用。

6.1.3 公钥传送给证书签发机构

订户或订户通过注册机构，将 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包，以电子文本的方式将公钥提交给天威诚信签发证书。当需要通过网络传送时将使用安全套接层协议（SSL）或其他安全加密方式。

6.1.4 CA 公钥传送给依赖方

天威诚信的公钥包含在天威诚信自签发的根 CA 证书和中级 CA 证书中，订户和依赖方可从天威诚信官网下载根 CA 证书和中级 CA 证书。

6.1.5 算法类型及密钥长度

天威诚信使用的密钥及算法信息如下：

根 CA 证书使用长度为 4096 位的 RSA 密钥及长度为 384 位的 ECC 密钥，签名算法为 SHA256RSA 和 SHA384ECDSA；

中级 CA 证书使用长度为 2048 位的 RSA 密钥和长度为 256 位的 ECC 密钥，签名算法为 SHA256RSA 和 SHA256ECDSA.

订户证书使用长度为 2048 位的 RSA 密钥和长度为 256 位的 ECC 密钥，签名算法为 SHA256RSA 和 SHA256ECDSA.

天威诚信将依据 BR 以及中国国家密码管理局发布的标准进行密钥算法及长度的调整。

6.1.6 公钥参数的生成和质量检查

公钥参数使用获得国家密码管理局许可资质的加密设备和硬件介质生成，并遵从这些设备的生成规范和标准。

对于参数质量的检查，由于使用获得国家密码管理局许可资质的加密设备和硬件介质生成和存储密钥，已经具备足够的安全等级要求。

6.1.7 密钥使用目的

天威诚信签发的 X.509v3 证书包含了密钥用法扩展项，其用法与 RFC 5280 标准相符。对于天威诚信在其签发证书的密钥用法扩展项内指明了的用途，证书订户必须按照该指明的用途使用密钥。

根 CA 密钥一般用于签发以下证书和 CRL：

1) 代表根 CA 的自签名证书；

2) 中级 CA 的证书、交叉证书；

3) 根 CA 和中级 CA 的 CRL（ARL）。

4) 特定用途的 PKI 体系功能证书（如 OCSP 证书）；

中级 CA 密钥一般用于签发以下证书和 CRL：

1) 订户证书；

2) 特定用途的 PKI 体系功能证书（如 OCSP 证书）；

3) 订户 CRL。

订户的密钥可以用于提供安全服务，如信息加密和签名等。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

天威诚信的密钥使用国家密码主管部门批准和许可的加密设备生成，该设备对密钥的生成、管理、存储、备份和恢复遵循 FIPS140-2 标准的相关规定。由于国家对于密码产品有严格的管理要求，而 FIPS140-2 标准并非是国家密码主管部门认可和支持的标准，因此 FIPS140-2 标准仅参照执行，是在通过国家密码主管部门鉴定、认证、并在国家密码管理政策许可前提下的选择性适用，具体参照设备制造商提供的资料。

CA 密钥对的生成过程，由天威诚信专门的密钥管理员及若干名可信雇员在天威诚信屏蔽机房按照天威诚信密钥生成规程完成。天威诚信密钥生成规程规定了 CA 密钥产生的流程控制及参加人员。

订户证书的密钥使用国家密码管理部门认可的密码模块生成和存储，订户应妥善保护、保管其密码模块，防止其失窃、丢失、损坏及被非授权的使用。

6.2.2 私钥多人控制（m 选 n）

天威诚信的各类 CA 私钥的生成、备份和恢复等操作采用多人控制机制，此机制通过加密设备的 5 选 3 分割管理权限实现，即将私钥的管理权限分割保存在 5 张 IC 卡中（称为秘密分割份额，或简称秘密分割），这 5 张 IC 卡由天威诚信 5 名可信雇员持有（称为秘密分管者），保存在天威诚信内部保险盒中。当需要使用管理员权限时，至少在其中 3 名秘密分管者在场并许可的情况下，插入管理员卡并输入 PIN 码，才能对私钥进行备份恢复等操作。当不使用时，这个被称为秘密分割份额存储在屏蔽机房的保险箱中。

天威诚信的 CA 私钥的激活需要由密钥管理者持有的用户管理 IC 卡。IC 卡保存在天威诚信屏蔽机房的保险盒中，直到要激活 CA 私钥时才使用。

6.2.3 私钥托管

天威诚信的根私钥和 CA 私钥不允许托管，也不向订户提供私钥托管服务。

6.2.4 私钥备份

天威诚信对根私钥和 CA 私钥进行备份，可分为两种，一是按照加密设备制造商提供的操作规范生成备份密文文件和备份恢复权限 IC 卡并保存到屏蔽机房的保险柜（或银行保管箱等安全等级不低于本地备份的场所）；一是按照加密设备制造商提供的操作规范生成克隆设备和管理员操作员 IC 卡并存放在屏蔽机房（或银行保管箱等安全等级不低于本地备份的场所）。

对于订户证书，如果存放证书私钥的密码模块允许私钥备份，天威诚信建议订户对私钥进行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改或泄露。

6.2.5 私钥归档

当天威诚信的 CA 密钥对超过使用期后，这些 CA 密钥对将归档保存至少 7 年。归档 CA 密钥对保存在本 CPS 第 6.2.1 节所述的硬件密码模块中。

天威诚信或注册机构不对订户证书的私钥进行归档，但如果订户存放证书私钥的密码模块允许私钥备份，天威诚信建议订户对私钥进行归档，并对归档的私钥采用口令或其它访问控制机制保护，防止非授权的泄露。

6.2.6 私钥导入、导出密码模块

天威诚信密钥对在硬件密码模块上生成，保存和使用。此外，为了实现恢复，天威诚信按照加密设备制造商提供的操作规范对 CA 密钥进行备份。另外天威诚信还有严格的密钥管理流程对 CA 密钥对复制进行控制。所有这些有效防止了 CA 私钥的丢失、失窃、修改、非授权的泄露、非授权的使用等。

对于订户证书，若使用的密码模块（软件或硬件）支持私钥的导出、导入，则天威诚信要求订户对导出、导入的私钥必须使用足够安全的口令进行保护，且订户需要确保导出的私钥不被丢失、失窃、修改、非授权的泄露、非授权的使用等。

6.2.7 私钥在密码模块的存储

天威诚信私钥以加密的形式存放在符合国家密码主管部门的要求硬件密码模块中，且私钥的使用也在硬件密码模块中进行。

对于订户证书，订户需将私钥保存在国家密码主管部门认可的密码模块中（包括 SSL 加速卡），且存放私钥的密码模块必须在订户其可控制的范围内，订户需要采取相应的安全手段防止对私钥的非授权访问、获取和使用，使用的手段包括私钥的使用受口令保护，服务器及密码模块位于安全可控的物理环境等。

6.2.8 激活私钥的方法

天威诚信 CA 私钥存放在硬件密码模块中，激活需要按本 CPS 第 6.2.2 节使用加密设备的操作员权限实现。当需要使用 CA 私钥时（在线或离线），需要密钥管理员提供操作员 IC 卡才能完成。

保存在密码模块中的订户证书私钥需在用户输入口令（或 PIN 码）或指纹等密钥保护信息（激活数据）后才能被激活和使用。

6.2.9 解除私钥激活状态的方法

对于天威诚信私钥，当 CA 系统向密码模块发出退出登录或密码管理软件向密码模块发出关闭指令，或存放私钥的硬件密码模块断电,，私钥进入非激活状态。

订户解除私钥激活状态由其自行决定，当服务程序关闭、系统注销或系统断电后私钥即进入非激活状态。

6.2.10 销毁私钥的方法

在天威诚信私钥生命周期结束后，天威诚信将 CA 私钥继续保存在一个备份硬件密码模块中，并进行归档，其他的 CA 私钥备份被安全销毁。同时，所有用于激活私钥的 PIN 码、IC 卡等也必须被销毁。归档的 CA 私钥在其归档期限结束后，需在多名可信人员参与的情况下安全销毁。CA 私钥的销毁将确保 CA 私钥从硬件密码模块中彻底删除，不留有任何残余信息。

对于订证书私钥，若不再使用，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。若私钥对应的公钥证书被吊销、到期作废后，还需要用于信息解密的，最终用户应该妥善保存一定期限，以便于解开加密信息。若私钥无需再保存，则将通过私钥的删除、系统或密码模块的初始化来销毁。

6.2.11 密码模块的评估

天威诚信使用国家密码管理局批准和许可的密码产品，密码模块的评估由国家密码管理局负责。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

天威诚信对证书公钥进行归档，证书存放在数据库中并进行异地备份，归档数据定期进行完整性校验。

6.3.2 证书操作期和密钥对使用期限

CA 证书的最长有效期不超过 25 年，订户 SSL 证书的有效期最长为 398 天。

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。

6.4 激活数据

6.4.1 激活数据的产生和安装

天威诚信私钥的激活数据按照加密设备制造商提供的操作规范，由加密设备产生。

如果订户证书私钥的激活数据是口令，这些口令必须：

- 至少 8 位字符或数字；
- 至少包含一个字符和一个数字；
- 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。

天威诚信还建议订户使用双因素机制（如硬件+密码，生物识别设备+密码等）来控制私钥的激活。

6.4.2 激活数据的保护

对于 CA 私钥的激活数据，天威诚信按照可靠的方式由可信人员掌管，存储在天威诚信屏蔽机房保险盒中。

订户的激活数据必须在安全可靠的环境下产生，必须进行妥善保管，或者记住以后进行销毁，不可被他人所获悉。如果证书订户使用口令或 PIN 码保护私钥匙，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法窃取。

6.4.3 激活数据的其他方面

存有天威诚信数字认证中心 CA 私钥、运营设备证书私钥的激活数据的 IC 卡，通常保存在天威诚信的屏蔽机房内，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在天威诚信两名可信人员的监督下进行。

通常情况下订户证书私钥的激活数据由订户自己产生、保管，不应传送给其他人员，若私钥激活数据因特别的原因需要进行传送时，订户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。

对于申请证书的订户激活数据的生命周期，建议如下：

1、订户用于申请证书的口令，申请成功后失效。

2、用于保护私钥或者 IC 卡、USB Key 的口令，建议订户根据业务应用的需要随时予以变更，使用期限超过 3 个月后应要进行修改。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

CA 系统的信息安全管理，按照国标《证书认证系统密码及其相关安全技术规范》、工业和信息化部公布的《电子认证服务管理办法》，参照 ISO27001 信息安全管理体系要求，以及其他相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。主要的安全技术和控制措施包括：身份识别和验证、逻辑访问控制、网络访问控制等。

对每位拥有系统（包括 CA 系统、RA 系统）业务操作权限的可信人员实行严格的双因素验证机制，即访问时同时采用用户名、口令以及数字证书双因素登录方式。

对系统运维人员，通过堡垒机登录系统实施操作，确保 CA 软件和数据文件安全可信，不会受到未经授权的访问。

核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。这种分离可以阻止除指定的应用程序外对网络的访问。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 CA 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通过口令访问 CA 数据库。

6.5.2 计算机安全评估

天威诚信的 CA 系统及其运营环境通过了国家密码管理局和工信部的审查，获得了相应资质。

6.6 生命周期技术控制

6.6.1 系统开发控制

天威诚信的 CA 软件是从具备资质的中国商业 CA 软件提供商购买。天威诚信通过内部变更控制流程来控制证书认证系统的上线工作，并要求运维人员严格按照审批和上线流程执行，以保证系统的安全性和可用性：

1) 系统软件必须在测试环境测试成功后，再申请部署于生产环境；

2) 申请部署时需要提供 changelog、测试报告、部署说明等文档；

3) 部署上线前根据规范要求进行审批；

4) 变更部署前进行有效的在线备份；

5) 变更部署后应立即进行测试，通过测试后方可对外服务。

天威诚信自主开发鉴证系统来对接 RA API 接口；鉴证系统开发使用的软硬件在安全可控的环境内，开发和测试流程均根据天威诚信已定义和文档记录的规范进行。该系统在进行上线之前也需要通过内部变更控制流程，参考上述要求，由运维人员按照规范执行上线流程。

6.6.2 安全管理控制

天威诚信已制定了各种安全策略、管理制度与流程对认证系统进行安全管理。

认证系统的信息安全管理，严格遵循国家密码管理局的有关运行管理规范进行操作。

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安全和使用，任何修改和升级会记录在案。

天威诚信定期对系统进行安全检查，用来识别设备是否被入侵，是否存在安全漏洞等。

6.6.3 生命周期的安全控制

天威诚信通过内部变更控制流程来控制证书认证系统的研发和上线工作，确保该系统安全可靠。

6.7 网络的安全控制

天威诚信的认证系统采用防火墙进行系统的访问控制，采用 IDS\IPS 进行网络的攻击防御，使用堡垒机对远程登录进行权限管理，使用路由器进行网络分层控制。

天威诚信所有与证书签发相关的系统均采用多因素认证。

认证系统应仅对指定的服务或人员开放，且只开放最小的访问权限。

认证系统应定期进行安全漏洞扫描、安全设备配置审核，并对相关日志进行审计。

天威诚信的网络安全控制符合 CA/B Forum NCSSR。

6.8 时间戳

天威诚信认证系统签发的数字证书、CRL 包含有日期信息，且这些日期信息是经过数字签名的。

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

认证系统所取的时间源是国家可信标准时间。

7. 证书、CRL 和 OCSP

7.1 证书

天威诚信签发的证书符合 ITU-T X.509v3 和 RFC 5280：Internet X.509 公钥基础设施证书和 CRL 结构。

天威诚信通过 CSPRNG 生成长度为至少 64 位的非序列性的证书序列号。

7.1.1 版本号

证书符合 X.509 V3 版证书格式，版本信息存放在证书版本格式栏内。

7.1.2 证书扩展项

天威诚信颁发证书的内容和扩展项参考如下表格：

	根证书	中级证书	订户证书
版本	X.509 版本号 V3	X.509 版本号 V3	X.509 版本号 V3
签名算法	SHA256RSA SHA384ECDSA	SHA256RSA SHA256ECDSA	SHA256RSA SHA256ECDSA
使用者	用来标识签发证书的 CA 的 X.500 DN 名字，包括国家、机构、部门、和通用名。	用来标识签发证书的 CA 的 X.500 DN 名字，包括国家、机构、部门、和通用名。	DV 证书：包含通用名； OV 证书：包含国家，机构，通用名。 EV 证书： 和 CA/B Forum 上 EVGL 中第 9.2 章节保持一致。
密钥长度	4096bits RSA	2048bits RSA	2048bits RSA
	384bits(P-384) ECC	256bits(P-256) ECC	256bits(P-256) ECC
基本约束	CA 证书的基本限制扩展项中的主体类型被设为 CA	CA 证书的基本限制扩展项中的主体类型被设为 CA	订户证书的基本限制扩展项的主体类型设为最终实体 (End-Entity)
增强密钥算法	无此属性	无此属性 （若 2019.1.1 以后创建中级 CA 证书，则必须包含此扩展）	服务器身份验证 (1.3.6.1.5.5.7.3.1) 客户端身份验证 (1.3.6.1.5.5.7.3.2)
证书策略	无	包含了颁发者 CA 的 CPS 发布地址	包含颁发者指定的 policy Identifier 和 CA/B

			Forum 中保留的 Policy Identifier。包含了颁发者 CA 的 CPS 发布地址
CRL 分发点	无	由天威诚信指定的 CRL 发布点扩展项，依赖方可根据该扩展项提供的地址和协议下载 CRL。	由天威诚信指定的 CRL 发布点扩展项，依赖方可根据该扩展项提供的地址和协议下载 CRL。
颁发机构信息访问	无	包含了颁发者的 OCSP 响应地址。(accessMethod = 1.3.6.1.5.5.7.48.1) 包含了颁发者证书的访问地址。(accessMethod = 1.3.6.1.5.5.7.48.2)	包含了颁发者的 OCSP 响应地址。(accessMethod = 1.3.6.1.5.5.7.48.1) 包含了颁发者证书的访问地址。(accessMethod = 1.3.6.1.5.5.7.48.2)
密钥用法	密钥用法指明已认证的公开密钥用于何种用途。对于 CA 证书的密钥用法，该项为关键扩展。	密钥用法指明已认证的公开密钥用于何种用途。对于 CA 证书的密钥用法，该项为关键扩展。	对于订户证书，该项为可选项，RSA 算法证书密钥用法为 Digital Signature, Key Encipherment (a0)，ECC 算法证书密钥用法为 Digital Signature (80)
证书起始时间	证书的生效日期和时间，使用 UTC/GMT+08:00	证书的生效日期和时间，使用 UTC/GMT+08:00	证书的生效日期和时间，使用 UTC/GMT+08:00
证书终止时间	证书的失效日期和时间，使用 UTC/GMT+08:00	证书的失效日期和时间，使用 UTC/GMT+08:00	证书的失效日期和时间，使用 UTC/GMT+08:00

7.1.3 算法对象标识符

天威诚信签发的证书中，密码算法的标识符为 sha256RSA、sha384RSA、sha256ECDSA、和 sha384ECDSA。

7.1.4 名称形式

天威诚信签发的证书名称形式的格式和内容符合 RFC5280 的要求，且符合 CA/B Forum Baseline Requirements 中 7.1.4 章节的要求。

7.1.5 名称限制

无规定。

7.1.6 证书策略对象标识符

证书策略对象标识符同本 CPS 第 1.2 节。

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 CRL

天威诚信定期签发 CRL，供订户和依赖方查询使用。

7.2.1 版本号

天威诚信的证书吊销列表符合 X.509 v2 的版本及格式要求。

7.2.2 CRL 和 CRL 条目扩展项

与 ITU X.509 和 RFC5280 规定一致。

- **CRL 的版本号：**用来指定 CRL 的版本信息，天威诚信采用的是和证书 X.509 V3 对应的 CRL X.509 V2 版本。
- **签名算法：**天威诚信采用 sha256RSA 和 sha256ECDSA 签名算法。
- **颁发者：**指定签发机构的 DN 名，由国家、省、市、机构、单位部门和通用名等组成。
- **生效时间：**指定一个日期/时间值，用以表明本 CRL 生成的时间。
- **更新时间：**指定一个日期/时间值，用以表明下一次 CRL 将要生成的时间（本标准强制使用该域）。
- **吊销证书列表：**指定已经吊销的证书列表。本列表中含有证书的序列号和证书被吊销的日期和时间。
- **颁发机构密钥标识符（Authority Key Identifier）：**本项标识用来验证在 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。
- **下次发布时间（Next CRL Publish）：**指定一个日期/时间值，用以表明下一次 CRL 将要发布的时间。
- **吊销原因代码（Reason Code）:** 用于中级 CA 证书 CRL，指出吊销原因。

  天威诚信使用以下原因代码，作为中级 CA 证书的吊销原因：

  Code 2，CA 私钥泄露

  Code 4, 证书废止（由于误签发或其他不合规的原因而被吊销）

  Code 5， 终止使用（由于中级证书不再使用而吊销。）

7.3 OCSP

天威诚信认证系统提供 OCSP 服务，签发的 OCSP 响应符合 RFC6960 标准，该标准定义了一种标准的请求和响应信息格式以确认证书状态。

7.3.1 版本号

RFC6960 定义的 OCSP V1 版本。

7.3.2 OCSP 扩展项

与 RFC6960 一致。

7.3.3 OCSP 请求和响应处理

一个 OCSP 请求包含以下数据：协议版本、服务要求、目标证书标识和可选的扩展项等。

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天威诚信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、已吊销、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
- 响应产生的时间
- 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，这些错误信息没有天威诚信证书签发者密钥的签名。出错信息可能包括：

- 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. 认证机构审计和其他评估

8.1 评估的频率和情形

天威诚信执行如下审计和评估：

1) 每季度进行一次运营工作质量评估，以保证运营服务的可靠性、安全性和可控性。

2) 每季度执行一次鉴证内审，抽取至少 3%的证书样本。

3) 每年根据 CA/B Forum 上 BR 的要求，进行一次 BR 自评估工作。

4) 每年对物理控制、密钥管理、操作控制、鉴证执行等情况执行一次审计，以确定实际发生情况是否与预定的标准、要求一致，并根据审查结果采取行动。

5) 每年进行一次运营风险评估工作，识别内部与外部的威胁，评估威胁事件发生的可能性及造成的损害，并根据风险评估结果，制定并实施处置计划。

6) 除了内部审计和评估外，天威诚信还聘请独立的审计师事务所，按照 WebTrust for CA， WebTrust for CA - Extended Validation SSL 和 WebTrust for CA - SSL Baseline with Network Security 三个规范进行外部审计和评估。

8.2 评估者的资质

内部审计和评估，由天威诚信内部审计评估小组执行此项工作。

外部审计，由具备以下的资质机构负责：

- 必须是经许可的、有执业资格的评估机构,在业界享有良好的声誉；
- 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作；
- 具备检查系统运行性能的专业技术和工具；
- 具备 WebTrust 审计的资质。

8.3 评估者与被评估者之间的关系

内部审计人员与本机构的系统管理员、业务管理员、业务操作员的工作岗位不能重叠。

外部评估者和天威诚信之间是相互独立的关系，双方无任何足以影响评估客观性的利害关系。

8.4 评估的内容

内部审计工作涉及以下内容：

1) 运营工作流程和制度是否得到严格遵守；

2) 是否严格按 CP、CPS、业务规范和安全要求开展认证业务；

3) 各种日志、记录是否完整，是否存在问题；

4) 是否存在其他可能存在的安全风险。

第三方审计师事务所按照 WebTrust For CA ,EV SSL, SSLBR & Network Secruity 规范的要求，对天威诚信进行独立审计。

8.5 对问题与不足采取的措施

对于本机构内部审计结果中的问题，由审计评估小组负责监督相关责任部门的改进情况。

第三方审计师事务所评估完成后，天威诚信按照其工作报告进行整改，并接受再次审计和评估。

8.6 评估结果的传达与发布

内部审计结果向本机构各责任部门进行正式通报，对可能造成的订户安全隐患，天威诚信将及时向订户通报。

第三方审计师事务所评估完成后，向天威诚信提供审计报告，天威诚信完成整改工作和再评估后，天威诚信将在官网公布最终审计结果。

8.7 其他评估

根据《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》等要求，每五年接受主管部门的换证审查。

9. 其他业务和法律事务

9.1 费用

9.1.1 证书签发和更新费用

天威诚信可根据提供的电子认证相关服务向本机构的证书订户收取费用，具体收费标准根据市场和管理部门的规定自行决定。在收费标准范围内，即不超过收费标准的情况下，天威诚信有权根据市场状况，针对不同订户群体推出不同的收费策略或优惠措施。

如果天威诚信签署的协议中指明的价格和天威诚信公布的价格不一致，以协议中的价格为准。

9.1.2 证书查询费用

在证书有效期内，天威诚信不对证书查询收取专门的费用。如果用户提出特殊需求，可能需要支付额外的费用，将由天威诚信营销部门与用户协商收取。

9.1.3 证书吊销或状态信息的查询费用

天威诚信对吊销列表（CRL）的获取不收取费用。

天威诚信不对 OCSP 服务收取费用。

9.1.4 其他服务费用

如果天威诚信向订户提供证书存储介质及相关服务，天威诚信将在与订户或者其他实体签署的协议中指明该项价格。

9.1.5 退款策略

如果由于天威诚信的原因，造成订户合同无法履行、订户证书无法使用，天威诚信会将相关费用返还给订户。

9.2 财务责任

9.2.1 保险范围

天威诚信向证书订户提供证书使用保障。如果由于天威诚信的原因造成用户在使用证书过程中遭受损失，天威诚信将向证书订户、依赖方提供赔偿（具体情形参见本 CPS 第 9.9 节）。

9.2.2 其他资产

无规定。

9.2.3 对最终实体的保险或担保

天威诚信提供的电子认证服务保障的最终实体是指证书订户及证书依赖方。

最终实体可依据本 CPS 规定或生效的法律文书（如判决书、裁决书等）要求天威诚信承担相应的赔偿责任（法定或约定免责的除外）。

最终实体欲向天威诚信提出索赔，在证书有效期内产生的损失，应在知道或应当知道损失发生之日起三年内书面提出索赔申请；超出三年的，该索赔无效。

天威诚信对按照本 CPS 第 9.9 节规定对最终实体承担有限赔偿责任。

9.3 业务信息保密

9.3.1 保密信息范围

在天威诚信提供的电子认证服务中，以下信息视为保密信息：

1） 审计记录包括：本地日志、服务器日志、归档日志的信息，这些信息被天威诚信视为保密信息，只有安全审计员和业务管理员可以查看；除法律要求，不可在公司外部发布。

2） 其他由天威诚信和注册机构保存的个人和公司信息应视为保密，除法律要求，不可公布。

9.3.2 不属于保密的信息

天威诚信将以下信息视为不保密信息：

1） 由天威诚信发行的证书和 CRL 中的信息。

2） 由天威诚信支持、CPS 识别的证书策略中的信息。

3） 天威诚信许可的只有天威诚信订户方可使用的、在天威诚信网站公开发布的信息。

4） 其它天威诚信信息的保密性取决于特殊的数据项和申请。

9.3.3 保护保密信息的责任

天威诚信有妥善保管与保护本 CPS 第 9.3.1 节中规定的保密信息的责任与义务。

CA、注册机构、订户以及与认证业务相关的参与方等，都有义务按照本 CPS 的规定，承担相应的保护保密信息的责任，必须通过有效的技术手段和管理程序对其进行保护。

当保密信息的所有者出于某种原因，要求天威诚信公开或披露他所拥有的保密信息时，天威诚信应满足其要求；同时，天威诚信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，天威诚信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。

当天威诚信在任何法律、法规、法院以及其他公权力部门通过合法程序的要求下，必须提供本 CPS 中规定的保密信息时，天威诚信应按照法律、法规以及法院判决的要求，向执法部门公布相关的保密信息，天威诚信无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4 个人隐私保密

9.4.1 隐私保密方案

天威诚信尊重证书订户的资料的隐私权，保证完全遵照国家对隐私保护的相关规定及法律。同时，天威诚信将确保全体职员严格遵从内部工作相关制度和规定。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括：

1） 订户的有效证件号码如身份证号码、单位机构代码。

2） 订户的联系电话。

3） 订户的通信地址和住址。

4） 订户的银行帐号。

5） 与天威诚信、天威诚信注册机构签订的协议。

9.4.3 不被视为隐私的信息

不被视为证书订户的隐私信息包括但不限于以下信息：

1） 证书及证书状态信息。

2） 订户姓名、单位名称等。

3） 订户性别、单位性质等。

4） 订户通信地址的邮政编码。

5） 订户的电子邮箱。

6） 订户要求出现在证书中的信息。

9.4.4 保护隐私的责任

天威诚信及注册机构有妥善保管与保护本 CPS 第 9.4.2 节中规定的隐私信息的责任与义务。

9.4.5 使用隐私信息的告知与同意

天威诚信将采取适当的步骤保护证书订户的个人隐私，并将采取可靠的安全手段保护已存储的个人隐私信息。

天威诚信及其注册机构如需超出约定范围及用途使用证书订户的隐私信息，应事先告知证书订户并获得同意及授权；如未获得同意及授权，天威诚信不会将订户隐私信息透露给任意第三方。

9.4.6 依法律或行政程序的信息披露

依据法律、行政法规、规章、决定、命令等，由于司法执行或法律授权的行政执行需要，天威诚信及其注册机构有可能需要将有关信息在订户知晓或不知晓的情况下提供有关执法机关、行政执行机关。即使出现这种情形，天威诚信及其注册机构也将尽可能地保护客户隐私信息。

9.4.7 其他信息披露情形

对其他信息的披露受制于法律、订户协议。

9.5 知识产权

天威诚信享有并保留对天威诚信签发的数字证书以及天威诚信通过网站等各种渠道对外公布并提供的所有软件、资料、数据、信息等的著作权、专利权等知识产权。

天威诚信对数字证书系统软件享受所有权、名称权、利益分享权；对所签发的证书、证书吊销列表及其中的信息享有拥有知识产权。

天威诚信对本 CPS 及相关的运营管理工作文件拥有知识产权， 同时根据 Mozilla Root Policy，Mozilla 可在遵照 CC BY 4.0 协议的前提下使用本 CPS

证书订户对证书注册信息及签发给他的证书中包含的商标、服务标志或商品名和甄别名拥有知识产权。

证书中的密钥对是证书中主体对应实体或实体拥有者的知识产权。

9.6 陈述与担保

9.6.1 CA 的陈述与担保

天威诚信在提供电子认证服务活动过程中对订户的承诺如下：

1) 签发给订户的证书符合本 CPS 的所有实质性要求。
2) 将向证书订户通报任何已知的，将在本质上影响订户的证书的有效性和可靠性事件。

3) 将根据 CPS 的要求及时吊销证书。

4) 若天威诚信与订户无关联，则天威诚信与订户是合法有效且可执行的订户协议双方，该订户协议符合 CA/浏览器论坛发布的 Baseline Requirements 等要求；若天威诚信与订户为同一实体或有关联，则申请人代表已认可使用条款；

5) 针对所有未过期的证书的当前状态信息（有效或已吊销）建立及维护 24*7 公开的信息库。

证书公开发布后，天威诚信保证除未经验证的订户信息外，证书中的其他订户信息都是准确的。

天威诚信不负责评估证书是否在适当的范围内使用，订户和依赖方依照订户协议和依赖方协议确保证书用于允许使用的目的。

9.6.2 RA 的陈述与担保

天威诚信的注册机构在参与电子认证服务过程中的承诺如下：

1) 提供给证书订户的注册过程完全符合本 CPS 的所有实质性要求；

2) 拒绝签发证书后，将立即向证书申请者归还所付的全部费用；

3) 验证申请者对列在证书主题字段及主题别名扩展（或，仅针对域名而言，获得了拥有域名使用权或控制权人士的授权）中的域名及 IP 地址拥有使用权或控制权；

4) 确认申请人或申请人的代表已被授权代表申请人申请证书；

5) 验证证书中所包含的全部信息的准确性（organizationalUnitName 信息除外）；

6) 采取验证措施以减小证书主题“organizationalUnitName”中所包含的信息存在误导的可能性；

7) 根据本 CPS 第 3.2 节的要求验证申请人的身份；

8) 注册机构将按 CPS 的规定，及时向天威诚信提交吊销、更新等服务申请。

9.6.3 订户的陈述与担保

订户一旦接受天威诚信签发的证书，就被视为向天威诚信、注册机构及信赖证书的有关当事人作出以下承诺：

1) 订户在申请证书时，已仔细阅读、知悉并接受天威诚信数字证书使用协议中的责任条款和本 CPS 中的所有条款和条件。
2) 订户将在证书的有效期内使用证书私钥进行数字签名。
3) 订户在申请证书时向注册机构提供的信息、资料及所做的陈述都是真实、完整和准确的，如前述信息、资料或陈述发生任何改变将及时书面通知注册机构。如因订户故意或过失提供虚假、伪造等信息资料或陈述，或已提供的信息资料及陈述改变后未及时书面通知注册机构的，由订户自行承担全部法律责任。
4) 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，通知天威诚信或其授权的注册机构。
5) 与订户证书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（证书没有过期、吊销），证书的私钥为订户本身访问和使用。
6) 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数字证书使用协议。
7) 一经接受证书，订户就应当承担如下责任：始终保持对其私钥的控制；使用可信的系统；采取安全、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，如订户知道或者应当知道证书私钥或密码已经或者可能已经遗失、泄露、被篡改或被未经授权使用的，应及时书面告知有关各方并终止使用证书。
8) 不得拒绝任何来自天威诚信公示过的声明、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) 证书在本 CPS 中规定的使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的，不将证书用于使用目的以外的场合。
10) 对于 EV SSL 证书，订户有责任和义务保证只在证书中列出的主题别名对应的服务器中部署证书。

9.6.4 依赖方的陈述与担保

依赖方声明并承诺：并评估了在特定应用中信赖证书的适当性，不在证书适用目的以外的应用中信任证书。依赖方在参与电子认证服务过程中的承诺如下：

1) 在任何信赖行为发生前，已阅读 CPS 及依赖方协议，并同意遵守本 CPS 及依赖方协议的所有规定及约束，同意本 CPS 中有关天威诚信责任限制的规定。
2) 在信赖证书前，评估特定应用中信赖证书的适当性，了解证书的使用目的，并确认证书的使用是否在规定的范围和期限内、是否符合本 CPS 的规定。
3) 在信赖证书前，对证书的信任链进行验证。
4) 在信赖证书前，通过查询 CRL 或 OCSP 确认证书是否被吊销。
5) 一旦由于疏忽或者其他原因违背了合理检查的条款，依赖方愿意对就此给天威诚信造成的损失进行赔偿，并且承担因此造成的自身或他人的损失。
6) 不得拒绝任何来自天威诚信公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

9.6.5 其他参与者的陈述与担保

从事电子认证活动的其他参与者须承诺遵守本 CPS 的所有规定。

9.7 担保免责

有下列情形之一的，应免除天威诚信之担保责任，天威诚信不向任何方承担任何法律责任，包括但不限于赔偿责任及补偿责任。

1) 订户在申请和使用天威诚信数字证书时，有违反如下义务之一的：

- 订户有义务提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息；
- 订户应当妥善保管天威诚信所签发的数字证书载体和保护 PIN 码，不得泄漏 PIN 码或将数字证书载体随意交付他人；
- 订户在应用自己的密钥或使用数字证书时，应当使用可依赖、安全的系统；
- 订户知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知天威诚信及相关各方，并终止使用该电子签名；
- 订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度。不得将数字证书用于天威诚信规定使用范围外的其他任何用途使用；

- 订户必须在证书有效期内使用该证书；不得使用已失密或可能失密、已过有效期、被冻结、被吊销的数字证书；
- 订户有义务根据规定按时向天威诚信交纳服务费用。

2) 由于不可抗力原因而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。本项所规定之“不可抗力”，是指不能预见、不能避免并不能克服的客观情况，包括但不限于：

- 自然现象或者自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；
- 社会现象、社会异常事件或者政府行为，包括政府颁发新的政策、法律和行政法规，或战争、罢工、骚乱等社会异常事件。

3) 因天威诚信的设备或网络故障等技术故障而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。本项所规定之“技术故障”引起原因包括但不限于：

- 不可抗力；
- 关联单位如电力、电信、通讯部门而致；
- 黑客攻击；
- 天威诚信的设备或网络故障。

4) 天威诚信已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.8 有限责任

证书订户、依赖方因天威诚信提供的电子认证服务从事民事活动遭受损失，天威诚信将承担不超过本 CPS 第 9.9 节规定的有限赔偿责任。

9.9 赔偿

9.9.1 CA 的赔偿责任

天威诚信只对由于自身原因造成证书订户、依赖方的直接损失承担责任，对间接损失不承担责任。

天威诚信对于直接损失所负法律责任的上限为：每张服务器证书赔偿额不得超过证书市场购买价格的 10 倍，且每张 EV 服务器证书基于每个订户或每个依赖方的赔偿额不低于 2000 美金。

如天威诚信违反了本 CPS 第 9.6.1 节中的陈述，证书订户、依赖方等最终实体可以申请赔偿（法定或约定免责除外）。如出现下述情形，天威诚信承担有限赔偿责任：

1） 天威诚信将证书错误的签发给订户以外的第三方，导致订户或依赖方遭受损失的；

2） 在订户提交信息或资料真实、完整、准确的情况下，天威诚信签发的证书出现了错误信息，导致订户或依赖方遭受损失的；

3） 在天威诚信明知订户提交信息或资料存在虚假谎报的情况，但仍然向订户签发证书，导致依赖方遭受损失的；

4） 由于天威诚信的原因导致证书私钥被破译、窃取、泄露，导致订户或依赖方遭受损失的；

5） 天威诚信未能及时吊销证书，导致依赖方遭受损失的。

另外，天威诚信赔偿限制如下：

1） 天威诚信所有的赔偿义务不得高于天威诚信所承担的上限额度，这种赔偿上限可以由天威诚信根据情况重新制定，天威诚信会将重新制定后的情况立刻通知相关当事人。

2） 对于由订户或依赖方的原因造成的损失，天威诚信不承担任何赔偿责任，由订户或依赖方自行承担。

3） 在证书有效期内产生的损失，订户或依赖方应在知道或应当知道损失发生之日起三年内向天威诚信书面提出索赔；超出三年的，该索赔无效。

9.9.2 订户的赔偿责任

订户有下列情形之一，给天威诚信、依赖方造成损失的，应当承担赔偿责任：

1） 订户申请注册证书时，因故意、过失或者恶意提供不真实、不完整、不准确资料，造成天威诚信及其授权的注册机构或者第三方遭受损害；

2） 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、遗失而没有及时告知天威诚信及其注册机构以及不当交付他人使用造成天威诚信及其注册机构、第三方遭受损害；

3） 订户使用证书的行为，有违反本 CPS 及相关操作规范，或者将证书用于非本 CPS 规定的业务范围；

4） 自证书订户或者其他有权提出吊销证书的实体提出吊销请求，至天威诚信将该证书吊销信息予以发布期间，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，如果天威诚信按照本 CPS 的规范进行了有关操作，那么该证书订户必须承担吊销信息发布之前的所有损害赔偿责任；

5） 证书中的信息发生变更但未停止使用证书并及时通知天威诚信和依赖方；

6） 没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄露等；

7） 在得知私钥丢失或存在危险时，未停止使用证书并及时通知天威诚信和依赖方；

8） 超出证书有效期限使用证书的；

9） 订户的证书信息侵犯了第三方的知识产权；

10） 在规定的范围及目的外使用证书，如从事违法犯罪活动的。

9.9.3 依赖方的赔偿责任

在如下情况，依赖方对自身原因造成的天威诚信损失承担责任：

1） 依赖方没有执行天威诚信与依赖方的协议或本 CPS 规定的义务，导致天威诚信及注册机构或第三方遭受损害；

2） 未能依照本 CPS 规定对证书进行合理审核，导致天威诚信及注册机构或第三方遭受损害；

3） 依赖方没有对证书的信任链进行验证，导致天威诚信及注册机构或第三方遭受损害；

4） 依赖方没有通过查询 CRL 或 OCSP 确认证书是否被吊销，导致天威诚信及注册机构或第三方遭受损害。

5） 在不合理的情形或环境下信赖证书，如依赖方明知证书存在超范围、超期限使用的情形或证书已经或有可能被人窃取的情形，但仍然信赖证书。

9.10 有效期限与终止

9.10.1 有效期限

本 CPS 在生效日期零时正式生效，上一版本的 CPS 同时失效；本 CPS 在下一版本 CPS 生效之日或在天威诚信终止电子认证服务时失效。

9.10.2 终止

当天威诚信终止电子证书业务时，本 CPS 终止。

9.10.3 效力的终止与保留

本 CPS 终止后，其效力将同时终止，但对终止之日前发生的法律事实，本 CPS 中对各方责任的规定及责任免除仍然适用，包括但不限于 CPS 中涉及审计、保密信息、隐私保护、知识产权等内容，以及涉及赔偿的有限责任条款，在本 CPS 终止后继续有效。

当由于某种原因，如内容修改、与适用法律相冲突，CPS、订户协议、依赖方协议和其他协议中的某些条款失效后，不影响文件中其他条款的法律效力。

9.11 对参与者个别通告与沟通

天威诚信及其注册机构在必要的情况下，如在主动吊销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。

本 CPS 终止后，天威诚信将就文档失效的有关事项通知有关当事人。

9.12 修订

9.12.1 修订程序

经天威诚信安全策略委员会授权，CPS 编写小组每年至少审查一次本 CPS，确保其符合国家法律法规和主管部门的要求及相关国际标准，符合 CP 的要求，并符合认证业务开展的实际需要。

本 CPS 的修改和更新，由 CPS 编写小组提出修订意见，经天威诚信安全策略委员会批准后，由 CPS 编写小组负责完成修订，修订后的 CPS 经过天威诚信安全策略委员会批准后正式对外发布。

9.12.2 通知机制与期限

修订后的 CPS 经批准后将立即在天威诚信官网发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，天威诚信将在合理的时间内通知有关各方，合理的时间应保证有关方受到的影响最小。

9.12.3 必须修改业务规则的情形

天威诚信必须对本 CPS 进行修改的情形包括：CPS 中相关内容与管辖法律的不一致、国家监管部门对本机构认证业务有明确的更改或调整要求等。

9.13 争议解决

天威诚信、证书订户、依赖方等最终实体在电子认证活动中产生争议的，首先应根据协议友好协商解决；协商未果的，可通过法律途径解决。

任何与天威诚信或注册机构就本 CPS 所涉及的任何争议提起诉讼的，各方同意提交天威诚信工商注册所在地人民法院管辖处理。

9.14 管辖法律

天威诚信的 CPS 受国家已颁布的《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》法律法规管辖。

9.15 与适用法律的符合性

无论天威诚信的证书订户、依赖方等实体在何地居住以及在何处使用天威诚信的证书，本 CPS 的执行、解释和程序有效性均适用中华人民共和国的法律。任何与天威诚信或注册机构就本 CPS 所涉及的任何争议，均适应中华人民共和国法律。

9.16 一般条款

9.16.1 完整协议

本 CPS 完整的文档结构包括 3 部分：标题、目录、主体内容。关于对目录和主体内容修改后的替代内容，将完全代替所有先前部分、并被放置在天威诚信的网站中以供查阅和浏览。

9.16.2 转让

天威诚信声明，根据本 CPS 中详述的认证实体各方的权利和义务，各方当事人在未经过天威诚信事先书面同意的情况下，不能通过任何方式进行转让。

9.16.3 分割性

如果本 CPS 的任何条款或其应用由于与天威诚信所在管辖区的法律产生冲突而被判定为无效或不具执行力时，天威诚信可以在最低必要的限度下修订该条款，使其继续有效，其余部分不受影响，天威诚信将在此章节批露修订的内容。

在根据修订后要求签发证书之前，天威诚信将发送邮件至 question@cabforum.org，通知 CAB 论坛 CPS 中已修订的信息，并确认其已被发至公共邮件列表和存在于公共档案列表(https://cabforum.org/pipermail/public/)。

若法律不再适用，或 CAB 论坛的要求被修改，使天威诚信同时符合 CAB 论坛的 Baseline Requirements 及法律要求，则本章节中任何对天威诚信业务操作的调整将不再继续适用。上述对业务操作进行的相关调整，对天威诚信的 CPS 的修订，及向 CAB 论坛的通知将在 90 天内完成。

9.16.4 强制执行

在天威诚信、注册机构、订户和依赖方之间出现纠纷、诉讼时，胜诉方可以要求对方支付有关诉讼费作为对其补偿的一部分。免除一方对某次合同违约的赔偿不意味着免除对其他合同违约的赔偿。

天威诚信声明，若证书订户、依赖方等实体未执行本 CPS 中某项规定，不被认为该实体将来不执行该项或其他规定。

9.16.5 不可抗力

当由于不可抗力，如地震、洪灾、雷电等自然灾害和战争等，造成天威诚信或注册机构无法提供正常的服务时，天威诚信和注册机构不承担由此给用户造成的损失。

9.17 其他条款

天威诚信对本 CPS 具有最终解释权。

10. 附件

10.1 附件 A：天威诚信对于不同类型证书的鉴证操作

证书类型	鉴证要求
DV SSL	1，天威诚信将按照本 CPS 3.2.2.4 中的域名鉴证方法，确认申请者对域名的所有权或使用权。当使用随机值时，天威诚信提供证书请求唯一的随机值，该随机值的有效期不超过 30 天。 2，天威诚信会根据 CPS 3.2.2.8 的要求检查 CAA 记录。 3、天威诚信将对域名与已知天威诚信自己维护的敏感域名进行对比，如包含敏感或类似域名，则必须经过附加的审核工作后再行签发或拒绝；若订户的证书请求信息在敏感名单中，需要请客户补充审核材料《订户书面授权书》。
OV SSL	1.通过第三方信息数据库查询或政府官方提供的查询通道进行查询该实体存在和业务存在，且不在当地政府法律法规禁止的名单中。 2，天威诚信将按照本 CPS 3.2.2.4 中的域名鉴证方法，确认申请者对域名的所有权或使用权。当使用随机值时，天威诚信提供证书请求唯一的随机值，该随机值的有效期不超过 30 天。

	3，天威诚信将按照本 CPS 3.2.2.1 中的要求，对申请者的组织机构信息进行鉴证。 4，天威诚信将按照本 CPS 3.2.2.2 对申请者的所在国家进行鉴证。 5，天威诚信将按照本 CPS 3.2.5 中的要求，确认该申请获得了有效的授权 6，天威诚信会根据 CPS 3.2.2.8 的要求检查 CAA 记录。 7、天威诚信将对订户的组织和申请人等信息与已知天威诚信自己维护的高风险申请库进行对比，如任意一项在高风险申请库中，则必须经过附加的审核工作后再行签发或拒绝；若订户的证书请求信息在敏感名单中时，需要请客户补充审核材料《订户书面授权书》。
EV SSL	1.通过第三方信息数据库查询或政府官方提供的查询通道进行查询该实体存在和业务存在，且不在当地政府法律法规禁止的名单中。 2. 天威诚信将按照本 CPS 3.2.2.1 中的要求，对申请者的组织机构信息进行鉴证。并确认订户申请证书中的组织名称已开展商业活动。 3. 天威诚信将按照本 CPS 3.2.2.2 对申请者的所在国家进行鉴证。 4，天威诚信将按照本 CPS 3.2.2.4 中的域名鉴证方法，确认申请者对域名的所有权或使

	用权。当使用随机值时，天威诚信提供证书请求唯一的随机值，该随机值的有效期不超过 30 天。5，EV 证书申请人需使用申请单位邮箱或属于被授权人的其他收费邮箱（EV 证书申请资料中不支持免费邮箱）。 6，天威诚信将按照本 CPS 3.2.5 中的要求，确认证书申请人获得了有效的授权。 7，天威诚信会根据 CPS 3.2.2.8 的要求检查 CAA 记录。 8、天威诚信将对订户的组织和申请人等信息与已知天威诚信自己维护的高风险申请库进行对比，如任意一项在高风险申请库中，则必须经过附加的审核工作后再行签发或拒绝,若订户在黑名单中，证书请求不予批准；若订户的证书请求信息在高风险申请库查询到并且不在黑名单中时，需要请客户补充审核材料《订户书面授权书》。

10.2 附件 B：CA 证书信息

根证书信息：

根名称	vTrus Root CA	vTrus ECC Root CA
国家	CN	CN
组织	iTrusChina Co.,Ltd.	iTrusChina Co.,Ltd.
通用名	vTrus Root CA	vTrus ECC Root CA
序列号	43e37113d8b359145db7ce8cfd35fd6fbc058d45	6e6abc59aa53be983967a2d26ba43be66d1cd6da
有效期	25 年	25 年

起始日期	2018-07-31 15:24:05	2018-07-31 15:26:44
到期日期	2043-07-31 15:24:05	2043-07-31 15:26:44
算法	RSA(4096 bits)	ECC(384 bits)
SHA256 指纹	8A:71:DE:65:59:33:6F:42:6 C:26:E5:38:80:D0:0D:88:A 1:8D:A4:C6:A9:1F:0D:CB:6 1:94:E2:06:C5:C9:63:87	30:FB:BA:2C:32:23:8E:2A: 98:54:7A:F9:79:31:E5:50:4 2:8B:9B:3F:1C:8E:EB:66:3 3:DC:FA:86:C5:B2:7D:D3
签名算法	sha256RSA	sha384ECDSA

子 CA 信息：

证书名称	vTrus DV SSL CA	vTrus ECC DV SSL CA
国家	CN	CN
组织	iTrusChina Co.,Ltd.	iTrusChina Co.,Ltd.
通用名	vTrus DV SSL CA	vTrus ECC DV SSL CA
颁发者	vTrus Root CA	vTrus ECC Root CA
序列号	5663e4e2e84aad4f80afa0fe14ab784fec000c9b	17ba09a81f8e368368c25e5e1ce3a5f284839ded
有效期	20 年	20 年
起始日期	2018-07-31 15:35:45	2018-07-31 15:43:31
到期日期	2038-07-31 15:35:45	2038-07-31 15:43:31
算法	RSA(2048 bits)	ECC(256 bits)
SHA256 指纹	5F:7E:8B:4A:8C:11:BA:F2: CB:E6:45:9B:47:FD:B6:D5: 0C:02:85:C4:A9:94:F4:EE: F2:FE:51:60:AA:0A:B7:8A	C9:7E:36:CE:BF:15:80:AB: 1B:DA:D6:1C:1D:53:B0:5C: 75:81:9E:85:D9:37:21:4B:E 6:84:C8:59:B2:2D:45:E0
签名算法	sha256RSA	sha256ECDSA

证书名称	vTrus OV SSL CA	vTrus ECC OV SSL CA
国家	CN	CN
组织	iTrusChina Co.,Ltd.	iTrusChina Co.,Ltd.
通用名	vTrus OV SSL CA	vTrus ECC OV SSL CA
颁发者	vTrus Root CA	vTrus ECC Root CA
序列号	1fa43d72635e7bf38135eef39ccfc9ddc3477986	6da164f12fab562ceb173c46bcaa9fa90beed246
有效期	20 年	20 年
起始日期	2018-07-31 15:33:57	2018-07-31 15:41:18
到期日期	2038-07-31 15:33:57	2038-07-31 15:41:18
算法	RSA(2048 bits)	ECC(256 bits)
SHA256 指纹	A5:3B:5C:9B:B5:AD:92:70: 3D:C4:F7:7F:E6:4D:91:3A: 23:9F:D3:72:07:3A:48:E2:7 A:04:81:58:0A:56:37:C4	23:58:1E:F1:92:1D:F2:F9:2 9:0D:BA:0D:4D:4F:48:A9: 7F:98:AE:AE:FB:5E:33:50: B3:F7:05:82:E8:CD:BE:78
签名算法	sha256RSA	sha256ECDSA

证书名称	vTrus EV SSL CA	vTrus ECC EV SSL CA
国家	CN	CN
组织	iTrusChina Co.,Ltd.	iTrusChina Co.,Ltd.
通用名	vTrus EV SSL CA	vTrus ECC EV SSL CA
颁发者	vTrus Root CA	vTrus ECC Root CA
序列号	7d746ea36e2136270e8fc2e2456d229cb90c80b7	302282d66df3b37a7f5bf373d4ae8e7c5c125376
有效期	20 年	20 年
起始日期	2018-07-31 15:31:06	2018-07-31 15:39:20
到期日	2038-07-31 15:31:06	2038-07-31 15:39:20

期		
算法	RSA(2048 bits)	ECC(256 bits)
SHA256 指纹	F3:AA:6D:71:2A:15:F6:3F:83:50:80:49:79:DB:54:24:19:A6:1B:2B:1D:22:E7:56:C4: 17:AB:FE:8D:74:A3:CA	BD:30:C0:D1:E7:AC:B8:3E:FC:4F:5F:6C:62:F8:F3:A5:79:BA:B2:75:27:AF:AE:66: 6C:69:6C:3A:86:71:75:F1
签名算法	sha256RSA	sha256ECDSA