天威诚信™

电子政务电子认证服务业务规则

1.3 版本

生效日期:2021 年 10 月 29 日

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

邮政编码：100085

电话：(8610)- 50947500

网址：www.itrus.com.cn

版本说明：

天威诚信电子政务电子认证服务业务规则版本控制表

版本	主要说明	完成时间	编写人
天威诚信电子政务电子认证服务业务规则 1.0	依据国家密码管理局《电子政务电子认证服务业务规则规范》，结合天威诚信开展电子政务电子认证服务的具体要求和实际情况，完成《天威诚信电子政务电子认证服务业务规则》的编制	2016 年 9 月	邹圆圆、成晋辉、史波洋、许蕾
天威诚信电子政务电子认证服务业务规则 1.1	依据国家密码管理局《电子政务电子认证服务业务规则规范》和《电子政务电子认证服务质量评估要求》，对《天威诚信电子政务电子认证服务业务规则》进行了修改，包括严格遵循规范的格式和内容的要求	2016 年 11 月	唐志红、邹圆圆、许蕾
天威诚信电子政务电子认证服务业务规则 1.2	修改包括增加规则依据文件的引用、修改证书办理周期、增加证书撤销受理时限等 7 项内容	2016 年 12 月	唐志红、成晋辉、邹圆圆、郝萱、许蕾
天威诚信电子政务电子认证服务业务规则 1.3	修订第 6 章关于流程的部分描述和 7.2.14 和 7.2.16 部分术语描述。	2021 年 9 月	朱超、朱晓影、韩芳、蔚玲、高丽君、许蕾

天威诚信电子政务电子认证服务业务规则

北京天威诚信电子商务服务有限公司版权所有

版权声明

目　录

1. 概括性描述

北京天威诚信电子商务服务有限公司（以下简称“天威诚信”），是首批获得《电子认证服务使用密码许可证》和《电子认证服务许可证》的电子认证服务机构。

《天威诚信电子政务电子认证服务业务规则》（Certification Practice Statement for E-Government，以下简称“电子政务 CPS”）的编制，遵从《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》以及《电子政务电子认证服务业务规则规范》，阐明了天威诚信面向电子政务活动中的政务部门和企事业单位、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、备份和恢复等服务内容，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。

本电子政务 CPS 详细阐述了天威诚信签发和管理证书及运营维护证书服务设施的活动，并提供在实际工作和运行中遵循的各项规范。

本电子政务 CPS（v1.3 版本）的生效日期是 2021 年 10 月 29 日。

2. 规则依据文件

本电子政务 CPS 的依据文件如下：

《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

《电子政务电子认证服务管理办法》 国家密码管理局 2009 年

《电子认证服务密码管理办法》 国家密码管理局 2009 年

《电子政务电子认证服务业务规则规范》 国家密码管理局 2018 年

《基于 SM 2 密码算法的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 2014 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

《SM2 椭圆曲线公钥密码算法》 国家密码管理局 2012 年

《SM3 密码杂凑算法》 国家密码管理局 2012 年

《SM4 分组密码算法》 国家密码管理局 2012 年

《SM2 密码算法使用规范》 国家密码管理局 2012 年

《SM2 密码算法加密签名消息语法规范》 国家密码管理局 2012 年

《数字证书认证系统密码协议规范》 国家密码管理局 2012 年

《基于 SM2 密码算法的数字证书格式规范》 国家密码管理局 2012 年

3. 术语和定义

3.1

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。

3.2

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。

3.3

鉴别 identification

辨别认定证书申请者提交材料真伪的过程。

3.4

实体鉴别 entity authentication

确认一个实体所声称的身份。

3.5

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。

3.6

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。

3.7

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。

3.8

电子认证服务机构 electronic certification service provider

提供电子认证服务的机构。

3.9

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。

3.10

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。

3.11

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。

3.12

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。

3.13

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。

4. 符号和缩略语

下列缩略语适用于本电子政务CPS：

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)
OCSP	在线证书状态协议(Online Certificate Status Protocol)
SSL	安全套接层（Secure Sockets Layer）
PIN	个人识别码（Personal Identification Number）

5. 业务规则管理

5.1. 管理机构

天威诚信安全策略委员会是本电子政务 CPS 的管理机构，负责本 CPS 的制定、发布和实施；天威诚信还会定期对存在的业务风险进行评估，并根据结果决定是否需要对 CPS 进行修订。

5.2. 联系方式

本《天威诚信电子政务电子认证服务业务规则》在天威诚信网站发布，对具体个人不另行通知。

天威诚信网站：https://www.itrus.com.cn/about/shengming/

电子邮箱：itrus_cps@itrus.com.cn

联系地址：北京市海淀区上地八街 7 号院 4 号楼 4 层

邮编：100085

电话：(8610)-50947500

传真：010-50947517/50947516

5.3. 批准程序

1、《天威诚信电子政务电子认证服务业务规则》（CPS）由安全策略委员会指定相关业务部门骨干组成编写小组进行编制及修订。

2、编写小组完成编制工作或修订工作、并检查与实际情况相符后，提交给安全策略委员会审批。

3、审批通过后将最新的《天威诚信电子政务电子认证服务业务规则》及时报国家密码管理局备案，以 PDF 格式在天威诚信官方网站上对外公布，并对旧版 CPS 进行归档。

6. 电子政务电子认证服务业务

天威诚信电子政务电子认证服务严格按照《电子政务电子认证服务管理办法》所规定的服务内容及要求开展。

6.1. 数字证书服务

6.1.1. 服务内容

天威诚信面向电子政务活动中的政务部门和企事业单位、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。

6.1.2. 数字证书类型

天威诚信面向电子政务活动提供以下类型的数字证书：

1） 机构证书

为政务机关和参与电子政务业务的企事业单位、社会团体或其他组织颁发的证书，用以代表机构单位或机构法人（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，用于标识各种设备身份（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，保证实体身份的唯一性，且名称类型支持 X.500、RFC-822、X.400 等标准协议格式。

6.1.3. 身份标识与鉴别

6.1.3.1. 命名

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，不使用匿名或假名。

根据证书主体类型不同，天威诚信签发的证书的主体名字可以是人员姓名、组织机构名、域名等，命名符合 X.501 甄别名规定。

运营设备证书的主体域中包含一个 X.501 甄别名，它的内容组成与服务器证书类似，只是其中的通用名(CN)对应的内容是设备的名称或 IP 地址，或者机构的名称。

6.1.3.2. 证书初始身份确认

A. 证明持有私钥的方法

天威诚信基于两个条件来证明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。

a） 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；

b） 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；

c） CA 使用证书持有者公钥验证证书持有者签名。

2）证书持有者必须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。

B. 组织机构身份的鉴别

申请组织机构证书、设备证书或组织机构代表人证书时，天威诚信要求申请者提交合法身份证明文件，天威诚信将对证书持有者所在的组织机构进行身份鉴别。包括：

1）申请组织机构证书或组织机构代表人证书

申请组织机构证书或组织机构代表人证书需要提交符合填写规范的《机构证书申请表》，并提交的合法身份证明文件包括：营业执照或事业单位法人证书等其他有效身份证件、加盖公章的授权申请文件。

天威诚信对组织机构的身份鉴别包括如下两个内容：

a) 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。

b) 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：使用从网络或其它常规途径获取验证电话号码，进行电话验证，获得组织机构有关申请及授权事宜的确认；或者，由该机构提供加盖公章的授权申请文件等信函确认。

2) 申请组织机构设备证书

申请组织机构设备证书需要提交符合填写规范的《机构设备证书申请表》，并提交的合法身份证明文件及其复印件包括：营业执照、拥有设备的证明文件（如：域名注册证明文件）、加盖公章的授权申请文件。

天威诚信对组织机构及其设备的身份鉴别包括如下三个内容：

a) 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，通过权威的第三方数据库确认。

b) 确认组织机构对设备的所有权或使用权。确认方式是通过有效的证明文件证明，对于域名有所有权或使用权，还会通过域名注册商、国家权威网站等确认域名所有者信息。

c) 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：使用从网络或其它常规途径获取验证电话号码，进行电话验证，获得组织机构有关申请及授权事宜的确认；或由该机构提供加盖公章的授权申请文件等信函确认。

天威诚信对上述材料进行审核和鉴证，做出批准申请或拒绝申请的操作。

如批准申请，将保留相关证明材料的电子版或复印件，与申请表一并存档保存。

C. 个人身份的鉴别

申请个人证书需要提交符合填写规范的《个人证书申请表》，并提交合法身份证明文件及其复印件。合法的身份证明文件包括：身份证、户口簿、护照、军官证、警官证、士兵证、士官证和文职干部证等。

天威诚信对个人进行身份鉴别包括如下两个内容：

a）确认个人的身份是确实存在的、合法的实体。确认的方式为：通过对合法身份证明文件进行确认；或利用权威第三方提供的身份证明或数据库服务进行确认，如：公安部门提供的个人身份数据库。

b）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、银行卡信息等辅助手段进行确认。

把证书签发给政府部门中的个人时，还将确认以下内容：

a）申请者提交由所属政府部门盖章的证明文件，明确部门的名称并证明申请人和证书持有者属于该部门。

b）通过申请者所在组织机构电话号码，然后联系组织机构的有关人员，确认申请者的身份及证书持有者确实被该组织机构雇佣，以及获得了所在组织机构的授权。

天威诚信对上述材料进行审核和鉴证，做出批准申请或拒绝申请的操作。

如批准申请，将保留相关证明材料的电子版或复印件，与申请表一并存档保存。

6.1.3.3. 密钥更新请求的识别与鉴别

A. 常规的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，证书持有者需要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。对申请的鉴别需满足以下条件：

1）密钥更新请求中，确保更新请求与申请者身份的关联和申请行为的有效性，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。

2）当用户证书已过期时，重新进行与初始身份确认相同的实体鉴别流程。

3）当用户证书未过期时，用户采取在线更新方式的，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。

B. 撤销之后的密钥更新请求的识别与鉴别

天威诚信在证书撤销后不允许进行密钥更新。

6.1.3.4. 撤销请求的身份标识与鉴别

在天威诚信的证书业务中，证书撤销请求可以来自证书持有者，也可以来自天威诚信

或其注册机构。

证书撤销的方式可以是证书持有者自己撤销，也可以由证书持有者要求天威诚信或其注册机构管理员撤销。

证书持有者通过天威诚信及其注册机构申请撤销证书时，天威诚信及其注册机构将对证书持有者进行身份鉴证。

证书持有者申请撤销证书时，填写证书撤销申请表，通过一定的方式，如在线、邮寄、邮件等，向天威诚信或其注册机构提交，并由天威诚信或其注册机构审核。

天威诚信或其注册机构的审核人员合理、审慎地核对申请资料的原件或复印件，根据审核人员的管理规定对申请者的资料的真实性进行审查，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，并进行批准或拒绝的操作。

如果是因为证书持有者没有履行《天威诚信电子政务电子认证服务业务规则》所规定的义务，由天威诚信或其注册机构申请撤销证书持有者的证书时，不对证书持有者身份进行标识和鉴别。

6.2. 数字证书服务操作要求

6.2.1. 证书申请

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

6.2.1.1. 信息告知

天威诚信在本电子政务 CPS 中阐述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。

对于个人证书，申请者到天威诚信受理点填写或到天威诚信网站下载填写《个人证书申请表》，并提供个人身份证明文件及其复印件一份，例如：身份证、军官证、学生证、护照、警官证、士兵证、士官证、文职干部证、及其他法律法规和政府政策认可的证明文件等。

政府、机构部门中的个人申请证书时，还需提交个人所在单位许可授权证明（申请表加盖单位公章）及单位证明文件；如果是委托申请的，还需提供经办人被授权证明，证明

代表他人提交证书申请的人是经过单位授权的。

对于机构证书，申请者到天威诚信受理点填写或到天威诚信网站下载填写《机构证书申请表》，申请者应提供单位对经办人的授权委托证明，单位的营业执照或事业单位法人登记证等及其他有效证件和天威诚信可能需要的其他文件。

任何需要在各类应用中采用数字证书进行真实身份标识和鉴别，实现信息保密，并提供信息源发性证明、完整性保障和抗抵赖的个人或机构，都可以申请个人证书或机构证书。

组织机构申请机构证书时，由机构授权人员申请。

服务器证书由域名拥有机构，或获得域名使用授权的机构中的授权人申请。

运营设备证书由天威诚信授权的人员或者设备所在注册机构的授权人申请。

6.2.1.2. 申请的提交

- 证书申请应由证书持有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。
- 天威诚信提供线上、线下多种方式的证书受理申请。

6.2.1.3. 注册过程与责任

证书申请者可到天威诚信的注册服务站点、或其授权注册机构的注册服务站点，申请各类证书。

对于机构证书，注册时申请者须正确填写以下信息：

- 机构的真实身份标识信息，如机构法定名称、统一社会信用代码等；
- 机构授权的申请人信息，如姓名、电话、邮件地址、身份证号码等。

对于个人证书，注册时申请者须正确填写以下信息：

- 个人的真实身份标识信息，如个人真实姓名、身份证号码、电话号码、所属机构（若需要）等；
- 其他信息，如邮件地址等。

对于服务器证书和运营设备证书，注册时申请者须正确填写以下信息：

- 服务器主机名、域名、IP 地址或设备名称、及所有者信息等；
- 申请人信息，如姓名、电话、邮件地址等。

天威诚信在处理每一个证书申请中，满足以下条件：

- 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；
- 注册过程保证所有证书申请者明确同意相关的证书申请者协议；
- 按本电子政务 CPS 的规定产生一个密钥对，并将公钥通过网络安全传输协议传给天威诚信或其注册机构。

6.2.2. 证书申请处理

6.2.2.1. 执行识别与鉴别功能

对于个人证书的申请，天威诚信及其注册机构按本 CPS 6.1.3 所述的方式对证书申请人进行识别和鉴别。

对于机构证书和设备证书，天威诚信及其注册机构按本 CPS 6.1.3 所述的方式对组织机构及其授权申请人进行识别和鉴别。

特别地，对组织机构代表人证书，除了对组织机构及其授权申请人进行识别和鉴别，还需确认包含在证书中的代表人个人信息是真实而准确的。

6.2.2.2. 证书申请批准和拒绝

在天威诚信或其注册机构完成对证书申请的鉴证、有关鉴证获得通过且证书申请者履行了其他应尽的责任后，天威诚信或其注册机构将批准证书申请，并妥善保管证书申请者申请时提交的所有材料。如果鉴证未获通过或证书申请者未履行其他应尽的责任，天威诚信或其注册机构将会拒绝该证书申请，并在 24 小时内通过现场或者电话、邮件、短信等方式告知拒绝原因。

6.2.2.3. 处理证书申请的时间

天威诚信及注册机构将在合理时间内完成证书请求处理。在申请者提交资料齐全且符合要求的情况下，处理证书请求的最长响应时间不超过 48 小时。

6.2.3. 证书签发

6.2.3.1. 证书签发中 RA 和 CA 的行为

在证书的签发过程中，天威诚信的 RA 管理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采用数字签名和数字信封的方式实现 RA 的身份鉴别与信息保密，确保请求发到正确的 CA 的证书签发系统。

天威诚信的 CA 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，CA 证书签发系统签发证书。

6.2.3.2. 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 系统均会通过邮件自动通知证书申请者。如果证书申请获得批准并签发，RA 将通过多种方式告诉证书申请者如何获取证书。

天威诚信对证书申请者的通告提供以下几种方式：

- 通过面对面的方式，通知证书申请者（如到注册机构领取等方式）；
- 邮政信函通知证书申请者；
- 通过电子邮件方式通知；
- 其他天威诚信认为安全可行的方式通知证书申请者。

6.2.4. 证书接受

6.2.4.1. 构成接受证书的行为

天威诚信证书申请者接受证书的方式可以有如下几种：

- 证书申请者可通过面对面的方式，从注册机构（天威诚信或其注册机构）接受载有证书和私钥的介质。
- 证书申请者也可根据电子邮件中的获取证书的指示信息，访问专门的证书下载服务站点将证书下载到本地存放介质，如 USB Key、智能卡等。

完成以上行为表明证书持有者接受证书。另外，证书持有者接受到证书后，应立即对证书进行检查和测试。

6.2.4.2. 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，天威诚信不发布该证书申请者证书信息。没有明确表示拒绝的，天威诚信将证书信息发布到目录系统。

6.2.4.3. CA 对其他实体的通告

除证书持有者、证书申请者和 RA 外，天威诚信不需要通知其他实体证书的签发。

6.2.5. 密钥对和证书使用

证书持有者的密钥对和证书须用于其规定的、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。密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受保障的。

6.2.5.1. 证书持有者的私钥和证书使用

证书持有者只能在指定的应用范围内使用私钥和证书，只有在接受了相关证书之后才能使用对应的私钥，并且在证书到期或被撤销之后，必须停止使用该证书对应的私钥。对于加密证书，其私钥可用于对采用对应公钥加密的信息解密。证书持有者应妥善保管其证书私钥。

6.2.5.2. 依赖方的公钥和证书使用

当依赖方接受到经数字签名的信息后，应该：

- 获得数字签名对应的证书及信任链；
- 确认该签名对应的证书是依赖方信任的证书；
- 证书的用途适用于对应的签名。
- 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。

当依赖方需要发送加密信息给接收方时，须先通过适当的途径获得接收方的加密证书，然后使用证书上的公钥对信息加密。依赖方应将加密证书连同加密信息一起发送给接收方。

6.2.6. 证书更新

6.2.6.1. 证书更新的情形

在证书到期前 30 天内或已过期后 30 天内，如证书持有者的注册信息没有改变的，证

书持有者可以进行证书更新。

在证书已到期后 30 天后或被撤销的证书，将不能进行证书更新，只能按照初始流程重新申请证书。

6.2.6.2. 更新请求的提交

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）在证书满足更新条件时，可以要求向天威诚信的注册机构提出更新申请。

更新请求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。

6.2.6.3. 处理证书更新请求

对于不更换密钥的证书更新请求，用户提交的证书签名请求（PKCS#10）包含有原有证书的公钥，并由原证书私钥签名。

接收到用户的证书更新请求后，天威诚信 CA 系统会自动完成如下验证操作：

- 确认、验证申请对应的原证书存在并且由天威诚信签发；
- 证书更新请求在允许的期限内；
- 用原证书上的用户公钥对更新申请的签名进行验证。

若以上自动验证通过，则天威诚信或其注册机构根据证书种类的不同，分别按如下方式和过程完成证书更新请求的鉴证、批准，及新证书的签发。

对于机构证书（包括机构单位证书和机构代表人证书）和设备证书（包括服务器证书和运营设备证书）根据用户以前提交的注册信息，按与新证书申请一样的流程完成证书申请的鉴证，包括机构身份信息正确性、有效性的验证和确认，证书申请人及证书申请授权的确认等。在进行鉴证时，若机构用户以前提交的机构身份证明文件（如组织机构代码、营业执照）仍在其有效期内，则更新申请人无需重新提交有关的机构身份证明文件，但天威诚信或其注册机构仍会通过第三方数据库确认有关材料是否继续有效。完成以上鉴证后，批准更新请求，签发新证书。

对于个人用户证书的更新，若包含在证书中的需鉴别的信息不包含该证书用户所属组织机构，则只要该证书用户履行了应尽的责任，则证书更新请求将获得批准，新证书将获得签发。以上过程可以是自动或手动的。若包含在证书中的需鉴别的信息包含该证书用户所属组织机构，则在批准更新请求、签发新证书前，需要确认该证书用户仍然是所属机构

的人员。

对于机构雇员证书的更新，则在完成如下确认后，批准证书更新请求，签发新证书：

1）该证书用户仍然是对应机构的雇员；

2）该用户的证书更新获得了该机构的许可。

以上过程可以是自动或手动的。

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：

1）面对面的更新方式；

2）在线的自动更新方式。

6.2.6.4. 通知证书持有者新证书的签发

同证书初次申请时的签发处理。

6.2.6.5. 构成接受更新证书的行为

同证书初次申请时的接受规则。

6.2.6.6. CA 对更新证书的发布

同证书初次申请时的发布规则。

6.2.6.7. CA 通知其他实体证书的签发

同证书初次申请时的通知方式。

6.2.7. 证书撤销

6.2.7.1. 证书撤销的条件

天威诚信、注册机构及证书持有者在发生下列情形之一时，申请撤销数字证书：

A. 政务机构的证书持有者工作性质发生变化；

B. 政务机构的证书持有者受到国家法律法规制裁；

C. 证书持有者提供的信息不真实；

D. 证书持有者没有或无法履行有关规定和义务；

E. 天威诚信、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；

F. 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；

G. 和证书持有者达成的证书持有者协议已经终止；

H. 证书持有者请求撤销其证书；

I. 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；

J. 法律、行政法规规定的其他情形。

6.2.7.2. 证书撤销的发起

以下实体可以请求撤销一个证书持有者证书：

A. 批准证书持有者证书申请的天威诚信、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。

B. 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。

C. 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。

D. 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。

6.2.7.3. 证书撤销的处理

A. 天威诚信、注册机构在接到证书持有者的撤销请求后，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。

B. 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。

C. 天威诚信、注册机构在确信出现证书撤销条件中的情况时，将在 8 小时内执行撤销证书操作；在需要立即撤销证书时，可以立即撤销证书；撤销证书将在 24 小时内发布到证书撤销列表中。

D. 证书撤销后，通过电子邮件、电话、短信等方式告知用户或依赖方证书撤销结果。

证书持有者可以通过以下方式要求撤销自己的证书：

- 直接访问天威诚信或注册机构提供的证书服务网页。在证书持有者提交撤销请求时，需同时提供证书申请时提供的挑战语作为身份鉴别的信息。这种方式适用于所有类别的证书。
- 用户现场提交撤销证书申请。

- 通过电子邮件、信函等可靠的方式告知天威诚信或其注册机构。

6.2.7.4. 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：

A. 必须根据用户证书标明的发布地址获取天威诚信的证书撤销列表，即 CRL。

B. 必须验证撤销列表的签名，确认其来自于天威诚信。

C. 必须验证证书撤销信息，确认用户证书是否被注销。

6.2.7.5. CRL 发布频率

天威诚信的认证系统每天零时为证书签发 CA 产生证书撤销列表。证书撤销列表更新的时间间隔为 24 小时。对于特别的证书签发 CA，天威诚信可定制证书撤销列表产生的频率。

CRL 的结构如下：

A. 版本号(version)

B. 签名算法标识符(signature)

C. 颁发者名称(issuer)

D. 本次更新(this update)

E. 下次更新(next update)

F. 用户证书序列号/撤销日期(user certificate/revocation date)

G. CRL 条目扩展项(crl entry extensions)

H. CRL 扩展域(crl extensions)

I. 签名算法(signature algorithm)

J. 签名(signature value)

6.2.7.6. CRL 发布的最大滞后时间

一个证书从它被撤销到它被发布到 CRL 上的滞后时间不超过 24 小时。

6.2.7.7. 在线状态查询的可用性

天威诚信提供证书状态的在线查询服务（OCSP），该服务 7X24 小时可获得，服务地址、服务接口在通过与电子政务信息系统应用集成时，发布给电子政务信息系统调用。

6.2.7.8. 在线状态查询要求

依赖方应检查证书的撤销状态。如果依赖方未通过 CRL 方式查询，则应通过 OCSP 在线方式查询。

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：

A. 须按照查询协议要求，向 OCSP 服务地址提交状态查询请求。

B. 查询过程须确保信息传输的机密性和完整性。

C. 须获得证书状态信息。

6.2.7.9. 撤销信息发布的其他形式

除了通过 LDAP 目录服务发布 CRL，或通过 OCSP 服务器提供证书状态查询外，天威诚信所发布的 CRL 也可通过天威诚信的相关服务网站获得。

6.2.8. 密钥生成、备份和恢复

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 USBKEY 或智能 IC 卡）生成并保存，加密密钥对的生成、备份和恢复由密钥管理中心提供密钥管理服务。

证书持有者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，证书持有者加密密钥对由密钥管理系统安全产生和保存，密钥恢复是一种严格受控的过程，只有在如下情况下才允许进行密钥恢复：

1 证书持有者提出申请：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。证书持有者到天威诚信提交恢复申请，并注明原因；天威诚信根据证书持有者的要求进行审核，审核通过后，由密钥管理系统的业务管理员和业务操作员进行恢复操作，生成下载挑战码，提供给证书持有者；证书持有者访问RA用户服务页面使用挑战码下载证书。

2 国家执法、司法机构因执法、司法的需要，取证人员出示相关法律文件，向密钥管理中心提出恢复密钥的申请，经审核后，由密钥管理系统的业务管理员和业务操作员进行恢复操作，生成加密密钥的密文文件，记录于特定载体中，提供给取证人员。

6.3. 应用集成支持服务

6.3.1. 服务策略和流程

天威诚信提供的服务内容有：

1 制定证书应用实施的管理策略和流程，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；

2 制定项目管理制度，规范系统和程序开发行为；

3 制定安全控制流程，明确人员职责；

4 实施证书软件发布版本管理，并进行证书应用环境控制；

5 项目开发程序和文档等资料妥善归档保存。

6.3.2. 应用接口

证书应用接口为上层提供简洁、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。

6.3.2.1. 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（如：USBKey）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》。

6.3.2.2. 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》，主要包括服务器端组件接口和客户端控件接口，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。

证书应用接口程序支持 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。

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。

6.3.3. 集成内容

天威诚信为电子政务应用单位提供证书应用接口程序集成工作。包括以下服务：

1 证书应用接口的开发包（包括客户端和服务器端）；

2 接口说明文档；

3 集成演示 Demo；

4 集成手册；

5 证书应用接口开发培训和集成技术支持；

6 协助应用系统开发商完成联调测试工作。

6.4. 信息服务

6.4.1. 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，天威诚信为证书应用单位提供以下信息服务，为其实现科学管理和领导决策提供可靠依据。

6.4.1.1. 证书信息服务

天威诚信的 CA 系统中签发、更新的数字证书，用户可通过与 CA 系统对接的电子政务信息系统进行查询。

6.4.1.2. 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。天威诚信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。

6.4.1.3. 服务支持信息服务

天威诚信面向电子政务用户、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。

6.4.1.4. 决策支持信息服务

天威诚信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。

6.4.2. 服务管理规则

1 天威诚信内部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记录；

2 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；

3 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；

4 对问责程序需要进行的信息访问，天威诚信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；

5 对监管部门应管理需求进行的信息访问，天威诚信按照相关的管理规定和调取程序， 为其提供信息访问权限；

6 对司法程序需要的信息访问，天威诚信严格审核司法人员的身份及授权文件，确认后方可提供信息访问。

天威诚信在提供信息服务时，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。

1 私有信息类型的敏感度

以下信息属于私有信息：

A. 个人隐私信息；

B. 商业机密；

C. 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

天威诚信在进行证书发行和管理时才收集私有信息。除有特殊要求外，天威诚信不收集更多私有信息。

3　允许的私有信息使用

天威诚信只使用 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　允许的个人信息发布

天威诚信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。

在特别紧急情况下，天威诚信经管理机构的同意，可以发布私有信息。

任何特定的私有信息发布应遵照相关法律和政策实行。

5　所有者纠正私有信息的机会

天威诚信允许用户在其证书生命周期内对其私有信息进行更正。

6　对司法及监管机构发布私有信息

天威诚信或者注册机构在以下情况下，可以执行将私有信息发给获得相应授权的人员：

A. 司法程序；

B. 经私有信息所有者同意；

C. 按照明确的法定权限的要求或许可。

6.4.3. 服务方式

天威诚信信息服务以页面或接口的形式向应用系统或证书用户提供服务，以接口形式提供的服务符合《电子政务数字证书应用接口规范》的要求。

6.4.3.1. 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，天威诚信的 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，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。

6.4.3.2. 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， 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 发布周期不超过 24 小时。

6.4.3.3. 服务支持信息服务

天威诚信通过 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；
- 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）。

天威诚信通过 线下方式或 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）。

天威诚信 通过 WEB 网站面向电子政务应用系统发布如下信息：

- 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）。

6.4.3.4. 决策支持信息服务

天威诚信面向应用提供方以 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。

6.5. 使用支持服务

6.5.1. 服务内容

使用支持服务是天威诚信面向证书使用用户（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。

6.5.1.1. 面向证书持有者的服务支持

A. 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。

B. 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。

C. 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。

D. 电子认证服务支撑平台使用

为用户提供在天威诚信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、无法提交撤销申请等。

6.5.1.2. 面向应用提供方的服务支持

A. 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。

B. 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。

6.5.2. 服务方式

天威诚信提供多种服务方式，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。

天威诚信建立了服务保障体系，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。服务保障体系能根据服务业务的变化及时更新。

6.5.2.1. 座席服务

用户拨打天威诚信的服务热线，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。

6.5.2.2. 在线服务

在线服务通过提供自助信息查询系统、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。

A. 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。

B. 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，天威诚信客服人员能够第一时间同登陆网站的访客取得联系，进行交流。

C. 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。

D. 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。

6.5.2.3. 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。

6.5.2.4. 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、短信等。向用户提供调查表格以供用户填写，调查表格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。

6.5.2.5. 投诉受理

天威诚信设立的专门的投诉处理部门、投诉电话和投诉邮件地址，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，投诉受理过程中记录投诉问题，并将结果及时反馈给客户。将投诉受理中产生的相关文档进行归档、保存。

6.5.2.6. 培训

天威诚信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。

培训方式可以由天威诚信与客户双方约定的形式开展。

6.5.3. 服务质量

座席服务、在线服务、现场服务时间充分满足各类用户的需要，为 7X12 小时工作时间。在有应急服务需求的特殊情况下，服务时间根据具体业务需求确定，提供 7X24 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，并制定相应处理流程和机制，以确保服务的及时性和连续性。技术支持响应时间以最大程度不影响客户使用为准则。

6.6. 安全保障

6.6.1. 认证机构设施、管理和操作控制

6.6.1.1. 物理控制

1 场地区域与建筑

天威诚信认证中心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，整体建筑由能够阻止物理入侵的材料建成。建筑物的外墙、地板和天花板都属于永久性建造，并互相联结，可以阻止未经过授权的进入、入侵。敏感区域只设置一个门作为的常规入口。根据消防要求置了消防紧急出口。

运营场地的物理安全是基于物理层级的保护，每一物理层就是一个屏障，设置了可以控制进出的带锁的门来控制每个人进出每一个区域。每一层区域有非常严格的控制方法防止未经授权的物理访问，而且每一个物理安全层在物理上完全包含下一个物理安全层，最外层的安全层是整个建筑物的外墙。

天威诚信认证机构的运营场地达到以下安全和控制风险要求：

- 防止物理非法进入

四层物理结构及完善的安全管理体系保护天威诚信的运营设施安全。

- 防止未经过授权的物理访问

确保未经过授权的人，或仅被授权访问有限物理区域的人员，不得访问天威诚信认证机构内的受限制区域。

- 维护 CA 服务的完整性、可用性

保障提供 CA 服务的系统、设施不受到破坏，保证认证服务不被中断。

2 物理访问

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。

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℃。

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 火灾预防和保护

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。

6 介质存储

天威诚信认证机构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）。

7 废物处理

天威诚信对敏感的文件和材料在处理之前将其切成碎片，使信息无法恢复。密码设备在作废处置前根据制造商的指南将其物理销毁或初始化。其他废物处理按天威诚信正常废物处理的要求进行。

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。

9 入侵侦测报警系统

天威诚信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，安装有移动侦测器报警器，发生非法入侵时能立即报警。

10 注册机构物理控制

天威诚信注册机构的物理场地有足够的安全措施，保证只有授权的人员才能进入，只有授权的人员才能接触系统进行证书管理。

6.6.1.2. 操作过程控制

1 可信角色

为了保证可靠的人员管理，保证证书服务具有高可靠性和高安全性，天威诚信对关键岗位人员定为可信角色，天威诚信可信人员包括：

- 安全策略委员会主任
- 安全管理人员
- 系统运行维护人员

- 鉴证及客户服务人员
- 密钥与密码设备管理人员
- 系统管理员
- 系统审计员
- 档案管理人员
- 可信雇员管理人员
- 技术研发人员
- 能够进入敏感工作区域的人员

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人员共同完成，这包括：

1) 屏蔽区场地访问设置为双人进出模式；
2) 保存 CA 密钥激活数据的保险柜设置为双人开启模式；
3) CA 密钥所在的密码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。

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。

对于进行用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。

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：

1) 数据库管理员与应用系统管理员和操作系统管理员不能兼任；
2) CA 系统操作员与审计员之间不能兼任；
3) RA 业务操作员的录入员和审核员两个角色不能兼任；
4) 认证系统的管理员和维护人员不能兼任持有密码设备分割密钥的分管者。

6.6.1.3. 人员控制

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。

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。

3 培训要求

为了使有关人员能胜任其承担的工作，天威诚信对所有入职员工提供专门的培训计划，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。

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 工作轮换周期和顺序

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。岗位轮换不

违背职责分割策略。

6 对下列行为的处罚

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。

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。

8 提供给员工的文档

提供给员工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。

6.6.1.4. 审计日志程序

天威诚信建立了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。

1 记录事件的类型

天威诚信对如下几类事件进行记录：

- CA 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。
  - 密码设备生命周期的管理事件，例如接收、使用、和销毁。

  这些记录都是密钥管理员完成的手工记录。
- CA 和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。
- 成功或失败的证书操作。

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。
  - 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。

2 日志记录的内容。**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。

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十年。

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 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。

天威诚信保存在 SVN 的手工电子记录，实行工作时间内每 15 分钟增量备份、每天夜间全量备份的备份策略。

6 审计收集系统

对于电子审计信息，天威诚信设置了专门的审计信息存储系统，自动或人工完成审计信息的收集。对于纸质的审计信息，则有专门的文件柜来实现审计信息的收集。

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。

8 脆弱性评估

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。

6.6.1.5. 记录归档

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) 系统安全事件记录；

5）审计记录；

6）各类外部、内部评估文档。

2 归档记录的保存期限

对于不同的归档记录，其保留期限是不同的。对于系统操作事件和系统安全事件记录，其归档保留到完成安全脆弱性评估或一致性审计。

- 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，信息保存期为证书失效后十年。
- 面向政务部门的电子政务电子认证服务，信息保存期为证书失效后十年。
- 对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生命周期。
- CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留十年。
- 对系统操作、物理场地访问、可信人员管理记录的保存期限不少于 1 年。

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。

4 归档文件的备份程序

对于系统生成的电子归档记录，每天备份到异地存放；对于手工生成的电子记录，归档到 SVN，SVN 数据实行工作时间内每 15 分钟增量备份、每天夜间全量备份的备份策略。

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 记录时间戳要求

天威诚信对每项日志有时间记录。对于纸质记录，有操作人员手工记录；对于电子记录，由系统自动增加时间。

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。

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。

6.6.1.6. 认证机构密钥更替

当 CA 密钥对的累计寿命超过规定的最大生命期，天威诚信将启动密钥更新流程，替换已经过期的 CA 密钥对。

1 CA 根密钥更替

天威诚信 CA 根密钥由国家密码管理局统一管理，由国家密码管理局签发相应的 CA 根证书，并遵从国家密码管理局相关规范要求进行密钥更替。

2 在线运营CA密钥更替

- 产生新的密钥对，签发新的上级 CA 证书。
- 在“停止签发证书的日期”之后，对于批准的下级 CA 或最终用户证书请求，将采用新的 CA 密钥签发证书。
- 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。

“停止签发日期”指：一个上级 CA 将在其私钥到期时间小于下级 CA 的生命期之前停止签发新的下级 CA 证书。

6.6.1.7. 数据备份

天威诚信建立了业务连续性计划和严格的备份管理策略，定期开展数据备份。

系统数据库采用本地（热备+冷备）和 灾备（热备）方式进行备份，“热备”是通过数据实时同步机制实现，“冷备”是通过定时备份任务实现。“冷备”涉及到备份保留策略，目前采用的是每周（或每天）进行一次全量备份，其他时间增量备份，全量数据最少保留 3 个副本。备份数据会存放在专用的数据库备份服务器上。

定期检查备份系统和设备的可靠性和可用性， 定期对系统数据备份进行测试检查，

确保其可用性，每季度进行一次备份数据库可用性恢复测试检查，确保系统备份数据库可用性。

6.6.1.8. 损害和灾难恢复

1 事故和损害处理程序

天威诚信已制定各种应急处理方案，规定了相应的事故和损害处理程序，这些应急处理方案包括：

- 认证系统应急方案；
- 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；
- 密钥管理应急方案等。

2 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。计算机资源、软件和/或数据的损坏

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。

3 实体私钥损害处理程序

对于实体证书私钥的损害，天威诚信有如下处理要求和程序：

1）当证书用户发现实体证书私钥损害时，用户必须立即停止使用其私钥，并立即访问天威诚信或相应的注册机构的证书服务网站吊销其证书，或者立即通过电话、电子邮件的方式通知天威诚信或注册机构吊销其证书。天威诚信按 6.2.7 发布证书吊销信息。

2）当天威诚信或注册机构发现证书用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，并通知证书用户，用户必须立即停止使用其私钥。天威诚信按 6.2.7 发布证书吊销信息。

3）当天威诚信的 CA 证书或其受委托的 CA 证书出现私钥损害时，天威诚信将立即吊销该 CA 证书并及时通过广达的途径通知依赖方，然后生成新的 CA 密钥对、签发新的 CA 证书。

4 灾难后的业务存续能力

天威诚信在异地建立了容灾系统，一旦物理场地出现了重大灾难，天威诚信能够根据业务连续性计划在最短时间内恢复业务。

5 业务连续性计划的保障方案

A. 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。

B. 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。

C. 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。

D. 定期测试备份设备、设施、后备电源等，确保其可用性。

E. 建立当 CA 签名密钥可信性受威胁时的应变计划。

F. 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。

6.6.1.9. 认证机构或注册机构终止

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《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。

1) 天威诚信拟暂停或者终止认证服务的，会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做出妥善安排，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。
2) 不能就业务承接事项做出妥善安排的，会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。
3) 按照相关法律的规定来安排好档案和证书的存档工作。
4) 向承接单位提供相关信息和文档。
5) 在 CA 终止期间，采用以下措施终止业务：
   - 起草 CA 终止声明；
   - 通知与 CA 停止相关的实体；
   - 关闭从目录服务器；
   - 撤销证书；

- 处理存档文件记录；
- 停止认证中心的服务；
- 存档主目录服务器；
- 关闭主目录服务器；
- 处理系统管理员和业务管理员证书；
- 处理加密密钥；
- 处理和存储敏感文档；
- 清除 CA 主机硬件。

6) 根据与 RA 签订的协议终止 RA 的业务。

6.6.2. 认证系统技术安全控制

6.6.2.1. 密钥对的生成和安装

生成公、私钥对的实体包括：证书持有者、注册机构或认证机构。

1 密钥对的产生

- CA密钥对的产生

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、备份和恢复遵循国家密码主管部门相关规范要求。

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，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。

- 用户密钥对的产生

对于个人证书和机构证书，用户可根据需要选择使用国家密码管理部门许可的密码模块（如 USB Key）生成密钥对。

对于服务器证书，用户使用服务器程序使用的密码模块（包括 SSL 硬件加速卡）提供的密钥生成功能生成密钥对。

对于运营设备证书，天威诚信或其注册机构将使用专门的程序软件在国家密码管理部门许可的密码模块（如加密卡或加密机）中生成密钥对。

对于管理员证书，私钥使用国家密码管理部门许可的客户端密码模块（如 USB Key）

产生。

2 私钥传送给用户

天威诚信各类 CA 证书密钥对由天威诚信数字认证中心在其运营场地产生，私钥由天威诚信自身持有和保存，不存在私钥的传送问题。

天威诚信各种运营设备证书的密钥对由天威诚信或其注册机构在设备所在地产生，并在本地保存，不存在私钥的传送问题。

对于天威诚信签发的其他最终用户证书，通常的情况下密钥对在用户本地的密码模块（如 USB Key）中产生，私钥由最终用户保存在本地密码模块中，不存在私钥的传送问题。但在一些特殊情况下，天威诚信或其注册机构可能会代替最终用户在用户的密码硬件中（如 USB Key）产生证书密钥对，且私钥保存在密码硬件中。在这种情形下，天威诚信或其注册机构将通过安全的途径将保存有证书私钥的密码硬件传送到最终用户手中，并确保在传送过程中私钥不会被非授权的使用、被泄露或被损坏。

3 公钥传送给证书签发机关

用户或用户通过注册机构，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。

4 CA公钥传送给依赖方

天威诚信的根 CA 公钥，通过如下方式之一传输给依赖方：

1）依赖方访问天威诚信的证书服务站点下载 CA 证书，该站点受到服务器证书的保护；

2）天威诚信、注册机构或其合作伙伴到依赖方业务系统现场将 CA 证书安装到业务系统中；

3）天威诚信、注册机构或其合作伙伴分发给依赖方的软件中绑定、包含有 CA 证书。

对于天威诚信的其他 CA 公钥，除了上面所述的方式传输给依赖方外，当证书用户获取证书时天威诚信通过 PKCS#7 格式将除根证书外的证书链传递给用户。

5 密钥长度

符合国家密码管理部门的要求。

6 公钥参数的生成和质量检查

符合国家密码管理部门的要求。

7 密钥使用目的

根 CA 的密钥用于签发运营 CA 的证书及 CRL，运营 CA 的密钥用于签发用户证书。用户的签名密钥可用于提供身份认证、抗抵赖、以及信息完整性等目的，加密密钥可用于信息加密和解密。

6.6.2.2. 私钥保护和密码模块工程控制

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、备份和恢复遵循国家密码主管部门相关规范要求。

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，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。

用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，用户应妥善保护、保管其密码模块，防止其失窃、丢失、损坏及被非授权的使用。

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，或分割密钥），这 5 张 IC 卡由天威诚信 5 名可信雇员持有（称为分管者），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，分割密钥存储在屏蔽机房的保险盒中。

天威诚信的 CA 私钥的激活需要由密钥管理者持有的用户权限 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。

3 私钥托管

天威诚信所有 CA（包括根 CA 和运营 CA）的私钥均未在其他地方托管。

根据国家密码管理部门的要求，天威诚信的用户的加密证书私钥托管在天威诚信屏蔽机房密钥管理系统中。

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；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。

对于用户证书，如果存放证书私钥的密码模块允许私钥备份，天威诚信建议用户对私钥进行备份，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。

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十年。归档 CA 密钥对保存在本节第 1 条所述的加密机中，并且天威诚信的密钥管理策略和流程阻止归档 CA 密钥对返回到产品系统中。对归档私钥到了归档保存期，天威诚信将按本节第 10 条销毁。

对于认证机构运营设备证书，天威诚信或其注册机构通常不进行私钥归档，因为这种归档是不需要的；但对某些特别的运营设备证书，如 CA 端的 AA 证书和时间戳证书，天威诚信数字认证中心会对其私钥进行归档，其归档过程和要求同 CA 密钥对。

天威诚信或其注册机构不对最终用户证书的私钥进行归档，但如果用户存放证书私钥的密码模块允许私钥备份，天威诚信建议用户对私钥进行归档，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 私钥导入、导出密码模块

天威诚信 CA 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。

对于用户证书，若使用的密码模块（软件或硬件）支持私钥的导出、导入，则天威诚信要求用户对导出、导入的私钥必须使用足够安全的口令进行保护，且用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。

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。

对于用户证书，用户需将私钥保存在国家密码主管部门认可的密码模块中，且存放私钥的密码模块必须在用户其可控制的范围内，用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。

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 6.6.2.2 使用加密设备的操作员权限实现，即需要密钥管理员提供操作员 IC 卡进行激活。

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。

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。

用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。

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。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。

对于用户证书私钥，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，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。

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。

6.6.2.3. 密钥对管理的其他方面

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。

2 证书操作期和密钥对使用期限

对于 CA 证书，密钥对通过证书更新允许的最长使用期限如下：

- 对于 256 位 SM2 根 CA 证书，其密钥对的最长允许使用年限是 30 年。
- 对于 256 位 SM2 中级 CA 证书，其密钥对的最长允许使用年限是 20 年。
- 对于用户证书的最长有效期不超过 5 年 3 个月。

A. 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。

B. 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。

C. 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。

D. 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。

E. 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。

6.6.2.4. 激活数据

1 激活数据的产生和安装

天威诚信 CA 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。

如果用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。

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

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。

用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。如果证书用户使用口令或 PIN 码保护私钥匙，用户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书用户使用生物特征保护私钥，用户也应注意防止其生物特征被人非法窃取。

3 激活数据的其他方面

1）激活数据的传送

存有天威诚信数字认证中心 CA 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。

通常情况下用户证书私钥的激活数据由用户自己产生、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，用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。

对于申请证书的用户激活数据的生命周期，建议如下：

1、用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，建议用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。

2）激活数据的销毁

存有天威诚信数字认证中心 CA 私钥的激活数据分割的 IC 卡，其销毁所采取的方法包括将 IC 卡初始化，或者彻底销毁 IC 卡，无论采取何种方式，都将保证不会残留有任何秘密信息。CA 私钥激活数据的销毁是在天威诚信安全管理人员和密钥管理人员的监督下进行。

当用户证书私钥的激活数据不需要时应该销毁，用户应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

6.6.2.5. 计算机安全控制

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。

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。

6.6.2.6. 生命周期安全控制

1 CA系统运行管理

A. CA 系统的操作流程采用文档化并进行维护。

B. CA 系统（包括软件、网络等方面）的变更按系统变更控制流程经管理层批准，经批准的变更实行前通过测试验证，并进行记录。

C. 可能对系统的安全性有影响的改动必须事先由管理层得进行风险评估，改动前进

行备份并得到管理层的明确批准。

D. CA 中心的测试系统、运营系统、网络设施等，都由专门的操作维护人员，并有相应明确的授权。

E. 操作维护人员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。

F. 建立了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。

G. 建立了监控流程，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。

H. 建立了相应制度，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。

2 CA系统的访问管理

A. 制定了 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 3/2 规则）等。

B. 制定了 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。

C. 制定了网络安全策略，并制定了访问网络的控制策略。

D. 制定了操作系统及 CA 软件的安全访问的策略。

E. 建立了对各种对 CA 系统访问的审计措施。

3 CA系统的开发和维护

A. 建立了 CA 系统软件修订控制流程，对系统新增或修改进行管理。

B. 严格控制对 CA 系统的源代码及测试数据的访问。

C. 操作系统升级变更时，对应用系统软件重新测试。

D. 在 CA 系统中，购买、使用或修改的软件，严格检查，避免“特洛伊木马”等攻击。

6.6.2.7. 网络安全控制

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。

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。

6.6.2.8. 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. 电子政务电子认证服务中的法律责任相关要求

7.1. 要求

天威诚信在开展电子认证服务时，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。

天威诚信在本电子政务CPS中明确一般性的业务和法律问题。在业务条款中说明不同服务的费用问题，和各参与方为了保证资源维持运营，针对参与方的诉讼和审判提供支付所需承担的财务责任；法律责任条款涉及保密、隐私、知识产权、担保及免责等内容，具体涵盖的内容见“7.2内容”。

7.2. 内容

7.2.1. 费用

1 证书服务涉及的费用标准：

- 天威诚信根据市场和管理部门的规定制定证书初始签发和更新的价格。
- 天威诚信不收取证书查询费用。
- 免费提供证书撤消和撤消列表（CRL）查询。
- 天威诚信有可能根据需要将在线查询（OCSP）服务作为增值服务收取费用。

2 退款规定

在实施证书操作和签发证书的过程中，天威诚信遵守并保持严格的操作程序和策略。一旦用户接受数字证书，天威诚信将不办理退证、退款手续。

如果由于天威诚信的原因，造成用户合同无法履行、用户证书无法使用，天威诚信将费用返还给用户。

如果由于不可抗力因素导致天威诚信暂停、终止部分或全部电子签名认证证书服务，天威诚信不承担退款责任。

7.2.2. 财务责任

1 保险范围

天威诚信向证书用户提供证书使用保障。如果由于天威诚信原因造成用户使用证书过程中遭受损失，天威诚信公司将向证书用户、依赖方提供赔偿（具体情形参见 7.2.9）。

2 其他资产

天威诚信具备国家密码主管部门所规定的资金实力，具备承担赔偿责任的条件。

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用户及证书依赖方。

最终实体可依据生效的法律文书（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 7.2.9 节规定对最终实体承担有限赔偿责任。

7.2.3. 业务信息保密

天威诚信有专门的信息保密制度，保护自身和客户的敏感信息、商业秘密。

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） 天威诚信订户的数字签名及解密密钥。

2） 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。

3） 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。

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。

其它天威诚信信息的保密性取决于特殊的数据项和申请。

3 保护保密信息的责任

天威诚信有妥善保管与保护 7.2.3 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、司法机关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、法规以及司法机关的要求，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。

7.2.4. 个人隐私保密

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

2 作为隐私处理的信息

作为隐私处理的信息包括订户注册证书中提交的、但不在证书中显示的信息，如联系电话、地址、个人与天威诚信、天威诚信注册机构签订的协议等。

3 不被视为隐私的信息

不被认为是隐私信息包括，要出现在证书中的信息、证书及证书状态信息。

4 保护隐私的责任

除非执法、司法方面的强制需要，天威诚信及其注册机构在没有获得客户授权的情况下，不会将客户隐私信息透露给任意第三方。

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。

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订户隐私信息。

7 其他信息披露情形

对其他信息的披露受制于法律、用户协议。

7.2.5. 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。

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。

7.2.6. 陈述和担保

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。

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。

2 RA 的陈述与担保

天威诚信认证机构的注册机构做出如下担保：

RA 在批准证书前，完成了所有必要的鉴证工作，并且确认了信息是正确的、准确的。

3 用户的陈述与担保

作为获得证书的一个条件，证书申请者在证书申请时已阅读了用户协议并且同意用户协议，并且：

- 在证书申请时，用户的所有陈述都是对的；
- 用户提供的，特别是包含在证书中的需要鉴别、验证的信息是真实的、准确的。

在证书的保存和使用过程中，用户同意做到：

- 按照天威诚信的 CPS 将证书用于规定的使用目的，不将证书用于证书使用目的以外的场合；
- 利用与证书中的公钥相对应的私钥产生的数字签名是用户的数字签名，用户知晓要签名的内容，产生数字签名时，用户已经接受了证书，且该证书没有过期或撤销。
- 用户对自己的私钥进行了有效的保护，其他人员无法使用用户的私钥。

4 依赖方的陈述与担保

依赖方确认，在任何信赖行为发生之前，阅读了依赖方协议，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。

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应遵守本 CPS 的所有规定。

7.2.7. 担保免责

天威诚信不对其签发的证书适用于其规定的目的以外的任何应用承担任何担保，对证书在其规定的目的以外的应用不承担任何责任。对由不可抗力，如战争、地震、洪灾、爆炸、恐怖活动等，造成的服务中断并由此造成的客户损失，天威诚信及注册机构不承担责任。

7.2.8. 偿付责任限制

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 7.2.9 节规定的有限赔偿责任。

7.2.9. 赔付责任

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：在任何情况下每张证书赔偿额不得超过证书购买价格的 10 倍。

如天威诚信违反了本 CPS 第 7.2.6 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。

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。

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。

有下列情形之一的，天威诚信不承担赔付责任：

1） 因订户原因致使依赖方遭受损失的；

2） 依赖方未经检验证书的状态即决定信赖证书的；

3） 依赖方明知或者应当知道证书存在超范围使用、超期限使用、被人窃取或者信息错误等情况，仍然信赖该证书并从事有关活动的；

4） 因不可抗力原因导致订户或者依赖方遭受损失的。

7.2.10. 有效期和终止

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政务电子认证服务时失效。

2 终止

当天威诚信终止业务时，天威诚信的电子政务 CPS 终止。

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。

7.2.11. 对参与者的个别通告与沟通

天威诚信及其注册机构在必要的情况下，如在主动撤销用户证书、发现用户将证书用于规定外用途及用户其他违反用户协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知用户或用户所属机构、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。

7.2.12. 修订

1 修订程序

本认证业务规则将不定期的进行修改，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，并符合认证业务开展的实际需要。

本 CPS 的修改和更新，由 CPS 编写小组负责完成，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。

2 通知机制与期限

修订后的 CPS 经批准后将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。

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。

7.2.13. 争议处理

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。

7.2.14. 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》、《电子政务电子认证服务管理办法》等法律法规的约束。

7.2.15. 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。

7.2.16. 一般条款

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。

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。

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。

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继续不执行该项或其他规定。

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、注册机构无法提供正常的服务时，天威诚信、注册机构不承担由此给客户造成的损失。

7.2.17. 其他条款

天威诚信对本 CPS 具有最终解释权。