天津数字认证有限公司

电子政务电子认证服务业务规则

V2.5

天津数字认证有限公司

2025年2月

版本信息

当前版本号	最近更新日期
V2.5	2025.2.11

修订记录：

日期	修订说明	修订版本	修订人	审核人
2018.11	创建本 CPS	V1.0	李维	安全策略委员会
2020.11.3	按照新版《电子政务电子认证服务业务规则规范》要求重新修订本CPS；修订官方网址、邮箱；增加云证书、事件证书、手机证书身份标识与鉴别；云证书、事件证书、手机证书生命周期操作要求；云证书、事件证书、手机证书密钥的安全控制。	V2.0	李维	安全策略委员会
2022.1.21	修订1.4.2联系人地址；6.1.3机房等级、相对湿度数值；2.2身份标识与鉴别。	V2.1	李维	安全策略委员会
2023.1.5	修订版权声明中联系电话； 修订3.2.2 组织机构身份的鉴别，增加法定代表人身份鉴别的方式。	V2.2	李维	安全策略委员会
2023.10.8	修订了修订1.1.1公司简介； 修订了1.4.2 联系方式中地址、联系方式，删除了传真； 修订了3.6 密钥更新、3.6.1密钥更新的情形、3.6.2证书更新的情形 修订6.1.1场地位置与建筑中UPS品牌型号； 公司名称变更。	V2.3	李维	安全策略委员会
2023.12.29	修订2.2.2 组织机构身份的鉴别 修订2.2.3 个人身份的鉴别 修订2.3密钥更新请求的标识与鉴 修订3.1.3 申请过程与责任	V2.4	李维	安全策略委员会

	修订3.4.2 认证机构对证书的发布 修订3.6.1 密钥更新的情形 修订3.6.2 证书更新的情形 修订3.6.3 证书更新的提交 修订3.7.1 证书变更的情形			
2025.2.11	修订1.1.1概述 修订1.3.5各方主要责任 修订1.4.2联系人 修订3.8.3证书撤销的申请 修订6.1.1.场所区域与建筑物 修订6.1.2.物理访问 修订6.1.3.电力与空调	V2.5	李维	安全策略委员会

电子政务电子认证服务业务规则

天津数字认证有限公司版权声明

目 录

1.概括性描述

1.1.概述

天津数字认证有限公司（以下简称“天津CA”）成立于2018年，注册资金5千万元，是天津数字经济产业集团有限公司的国有控股子公司，致力于为电子政务、电子商务及社会信息化等应用提供优质的电子认证服务。

天津数字认证有限公司依照《中华人民共和国电子签名法》、《电子认证服务密码管理办法》和《电子政务电子认证服务管理办法》的要求，于2017年10月完成系统建设。天津CA机房位于天津市滨海高新区兰苑路13号OVU中电科创园A1座507，占地面积142平方米、整体设施设备齐全、系统建设符合国家相关标准要求。

天津CA自成立以来，严格按照国家规定的各项要求进行系统建设和管理，于2018年5月首次获得了国家密码管理局颁发的《电子认证服务使用密码许可证》，2018年11月首次获得了工业和信息化部颁发的《电子认证服务许可证》，2019年1月通过了国家密码管理局电子政务电子认证服务能力评估

1.2.电子政务电子认证业务范围

电子政务电子认证业务范围包括面向政务部门、企事业单位、社会团体和社会公众的电子政务电子认证服务。

1.3.电子政务电子认证活动参与者

1.3.1.电子政务认证机构

天津CA是根据《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法（试行）》规定，依法设立的电子政务电子认证服务机构（简称：CA机构）。

CA机构是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。

1.3.2.注册机构

注册机构（简称：RA机构）是受理数字证书的申请、更新、恢复和撤销等业务的实体。

1.3.3.依赖方

依赖方是指信赖于证书所证明的基础信任关系并开展业务活动的实体。

1.3.4.其他参与者

其他参与者指为CA证书服务体系提供相关服务的其他实体。

1.3.5.各方主要责任

CA机构可以授权下属机构或委托外部机构作为注册机构，负责提供证书业务办理、身份鉴证与审核等服务。

CA机构授权外部机构作为注册机构，对注册机构开展电子签名认证证书注册业务的行为进行监督，应在与外部机构签署的合同中，明确双方的权利、义务以及法律责任。

1.4.电子政务电子认证策略管理

1.4.1.管理机构

策略文档管理机构为天津CA安全策略委员会，作为策略管理机构负责制订、发布、更新本CPS。天津CA安全策略委员会来自于公司管理层、运营管理部、安全管理部、客户服务部、行政管理部等拥有决策权的合适代表。

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

本策略文档的对外咨询服务等日常工作由安全管理部负责。

1.4.2.联系方式

天津CA将对电子政务电子认证服务业务规则进行严格的版本控制，并由天津CA指定专人负责。

联系人：李维

电话：022-23522103/400-0566-110

地址：天津市滨海高新区兰苑路13号OVU中电科创园A1座507（300060）

电子邮件：tjzhca@126.com

网站地址：https://www.tjzhca.com

1.4.3.批准程序

1. 按照国家密码管理局规定的《电子政务电子认证服务业务规则规范》的要求，在天津CA电子政务电子认证服务业务规则作出的任何变动之前，由天津CA安全部门对提供的变动建议进行研究,并征询天津CA法律顾问有关方面的意见。

2. 提交天津CA安全策略委员会审核。

3. 天津CA根据《电子政务电子认证服务管理办法》中规定，在本机构网站（https://www.tjzhca.com）予以公布，并从对外公布之日起三十日之内向国家密码管理局备案。

1.5.定义和缩写

A.公钥基础设施(PKI)

公钥基础设施（Public Key Infrastructure，简称PKI）是利用公钥加密技术为电子认证的开展提供一套安全基础平台的技术和规范。它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，提供互联网环境的身份鉴别、信息加解密、数据完整性和不可否认性服务。

B.电子认证业务规则(CPS)

电子认证业务规则（Certificate Practice Statement ，简称CPS）是关于CA的颁发和管理证书的运作规范的描述，包括CA整体运行规范和证书的颁发、管理、撤销和密钥以及证书更新的操作规范等事务。

C.电子认证服务机构(CA)

电子认证服务机构（Certification Authority，简称CA）是受证书持有者信任的，负责签发数字证书的权威机构，又称为数字证书认证中心。作为电子交易中受信任的第三方，负责为电子认证业务中各个实体颁发数字证书，以证明各实体身份的真实性，并负责在交易中检验和管理证书。

D.注册机构(RA)

注册机构（Registration Authority，简称RA）是具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销或冻结证书。处理证书持有者撤销或冻结其证书的请求，同意或拒绝证书持有者延期其证书或更新密钥的请求。但是，RA并不签发证书（即RA代表CA承担某些任务）。

E.数字证书(证书)

数字证书是电子认证服务机构签发的用以证明证书持有者的电子签名、身份、资格及其他有关信息的电子文件。证书包含有公开密钥拥有者的信息、公开密钥、签名算法和CA的数字签名。

F.证书撤销列表(CRL)

证书撤销列表(Certificate Revocation List，简称CRL)，是一种包含撤销的证书列表的签名数据结构。CRL是证书撤销状态的公布形式，就像信用卡的黑名单，它通知证书持有者某些电子证书不再有效。

G.CA注销列表(ARL)

一个经电子认证服务机构电子签名的列表，标记已经被撤销的CA的公钥证书的列表，表示这些证书已经无效。

H.在线证书状态协议（OCSP）

在线证书状态协议是用于检查数字证书在某一交易时间是否有效的标准。

I.证书策略（CP，Certificate Policy）

策略（Certificate Policy，简称CP）是一套命名的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。

J.私钥 Private Key

私钥（Private key）是在公钥基础设施（PKI）中为一个密码串，由特定算法与公钥一起生成，用于解密信息或进行数字签名。在数字签名中又称为电子签名制作数据，是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。

K.公钥 Public Key

公钥(Public key)是在公钥基础设施（PKI）中为一个密码串，由特定算法与私钥一起生成，用于加密信息或验证数字签名。在数字签名中又称为电子签名验证数据，是用于验证电子签名的数据，包括代码、口令等。

L.甄别名(DN , Distinguished Name)

甄别名(DN , Distinguished Name)是在数字证书的主体名称域中，用来唯一标识证书持有者的X.500名称。此域需要填写反映证书持有者真实身份的、具有实际意义的、与法律不冲突的内容。

1.6.电子政务电子认证业务规范

1.6.1.适合的证书应用

天津CA签发的数字证书适合应用在电子政务领域，用于证明证书持有者在电子化环境中所进行的身份认证和电子签名，以及数据加密等服务。

根据证书的功能以及使用证书的实际应用，目前天津CA签发的主要证书类型分为通用型证书（机构、个人和设备等证书）、云证书、事件证书、手机证书，具体如下：

A.机构证书：机构包括政务机关、事业机构和参与电子政务业务的社会公众团体等。此类证书通常用于数字签名、加密解密以及网上身份认证等，在不违背相关法律法规、本CPS以及数字证书服务协议的情况下，此类证书也可以用于其他用途；

B.个人证书：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，此类证书通常用于数字签名、加密解密等；

C.设备证书：设备包括电子政务系统中的或其他设备服务器等，此类证书通常用于网上设备的身份认证，在不违背相关法律法规、本CPS以及数字证书服务协议的情况下，此类证书也可以用于其他用途。

D.云证书：面向移动互联网和云服务等新技术领域业务场景的签名需要，天津CA签发基于云服务的数字证书。该证书是在业务过程中证书持有者通过应用系统实名认证后，向天津CA申请签发的证书。证书持有者将证书私钥托管到天津CA的专用的密码设备中保存，天津CA确保证书持有者私钥的安全性。证书持有者自己保存调用私钥的方法（包括但不限于PIN码、短信验证码等）。

E.事件证书：天津CA面向签名行为业务场景签发出的数字证书。在业务过程中，根据证书持有者提交的业务场景中相关信息（电子文档、签名行为特征信息、手写笔迹或其他签名行为证据信息等）自动固化至数字证书的扩展域，签发出事件证书。事件证书所对应的私钥为一次性使用，对业务场景的信息数据进行电子签名，在使用后即被销毁。

F.手机证书：天津CA面向移动互联网等新技术领域所签发出的手机证书，该类型证书支持在使用移动端设备的环境中应用数字签名、身份认证等证书服务功能。通过手机证书与服务，在移动互联网领域可以实现各参与主体身份的真实性、信息的完整性以及签名行为的不可抵赖性。

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

1.6.2.限制的证书应用

本CA机构发放的数字证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，由此造成的法律后果由证书持有者负责。

1.7.策略发布与管理

1.7.1.策略的发布

天津CA在官方网站https://www.tjzhca.com发布信息库，该网站是天津CA发布所有策略最主要、最及时、最权威的渠道。

天津CA通过目录服务器发布证书持有者的证书和CRL，证书持有者或依赖方可以通过访问天津CA的目录服务器获取证书的信息和撤销证书列表；天津CA也提供在线证书状态查询服务，证书持有者或依赖方可实时查询证书的状态信息。同时，天津CA也将会根据需要采取其他可能的形式进行信息发布。

1.7.2.策略发布的时间和频率

天津CA在证书持有者证书签发或者撤销时，通过目录服务器或官方网站自动将证书和CRL发布，发布周期为不大于24小时，即在24小时内发布最新CRL；在紧急的情况下，天津CA可以自行决定证书和CRL的发布时间。信息库其他内容的发布时间和频率，由天津CA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。

1.7.3.策略访问控制

对于公开发布的CP、CPS 和CA证书等公开策略，天津CA允许公众自行通过网站进行查询和访问。

天津CA设置了电力访问控制和安全审计措施，保证了CPS、证书、CRL等电子认证信息库只有经过授权的天津CA工作人员才能控制和修改。

1.7.3.1.策略的发布与处理

对于以网站方式公布的策略，天津CA允许任何公众进行查询和访问。证书和CRL除公司网站外，还可通过LDAP方式发布，同时提供OCSP在线验证方式。但只有天津CA有权对公布的各类策略进行处理。

1.7.3.2.策略访问控制和安全审计

天津CA设置了策略访问控制和安全审计措施，保证了CPS、证书、CRL等电子认证策略只有经过授权的天津CA工作人员才能控制和修改。

2.身份标识与鉴别

2.1.命名

2.1.1.名称类型

天津CA颁发的数字证书，根据证书对应实体的类型不同，其实体名字可以是人员姓名、组织机构名称、部门名、域名等，证书包含证书持有者和颁发机构主题甄别名，对证书申请者的身份和其他属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是证书持有者的唯一识别名。

天津CA的证书符合X.509标准，分配给证书持有者实体的甄别名，采用X.500标准命名方式，格式如下：

属性	值	举例
Country（C） =	国家	CN
Organization（O） =	组织	津投资本
Organizational Unit（OU） =	组织机构	数字经济产业集团
State or Province （S） =	省	天津
Locality（L） =	区	河西区
Common Name（CN） =	通用名	天津数字认证有限公司
Email=	邮件地址	tjzhca@126.com

天津CA的证书包含颁发者的甄别名称，格式如下：

属性	值	举例
Country（C） =	国家	CN
Organization（O） =	组织	ZHCA
Common Name（CN） =	通用名	ZHCA

2.1.2.对名称意义化的要求

天津CA签发的机构证书、个人证书、设备证书、云证书、事件证书、手机证书等包含的命名应具有通常理解的语义，用它可以确定证书主题中的证书持有者

的身份。对于具有特殊要求的应用中，天津CA可以按照一定的规则为证书持有者指定特殊的名称，并且能够把该类特殊的名称与一个确定的实体唯一联系起来。

2.1.3.证书持有者的匿名或假名

证书持有者在证书中的名称不可以是假名或匿名，仅接受可追溯的名称作为唯一标识符。使用假名或伪造材料者申请的证书无效，一经证实立即予以撤销。

2.1.4.理解不同名称形式的规则

天津CA签发的数字证书符合X.509标准，甄别名格式遵守X.500标准，甄别名的命名规则由天津CA定义与解释。

2.1.5.名称的唯一性

在天津CA信任域内，不同证书持有者证书的主题甄别名不能相同，必须是唯一的。但对于同一证书持有者，可以用其主体名为其签发多张证书，但证书的密钥用法扩展项不同。当证书申请中出现不同证书持有者存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

2.2.身份标识与鉴别

2.2.1.证明拥有私钥的方法

天津CA证明拥有私钥的方法是根据证书申请信息进行验证。在天津CA证书服务体系中，用户证书请求信息中包含用私钥进行的数字签名，天津CA用其对应的公钥来验证这个签名，验证成功后，证书申请人被视作其签名私钥的唯一持有者。

2.2.2.组织机构身份的鉴别

对组织机构的身份或组织机构中个人身份的鉴别按照以下方式进行：

1. 组织机构证明材料的提交方式分为以下几种：

1）组织机构经办人携带机构有效证件原件或复印件（加盖公章）、法定代表人身份证原件或复印件（加盖公章）、经办人身份证原件或复印件（加盖公章），到数字证书业务受理机构，填写数字证书申请表，经过机构盖章，表示接受证书业务申请的有关条款，并承担相应的责任。

2）组织机构通过在线化、移动化的方式提交用户身份鉴别申请，分为线上材料审核和第三方数据审核两种方式。线上材料审核组织机构需要提交授权

委托书、机构有效证件原件或复印件（加盖公章）、法定代表人身份证原件或复印件（加盖公章）、经办人身份证原件或复印件（加盖公章）扫描件或照片。第三方数据审核由天津CA通过组织机构身份信息权威数据源比对、对公账号信息验证或者法定代表人人体生物特征识别、活体检测、身份信息权威数据源比对、金融验证、手机验证等认证技术进行身份鉴别。

3)对于证书应用于甲方内部环境中，可由甲方单位出具证明的形式进行身份确认，由甲方委托的经办人进行证书申请。

2. 天津CA发证机构的审核人员对证书持有者申请资料的真实性进行审查并进行批准或拒绝的操作。

2.2.3.个人身份鉴别

天津CA的个人证书签发给合法的个人申请者，天津CA需要严格审核个人申请者的身份。

通过鉴别政府机构发放的合法性文件，如：居民身份证、军官证、护照等证明证书持有者的身份。若委托他人进行证书申请的，应同时提供被委托人的身份证明。

天津CA对个人身份鉴别的模式有以下几种：

1.面对面方式

个人可持上述有效身份证件亲自到天津CA授权的注册机构提交书面证书申请表和身份证件的复印件等申请材料到现场办理。

2.在线方式

个人可在线提交本人签字确认的证书申请表、有效的个人身份证件原件的电子版，天津CA发证机构的审核人员对证书持有者申请资料的真实性进行审查并进行批准或拒绝的操作。

或使用具有人体生物特征识别、活体检测、身份信息权威数据源比对、金融验证、手机验证等认证技术进行身份鉴别。

3.对于应用于甲方内部环境的个人证书，可由甲方单位出具证明的形式进行个人身份确认，由甲方委托的经办人进行证书申请。

2.2.4.政府部门个人身份鉴别

政府部门个人身份鉴别参照个人身份鉴别方法进行鉴别。

2.2.5.设备身份鉴别

如果证书的名称为域名（或IP地址），除了在对申请者递交的书面材料进行审核外，天津CA需要申请者提供额外的域名（IP地址）使用权证明材料，以确定申请者是否有权使用相应的域名（IP 地址）。天津CA在进行了法律规定的有限审查后，不承担对申请者申请资料进行合法的鉴别，申请者自行负责申请材料的真实性。

2.2.6.云证书证书持有者身份的鉴别

云证书证书持有者身份的鉴别参照个人身份和机构身份鉴别方法进行鉴别。

2.2.7.事件证书证书持有者身份的鉴别

事件证书证书持有者身份的鉴别参照个人身份和机构身份鉴别方法进行鉴别，也可以采取包括录音、录像等有效的身份核验方式进行自动鉴别。

2.2.8.手机证书证书持有者身份的鉴别

手机证书证书持有者身份的鉴别参照个人身份和机构身份鉴别方法进行鉴别。

2.2.9.没有验证的证书持有者信息

除该类型证书所必须要求的身份信息需要得到明确、可靠的验证以外，天津CA不对申请时的其他信息予以验证。

对于没有验证过的证书持有者信息，天津CA将不承诺此类信息的真实性，并不承担由于此类信息引起的任何责任和解决纠纷的义务。

2.2.10.授权确认

证书申请者申请某一类型的证书时，天津CA和其授权的证书服务机构还需审核申请经办人的身份和资格，包括必需的身份资料和授权证明文件。机构或个人在天津CA数字证书申请文件上签字或加盖公章后，则证明其对办理人员的授权确认。

2.2.11.互操作准则

对于天津CA外的其他证书服务机构颁发的证书，可以与天津CA进行互操作，但是必须符合天津CA的电子认证业务规则，并且与天津CA签署了相应的协议。

2.3.密钥更新请求的标识与鉴别

在订户证书到期前，为了保证证书使用的连续性，订户需要获得一张新的证书。天津CA一般要求订户产生一个新的密钥对代替原密钥对，称为“密钥更新”。在某些应用场景下，天津CA允许订户使用原密钥对申请一张新证书，称为“证书更新”。对于密钥更新而言，订户证书除公钥、有效期和序列号改变外，其他信息都没改变；对于证书更新而言，和密钥更新相比，订户证书公钥也不改变。

2.3.1.常规密钥更新的标识与鉴别

对于常规通用型证书密钥更新，证书持有者可以用原有的私钥对更新请求进行签名。天津CA认证系统会对证书持有者的签名和更新请求进行鉴别。

证书持有者也可以选择一般的初始证书申请流程，按照申请人身份验证步骤进行常规密钥更新，按照要求提交相应的证书申请和身份证明资料。

天津CA授权的发证机构的审核人员合理、审慎地核对申请资料的原件与复印件，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，并进行批准或拒绝的操作。

密钥更新会造成使用原密钥对加密的文件或数据无法解密，因此，证书持有者在申请密钥更新前，天津CA会告知证书持有者使用原密钥对加密的文件或数据进行解密，如证书持有者未按照天津CA所告知的内容进行文件或数据解密，由此造成的损失，天津CA将不承担责任。

云证书密钥更新中，通过证书持有者使用当前有效私钥对包含新公钥的密钥更新请求进行签名，CA机构使用证书持有者原有公钥验证确认签名来进行证书持有者身份标识和鉴别。

事件证书没有密钥更新。

手机证书的密钥更新，和通用型证书的密钥更新的标识与鉴别要求一致。

2.3.2.撤销后密钥更新的标识与鉴别

天津CA不提供证书被撤销后的密钥更新。证书持有者必须重新进行身份鉴别，按照初始身份验证步骤向天津CA申请重新签发证书。

2.3.3.证书变更的标识与鉴别

证书变更是指证书持有者的证书信息发生变更，申请重新签发一张证书，对原证书进行撤销处理。

证书变更的标识与鉴别使用原始身份验证相同的流程，其要求与2.2.2至2.2.7节相同。

事件证书没有证书变更。

2.4.撤销请求的标识与鉴别

在天津CA的证书业务中，证书撤销请求可以来自证书持有者，也可以来自天津CA。当天津CA授权的发证机构发现证书持有者有如本CPS3.8.1中描述的证书撤销的情况时，有权撤销证书，这种情况无须进行鉴证。如果证书持有者主动要求撤销证书，则需要递交初始身份验证时的申请材料。如果是司法机关依法提出撤销，天津CA将直接以司法机关提供的书面撤销请求文件作为鉴别依据，不再进行其他方式的鉴别。

3.数字证书服务操作规范

3.1.证书申请

3.1.1.证书申请流程

1.用户到天津CA受理点索取或网站下载《天津CA数字证书申请表》，以及《天津CA数字证书服务协议》。

2.用户填写《天津CA数字证书申请表》之前需仔细阅读《天津CA数字证书服务协议》，同意后签章，遵守其中的各项规定。

3.用户按《天津CA数字证书申请表》所列各项如实填写并签章。

4.以个人用户现场新申请证书为例：

A.用户办理证书申请业务时应在“证书申请”选项上打勾，填写用户基本信息，签字确认。《天津CA数字证书申请表》一式二联，一联受理机构存档，一联申请人留存。

B.填写完毕后，为确定申请者的真实身份，申请者需携带本人身份证原件、《天津CA数字证书申请表》一式二联、《天津CA数字证书服务协议》一式二联前往天津CA业务受理点，即可办理个人数字证书申请业务。

C.天津CA鉴证服务员对用户提交的以上资料进行审核，审核通过后（24小时之内），用户缴纳证书相关费用。

D.天津CA鉴证服务员将用户相关资料及缴费证明交由天津CA业务办理员，由业务办理员为用户签发个人数字证书（一个工作日之内）。

E.证书签发完毕后，由天津CA业务办理员直接下载，并将装有个人数字证书的USB KEY交给用户。

5. 以机构用户线上新申请证书为例：

A.用户登录天津CA自助服务网站;

B.选择业务类型“证书申请”后选择所属应用;

C.阅读并同意《天津数字认证有限公司数字证书服务协议》;

D.在线填写申请信息生成并打印申请表;

E.上传证书申请所需材料;

F.在线生成申请订单;

G.由鉴证服务员对资料的真实性进行审查;

H.审核通过后由业务办理员为签发证书;

I.采用邮寄方式送达用户手中。

6. 天津CA客户服务部为客户办理证书业务提供的服务方式有：热线电话支持、现场服务支持、邮箱方式等。

3.1.2.证书申请实体

证书申请实体包括政府机关、事业单位、政府部门的工作人员及参与电子政务业务的社会团体和公众。

3.1.3.申请过程与责任

3.1.3.1.证书的申请过程

天津CA的数字证书申请有线下申请和在线申请两种方式，证书持有者将证书申请资料及身份鉴别资料递交给天津CA的注册机构进行证书申请，注册机构审核通过后，录入申请资料。其中审核员和业务办理员分别为两个不同的系统操作人员。

注册机构向天津CA提交证书请求，通过应用安全协议发送至天津CA。

天津CA根据注册机构的请求签发证书。

3.1.3.2.责任

证书持有者有责任向天津CA提供真实、完整和准确的证书申请信息和资料。

注册机构承担对证书持有者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。

3.2.证书申请处理

3.2.1.执行识别与鉴别功能

当天津CA及其注册机构接受到证书持有者的证书申请后，应按2.2.2至2.2.8节中申请的身份确认的要求，对证书持有者进行身份识别与鉴别。

天津CA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。

3.2.2.证书申请批准和拒绝

依据识别与鉴别的信息，天津CA授权的发证机构有权决定接受或拒绝证书持有者的申请。

如果符合下述条件，天津CA授权的发证机构接受证书持有者的证书申请：

1）成功标识和鉴别了证书持有者的身份信息；

2）证书持有者接受数字证书服务协议的内容和要求；

3）证书持有者按照规定支付了相应的费用，另有协议规定的情况除外。

如果发生下列情形之一，天津CA授权的发证机构有权拒绝证书持有者的证书申请：

1）证书持有者不提供鉴别所需材料或在鉴别过程中不予配合；

2）证书持有者不能提供所需要的补充文件；

3）证书持有者不接受或者反对数字证书服务协议的内容和要求；

4）没有或者不能够按照规定支付相应的费用；

5）天津CA授权的发证机构认为批准该申请将会对天津CA带来争议、法律纠纷或者损失。

3.2.3.处理证书申请的时间

天津CA授权的发证机构必须在1个工作日内对证书申请者提交的证书信息进行识别，并完成证书申请处理。

事件证书申请为即时处理。

3.3.证书签发

3.3.1.证书签发中注册机构和认证机构的行为

在证书的签发过程中RA的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有RA的身份签名信息与信息加密措施，并确保请求发至正确的CA证书签发系统。

CA的证书签发系统在获得RA的证书签发请求后，对来自RA的信息进行身份鉴别与信息解密，对于有效的证书签发请求，证书签发系统签发证书持有者证书。

天津CA在批准证书申请之后，将签发证书。证书的签发意味着天津CA最终完全正式地批准了证书申请。

通常天津CA签发的证书在24小时内生效。

3.3.2.认证机构和注册机构对证书持有者的通告方式

对于通用型证书，天津CA会采取以下几种通告方式告知证书持有者：

1、通知证书持有者到注册机构或受理点面对面的方式领取证书；

2、电子邮件（Email）或短信；

3、其他天津CA认为安全可行的方式。

对于云证书，通过证书申请程序或系统对证书持有者进行通告。

对于事件证书，证书持有者成功完成数字签名，即视为CA机构证书签发成功，CA机构不再就证书签发向证书持有者进行其他方式的通告。

对于手机证书，证书持有者所使用移动终端应用程序会有数字证书已签发或下载成功的展示，天津CA不再就证书签发向证书持有者进行其他方式的通告。

3.3.3.证书获取方式

对于通用型证书，证书持有者获取证书的方式：

1、证书持有者到注册机构或受理点面对面的方式获取证书；

2、通过邮寄、快递的方式获取证书；

3、其他天津CA认为安全可行的方式。

对于云证书，通过证书申请程序或应用系统获取证书信息。

对于事件证书，证书持有者成功完成数字签名，即视为CA机构证书签发完成，证书持有者成功获取证书。

对于手机证书，通过移动终端应用程序获取证书信息。

3.4.证书接受

3.4.1.构成接受证书的行为

在天津CA通用型数字证书签发完成后，天津CA将把数字证书当面给证书持有者，证书持有者从获得证书起就被视为已同意接受证书。证书持有者接受数字证书后，应妥善保存其证书对应的私钥。

云证书签发完成后，并将证书应用于对应的电子签名时起，就被视为同意接受证书。

天津CA签发事件证书给证书持有者，证书应用于对应的电子签名时起，就被视为同意接受证书。

天津CA为证书持有者签发手机证书，证书持有者所使用移动终端设备或 APP 应用程序接收到数字证书起，就被视为同意接受证书。

3.4.2.认证机构对证书的发布

通用型证书的证书持有者接受证书后，天津CA在24小时内将该证书持有者证书发布到天津CA的目录服务系统。

天津CA采用主、从目录服务器结构来发布所签发证书。签发完成的数据直接发布到主目录服务器中，然后通过主从映射，将主目录服务器的数据自动同步到从目录服务器中，供证书持有者和依赖方查询和下载。

天津CA签发的云证书、手机证书、事件证书会将证书信息记录在指定的数据库中。根据依赖方约定，可向依赖方提供状态查询服务。

3.5.密钥对和证书的使用

天津CA要求证书持有者密钥对和证书的使用不能超过其规定使用范围，否则天津CA不承担由证书持有者违规使用而造成的任何责任。

3.5.1.证书持有者私钥和证书的使用

通用型证书的证书持有者接受到数字证书后，应妥善保存其证书对应的私钥。

对于签名证书，其私钥仅用于对信息的签名。证书持有者使用私钥对信息签名时，应该确认被签名的内容。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。

云证书由证书持有者通过PIN码或短信验证码等方式调用云端托管私钥完成数字签名。证书持有者只能在指定的应用范围内使用私钥和证书，证书持有者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，订证书持有者必须停止使用该证书对应的私钥。

事件证书仅应用于证书持有者对应的电子签名行为，证书持有者只能在该次电子签名中使用私钥和证书，证书持有者只有在接受了相关证书之后，才能使用对应的私钥执行电子签名运算。私钥将在完成本次电子签名运算后进行销毁，之后证书持有者须停止使用该证书对应的私钥。

手机证书必须由证书持有者移动端和签名服务云端协同配合才能完成一次数字签名。证书持有者只能在指定的应用范围内使用私钥和证书，证书持有者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，证书持有者必须停止使用该证书对应的私钥。

3.5.2.依赖方对公钥和证书的使用

依赖方只能在接受天津CA协议要求的前提下，才能依赖天津CA证书持有者证书。在信任证书和签名前，依赖方必须根据环境和条件进行合理地判断并做出决定。

在依赖证书前，依赖方必须独立的进行如下评估和判断：

1）证书是否由可信任的CA所签发；

2）证书被适当的使用，判断该证书没有被用于电子政务电子认证服务业务规则或者法律法规禁止或限制的使用范围；

3）证书的使用与证书密钥用途包含内容是否一致；

4）查询证书及其证书信任链中的证书状态，如果证书持有者证书或其信任链内的任何证书已经被撤销，依赖方必须独立去了解该证书持有者证书对应的私钥所做的签名是否是在撤销之前做的，是否可以依赖，并独立承担相应的风险。

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

获得对方的证书和公钥，可以通过查看证书以了解对方的身份，通过公钥验证对方电子签名的真实性，实现通信的不可抵赖性，并实现通信双方数据传输的保密性和完整性。

3.6.密钥更新

证书密钥更新定义：在不改变订户的信息下生成新密钥并申请新公钥签发新证书。除必须更新密钥的情形外，天津CA不采取证书密钥更新。

3.6.1.密钥更新的情形

订户申请更新密钥的情形主要有：

（1）证书即将到期或已经过期；

（2）证书载体丢失、损坏；

（3）证书的密钥泄露。对此，订户负有立即告知天津CA的责任。

事件证书密钥在使用过一次后即销毁，不提供证书密钥更新服务。

3.6.2.证书更新的情形

为保证通用型证书、云证书、手机证书及其密钥对的安全有效和证书持有者为保证数字证书及其密钥对的安全有效和订户的权利，天津CA会为签发的证书设置有效期。订户须在证书有效期到期前90日内到天津CA授权的发证机构申请证书更新。证书更新可以更换密钥对，也可以使用原有密钥对，视更新的具体证书应用场景而定。

事件证书密钥在使用过一次后即销毁，不提供证书证书更新服务。

3.6.3.更新申请的提交

证书持有者或其授权人通过已有私钥，在天津CA授权的发证机构通过PIN码验证和身份信息核查，进行更新请求；天津CA授权的发证机构按照身份识别与鉴定的规定对证书持有者提交的证书延期申请进行审核。发证机构审核通过后，为证书持有者制作证书；证书签发后，发证机构将证书当面发给证书持有者。证书持有者接受证书，新证书签发后原有证书将被撤销。天津CA将实时在LDAP上发布证书持有者的新证书。证书持有者被撤销的原有证书将在24小时内通过CRL发布。

证书持有者也可以选择一般的初始证书申请流程进行证书延期，按照要求提交相应的证书申请和身份证明资料。天津CA在任何情况下都可将这种初始证书申请的鉴别方式作为证书延期时的鉴别处理手段。

提出延期申请的证书持有者在进行证书延期之前应将加密邮件等加密过的文件进行解密，同时备份（例如将邮件内容复制以明文方式存储或将邮件附件保存），然后将证书删除。以上操作完成后才能进行证书的更新。如证书持有者未解密文件而进行证书延期，由此造成的可能损失，天津CA不承担任何责任。

3.6.4.更新申请的鉴别

同2.3密钥更新请求的标识与鉴别。

3.6.5.密钥更新方式

证书持有者在证书有效期到期前90日内，到天津CA授权的发证机构申请证书更新，也可以通过天津CA自助服务平台和天津CA证书助手进行线上更新。证书到期后将失效，用户无法使用证书。证书到期前90日内没有更新证书，证书持有者如需继续使用，必须重新申请新证书。

3.6.6.通知证书持有者密钥更新

证书持有者在证书有效期到期前90日内使用证书，天津CA证书助手会对证书持有者进行到期提示。

3.6.7.构成接受密钥更新的行为

同3.4.1构成接受证书的行为。

3.6.8.认证机构对密钥更新的发布

同3.4.2认证机构对证书的发布

3.6.9.认证机构对其他实体的通告

天津CA不具有向其它实体进行单独通告的义务，但使用证书的各类实体可以通过天津CA查询服务获得所需证书信息。

3.7.证书变更

3.7.1.证书变更的情形

证书变更指改变证书中除有效期之外的信息而签发新证书的情形。证书持有者证书只有在有效期内，才可能发生证书变更的情况。证书变更的原因有：

证书证书持有者甄别名更改，如通用名、组织、角色改变等原因。

事件证书仅用于业务场景的一次性的电子签名，不提供证书变更服务。

3.7.2.证书变更的申请

请求证书变更实体为证书持有者本人或其授权代表。

3.7.3.证书变更的鉴别

证书变更按照初次申请证书的注册过程进行处理。

3.7.4.认证机构对证书变更的发布

同3.4.2认证机构对证书的发布。

3.7.5.通知证书持有者证书变更

同3.3.2认证机构和注册机构对证书持有者的通告方式。

3.7.6.构成接受证书变更的行为

同3.4.1构成接受证书的行为。

新证书签发后，旧证书将被撤销。天津CA在目录服务器上发布新证书，用户旧证书通过CRL发布。

3.8.证书撤销

3.8.1.证书撤销的情形

当发生下列情形之一时，证书必须被撤销：

1）私钥失窃、篡改、未经授权的泄露和其它安全威胁；

2）证书主体(无论是CA还是证书持有者)违反了CPS规定的重要职责；

3）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；

4）证书持有者主动提出撤销请求；

5) 天津CA发现证书持有者在申请时提供的证明材料不真实；

6) 天津CA已经履行催缴义务后，证书持有者仍未缴纳服务费。

3.8.2.可以发起请求撤销证书的实体

请求证书撤销的实体包括：

1）证书持有者本人或其授权代表；

2）天津CA或其授权机构；

3）司法机关等公共权力部门的授权代表。

3.8.3.证书撤销的申请

通用型证书的证书持有者到天津CA，订户可通过线上或线下方式进行撤销，提交撤销申请时注明撤销原因。天津CA授权的发证机构按照身份识别与鉴定的规定对证书持有者提交的证书撤销申请进行审核。天津CA撤销证书持有者证书后，发证机构将当面通知证书持有者证书被撤销。

如是强制撤销，天津CA授权的发证机关管理员可以对证书持有者证书进行强制撤销，撤销后立即通知该证书持有者。强制撤销的命令来自于：天津CA、天津CA授权的发证机构或司法机关等公共权力部门。

云证书支持在线提交证书撤销到CA机构或授权的注册机构。的证书撤销请求的处理采用与原始证书签发相同的过程。证书的撤销状态实时通过CRL向外界公布。

事件证书没有证书撤销。

证书持有者证书在24小时内进入CRL或被直接签发CRL，向外界公布。

3.8.4.撤销请求宽限期

当出现证书撤销条件中的情形时，应该尽快提出证书撤销请求，撤销请求必须在发现密钥泄密或发现有泄密嫌疑8小时以内发现提出，其它撤销原因从发现需要撤销证书到向天津CA或注册机构提出撤销请求的时间间隔必须在24小时以内提出。

3.8.5.电子政务电子认证服务机构处理撤销请求的时限

天津CA从收到证书撤销请求起一个工作日内完成请求的处理。

3.8.6.依赖方检查证书撤销的要求

依赖方在信任证书前，必须对证书的状态进行检查，包括：

1）在使用证书前根据天津CA最新公布的CRL检查证书的状态；

2）验证CRL的可靠性和完整性，确保它是经天津CA发行并电子签名的。

依赖方应根据天津CA公布的最新CRL或提供的OCSP服务确认使用的证书是否被撤销。如果公布证书已经撤销，而依赖方没有检查，由此造成的损失由依赖方本身承担。

3.8.7.CRL发布频率

天津CA的CRL发布周期为24小时，特殊紧急情况下可以立即签发CRL。

3.8.8.CRL发布的最大滞后时间

天津CA撤销的证书从被撤销到被发布到CRL上的滞后时间最大为24小时。

3.8.9.在线状态查询的可用性

天津CA向证书持有者提供7×24在线证书状态查询服务（OCSP）。

事件证书仅用于业务场景的一次性的电子签名，证书私钥在使用过一次后即销毁，不提供证书状态服务。

3.8.10.撤销状态查询要求

依赖方在信赖一个证书前必须通过证书状态查询检查该证书的状态。如果依赖方不希望通过最新的相关证书撤销列表来检查证书状态，则应通过可用的OCSP服务对证书状态进行在线检查。

3.8.11.撤销信息的其他发布形式

天津CA网站（https://www.tjzhca.com）提供CRL文件下载。

3.9.密钥生成、备份与恢复

证书的加密密钥由天津市密钥管理中心（KMC）生成、托管、备份，当证书证书持有者本人、国家执法机关、司法机关或其他管理部门因管理需要提出恢复加密密钥时，由天津CA通过相应程序从KMC为其取得相应的加密密钥。加密密钥被加密存放在KMC管理中心。签名密钥对由证书持有者的密码设备生成，由证书持有者自行保管。

3.9.1.证书持有者密钥恢复

证书持有者加密密钥恢复：当证书持有者的加密密钥损坏或丢失后，某些密文数据将无法还原，此时证书持有者可向天津CA提交申请，经过审核后，通过天津CA向天津市密钥管理中心发送请求，天津市密钥管理中心同意证书持有者的恢复请求，天津CA恢复证书持有者的密钥并下载于证书持有者证书载体中。

证书持有者签名密钥由证书持有者保存，天津CA无法对签名密钥进行恢复。

3.9.2.问责取证密钥恢复

问责取证密钥恢复：问责取证人员向天津CA提交申请，经过审核后，通过天津CA向天津市密钥管理中心发送恢复请求，经天津市密钥管理中心同意后，由密钥恢复模块恢复所需的密钥并记录。

4.应用集成支持与信息服务操作规则

4.1.服务策略和流程

1.整体调研和需求分析：根据待集成证书服务的系统平台，天津CA将形成方案解决小组，先对其进行整体调研，通常调研会采用现场会议、电话沟通或微信等方式，确认本次系统的集成目的、集成难易度等，以明确本次的需求和开发任务。

2.制定解决方案：根据上述需求分析中所确认的需求点，天津CA方案解决小组将逐一进行进一步分析，并确定技术选型和最终集成方式，形成技术解决方案说明。

3.解决方案评审：对方案解决小组出具的技术解决方案说明进行评估，确认其可行性，以及对研发和实施中可能的风险进行评估，并完成风险应对方案。

4.系统集成：天津CA方案解决小组将符合解决方案的相应的开发包、文档等交付于系统集成方，由系统集成方实现系统的功能升级。在系统集成期间，天津CA将保持对集成开发方的技术支持，如技术文档答疑、接口调试、相关问题解决等。

5.测试：天津CA方案解决小组随提供的开发包等技术资料，还根据具体需要，对涉及到CA技术的部分提供相应的应用测试，如测试接口服务地址、测试用户账户密码，测试密码设备等，以保证系统集成方集成后的系统运行稳定。

6.实施：在系统实施过程中，如需要天津CA提供相应安全产品或设备进行部署时，由天津CA指派专业的技术人员完成部署。业务系统升级部分由系统集成方完成。安全产品或设备所需的网络拓扑环境等必要的运行资源，由部署需求方完成协调。

7.运行维护：对进入运行维护期的项目，天津CA可提供微信沟通、电话支持、远程指导等方式解决相关问题的解答。对于无法通过上述途径解决的问题，天津CA提供上门方式进行协助。

4.2.应用接口

天津CA提供证书应用接口程序供应用系统集成和调用。

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

4.2.1.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。

天津CA的服务器端密码设备的底层应用接口，符合国家密码管理局《通用密码服务接口规范》和《公钥密码基础设施应用技术体系密码设备应用接口规范》。

天津CA提供的客户端证书介质的底层应用接口应符合国家密码管理局《智能IC卡及智能密码钥匙密码应用接口规范》。

4.2.2.证书应用接口

通用密码服务接口是屏蔽了底层不同密码设备类型和底层接口的通用中间件，该接口符合《电子政务数字证书应用接口规范》。其主要包括服务器端组件接口和客户端控件接口。服务器端组件和客户端控件支持不同认证机构所签发的符合《电子政务数字证书格式规范》的数字证书。证书应用接口程序应支持Windows、AIX、Solaris、linux等多种系统平台，并提供C、C#、Java等多种接口形态，可通过com组件、java组件、ActiveX控件、Applet插件等多种形态提供服务。

4.2.3.证书应用方案支持

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

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

4.2.4.证书应用接口集成

天津CA具备面向各类应用的证书应用接口集成能力，并达到以下要求：

1.应具备在多种应用环境下进行系统集成的技术能力，包括基于Java、.NET等B/S应用模式和基于C、VC等C/S应用模式的系统集成能力。

2.应提供满足不同应用系统平台的证书应用接口组件包，包括com组件、java组件、ActiveX控件、 Applet插件等。

3.应提供集成辅助服务，包括接口说明、集成手册、测试证书、集成示例、演示DEMO等。

4.3.集成内容

天津CA为电子政务应用单位提供证书应用接口，并负责相关程序集成工作。集成工作包括以下服务内容：

1）证书应用接口的开发包（包括客户端和服务器端）；

2）接口说明文档和开发使用手册；

3）集成演示Demo；

4）证书应用接口开发培训和集成技术支持；

5）协助应用系统开发商完成联调测试工作；

6）具备在多种应用环境下进行系统集成的技术能力，包括B/S和C/S架构的系统集成能力；

7）提供集成辅助服务，包括接口说明及开发使用手册、测试证书、集成示例等。

4.4.信息服务内容

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，天津CA可以并且能够为证书应用单位提供相应的信息服务，为其实现科学管理和领导决策提供可靠依据。

4.4.1.证书信息服务

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

4.4.2.CRL信息服务

CRL在天津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。天津CA提交的数据包括业务类型、认证机构身份标识、CRL文件、同步时间等。

4.4.3.服务支持信息服务

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

4.4.4.决策支持信息服务

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

4.5.信息服务管理规则

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

对CA机构内的工作人员按其工作角色设定与之相应的信息访问权限，并对其所有访问操作进行详细记录；

对证书应用单位的管理员设定信息访问权限，限定其仅能访问本应用所签发证书信息。

应用单位管理员对非授权信息的访问，须依照政策管理规定，须经上级主管部门批准后方可进行。

对问责程序需要进行的信息访问，应严格审核相应的问责人员身份及授权文件，无误后方可进行问责举证。

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

1.私有信息类型的敏感度

以下信息应属于私有信息：

个人隐私信息；

商业机密；

政府部门的敏感信息和工作秘密。

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

2.允许的私有信息采集

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

3.允许的私有信息使用

认证机构应只使用CA或者RA收集的私有信息。因在某项业务中开展证书应用而获得的私有信息，在使用时，必须首先得到该业务应用单位的许可。

4.允许的个人信息发布

认证机构和注册机构仅能面向证书应用单位发布与之相关的私有信息，以协助证书应用单位进行证书业务管理。

在特别紧急情况下，认证机构经管理机构的同意，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

认证机构应允许用户在其证书生命周期内对其私有信息进行更正。

6.对司法及监管机构发布私有信息

认证机构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：

司法程序；

经私有信息所有者同意；

按照明确的法定权限的要求或许可。

4.6.信息服务方式

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

4.6.1.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，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。

4.6.2.CRL信息同步服务

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天津CA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发布周期为24小时。

4.6.3.服务支持信息服务

1）天津CA通过WEB网站面向电子政务用户发布如下信息：

A.电子政务电子认证服务业务规则

B.证书撤销列表（CRL）查询

C.在线证书状态（OCSP）查询

D.获得证书帮助联系方式

客户服务热线电话:400-0655-110

办公地址：天津市河西区体院北环湖中道9号

邮政编码：300060

投诉电话：022-23522103

E.其他应该发布的相关信息。

2）天津CA面向电子政务应用系统集成商提供如下服务：

A.数字证书应用接口软件包

B.数字证书应用接口实施指南

C.证书常见问题解答（FAQ）

D.获得证书帮助联系方式

客户服务热线电话:400-0655-110

办公地址：天津市河西区体院北环湖中道9号

邮政编码：300060

投诉电话：022-23522103

E.其他应该发布的相关信息。

3）天津CA面向电子政务应用系统以接口形式提供如下服务：

A.时间戳服务数据接口

B.http协议的CRL发布服务接口

C.LDAP协议的CRL发布接口

D.LDAP协议的证书发布接口

E.OCSP服务接口（可选）

4.6.4.决策支持信息服务

天津CA面向应用提供方以Web或WebService方式提供如下信息服务：

A.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；

B.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；

C.客户满意度信息：提供面向业务的客户满意度调查信息；

D.服务效率信息：提供面向业务服务效率分析信息，如处理时间、服务接通率等。

5.使用支持服务操作规则

5.1.服务内容

面向证书使用用户（即证书申请者、证书持有者）及证书应用单位提供的一系列售后服务及技术支持工作。

服务内容主要包括：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。

5.1.1.面向证书持有者的服务支持

1）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。

2）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。

3）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。

4）电子认证服务支撑平台使用

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

5.1.2.面向应用提供方的服务支持

1）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。

2）电子签名服务中间件的应用

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

5.2.服务方式

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

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

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

5.2.1.座席服务

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

5.2.2.在线服务

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

5.2.3.现场服务

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

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

5.2.5.投诉受理

应向用户公布电子政务电子认证服务监管部门的投诉受理方式。可通过电话、网站平台、电子邮件、即时通讯工具等方式及时接受客户投诉，投诉受理过程中应记录投诉问题，并将结果及时反馈给用户。将投诉受理中产生的相关文档进行归档、保存。

5.2.6.培训

培训方式可以由认证机构与客户双方约定的形式开展。培训内容主要包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答（FAQ）、操作手册等。

5.3.服务质量

服务质量应明确以下内容：

服务的获取方式；

座席服务、在线服务、现场服务的服务时间，响应效率；

投诉处理承诺；

培训效果的评估及处理；

服务响应机制及流程。

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

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

6.认证机构设施、管理和操作控制

6.1.物理控制

天津CA电子政务电子认证服务机构的物理环境满足以下安全要求：

防止物理非法进入，天津CA通过入侵报警、视频监控等安防设施对定义的管理区域进行实时监测，并建立完善的安全管理制度，保护天津CA的电子政务电子

认证服务设施。防止未授权访问天津CA通过门禁系统和权限分割的管理模式，确保不发生未经过授权或越权的区域访问。

6.1.1.场所区域与建筑物

天津CA电子认证服务业务的运行场地位于天津市滨海高新区兰苑路13号OVU中电科创园A1座505。 根据GM/T 0034-2014《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》要求，机房分为以下各区域：

1.管理区(限制区，面积21m²)：

管理区是管理人员管理、操作CA系统和RA系统的区域，配备了RA管理终端、RA审计终端、安全管理终端、CA管理终端和CA审计终端，以及保险箱和文件柜，使用门禁控制出入。

2.服务区(敏感区，面积60m²)：

该区域是电子认证RA、0CSP系统部署区域，主要用于放置RA系统、0CSP系统的软硬件设备，区域内安装有精密空调和柜式七氟丙烷气体灭火系统，门禁采用双人控制出入。

3.缓冲区(屏蔽区，面积6m²)：

缓冲区需要一人指纹一人密码方可开启，进入后关闭A门才可以开启B门，同时要更换门禁验证方式，保证了核心区的安全。

4.核心区(屏蔽区，面积22m²)：

核心区是CA系统、根密钥密码设备、数据库系统软硬件存放的区域。配备有精密空调和柜式七氟丙烷气体灭火系统。核心区还专门配备了氧气呼吸机防止突发情况的发生。

5.配电间(面积33m²)：

配电间装有外部市电双回路，由两路独立变电所提供，内部配备ATS自动电源切换系统，配置了2台UPS主机，可持续供电8小时的2组电池，保障计算机设备供电可靠性。

6.1.2.物理访问

天津CA的核心机房和各功能区域的访问控制系统是与控制各区域进出的门禁系统相结合的，并实现了以下安全功能：

进出每一区域的门都有记录作为审计依据；

核心机房的安全区域采用身份鉴别卡和指纹验证的结合方式控制，服务区采用身份鉴别卡和指纹结合方式控制进出；

其他功能区域只采用身份鉴别卡或指纹控制门的进出；

授权人员进出每一道门都会有时间记录；

只有相关授权人员使用授权口令才可以登录访问物理设备；

根据操作性质及安全性的不同，物理设备设置多种权限级别账户（组）对人员进行访问控制，确保物理设备系统安全性；

涉及物理设备密码及重大系统操作的，必须两人以上同时在场才可操作；

高安全级别的重要系统设备的操作与维修，必须在机房内多人现场监控下现场完成且有相关记录。

6.1.3.电力与空调

为保证系统设备的正常运转，避免服务器在过热的条件下工作，

核心区和配电间各设置1台机房精密空调；服务区域配置2台机房精密空调，主备轮询工作。机房电源供电系统包括机房区的动力、

照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供配电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱 及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。为保证系统设备的正常运转，避免服务器在过热的条件下工作，在屏蔽机房内安装了STULZ精密空调。

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供配电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

使用不间断电源（UPS）来保证供电的稳定性和可靠性。采用双电源，在单路电源损坏时，可以自动切换，维持系统正常运转。

6.1.4.水患防治

天津CA在机房设计建设时已充分考虑水患进行防水设计和建设，并采取相应措施，防止水侵蚀，充分保障系统安全。

6.1.5.火灾预防和保护

天津CA在设备机房内按照国家标准建设安装有火灾报警系统和消防应急联动处理系统，并通过与专业消防部门协调，实施消防灭火等应急响应措施，避免火灾的威胁，防止明火或者烟雾对系统造成损害或不利影响，充分保障系统安全。

6.1.6.介质存储

天津CA对存储有系统程序、证书持有者数据、维护记录、审计记录、日志文件、备份数据等信息的介质保存到相应的安全区域中，介质得到安全可靠的保护，避免诸如温度、湿度和磁力等环境变化可能产生的危害和破坏，并且只有授权人员才能访问。

6.1.7.废物处理

天津CA对作废的相关业务文件和材料按照数据和记录销毁流程经安全管理部审批通过后，通过粉碎、焚烧或其它不可恢复的方法处理，废弃的密码设备在销毁处置前根据产品提供商的操作指南将其物理销毁或初始化，其他废物处理按照天津CA的相关处理要求进行，所有处理行为将记录在案。

6.1.8.异地备份

天津CA对业务系统中的程序、数据等关键信息按照数据备份策略和流程进行安全备份。备份介质按照备份策略和流程保存在本地机房和异地。在异地备份时按照策略和流程由专人送交到银行保险柜保管。以上所有操作流程将记录在案。

6.1.9.入侵侦测报警系统

天津CA在机房区域安装了入侵侦测报警系统，天花板上安装了活动侦测器，发生非法入侵时会立即且一直发出报警警示音。

6.2.操作过程控制

6.2.1.可信角色

在天津CA提供的电子政务电子认证服务过程中，能从本质上影响证书的签发、使用、管理和撤销等涉及密钥操作的职位都被天津CA视为可信角色。这些角色包括但不限于：密钥管理员、系统管理员、网络安全管理员、审计员、业务管理人员及业务操作人员等，具体岗位名称和要求以天津CA的岗位说明书为准。

天津CA中与密钥和证书生命周期管理操作有关的工作人员，包括系统管理员、安全管理员、审计管理员等都是可信角色，必须由可信人员担任，主要职责如下：

1）CA系统管理员

主要职责：负责对生产系统以及运营场地、设备等基础设施运行进行监督，规避主要风险。

2）CA系统运营管理员

主要职责：负责协调、监督CA生产系统，保证CA场地、设备、电力和网络基础设施的安全运行等。

3）网络安全管理员

主要职责：负责维护电子认证机构计算机相关的电子设备、操作系统、数据中心的应用进程及网站建设、保证硬件和软件的正常运行，及时发现并排查故障。

4）系统维护管理员

主要职责：负责因特网的正常使用，网站发布及更改防火墙配置，硬件故障的排查及维修等，能够迅速而准确地定位和排除各类故障，保证系统正常运行，确保所承载的各类应用和业务正常。

5）核心机房管理人员

主要职责：负责监控计算机中心的操作系统、数据库、备份系统的运行。

6）安全管理员

主要职责：负责本机构场地安全、日常安全管理，定期检查门禁系统运行状况，定期对物理场地进行安全评估，并对安全事件提出可行性解决方案。

7）密钥管理员

主要职责：负责机房加密机的保管操作，及申请密钥对，并定期给天津市国家密码局提交密钥使用情况说明。

8）物理环境安全管理员

主要职责：负责机电、门禁监控设备、消防设备的管理及维护，各项应急预案编写及更新，工程建设和改造维护等。

9）鉴证人员

主要职责：负责快速、无差错的实施证书鉴证服务，解决客户关于证书申请及使用方面的问题，妥善保管管理员证书的安全等。

10）客户服务负责人

主要职责：负责管理客户服务中心工作，服务并维护现有的客户，辅导普通客服人员，改进服务流程等。

11）客户档案管理员

主要职责：负责建立和维护客户档案资料，管理客户档案借阅工作等。

天津CA确保单个角色不能接触、导出、恢复、更新、废止天津CA系统存储的根证书对应的私钥。对于关键的操作进行物理与逻辑上的分割控制，使掌握设备物理权限的人不能再拥有逻辑权限。至少三个可信角色才能使用一项对参加操作人员保密的密钥分割和合成技术来进行任何密钥恢复的操作。

天津CA对与运行和操作相关的职能有明确的分工，贯彻互相牵制的安全机制，保证至少一人操作，一人监督记录。

6.2.2.角色的识别与鉴别

所有天津CA的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡、密码或者指纹识别；进入系统需要使用数字证书进行身份鉴别。天津CA将独立完整地记录其所有的操作行为。

6.2.3.角色职责分离设置

所谓职责分割，是指如果一个人担任了完成某一职能的角色，就不能再担任完成另一特定职能的角色。天津CA人员职责分割的角色包括（但不限于）以下几种：

审计员；

网络安全管理员；

密钥管理员；

系统维护员；

物理环境管理员；

数据库管理员；

6.3.人员控制

6.3.1.可信人员要求

天津CA员工的录取经过严格的审查，根据岗位需要增加相应可信任的员工。

一般员工需要有3个月的考察期，核心和关键岗位的员工考察期为半年，根据考察的结果安排相应的工作或者辞退。天津CA根据需要对员工进行职责、岗位、技能、政策、法律、安全等方面的培训。

天津CA会对其关键的CA职员进行严格的背景调查。背景调查主要通过（但不限于）以下方式：

1）身份验证，包括个人身份证件、户籍证件等；

2）学历、学位等其他资格、资历证书；

3）个人履历，包括家庭状况、教育经历、工作经历及相关证明人等；

4）无犯罪记录证明材料。

天津CA确立流程管理规则，所有的员工与天津CA签订保密协议，据此天津CA员工受到合同和章程的约束，不得泄露天津CA证书服务体系的敏感信息。

6.3.2.可信人员背景审查

天津CA制定了严格的员工背景审查程序，完成对天津CA可信任员工的背景调查。身份背景调查过程中，存在（但不限于）下列情形之一，不得通过可信审查：

1）伪造相关证件材料的；

2）伪造工作经历及工作证明人虚假的；

3）虚假声称具有某种技能、能力的证件；

4）以往工作中存在重大不诚实行为的；

5）有犯罪记录的。

6.3.3.人员培训及再培训

天津CA对天津CA员工进行以下内容的综合性培训：

1）员工手册；

2）天津CA电子政务电子认证业务规则；

3）岗位职责及说明书 ；

4）公司各项管理制度；

5）PKI基础知识；

6）天津CA应急预案管理；

7）国家关于电子认证服务的法律、法规及标准、程序；

8）其他需要进行的培训等。

根据天津CA策略调整、系统更新等情况，天津CA将对员工进行继续培训，以适应新的变化。对于公司安全管理策略，每年对员工进行一次以上的培训，对于相关业务技能培训应每年进行一次以上的业务技能培训。

6.3.4.工作岗位轮换周期和顺序

根据岗位人员和业务上的实际情况内部自行安排。

6.3.5.违规行为处罚

当天津CA员工进行了未授权或越权操作，天津CA在确认后将立即中止该员工进入天津CA证书服务体系，根据情节严重程度实施包括提交司法机关处理等措施。

一旦发现上述情况，天津CA立即作废或终止该人员的安全令牌。

6.3.6.外包服务人员及要求

天津CA的外包服务人员及顾问执行与普通员工一致的可信资格确认，此外外包服务人员及顾问进入关键区域必须有专人的陪同与监督。

6.3.7.提供给员工的文档及保密策略

在培训或再培训期间，天津CA提供给员工的培训文档包括（但不限于）以下几类：

1)员工手册；

2)电子认证业务规则；

3)岗位说明书；

4)安全管理制度等。

6.4.审计日志程序

6.4.1.记录事件的类型和内容

天津CA的CA和RA运行系统，记录所有与系统相关的事件，以备审查。这些记录，无论是纸质或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。

天津CA应记录的内容包括（但不限于）：

1）系统安全事件，包括：CA系统、RA系统和其他服务系统的活动，系统崩溃，硬件故障和其他异常；

2）电子认证服务系统操作事件，包括系统的启动和关闭；

3）认证机构设施的访问，包括授权人员进出认证机构设施、非授权人员进入认证机构设施及陪同人员和安全存储设施的访问；

4）证书生命周期相关事件。

6.4.2.处理日志的周期

对于CA和证书持有者证书生命周期内的管理事件日志，天津CA将每月进行一次内部检查、审计。

对系统安全事件和系统操作事件日志，天津CA将每月进行一次检查、处理。

对物理设施的访问日志，天津CA将每月进行一次检查、处理。

6.4.3.审计日志的保存期限

天津CA会妥善保存认证服务的审计日志，本地保存期限至少两个月，离线存档为五年。

6.4.4.审计日志的保护

天津CA执行严格的保护和管理，确保只有天津CA授权的人员才能访问这些审查记录。并且实现异地备份，并禁止访问、阅读、修改和删除等操作。

6.4.5.审计日志备份程序

天津CA保证所有的审查记录和审查总结都按照天津CA备份标准和程序进行。根据记录的性质和要求，采用在线和离线的各种备份工具，系统日志随数据备份一并进行备份保存，每周备份一次，保存在机房保险柜中。每月进行异地备份保存。

6.4.6.审计日志检测系统

天津CA审查采集系统涉及：

证书签发系统；

证书注册系统；

证书目录系统；

证书审批受理系统；

访问控制系统（包括防火墙）；

门禁管理系统；

视频监控系统；

网站、数据库安全保障系统；

其他天津CA认为有必要审查的系统。

6.4.7.对导致事件实体的通告

天津CA将依据法律、法规的监管要求，对一些恶意行为，如网络攻击等，通知相关的主管部门，并且天津CA保留进一步追究责任的权利。

6.4.8.脆弱性评估

CA安全程序根据政策、技术和管理的变化及时进行薄弱环节分析，属于可以弥补的薄弱环节，及时弥补，属于不可弥补的薄弱环节，天津CA每年对系统进行脆弱性评估，以降低系统运行的风险。

6.5.规定事件记录的类型

天津CA的CA和RA运行系统，记录所有与系统相关的事件，以备审查。这些记录，无论是纸质或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。

6.6.规定事件记录的内容

天津CA规定事件记录的内容包括（但不限于）：

1）系统安全事件，包括：CA系统、RA系统和其他服务系统的活动，系统崩溃，硬件故障和其他异常；

2）电子认证服务系统操作事件，包括系统的启动和关闭；

3）认证机构设施的访问，包括授权人员进出认证机构设施、非授权人员进入认证机构设施及陪同人员和安全存储设施的访问；

4）证书生命周期相关事件。

6.7.记录归档要求

6.7.1.归档记录的类型

天津CA按照制度和流程定期对电子生成或者手工生成的重要数据定期存档。存档的内容包括证书持有者资料、电子认证系统签发的系统证书和证书持有者证书、证书撤销列表CRL、电子认证系统维护操作记录、可信人员进出机房操作记录、外来人员进出记录、数据备份记录、涉及电子认证安全的事件记录及审计数据等。

6.7.2.归档记录的保存期限

天津CA归档存档期限一般规定为五年。证书持有者资料保存期限为证书持有者证书失效后五年。

6.7.3.归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能获取。天津CA保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力等的破坏。

6.7.4.归档文件的备份程序

所有纸质归档记录按照备份策略和流程由专人定期执行，备份介质在天津CA公司本地备份管理。按照备份策略和流程，电子存档文件除了在天津CA内本地备份外，还将在异地保存其备份。

6.7.5.记录时间戳要求

所有存档内容都按照归档策略和流程分别由专人收集、归档、审核和保管。所有归档记录上均有参与归档操作的人员与时间记录。天津CA的所有硬件设备采用NTP服务器，保证各种操作的时间同步。

6.7.6.归档收集系统

天津CA的档案收集系统由人工操作和自动操作两部分组成。

6.7.7.获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。所有记录被访问后，需验证其完整性。此外，天津CA每年验证存档信息的完整性。

6.8.认证机构密钥更替

在CA的密钥对遭受攻击或因为密钥生命期而需要更新密钥对的情况下，由安全策略委员会授权，所有密钥管理员在场，共同启动密钥管理程序，执行密钥更新指令，硬件加密设备重新生成根密钥。密钥更换及自签名证书按照规定报告上级管理机构。

6.9.数据备份

备份不仅是数据的保护，同时也是为了在认证系统遇到人为或自然灾难时，能够通过备份内容对系统进行有效的灾难恢复。

6.9.1.认证系统全备份

认证系统全备份是指认证系统初始化后进行的包括认证系统安装包、认证系统各子系统安装目录（含配置文档）、各数据库、网络设备配置情况和策略、WEB 网站源代码及程序、操作系统安装包、数据库安装包等在内的总体性备份。之后每次对系统部署的调整或配置更改，均应进行所涉及内容的补充备份，必要时也可按初始化后进行全备份的规模进行全备份。

6.9.2.认证系统数据备份

认证系统数据备份包括：CA数据库备份、RA 数据库备份。

认证系统数据备份应保证在同一时间点进行，以保证每个数据库中数据信息的一致性。

天津CA每日17：00数据库自动进行增量备份，存储在数据库存储系统中。每周五17：00数据库进行全备份，一份存储在数据库存储系统，另一份刻录成光盘保存在机房保险柜中。每月进行一次异地备份，将刻录的数据库全量备份光盘存在银行保险柜中。

6.9.3.认证系统日志备份

对认证系统进行任何操作，其操作日志均会被记录在认证系统相应子系统的安装目录下。认证系统日志随数据库备份一并进行，每日17：00数据库自动进行增量备份，存储在数据库存储系统中。每周五17：00数据库进行全备份，一份存储在数据库存储系统，另一份刻录成光盘保存在机房保险柜中。每月进行一次异地备份，将刻录的数据库全量备份光盘存在银行保险柜中。

6.9.4.网络日志备份

安全可靠的网络环境，是保证认证系统稳定运行的根本条件。对网络日志进行备份和分析，不仅可以预防网络危险事件的发生，一旦出现危机，还能为事件分析提供数据信息支持。

现阶段网络日志备份采取手工方式进行，主要包括：入侵检测设备日志、三台不同厂商防火墙以及 VPN 设备等。

根据网络设备存储容量大小的差异，网络日志备份分为隔日进行和一周进行。其中，核心区防火墙日志每周一采用专用移动设备进行导出备份，其他设备日志隔天导出一次。

6.9.5.操作系统日志备份

认证系统主机服务器的操作系统日志需定期进行备份和分析。主机服务器主要包括：CA系统主机服务器、CA数据库和主目录服务器主机服务器、RA系统和数据库主机服务器、从目录服务器、OCSP服务器、WEB主机服务器、防病毒服务器等。

认证系统主机服务器采用Windows server 2012 R2 操作系统，操作系统日志分为windows日志、应用程序和服务日志两大类。系统日志分为应用系统、安全、操作、系统、已转发事件五小类，应用程序和服务日志按应用不同也分为若干小类。

操作系统日志各小类属性中“达到事件日志最大大小时”选项选择均设置为“日志满时将其存档，不覆盖事件（A）”。

现阶段，操作系统日志备份每周一进行一次。备份时使用专用移动设备拷贝备份。

6.9.6.物理控制日志备份

物理控制日志分为两种：门禁日志和视频监控数据。

门禁系统日志，每月月初导出数据进行备份，备份采取电子和纸质的两种方式。电子版资料存放在门禁系统主机内，纸质版资料存放在档案室中。

视频监控数据本地保存六个月。所有录像资料存放在硬盘录像机中。

6.10.损害与灾难恢复

6.10.1.事件和损害的列表

天津CA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，应急处理方案包括：

根密钥泄露应急制度；

消防系统应急处理预案；

电力系统应急处理预案；

水灾应急处理预案；

通信系统应急处理预案；

网络系统瘫痪应急处理预案；

黑客攻击应急处理预案；

病毒应急处理预案；

系统数据应急处理预案；

人员应急处理预案。

涉及电子政务电子认证机构的重大事故应按照规定及时上报管理机构。

6.10.2.计算资源、软件或数据的损坏

天津CA对业务系统及其他重要系统的资源、软件或数据进行了备份，并制定了相应的应急处理流程。当出现计算机资源、软件或数据的损坏时，能在最短的时间内恢复被损害的资源、软件或数据。

6.10.3.实体私钥损害处理程序

对于实体私钥的损害，天津CA有如下处理要求和程序：

1）当证书持有者发现实体证书私钥损害时，证书持有者必须立即停止使用其私钥，并立即通知天津CA或注册机构撤销其证书。天津CA发布证书撤销信息；

2）当天津CA或注册机构发现证书持有者的实体私钥受到损害时，天津CA或注册机构将立即撤销证书，并通知证书持有者，证书持有者必须立即停止使用其私钥。天津CA发布证书撤销信息；

3）当天津CA的证书出现私钥损害时，天津CA将立即撤销CA证书并及时通过途径通知依赖方，然后生成新的CA密钥对、签发新的CA证书。

6.10.4.灾难后的业务连续性能力

除非物理场地出现了毁灭性的、无法恢复的灾难，天津CA的灾难恢复时间目标RTO小于7天，恢复点目标RPO小于24小时。天津CA计划建立异地灾难恢复中心，灾难恢复中心的建立，将进一步增强天津CA的灾后业务存续能力。

6.10.5.业务连续性计划

针对证书系统的核心业务系统，证书签发系统和证书接口系统采用双机热备方式；对核心数据库，证书管理系统数据库采用磁盘阵列方式来确保证书系统的高可靠性和可用性。具体的安全措施参照天津CA业务连续性计划。

6.11.认证机构或注册机构的终止

当天津CA打算终止经营时，会在终止经营前三个月给天津CA授权的发证机构、垫付商和证书持有者书面通知，并在终止服务六十日前向国务院信息产业主管部门、国家密码管理主管部门报告，按照相关法律规定的步骤进行操作。

天津CA会按照相关法律的规定来安排好档案和证书的存档工作。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；

证书撤销；

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；

处理加密密钥；

处理和存储敏感文档；

清除CA主机硬件。根据天津CA与RA签订的协议终止RA的业务。

由于密钥受损和非密钥受损原因而终止天津CA，要完成相似的操作，唯一不同在发送天津CA终止通知的时间限制上：由于密钥受损原因终止天津CA，要求天津CA通知证书持有者的过程尽快完成；由于非密钥受损的原因终止天津CA，在通知所有证书持有者后，采取适当的步骤减轻天津CA终止对证书持有者的影响。

7.认证系统技术安全控制规则

7.1.密钥对的生成和安装

由于密钥对是安全机制的关键，所以在电子政务电子认证服务业务规则中制定了相应的规定，通过物理安全控制和密钥安全存储控制来确保密钥对的产生、传送、安装等过程中符合保密性、完整性和不可否认性的需求。

7.1.1.密钥对的生成

加密密钥对是由中华人民共和国国家密码管理局许可的、天津CA证书签发系统申请的、天津市密钥管理中心的加密机设备生成的。

签名密钥对是由国家密码主管部门许可的、天津CA数字证书签发系统支持的密码设备生成签名密钥对。签名密钥存储在密码设备中不可导出，保证天津CA无法复制签名密钥对。天津CA支持多种密码设备，如智能密码钥匙、智能IC卡、服务器密码机、签名验签服务器等。天津CA可根据证书申请者要求或自身选择签名密钥对生成的密码设备。

云证书签名密钥对，由服务云端经过国家密码局主管部门许可的服务器密码机产生。

事件证书的签名密钥由签名设备生成。

手机证书签名密钥对，由证书持有者移动终端和签名服务云端共同计算协同产生。服务端密钥因子应在国家密码主管部门许可的服务器密码机中产生，客户

端密钥因子应包含终端设备信息、用户知晓的（例如用户设置的PIN）、随机数等部分计算得到。

7.1.2.加密私钥传送给证书持有者

证书持有者的加密私钥是在天津市密钥管理中心产生的，该私钥只保存在天津市密钥管理中心。在加密私钥从天津市密钥管理中心到证书持有者的传递时，采用国家密码主管部门许可的对称密钥算法加密，天津CA无法获得，这样就保证了证书持有者加密私钥的安全。

7.1.3.公钥传送给证书签发机构

天津CA从天津市密钥管理中心取得证书持有者加密公钥后为其签发证书，在此过程中采用国家密码主管部门许可的对称密钥算法加密，保证了传输中密钥的安全。自生成密钥对证书持有者向天津CA提交证书申请时，该请求信息内的公钥，使用安全通道保证信息的机密性和完整性。

电子认证服务机构公钥传送给依赖方天津CA的根公钥包含在天津CA自签发的根证书中。

证书持有者可以从天津CA的网站（https://www.tjzhca.com）上下载天津CA根证书，也可以由天津CA通过目录系统、业务系统的安装、电子邮件和软件绑定等方式提供给依赖方。

7.1.4.认证机构公钥传送给依赖方

依赖方可以天津CA的网站（https://www.tjzhca.com）下载根证书和CA证书，从而得到CA的公钥。

7.1.5.密钥的使用

天津CA的签名密钥用于签发RA证书和证书撤销列表（CRL）；

在天津CA证书服务体系中的密钥用途和证书类型紧密相关，被分为签名和加密两大类。

证书持有者的签名密钥用于提供网络安全服务，如信息在传输过程中不被篡改、接收方能够通过数字证书来确认发送方的身份、发送方对于自己发送的信息不能抵赖等；

证书持有者加密密钥用于对网络上传送的信息进行加密，保证信息除发送方和接受方外不被其他人窃取、篡改。更多与协议和应用相关的密钥使用限制请参阅X.509标准中的密钥用途扩展域。

7.1.6.公钥参数的生成和质量检查

公钥参数由国家密码管理部门许可的密码设备或密码模块生成。对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均符合国家密码管理部门要求。

7.1.7.密钥使用目的

证书持有者的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

7.2.私钥保护和密码模块工程控制

7.2.1.在CA私钥保护方面的要求

1.密码模块的标准和控制

天津CA使用国家密码主管部门许可的产品，密码模块的标准符合国家规定的要求。

2.私钥多人控制（5选3）

天津CA采用多人控制策略激活、使用、备份、停止和恢复天津CA的签名密钥，采取5个管理人员中至少3个在场才可进行操作的原则。

3.私钥备份

天津CA根私钥的备份必须经安全策略委员会的批准，并填写《根私钥操作审批记录表》，将结果汇报给安全策略委员会。在生成密钥后，应立即做好根私钥的备份。备份过程中密钥分管者不得离场。根私钥应该备份到5张管理员卡上，5张备份卡分别由5名密钥分管者保存，备份的管理员卡的保存在核心机房的保险柜中。

4.私钥归档

天津CA根私钥过期后，应在5个工作日内完成归档。根私钥的归档必须经安全策略委员会的批准，并填写《根私钥操作审批记录表》，将结果汇报给安全策略委员会。根私钥归档期限为5年在归档期内，根私钥不得重新投入生产环境使用。每年应检查归档的根私钥是否仍在归档期限内，归档期满5年后应立即启动销毁流程。

5.私钥导入、导出密码模块

私钥在硬件密码模块上生成或可以通过CA软件导入到密码模块中，私钥无法从密码模块中导出。

6.私钥在密码模块的存储

私钥以加密的形式存放在硬件密码设备中，并在该设备中使用。

7.激活私钥的方法

天津CA根私钥存在核心区密码设备中，只有具有激活权限的3位以上密钥分管者使用管理员卡登陆，启动密钥管理程序，才能进行激活私钥的操作。

8.解除私钥激活状态的方法

天津CA根私钥存在核心区密码设备中，只有具有激活权限的3位以上密钥分管者使用管理员卡登陆，启动密钥管理程序，才能进行激活私钥的操作。

9.销毁私钥的方法

天津CA根私钥，只有具有激活权限的3位以上密钥分管者使用管理员卡登陆，启动密钥管理程序，才能进行摧毁私钥的操作。

10.密码模块的评估

天津CA使用国家密码主管部门批准和许可的密码产品。

7.2.2.用户私钥保护方面的要求

1.私钥托管

通用型证书签名私钥由证书持有者自己保管，以保证其不可否认性。

云证书的签名密钥对，由服务器密码机生成，在服务云端经过密码机主密钥加密后保存。

事件证书无密钥托管。

手机证书的密钥对，由证书持有者移动终端和签名服务云端协同计算产生并分别保管。

2.私钥备份

云证书的证书私钥由服务云端备份，备份数据以密文形式存在。

手机证书由证书持有者移动终端和签名服务云端各自备份各自的私钥因子。

3.私钥归档

云证书的私钥通过数据库备份进行归档保存。

4.私钥导入、导出密码模块

私钥在硬件密码模块上生成或可以通过CA软件导入到密码模块中，私钥无法从密码模块中导出。

5.私钥在密码模块的存储

私钥以加密的形式存放在硬件密码设备中，并在该设备中使用。

6.激活私钥的方法

天津CA将用户私钥保存在USBKEY或密码机等密码设备中，只有用户通过PIN码，私钥才能被激活使用。

7.解除私钥激活状态的方法

对于存放在硬件密码模块中的证书持有者证书私钥，通过PIN码激活私钥后仅活动一次后即解除其激活状态。

8.销毁私钥的方法

事件证书的证书持有者私钥仅用于业务场景的一次性的电子签名，证书私钥在使用过一次后即销毁。

9.密码模块的评估

天津CA使用国家密码主管部门批准和许可的密码产品。

7.3.密钥对管理的其他方面

7.3.1.公钥归档

对于生命周期外的CA和证书持有者证书，天津CA将进行归档。归档的证书存放在归档数据库中。

7.3.2.证书操作期和密钥对使用期限

证书操作期终止于证书过期或者被撤销。天津CA为证书持有者颁发的证书操作周期通常与密钥对的使用周期是相同的。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。为了保证能够验证在证书有效期内的签名的信息，公钥的使用期限可以在证书的有效期限外。

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。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。

7.4.激活数据

7.4.1.激活数据的产生和安装

存放有天津CA根私钥备份分量的密码机管理员卡，其产生按天津CA《根私钥生命周期管理制度》中的规定进行。所有密钥分割的创建和分发有相应的记录，包括产生时间、持有人等信息。

天津CA根私钥由密码机产生，并分割保存在5个管理员卡中，需通过对应的密码机读取。

如果证书持有者证书私钥的激活数据是口令，这些口令必须：

由证书持有者产生；

至少6位字符或数字。

7.4.2.激活数据的保护

保存有天津CA根私钥备份分量的密码机管理员卡，由天津CA5个不同的密钥分管者掌管，密钥分管者必须由安全策略委员会任命，需知悉密钥分管者相关职责。

如果证书证书持有者使用口令或PIN码保护私钥，证书持有者应妥善保管好其口令或PIN码，防止泄露或窃取。

7.4.3.激活数据的其他方面

1.激活数据的传送

存有天津CA根私钥备份分量的密码机管理员卡，通常保存在天津CA的安全设施中，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在天津CA安全管理人员的监督下进行。

当证书持有者证书私钥的激活数据需要进行传送时，证书持有者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。

2.激活数据的销毁

存有天津CA根私钥备份分量的密码机管理员卡，其销毁所采取的方法包括将管理员卡初始化，或者彻底销毁管理员卡，保证不会残留有任何秘密信息。CA根私钥激活数据的销毁是在天津CA安全管理人员的监督下进行。

当证书持有者证书私钥的激活数据不需要时应该销毁，证书持有者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。

7.5.系统安全控制

7.5.1.安全技术要求

天津CA的数字证书签发系统的数据文件和设备由天津CA系统维护员维护，未经天津CA安全部门授权，其它人员不能操作和控制天津CA系统；其它普通人员无系统账号和密码。天津CA系统部署在多级不同厂家的防火墙之内，确保系统网络安全。天津CA系统密码有最小密码长度要求，而且必须符合复杂度要求，天津CA系统维护员定期更改系统密码。

7.5.2.安全技术措施

天津CA证书系统设计、建设实施严格遵守《GM/T0034-2014基于SM2密码算法的证书认证系统密码及其相关安全技术规范》的相关要求。

7.6.生命周期技术控制

7.6.1.系统开发控制

按照天津CA内部系统开发流程进行控制。

7.6.2.安全管理控制

天津CA的配置以及任何修改和升级都会记录在案并进行控制，并且天津CA采取一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。认证系统只开放与业务相关的功能，只有天津CA授权的员工能够进入天津CA的系统或设备。

7.6.3.生命周期的安全控制

天津CA的证书认证系统在系统设计过程中充分进行了安全性考虑，在开发过程中有严格的流程进行代码安全管理，在开发完成后进行了严格的安全测试，在正式使用前通过了国家有关部门的系统安全性审查和技术鉴定。

7.7.网络的安全控制

天津CA网络中有防火墙、入侵检测、漏洞扫描和网络防病毒等安全机制保护，其配置只允许已授权的机器访问。只有经过授权的天津CA员工才能够进入天津CA签发系统、注册系统、目录服务器、证书发布系统等设备或系统。所有授权人员必须有合法的安全令牌，并且通过密码验证。

CA系统只开放与申请证书、查询证书等相关操作功能，其他端口和服务全部关闭。CA系统的边界控制设备拒绝一切非电子政务电子认证业务的服务。

7.8.时间戳

天津CA认证系统的各种系统日志、操作日志有对应的记录时间。天津CA的所有硬件设备采用NTP服务器，保证各种操作的时间同步。

8.认证机构审计和其他评估

8.1.评估的频率或情形

根据情况而定，有年度评估、运营前评估、安全时间发生后的评估和随时进行评估。

天津CA本身也需要对天津CA的关联机构（包含天津CA授权的注册机构、注册分支机构、受理点等证书体系成员）所有的流程和操作进行审计，检验其是否符合本电子认证业务规则和相应的证书政策的规定，其频率可由天津CA决定或由法律制定的监管机构决定。

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》的要求，按照上级主管部门的要求接受合规性审计。

根据审计结果，需要整改后复审的，应接受复审。

8.2.评估者的资质

对天津CA实施规范审计的第三方所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：必须是经许可的、有营业执照的、具有计算机安全专门技术知识的审计人员或审计评估机构，且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。

8.3.评估者与被评估者之间的关系

对天津CA进行审计的第三方，必须是一个独立于天津CA的合法审计实体。天津CA内部审计员不能与系统管理员、业务管理员、业务操作员等岗位重叠。

8.4.评估内容

审计工作包括：

安全策略是否得到充分实施；

运营工作流程和制度是否严格遵守；

电子认证业务规则是否符合证书策略的要求；

是否严格按照本CPS、业务规范和安全要求开展业务；

各种日志、记录是否完整，是否存在问题；

是否存在其它可能的安全风险；

天津CA支持的证书认证操作规程是否完全与本电子认证业务规则表达一致，包括天津CA的技术、手续、员工的相关管理制度和电子认证业务规则；

天津CA是否实施了相关技术、管理、相关制度和电子认证业务规则；

审计者或天津CA认为有必要审计的其他方面。

8.5.对问题与不足采取的措施

如果在审计过程中发现执行有不足之处，发生问题的职能部门对业务进行改进和完善，由安全策略委员会进行监督，完成对评估结果的改进后，各职能部门必须向安全策略委员会提交业务改进工作总结报告。

如果在外部评估过程中发现执行有不足之处，天津CA必须根据评估的结果检查缺失和不足，根据提出的整改要求，提交修改和预防措施以及整改方案，并接受对整改方案的审查，以及对整改情况的再次评估。

8.6.评估结果的传达与发布

除非法律明确要求，天津CA一般不公开审计结果。在必要的情况下，天津CA可依照与关联机构（例如垫付商、注册机构、注册分支机构、受理点）签订的协议中有关规定，向关联机构通知审计结果。

9.证书、证书撤销列表和在线证书状态协议

9.1.证书

天津CA签发的证书均符合X.509 V3证书格式，遵循RFC 5280标准。

9.1.1.版本号

X.509 V3

9.1.2.证书标准项及扩展项

1. 证书标准项：

- 证书版本号（Version）指明X.509证书的根式版本，值为V3。
- 证书序列号（SerialNumber）指唯一标识该证书的一组32位字符。
- 证书签名标识符（Signature）指定签发证书时所使用的签名算法。
- 签发机构名（Issuer）用来标识签发证书的CA的DN名字。

- CN = network trustCA，为通用名。
- C = CN，表示中国。
- 证书有效期（Validity）指证书的起止时间。
- 主题（Subject）指为证书证书持有者申请证书时所填写的申请信息。即证书持有者的甄别名。详细请参看第3.1节。
- 公钥（SubjectPublicKeyInfo）证书持有者公开密钥信息域包含两个重要信息：证书持有者的公开密钥的值；公开密钥使用的算法标识符。
- 微缩图算法。
- 证书内容的签名算法。
- 微缩图证书内容的签名值。

2.证书扩展项：

天津CA证书扩展项除使用RFC 5280中定义的证书扩展项，还支持私有扩展项。

天津CA采用的IETF RFC 5280中定义的扩展项有：

- 颁发机构密钥标识符Authority Key Identifier
- 主题密钥标识符Subject Key Identifier
- 密钥用法Key Usage
- 扩展密钥用途Extended Key Usage
- 基本限制Basic Constraints
- CRL分发点CRL Distribution Points

私有扩展项可支持以下类型：

- 个人身份标识码
- 个人社会保险号
- 企业组织机构代码
- 企业工商注册号
- 企业税号

9.1.3.算法对象标识符

天津CA签发的证书按照RFC 5280标准，用SM2算法签名。

9.1.4.名称形式

天津CA签发证书的甄别名符合X.500关于甄别名的规定。详情参见第3.1节内容。

9.1.5.名称限制

证书持有者在证书中的名称可以是假名，但不能使用匿名，并在天津CA的数据库中记录证书持有者的相关信息。天津CA可以按照一定的规则为证书持有者指定特殊名称，并且能够把该类特殊的名称与一个确定的实体（个人、机构或设备）唯一联系起来。

9.1.6.证书策略对象标识符

没有定义。

9.1.7.策略限制扩展项的用法

没有使用。

9.1.8.策略限定符的语法和语义

没有规定。

9.1.9.关键证书策略扩展项的处理规则

与X.509和PKI相关规定一致。

9.2.证书撤销列表

天津CA定期签发证书撤销列表（CRL），其所签发的CRL遵循RFC 3280标准。

9.2.1.版本号

采用X.509 V2格式。

9.2.2.CRL和CRL条目扩展项

CRL扩展项：颁发机构密钥标识符。

CRL条目扩展项：不使用CRL条目扩展项。

9.3.在线证书状态协议

RFC2560中定义了在线证书状态协议（Online Certificate Status Protocol, OCSP）,它克服了基于CRL的撤消方案的局限性，并且为证书状态查询提供即时的最新响应。

9.3.1.版本号

OCSP版本：V1。

9.3.2.OCSP扩展项

与RFC 2560一致。

10.法律责任和其他业务条款

10.1.费用

证书相关费用在天津CA的网站上公布（https://www.tjzhca.com）。价目表按天津CA明确指定的时间生效，若没有指定生效时间的，自价目表公布之日起生效。天津CA也可以通过其他方法通知证书持有者或其他各方费用变化。

10.1.1.证书签发和密钥更新费用

根据天津CA的价目确定。

10.1.2.证书查询费用

天津CA目前不对证书查询收取专门的费用。

10.1.3.证书撤销或状态信息的查询费用

证书撤销列表（CRL）的获取不收取任何费用。天津CA有可能根据需要OCSP服务作为增值服务收取费用。

10.1.4.其他服务费用

根据天津CA的价目确定。

10.2.财务责任

天津CA保证具有维持、运作和履行其责任的经济基础，有能力承担对证书持有者、依赖方因合法使用数字证书时而造成的责任风险，并依据本电子认证业务规则规定的方式和范围进行有过错时的赔偿。

10.2.1.责任担保范围

出现下列情形并经公司确认后，证书证书持有者、依赖方等实体可以申请赔偿（法定或约定免责除外）。

1）天津CA在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发，并导致证书持有者或依赖方遭受损失的；

2）天津CA将证书错误的签发给证书持有者以外的第三方，导致证书持有者或者依赖方遭受损失的；

3）由于天津CA的原因导致证书私钥被破译、窃取，导致证书持有者或者依赖方遭受损失的；

4）天津CA未能及时撤销证书，导致证书持有者或者依赖方遭受损失的。

10.2.2.责任赔付声明

天津CA承担证书持有者或依赖方在使用证书过程中造成损失时的举证责任，如无证据证明证书持有者或依赖方使用过程中存在错误操作，则天津CA将按照发布的赔偿办法予以赔偿。

10.3.业务信息保密

天津CA对业务过程中所接收的属于私有信息的业务信息负有保密责任。天津CA有专门的保密管理制度，保护自身和证书持有者的敏感信息及商业秘密。

10.3.1.保密信息范围

天津CA保密的信息包括（但不限于）：

1.系统方面

认证系统结构、配置，包括系统、网络、数据库等；

认证系统安全策略和方案；

系统操作、维护记录；

各类系统操作口令。

2.运营管理方面

物理安全策略与实施方案，包括场地、访问控制、入侵检测等实施方案；

密钥管理策略与操作记录；

CA或RA批准或拒绝的申请纪录；

可信人员名单；

内部安全管理策略与制度；

审计记录。

3.证书持有者信息

证书持有者的注册信息；

证书持有者系统、应用访问CRL、OCSP的记录（时间、频度）；

证书持有者与认证机构、注册机构签订的协议。

10.3.2.不属于保密的信息

天津CA电子认证业务规则、证书申请流程、手续、申请操作指南、证书撤销列表等。

10.3.3.保护保密信息的责任

天津CA有各种严格的管理制度、流程和技术手段保护自身的商业秘密，每个员工都必须接受信息保密方面的培训，并与公司签订保密协议。任何参与方有责任保证不泄露保密信息。

10.4.个人隐私保密

10.4.1.保护隐私的责任

除非执法、司法方面的强制需要，天津CA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第三方。

10.4.2.使用隐私信息的告知与同意

天津CA或其注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，则需要事先告知证书持有者并获得证书持有者同意和授权，证书持有者同意和授权信息以下列方式之一传送给天津CA或其注册机构：

1）将手写签名的同意和授权文件邮寄、快递到天津CA或其注册机构；

2）将手写签名的同意和授权文件传真到天津CA或其注册机构；

3）以签名电子邮件的形式同意并授权。

10.4.3.依法律或行政程序的隐私信息的使用

当天津CA在任何法律、法规或规章条款的要求下，或在司法机关的要求下必须披露本电子认证业务规则中具有保密性质的信息时，天津CA可以按照法律、法规或规章条款以及司法机关的要求，向执法部门公布相关的保密信息。这种披露不视为违反了保密的要求和义务。

10.4.4.不被视为隐私的信息

对其他信息的披露受制于法律、数字证书服务协议。

10.5.知识产权

天津CA保留对本CPS的所有知识产权。天津CA保留其签发的证书和证书撤销信息的所有知识产权。任何人可以免费地复制、分发证书和证书撤销列表，只要他们进行完整复制并且证书和证书撤销列表的使用符合相应的依赖方协议。证书申请者保留证书申请中包含的申请者拥有的商标、服务标志或商业名称以及签发给该证书申请者的证书中的可辨识名的所有权利。

10.6.陈述与担保

10.6.1.认证机构的陈述与担保

除非天津CA做出特别约定，若本电子政务电子认证服务业务规则的规定与其他天津CA制定的相关规定、指导方针相互抵触，证书持有者必须接受本电子政务电子认证服务业务规则的约束。在天津CA与包括证书持有者在内的其他方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本电子政务电子认证服务业务规则的规定执行。

天津CA承担的责任和义务是：

保证电子政务电子认证服务机构本身使用的公钥算法在现有通常技术条件下不会被攻破；保证天津CA的签名私钥在天津CA内部得到安全的存放和保护；天津CA建立和执行的安全机制符合国家政策的规定。天津CA不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担任何损失、损坏或赔偿责任。这些事件包括劳动纠纷、交易一方故意或无意的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、洪灾或其他大灾难等。针对上述内容补充解释如下：

第一：除上述所规定的职责条款，天津CA的服务机构、天津CA授权的发证机构、天津CA的雇员不承担其它任何义务。必须指出，本电子政务电子认证服务业务规则的内容，没有任何信息可以暗示或解释成天津CA必须承担其它的义务或天津CA必须对其行为做出其它的承诺。

第二：在上述内容中所罗列不可抗力的任何情况下，天津CA由于受到影响，可免除本节所述的责任和相应的证书策略规定的责任和义务。

第三：由于技术的进步与发展，为保证证书的安全性，天津CA会要求证书持有者及时更换证书以保证天津CA能更好地履行本节所述的责任。

10.6.2.注册机构的陈述与担保

注册机构必须遵守所有的登记程序和安全保障措施。这些程序和保障由天津CA决定，并在本电子认证业务规则或相应的注册机构协议中规定，以后天津CA可以根据情况修改有关内容，并及时公布。注册机构必须遵守和符合本电子认证业务规则的条款。

10.6.3.用户的陈述与担保

所有的证书持有者必须严格遵守关于证书申请以及私钥的所有权和安全保存相关的程序：

证书持有者在证书申请表上填写的所有声明和信息必须是完整、精确、真实和正确的，可供天津CA或受理点检查和核实；

证书持有者必须严格遵守和服从电子政务电子认证服务业务规则规定或者由天津CA推荐使用的安全措施；证书持有者需熟悉本电子政务电子认证服务业务规则的条例和与证书相关的证书政策，遵守证书持有者证书使用方面的有关限制；

一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘或泄密以及其他情况，证书持有者应立刻通知天津CA或天津CA授权的发证机构，申请采取冻结、撤销等处理措施。

10.6.4.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。

10.6.5.其他参与者的陈述与担保

遵守本CPS的所有规定。

10.7.担保免责

有下列情形之一的，应当免除天津CA的责任：

1）证书持有者在申请和使用天津CA数字证书时，有违反如下义务之一的：

A.证书持有者应当提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息；

B.证书持有者应当妥善保管天津CA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；

C.证书持有者在应用自己的密钥或使用数字证书时，应当使用可依赖的、安全的系统；

D.证书持有者知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知天津CA及相关各方，并终止使用该电子签名制作数据；

E.证书持有者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，不得将数字证书在天津CA规定使用范围之外的其他任何用途使用；

F.证书持有者必须在证书有效安全期内使用该证书，不得使用已失密或可能失密、已过有效期、被冻结、被撤销的数字证书；证书持有者应当根据规定按时向天津CA及当地业务受理点缴纳服务费用。

2）由于不可抗力原因而导致数字证书签发错误、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）：

A.自然灾害，包括地震、洪灾、火山爆发、滑坡、泥石流、雪崩、台风等；

B.社会异常或者政府行为，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）天津CA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。

10.8.偿付责任限制

对于由如下原因造成的用户或依赖方损失，天津CA对用户或依赖方进

行赔偿：

在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发；

由于天津CA的原因，使得证书中出现了错误信息；

因天津CA的原因，导致用户无法正常验证证书状态，使用户或依赖方利益受损。天津CA对于每份证书产生的所有数字签名和交易处理，对所有当事实体（包括但不限于用户、申请人或信赖方）有关该特定证书的合计责任应不超过赔付责任上限，这种赔付上限可以由天津CA视情况重新制定，天津CA会将重新制定后的情况立刻通知相关当事人。

天津CA所颁发数字证书的赔付责任上限如下：

A.个人证书500元；

B.机构证书500元；

C.设备证书2000元。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任，每份证书的责任均有封顶而不考虑数字签名和交易处理等有关的其他索赔的数量。当超过责任封顶时，可用的责任封顶将首先分配给最早得到索赔解决的一方，天津CA没有责任为每个证书支付高出责任封顶的赔付，而不管责任封顶的总量在索赔提出者之间如何分配。

10.9.赔偿责任

1.对于由如下原因造成的证书持有者或依赖方损失，天津CA对证书持有者或依赖方进行赔偿：

1）天津CA在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发；

2）由于天津CA的原因，使得证书中出现了错误信息。

2.在如下情况，证书持有者对自身原因造成的天津CA、依赖方损失承担责任：

1）证书持有者在证书申请中对事实的虚假或错误描述；

2）在证书申请中证书持有者没有披露重要的事实，如果这种错误表述或遗漏是因为粗心或故意欺骗任何一方；

3）证书持有者没有使用可信系统保护私钥，或者没有采取必要的措施防止证书持有者私钥的安全损害、丢失、泄漏、修改或非授权的使用；

4）证书持有者使用的名字（包括但不限于通用名、域名和Email地址）破坏了第三方的知识产权法。

3.在如下情况，依赖方对自身原因造成天津CA损失承担责任：

1）依赖方没有执行依赖方职责义务；

2）依赖方在不合理的环境下信赖一个证书；

3）依赖方没有检查证书状态确定证书是否过期或撤销。

4.天津CA承担赔偿责任（法定或约定免责除外）的赔偿限制如下：

1）天津CA对任何证书证书持有者、依赖方等实体有关证书赔偿的合计责任限制赔偿上限可以由天津CA根据情况重新制定，天津CA会将重新制定后的情况立刻通知相关当事人；

2）对于由证书持有者或依赖方的原因造成的损失，天津CA不承担责任，由证书持有者或依赖方自行承担；

3）天津CA只有在其证书有效期限内承担损失赔偿。

10.10.有效期限与终止

10.10.1.有效期限

本CPS自发布之日起生效。

10.10.2.终止

当新版本的CPS生效时或天津CA终止业务时，旧版本CPS自动终止；当天津CA中止业务时，天津CACPS自动终止。

10.10.3.效力的终止与保留

本CPS终止后，已签发符合证书策略的证书，效力作用直到证书到期或撤消。当由于某种原因，如内容修改、与适用法律相冲突，证书策略、电子政务电子认证服务业务规则、数字证书服务协议、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。

10.11.对参与者的个别通告与沟通

天津CA及其注册机构在必要的情况下，如在主动撤销证书持有者证书、发现证书持有者将证书用于规定外用途及其他违反数字证书服务协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，通知证书持有者、依赖方。

10.12.修订

10.12.1.修订程序

CPS中所列条款不能适应运营的实际需求，或者与现行法律相抵触时，天津CA有权在合适的时间修订本CPS中任何术语、条件和条款，而且无须预先通知任何一方。

本CPS的修订，由安全管理部门讨论，提出修订报告，经天津CA安全策略委员会批准后，由安全管理部门负责组织修订，修订后的CPS经过天津CA安全策略委员会审查通过后正式实施。

10.12.2.通知机制和期限

修改后的CPS经批准后将立即在天津CA网站更新通告栏发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，天津CA将在合理的时间内通知有关各方，合理的时间保证有关方面受到的影响最小。

天津CA保留随时对CPS进行修订的权利，进行下列（但不限于）不重要的修订后将不作通知：对印刷错误的更正、URL的改变和联系人信息的变更等。

10.12.3.必须修改业务规则的情形

由天津CA安全管理部门根据公司业务情况提出，天津CA安全策略委员会审批。

10.13.争议处理

如果各参与方之间无法协商解决出现的问题和争端，可通过法律途径解决。

10.14.管辖法律

本规则在各方面服从《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》等中华人民共和国法律、规则、规章、法令和政令的约束和解释。

天津CA的任何业务活动受有关法律、法规的制约，任何业务和法律文件、合同的解释、执行不能同有关法律、法规相冲突。

10.15.与适用法律的符合性

本CPS的使用也必须遵从使用地的相关法律和法规。

10.16.一般条款

10.16.1.完整协议条款

CPS、数字证书服务协议及依赖方协议及其补充协议将构成天津CA信任域参与者间的完整协议。

10.16.2.转让条款

天津CA、注册机构、证书持有者及依赖方之间的责任、义务不能通过任何形式转让给其他方。

10.16.3.分割性条款

法律允许的范围内，在天津CA数字证书服务协议、依赖方协议内出现可以同其他条款分割的条款时，协议中的可分割条款的无效不应该影响协议中其他条款效力。

10.16.4.强制执行条款

在天津CA、注册机构、证书持有者和依赖方之间出现法律诉讼时，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。

10.16.5.不可抗力条款

当由于不可抗力，如战争和地震、洪灾、火山爆发等自然灾害等，造成天津CA、注册机构无法提供正常的服务时，天津CA、注册机构不承担由此给客户造成的损失。

10.17.其他条款

天津CA对本CPS具有最终解释权。