天津滨海CA电子政务电子认证
服务业务规则

V2.0

天津市滨海数字认证有限公司

二〇二三年十二月

修订历史记录

版本号	版本日期	修改者	说 明	批准
V1.0	2017.3	王洪艳 金红艳	创建	2017 年 3 月 31 日安全策略（管理）委员会批准发布执
V1.1	2017.6	王洪艳 金红艳	按照《电子政务电子认证服务业务规则规范》和国家密码管理局审核要求，对文档进行了进一步的细化和完善，调整了文档的结构布局。	2017 年 6 月 1 日安全策略（管理）委员会批准发布执行。
V1.2	2018.6	王洪艳 金红艳 张铁夫	1、根据现行业务修订证书业务相关内容；2、根据安全运维实际情况，修订安全保障规范；3、根据实际服务情况，修订服务规范。	2018 年 6 月 25 日安全策略（管理）委员会批准发布执行。

V1.3	2021.11	金红艳 王洪艳	1、组织机构身份的鉴别，增加一项身份鉴别资料：授权委托书（加盖公章）。申请机构授权经办人负责办理数字证书相关事宜的证明文件。证书均有明确的证书有效期,用户应在证书有效期到期前“90天内”到天津滨海CA授权的注册机构申请更换新证书。 2、“三管一操”相关内容更新为“五管一操”相关内容	2021 年 11 月 10 日安全策略（管理）委员会批准发布执行。
V2.0	2023.12	王洪艳	证书生命周期操作要求中，增加了线上业务相关内容	2023 年 1 月 31 日安全策略（管理）委员会批准发布执行。

版权声明

地址：天津市空港经济区西七道 26 号

邮编：300308

电话：400-872-5550

电子邮件：tjbhca@tjbhca.com

目　录

1.公司概述 1

2.参考文件 3

3.术语和定义 4

4.符号和缩略语 6

5.《电子政务电子认证服务业务规则》管理规范 7

5.1 管理机构 7

5.2 联系方式 7

5.3 批准程序 7

6.电子政务电子认证服务操作规范 8

6.1 数字证书服务操作规范 8

6.1.1 数字证书格式 8

6.1.2 身份标识与鉴别 14

6.1.3 数字证书服务操作要求 18

6.1.3.1 证书申请 18

6.1.3.2 证书申请处理 19

6.1.3.3 证书签发 20

6.1.3.4 证书接受 20

6.1.3.5 密钥对和证书使用 21

6.1.3.6 证书更新 21

6.1.3.7 证书撤销 22

6.1.3.8 密钥生成、备份和恢复 25

6.2 应用集成支持服务操作规范 25

6.2.1 服务策略和流程 25

6.2.2 应用接口 25

6.2.3 集成内容 26
6.2.4 应用集成流程 26
6.3 信息服务规范 28
6.3.1 服务内容 28
6.3.2 服务管理规则 29
6.3.3 服务方式 29
6.4 使用支持服务操作规范 31
6.4.1 服务内容 31
6.4.2 服务方式 32
6.4.3 服务质量 33
6.5 安全保障规范 34
6.5.1 认证机构设施、管理和操作控制 34
6.5.1.1 物理控制 34
6.5.1.2 操作过程控制 36
6.5.1.3 人员控制 37
6.5.1.4 审计日志程序 39
6.5.1.5 记录归档 40
6.5.1.6 认证机构密钥更替 42
6.5.1.7 数据备份 42
6.5.1.8 损害和灾难恢复 44
6.5.1.9 认证机构或注册机构终止 48
6.5.2 认证系统技术安全控制 49
6.5.2.1 密钥对的生成和安装 49
6.5.2.2 私钥保护和密码模块工程控制 50
6.5.2.3 密钥对管理的其他方面 51
6.5.2.4 激活数据 51
6.5.2.5 计算机安全控制 52
6.5.2.6 生命周期安全控制 53

6.5.2.7 网络安全控制 54
6.5.2.8 时间戳 56
7. 电子政务电子认证服务中的法律责任及相关要求 57
7.1 要求 57
7.2 内容 57
7.2.1 费用 57
7.2.2 财务责任 58
7.2.3 业务信息保密 58
7.2.4 个人隐私保密 59
7.2.5 知识产权 60
7.2.6 陈述和担保 60
7.2.7 担保免责 61
7.2.8 偿付责任限制 62
7.2.9 赔付责任 63
7.2.10 有效期和终止 64
7.2.11 对参与者的个别通告与沟通 64
7.2.12 修订 64
7.2.13 争议处理 64
7.2.14 管辖法律 64
7.2.15 与适用法律的符合性 65
7.2.16 一般条款 65
7.2.17 其他条款 66

1.公司概述

天津市滨海数字认证有限公司（以下简称天津滨海 CA），成立于 2015 年 5 月，是国有控股有限公司。

天津滨海 CA 位于天津空港经济区西七道 26 号，整体占地面积约 700 平方米，整体环境设备设施完善，符合国家相关部门的要求。

天津滨海 CA 是设计、建设、运行，可实现跨地区、跨行业统一认证和安全服务的电子认证服务机构。该机构遵循 PKI 体系标准，在地域或行业两方面进行全方位的布局，可实现交叉认证。天津滨海 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，在 2016 年 3 月和 2016 年 4 月分别通过了国家密码管理局组织的天津滨海电子认证服务系统技术测试、技术文档鉴定和安全性审查，并于 2016 年 5 月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》，成为了全国通过安全性审查的第三方区域性数字证书认证中心之一。

2017 年 3 月，天津滨海 CA 取得了工业和信息化部《电子认证服务许可证》。2017 年 6 月，天津滨海 CA 取得了国家密码管理局电子政务电子认证服务资质。

天津滨海 CA 为互联网络的交易和作业方提供认证机制，保证交易主体身份的真实性，为信息的保密性、完整性以及交易的不可抵赖性提供全面和可靠的服务。其宗旨是保证互联网提供的服务和享受服务的客户实现交易和信息传输安全，为互联网络的客户提供网上身份

认证服务。

天津滨海 CA 作为被信任的第三方，为网上交易和网上安全作业的参与方颁发数字证书。在天津滨海 CA 或天津滨海 CA 授权的发证机构确定参与方的真实身份后，由天津滨海 CA 或天津滨海 CA 授权的发证机构发放数字证书，发放的所有数字证书均遵循 X.509 V3 的规范。天津滨海 CA 承诺，在证书有效的情况下，保证证书能唯一地与身份明确的实体相关联，公钥能与身份确定的实体唯一相对应。

天津滨海 CA 拥有一支专业、强大的技术及研发团队，团队专注于研发构建网络信任体系结构所需要的技术产品与服务，为了配合证书业务的正常开展，天津滨海 CA 制定了证书策略和电子认证业务规则，这些为开展电子认证服务的各项工作提供了完善的条件。

天津滨海 CA 作为依法设立的第三方电子认证服务机构，其安全体系与运营体系完备，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及强有力的支持和保障。

2.参考文件

《电子政务电子认证服务业务规则规范》

《电子政务电子认证服务管理办法》

《电子认证服务密码管理办法》

《证书认证系统密码及其相关安全技术规范》

《电子政务数字证书格式规范》

《电子政务数字证书应用接口规范》

《中华人民共和国电子签名法》

3.术语和定义

A. 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。

B. 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。

C. 鉴别 identification

辨别认定证书申请者提交材料真伪的过程。

D. 实体鉴别 entity authentication

确认一个实体所声称的身份。

E. 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。

F. 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。

G. 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。

H. 电子认证服务机构 electronic certification service provider

提供电子认证服务的机构。

I. 证书注册机构 certificate register center

接收公钥证书的申请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。

J. 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。

K. 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。

L. 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。

M. 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。

N. 公钥基础设施 Public Key Infrastructure

公钥基础设施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。

O. 在线证书状态协议 Online Certificate Status Protocol

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。

P. 证书策略 Certificate Policy

证书策略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。

Q. 电子政务电子认证业务服务规则 Certificate Practice Statement

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文档。

R. 私钥 Private key

私钥是在公钥基础设施 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。

S. 公钥 Public key

公钥是在公钥基础设施中为一个密码串，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。

T. 甄别名 Distinguished Name

甄别名是在数字证书的主体名称域中，用来唯一标识用户的 X.509 名称。此域需要填写反映用户真实身份的、具有实际意义的、与法律不冲突的内容。

4.符号和缩略语

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)

DN 唯一甄别名（Distinguished Name）

PIN 个人识别码（Personal Identificate Number）

PKI 公钥基础设施（Public Key Infrastructure）

5.《电子政务电子认证服务业务规则》管理规范

5.1 管理机构

管理本文档的机构是天津滨海 CA 安全策略（管理）委员会。

天津滨海 CA 电子政务电子认证服务业务规则严格按照国家密码管理局的《电子政务电子认证服务管理办法》等要求编写，接受国家密码管理局的审查监督，以及备案要求。天津滨海 CA 安全策略（管理）委员会作为最高策略管理机构，是电子认证业务规则符合策略的决定机构。

5.2 联系方式

天津滨海 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，并由天津滨海 CA 负责解释。

电 话：400-872-5550

地址：天津空港经济区西七道 26 号（邮编：300308）

电子邮件：tjbhca@tjbhca.com

5.3 批准程序

CPS 批准主要分为计划、编写（修订）、审议和发布四个阶段。规则编写组根据相关法律政策和运营策略提出规则编写（修订）计划，再由规则编写组完成具体条款编写工作，编写（修订）后的规则交由天津滨海 CA 安全策略（管理）委员会审议，审议通过后，通过天津滨海 CA 网站正式对外发布，并向国家密码管理局备案。

6.电子政务电子认证服务操作规范

6.1 数字证书服务操作规范

6.1.1 数字证书格式

天津滨海 CA 签发的数字证书格式严格符合《电子政务数字证书格式规范》有关要求。

A. 机构证书

1）机构签名证书

天津滨海 CA 机构签名证书格式

证书字段	证书域		证书项	内容	注释
基本证书字段（TBSCertificater）	X509 V1 版本域	版本		V3	
		序列号			
		签名算法		1.2.156.10197.1.501	基于 SM3 的 SM2 算法
		颁发者	CN	TJCA	机构名称
			O	TJCA	
			C	CN	
		有效期从			有效开始日期
		到			有效结束日期
		使用者	CN	组织机构名称	使用者主体
			O	TJCA	
			C	CN	
		公钥		ECC	
		公钥参数		1.2.156.10197.1.301	
	标 准 扩展域	CRL 分发点			
		使用者密钥标识符			证书公钥的摘要
		授权信息访问			
		授权密钥标识符			根证书公钥的摘要

		证书策略		
		密钥用法	数字签名	不可否认性
				（可自定义）
				（可自定义）
	自定义扩展域			（可自定义）
				（可自定义）
签名算法字段		指纹算法	Sha1	
签名值字段		指纹	签名值	证书摘要

2）机构加密证书

天津滨海 CA 机构加密证书格式

证书字段	证书域	证书项		内容	注释
基本证书字段（TBSCertificater）	X509 V1 版本域	版本		V3	
		序列号			
		签名算法		1.2.156.10197.1.501	基于 SM3 的 SM2 算法
		颁发者	CN	TJCA	机构名称
			O	TJCA	
			C	CN	
		有效期从			有效开始日期
		到			有效结束日期
		使用者	CN	组织机构名称	使用者主体
			O	TJCA	
			C	CN	
		公钥		ECC	
		公钥参数		1.2.156.10197.1.301	
	标 准 扩展域	CRL 分发点			
		使用者密钥标识符			证书公钥的摘要
		授权信息访问			

		授权密钥标识符		根证书公钥的摘要
		证书策略		
		密钥用法	密钥加密	数据加密
				（可自定义）
				（可自定义）
	自定义			（可自定义）
	扩展域			（可自定义）
签名算法字段		指纹算法	Sha1	
签名值字段		指纹	签名值	证书摘要

B. 个人证书

1）个人签名证书

天津滨海 CA 个人签名证书格式

证书字段	证书域	证书项		内容	注释
基本证书字段（TBSCertificater）	X509 V1 版本域	版本		V3	
		序列号			
		签名算法		1.2.156.10197.1.501	基于 SM3 的 SM2 算法
		颁发者	CN	TJCA	机构名称
			O	TJCA	
			C	CN	
		有效期从			有效开始日期
		到			有效结束日期
		使用者	CN	个人姓名	使用者主体
			O	TJCA	
			C	CN	
		公钥		ECC	
		公钥参数		1.2.156.10197.1.301	
	标 准 扩展域	CRL 分发点			
		使用者密钥标识符			证书公钥的摘要

		授权信息访问		
		授权密钥标识符		根证书公钥的摘要
		证书策略		
		密钥用法	数字签名	不可否认性
				（可自定义）
				（可自定义）
	自定义扩展域			（可自定义）
				（可自定义）
签名算法字段		指纹算法	Sha1	
签名值字段		指纹	签名值	证书摘要

2） 个人加密证书

天津滨海 CA 个人加密证书格式

证书字段	证书域	证书项		内容	注释
基本证书字段（TBSCertificater）	X509 V1 版本域	版本		V3	
		序列号			
		签名算法		1.2.156.10197.1.501	基于 SM3 的 SM2 算法
		颁发者	CN	TJCA	机构名称
			O	TJCA	
			C	CN	
		有效期从			有效开始日期
		到			有效结束日期
		使用者	CN	个人姓名	使用者主体
			O	TJCA	
			C	CN	
		公钥		ECC	
		公钥参数		1.2.156.10197.1.301	
	标　准	CRL 分发点			

	扩展域	使用者密钥标识符		证书公钥的摘要
		授权信息访问		
		授权密钥标识符		根证书公钥的摘要
		证书策略		
		密钥用法	密钥加密	数据加密
				（可自定义）
				（可自定义）
	自定义扩展域			（可自定义）
				（可自定义）
签名算法字段		指纹算法	Sha1	
签名值字段		指纹	签名值	证书摘要

C. 设备证书

1）设备签名证书

天津滨海 CA 设备签名证书格式

证书字段	证书域	证书项		内容	注释
基本证书字段（TBSCertificater）	X509 V1 版本域	版本		V3	
		序列号			
		签名算法		1.2.156.10197.1.501	基于 SM3 的 SM2 算法
		颁发者	CN	TJCA	机构名称
			O	TJCA	
			C	CN	
		有效期从			有效开始日期
		到			有效结束日期
		使用者	CN	服务器域名	使用者主体
			O	TJCA	
			C	CN	
			OU	TJCA	部门
		公钥		ECC	

		公钥参数	1.2.156.10197.1.301	
	标 准 扩展域	CRL 分发点		
		使用者密钥标识符		证书公钥的摘要
		授权信息访问		
		授权密钥标识符		根证书公钥的摘要
		证书策略		
		密钥用法	数字签名	不可否认性
				（可自定义）
				（可自定义）
	自定义 扩展域			（可自定义）
				（可自定义）
签名算法字段		指纹算法	Sha1	
签名值字段		指纹	签名值	证书摘要

2） 设备加密证书

天津滨海 CA 设备加密证书格式

证书字段	证书域	证书项		内容	注释
基本证书字段（TBSCertificater）	X509 V1 版本域	版本		V3	
		序列号			
		签名算法		1.2.156.10197.1.501	基于 SM3 的 SM2 算法
		颁发者	CN	TJCA	机构名称
			O	TJCA	
			C	CN	
		有效期从			有效开始日期
		到			有效结束日期
		使用者	CN	服务器域名	使用者主体
			O	TJCA	
			C	CN	

			OU	TJCA	部门
		公钥		ECC	
		公钥参数		1.2.156.10197.1.301	
	标　准 扩展域	CRL 分发点			
		使用者密钥标识符			证书公钥的摘要
		授权信息访问			
		授权密钥标识符			根证书公钥的摘要
		证书策略			
		密钥用法		密钥加密	数据加密
					（可自定义）
					（可自定义）
	自定义 扩展域				（可自定义）
					（可自定义）
签名算法字段		指纹算法		Sha1	
签名值字段		指纹		签名值	证书摘要

6.1.2 身份标识与鉴别

A. 命名

1） 名称类型

证书从应用角度分为系统证书和用户证书，命名由用户应用决定。

天津滨海 CA 证书体系中采用 X.500 定义的甄别名（DN）标准来标识一张证书使用者的身份信息。

天津滨海 CA 使用符合 X.500 甄别名规定的命名规则。天津滨海 CA 签发的证书的实体名可以是人员姓名、组织机构名、域名。

天津滨海 CA 证书的主题域中包含 X.500 甄别名。天津滨海 CA 的主题甄别名由以下几项组成：

Country（C）

Organization（O）

Organizational Unit（OU）

Common Name（CN）

E-mail 地址（E）

2） 对名称有意义的要求

用户的甄别名(DN)必须具有一定的代表意义。

证书通用名标识本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

3） 证书持有者的匿名或伪名

天津滨海 CA 规定，证书持有者不能使用匿名或伪名申请证书。

4） 理解不同名称形式的规则

依 X.500 甄别名命名规则解释。

5） 名称的唯一性

天津滨海 CA 规定，在用户信息中 DN 必须唯一标识该用户。

6） 商标的识别、鉴别和角色

证书申请者不应使用任何可能侵犯知识产权的名称。天津滨海 CA 不对证书申请者是否拥有命名的知识产权进行判断和决定，也不负责解决证书中任何关于域名、商标等知识产权的纠纷。天津滨海 CA 没有权利，也没有义务拒绝或者质疑任何可能导致产生知识产权纠纷的证书申请。

B. 证书申请人的身份确认

1） 证明拥有私钥的方法

天津滨海 CA 证明拥有私钥的方法是根据证书申请信息进行验证。在天津滨海 CA 证书服务体系中，用户签名私钥在用户端生成，用户证书请求信息中包含用私钥进行的数字签名，CA 用其对应的公钥来验证这个签名。

证书申请人被视作其签名私钥的唯一持有者，因此天津滨海 CA 要求证书申请人妥善保管自己的签名私钥。

2） 组织机构身份的鉴别

采用线上业务模式时，天津滨海 CA 或授权的发证机构采用单位名称及统一社会信用代码在线核验模块、姓名及居民身份证号在线核验模块、人脸核验意愿核身模块，以及其他可靠的技术方法、管理方法为辅助手段，对申请机构的身份进行鉴别。

采用线下业务模式时，组织机构申请者填写书面申请表，经过单位授权代表的签署及单位盖章，表示接受证书申请的有关条款，并承担相应的责任。

天津滨海 CA 授权的发证机构必须对用户进行以下资料鉴别：

（1）申请机构的工商营业执照副本及复印件（加盖公章）。如果没有营业执照，则提供以下有效证件的副本及复印件：

a.营业执照

b.企业法人营业执照

c.事业单位法人登记证

d.社会团体法人登记证

e.政府批文

f.其他有效证件

（2）经办人身份证原件与复印件（加盖公章）。

（3）授权委托书（加盖公章）。申请机构授权经办人负责办理数字证书相关事宜的证明文件。

如申请机构尚未取得统一社会信用代码，则还需提供组织机构代码证的复印件（加盖公章），以及国税、地税的税务登记证及复印件（加盖公章）。

天津滨海 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，并严格按照用户身份鉴别规范进行鉴别。

3） 个人身份鉴别

采用线上业务模式时，天津滨海 CA 或授权的发证机构采用姓名及居民身份证号在线核验模块、人脸核验意愿核身模块，以及其他可靠的技术方法、管理方法为辅助手段，对申请人的身份进行鉴别。

采用线下业务模式时，个人申请者填写书面申请表，签字确认，表示接受证书申请的有关条款，并承担相应的责任。

申请人需要提供合法身份证明文件，如：居民身份证、军官证、护照等证明用户的身份。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文件，以及申请人对被委托人的授权委托文件。

对居民身份证的鉴别，天津滨海 CA 借助身份证识别仪来进行。

4） 设备身份的鉴别

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，天津滨海 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)。天津滨海 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文件进行合法性甄别的义务，申请者自行负责材料真实性。

5） 集团用户身份鉴别

集团用户是指为其下辖或管理的机构、部门、组织、人员等统一申请办理证书业务的用户。集团用户可以是证书依赖方（依赖证书中的数据来做决定的用户），也可以是其他形式的合作方。

与集团用户签署合作协议或合同时，应约定集团用户负责为其代为申请证书服务的证书用户进行身份鉴别，保证其身份的真实有效，并愿意承担由于提供的资料虚假失实而导致的一切后果。

集团用户统一申请办理证书业务时，应承诺遵守天津滨海 CA《电子认证服务协议》中的各项规定。该协议在天津滨海 CA 官网（http://www.tjbhca.com)上发布。

集团用户统一申请办理证书业务时，应提供以下资料：

（1）统一办理数字证书的申请（加盖公章）；

（2）统一申请办理数字证书信息清单（加盖公章）。

在天津滨海 CA 与集团用户同时认为有必要的情况下，集团用户还可为其统一申请办理的证书业务提供证书持有人的相关资料。证书持有人为单位的，按组织机构身份的鉴别要求提供资料。证书持有人为个人的，按个人身份鉴别要求提供资料。集团用户负责鉴证相关资料的真实、完整、有效。

6） 没有验证的证书持有者信息

用户提交鉴证文件以外的信息为没有验证的用户信息。

7） 授权确认

证书申请者申请某一类型的证书时，天津滨海 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。组织机构或个人在天津滨海 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。

C. 密钥更新请求的识别与鉴别

在常规密钥更新中，通过用户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，天津滨海 CA 使用用户原有公钥验证确认签名来进行用户身份标识

和鉴别。申请的鉴别应满足以下条件：

1）申请对应的原证书存在并且由天津滨海 CA 签发；

2）用原证书上的证书持有者公钥对申请的签名进行验证；

3）基于原注册信息进行身份鉴别。

D. 撤销后密钥更新的标识与鉴别

证书撤销后不能进行密钥更新。

撤销后密钥更新中对身份标识和鉴别的要求，使用与原始身份验证相同的流程，详见组织机构身份的鉴别、个人身份的鉴别和设备身份的鉴别。

在天津滨海 CA 的证书业务中，证书撤销请求可以来自用户，也可以来自天津滨海 CA。当天津滨海 CA 授权的发证机构有充分的理由撤销用户时，有权依法撤销证书，这种情况无须进行鉴证。如果用户主动要求撤销证书，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，天津滨海 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。

6.1.3 数字证书服务操作要求

6.1.3.1 证书申请

A. 证书申请实体

证书申请实体包含个人、企业单位、事业单位、社会团体、人民团体等各类组织机构。

B. 注册过程与责任

天津滨海 CA 接受线上和线下两种方式的证书申请。

线上申请证书是指用户通过天津滨海 CA 自助服务平台、其他定制化服务平台、电子邮件等形式申请证书。

线下申请证书指用户来天津滨海 CA 或授权的发证机构现场，面对面提交证书申请。

证书申请流程如下：

1）对于个人证书，申请者到天津滨海 CA 授权的发证机构领取证书申请表，并提供个人身份证明文件原件及其复印件，例如：身份证、军官证、学生证、护照等。如果是委托办理，需同时递交申请人和被委托人的上述文件，并递交申请人对被委托人的授权委托文件。

2）对于单位证书，申请者到天津滨海 CA 授权的发证机构领取单位证书申请表，申请者应提供单位的营业执照（事业单位法人登记证、社会团体法人登记证、政府批文或其他有效证明文件）、经办人的身份证、单位对经办人的授权委托证明和天津滨海 CA 可能需要的其他文件。如申请者尚未取得统一社会信用代码，则还需提供组织机构代码证，以及国税、地税的税务登记证等。

3）对于设备证书的申请资料，与单位证书的申请相同，同时还需要提供国家认可的互联网服务提供商或管理机构或申请单位出具的与设备证书申请有关的证明文件。

4）与集团用户签署合作协议或合同时，应约定集团用户负责为其代为申请证书服务的证书用户进行身份鉴别，保证其身份的真实有效。集团用户统一申请办理证书业务，应承诺遵守天津滨海 CA《电子认证服务协议》中的各项规定。同时，还应出具统一办理数字证书的申请、统一申请办理数字证书信息清单。

客户的申请表和相关证明文件的复印件存档期为电子签名认证证书失效后五年。

天津滨海 CA 作为电子认证服务的发证机构有责任对申请人的身份进行充分的验证。出于安全性和审查的需要，申请表应由验证人签名并注明日期。申请者必须真实填写证书申请信息，并遵守天津滨海 CA《电子认证服务协议》中的相关规定，否则，天津滨海 CA 有权拒绝签发证书，且由此造成的后果，天津滨海 CA 不承担任何责任。

6.1.3.2 证书申请处理

A. 执行识别与鉴别功能

天津滨海 CA 授权的发证机构遵循第 6.1.2 节对证书申请者提交的信息进行识别，并由双人复合鉴别验证。

B. 证书申请批准和拒绝

依据识别与鉴别的信息，天津滨海 CA 授权的发证机构有权决定接受或拒绝用户的申请。

天津滨海 CA 成功标识和鉴别了用户的身份信息；用户接受用户协议的内容和要求，且按照规定支付了相应的费用等，天津滨海 CA 授权的发证机构将接受用户的证书申请。

用户申请未完成标识和鉴别的过程；用户不能提供所需要的补充文件；用户不接受或者反对用户协议的内容和要求；用户没有或者不能够按照规定支付相应的费用；天津滨海 CA 授权的发证机构认为批准该申请将会对天津滨海 CA 带来争议、法律纠纷或者损失。以上情形之一，天津滨海 CA 授权的发证机构有权拒绝用户的证书申请。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

6.1.3.3 证书签发

A. 证书签发过程中电子认证服务机构的行为

天津滨海 CA 在接受证书申请之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地受理了证书申请。通常，天津滨海 CA 所签发的证书在 24 小时内生效。

B. 电子认证服务机构对证书持有者的通告

电子认证服务机构通过注册机构，对用户的通告有以下几种方式：

1）通过面对面的方式，通知用户本人到注册机构领取数字证书，注册机构把证书等直接提交给用户；

2）邮政信函通知用户；

3）其他天津滨海 CA 认为安全可行的方式通知用户。

6.1.3.4 证书接受

A. 构成接受证书的行为

证书持有者接受证书的方式可以有如下几种：

1）通过面对面的提交，证书持有者接受载有证书和私钥的介质；

2）按 CA 或 RA 的提示，通过网络将证书下载到本地存放介质，如智能 USB KEY 或智能 IC 卡。

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

B. CA 对证书的发布

对于证书持有者证书，CA 将证书信息自动发布到目录系统，或不进行发布。

C. CA 通知其他实体证书的签发

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

6.1.3.5 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。

A.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，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。

B.依赖方的公钥和证书使用

当依赖方接受到签名的信息后，应该：

1）获得对应的证书及信任链；

2）验证证书的有效性；

3）确认该签名对应的证书是依赖方信任的证书；

4）证书的用途适用于相应的签名；

5）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。

6.1.3.6 证书更新

A. 证书更新的情形

证书均有明确的证书有效期,用户应在证书有效期到期前 90 天内到天津滨海 CA 授权的注册机构申请更换新证书。

证书更新的具体情形如下：

1）证书的有效期将要到期；

2）密钥对的使用期将要到期；

3）因加密密钥的丢失、损坏或泄漏导致原证书被吊销且还有证书使用需求；

4）其他。

B. 请求证书更新的实体

由天津滨海 CA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体。

C. 证书更新请求的处理

线上更新证书是指用户通过天津滨海 CA 自助服务平台、其他定制化服务平台、电子邮件等形式更新证书。

线下更新证书流程：申请者到天津滨海 CA 或授权的发证机构书面填写申请表，并注明更新的原因；天津滨海 CA 或授权的发证机构按照 6.1.2 节中身份标识与鉴别办法对用户提交的证书更新申请进行审核。审核通过后，进行数字证书更新操作；证书更新后，发证机构将证书当面发给用户，新证书签发后旧的证书将被撤销。

D. 对证书持用者的通告

电子认证服务机构通过注册机构，对用户的通告有以下几种方式：

1）通过面对面的方式，通知用户本人到注册机构领取数字证书，注册机构把证书等直接提交给用户；

2）邮政信函通知用户；

3）其他天津滨海 CA 认为安全可行的方式通知用户。

E. 构成接受更新证书的行为

1）系统记录证书持有者下载了证书即表明证书持有者接受了证书；

2）当证书持有者接受了载有证书的介质即表明证书持有者接受了证书。

F. 电子认证服务机构对更新证书的发布

一旦证书用户接受证书，发证机构将在目录服务器及由天津滨海 CA 和其授权发证机构决定的其它合理的方式来发布证书。

G. 电子认证服务机构对其他实体的通告

天津滨海 CA 不具有向其他实体进行单独通告的义务，其他实体可以通过从目录服务器中查询到天津滨海 CA 已经签发的数字证书。

6.1.3.7 证书撤销

A. 证书撤销的情形

1）新的密钥对替代旧的密钥对；

2）密钥失密：与证书中的公钥相对应的私有密钥被泄密或用户怀疑自己的

密钥失密；

3）从属关系改变：与密钥相关的用户的主题信息改变，证书中的相关信息有所变更；

4）操作终止：由于证书不再需要用于原来的用途，但密钥并未失密，而要求终止（例如用户离开了某个组织）；

5）证书到期：到期后用户未续约；

6）证书的更新费用未收到；

7）用户不能履行电子政务电子认证服务业务规则或其他协议、法律及法规所规定的责任和义务；

8）用户申请初始注册时，提供不真实材料；

9）证书已被盗用、冒用、伪造或者篡改；

10）CA 失密：电子认证服务机构因运营问题，导致 CA 内部重要数据或 CA 根密钥失密等原因；

11）利用数字证书在网上进行违法犯罪活动的；

12）其他情况：这些情况可以是因法律或政策的要求天津滨海 CA 采取的临时撤销措施，也可以是用户申请撤销证书时填写的其他原因。

B. 请求证书撤销的实体

请求证书撤销的实体包括：

1）用户本人或其授权代表；

2）天津滨海 CA 或其授权机构的授权代表；

3）司法机关等公共权力部门的授权代表。

C. 撤销请求的流程

线上撤销证书是指用户通过天津滨海 CA 自助服务平台、其他定制化服务平台、电子邮件等形式撤销证书。

线下撤销证书流程：申请者到天津滨海 CA 或授权的发证机构书面填写申请表，并注明撤销的原因。然后天津滨海 CA 或授权的发证机构按照身份标识与鉴别办法对用户提交的相关业务申请进行审核。

对于强制撤销，天津滨海 CA 或经天津滨海 CA 授权的发证机构可以对用户证书进行强制撤销，撤销后必须立即通知该证书用户。被撤销的用户证书在 24 小时内通过 CRL 向外界公布。

D. 撤销请求宽限期

证书持有者一旦发现需要撤销证书，应向发放该证书的注册机构及时提出撤销请求。如果出现私钥泄露等事件，撤销请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他撤销原因的撤销请求必须在 24 小时内提出。

E. 电子认证服务机构处理撤销请求的时限

发证机构在接到用户挂失、撤销等数字证书撤销申请时，应及时受理。在受理后 24 小时内保证数字证书撤销操作正式生效。证书持有者在正式提出证书撤销申请后不得在工作中继续使用此证书，否则由此产生的后果，由证书持有者自行承担。证书持有者在正式提出证书撤销申请后必须立即将此情况通知与此证书相关的依赖方，以便在工作中停止使用该证书，否则由此产生的后果，由证书持有者自行承担。在用户办理数字证书撤销相关手续前及发证机构受理用户证书撤销相关申请时起到证书撤销生效时 24 小时内造成的损失，发证机构不承担相关法律责任。天津滨海 CA 每 24 小时签发一次 CRL，并将最新的 CRL 发布到目录服务器指定的位置，供请求者查询下载。

F. 依赖方检查证书撤销的要求

CRL 查询：利用证书中标识的 CRL 地址，通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的检验。

G. CRL 发布频率

CRL 发布频率为 24 小时一次，在发布的同时对原有内容进行更新。

H. CRL 发布的最大滞后时间

CRL 发布的最长滞后时间为 24 小时。

I. 在线状态查询的可用性

天津滨海 CA 向证书用户提供 7*24 小时在线证书状态查询服务（OCSP）。

J. 在线状态查询要求

依赖方在信赖一张证书前必须对此证书进行证书状态查询，查询方式为检查 CRL。

K. 撤销信息的其他发布形式

除了 CRL 外，天津滨海 CA 所发布的撤销信息也可通过 OCSP 来查询和获得。

L. 密钥损害的特别处理要求

无论是证书持有者还是电子认证服务机构、注册机构，发现证书密钥受到安全损害时应立即撤销证书。

6.1.3.8 密钥生成、备份和恢复

A. 密钥生成与备份

1）加密密钥对：由中华人民共和国国家密码管理局许可的、天津滨海 CA 证书签发系统申请的、天津市密码管理局的 KMC 的加密机设备生成的，并由天津市密码管理局负责备份；

2）签名密钥对：证书申请者可使用国家密码管理局认可的、天津滨海 CA 证书签发系统支持的介质生成签名密钥对。签名私钥存储在介质中不可导出。

B. 密钥的恢复

1）证书持有者密钥恢复：当证书持有者的密钥损坏或丢失后，某些密文数据将无法还原，此时证书持有者可向天津滨海 CA 提交申请，经过审核后，通过天津滨海 CA 向天津市密码管理局的 KMC 发送请求，密钥恢复模块接受证书持有者的恢复请求，恢复证书持有者的密钥并下载于证书持有者证书载体中；

2）问责取证密钥恢复：问责取证人员向天津滨海 CA 提交申请，经过审核后，通过天津滨海 CA 向天津市密码管理局的 KMC 发送请求，由密钥恢复模块恢复所需的密钥并记录。

6.2 应用集成支持服务操作规范

6.2.1 服务策略和流程

1）天津滨海 CA 负责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）天津滨海 CA 负责制定项目管理制度，规范集成实施人员技术操作；

3）天津滨海 CA 负责制定安全控制流程，明确人员职责；

4）天津滨海 CA 负责实施证书软件发布版本管理，并进行证书应用环境控制；

5）天津滨海 CA 承诺妥善保存项目开发程序和文档等资料。

6.2.2 应用接口

天津滨海 CA 为上层提供简洁、易用的调用接口，主要包括密码设备接口和证书应用综合服务接口。

A. 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。

天津滨海 CA 提供的服务器端密码设备的应用接口，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》。

天津滨海 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》。

B. 证书应用综合服务接口

天津滨海 CA 提供证书应用综合服务接口，该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，该接口符合国家密码管理局《证书应用综合服务接口规范》。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应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。

6.2.3 集成内容

天津滨海 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。

6.2.4 应用集成流程

天津滨海 CA 通过总结以往集成服务项目经验总结形成了一套较为完善的标准化的工作流程和集成规范。整个集成流程中研发部作为主导，公司其他部门共同参与，保证整个项目集成服务的顺利有序的完成。其中整个流程分为七个阶段：需求分析阶段、解决方案阶段、方案评审阶段、方案集成阶段、集成测试阶段、

系统实施阶段以及运行维护阶段。在这七个阶段中最重要的是需求分析阶段与解决方案解决阶段。需求分析是保证集成项目满足最终客户要求的基础；解决方案是在需求分析的前提下，综合考虑整个项目中可能出现的情况与风险，最终形成的方案，是以后各阶段的基础，起指导作用。

A. 需求分析阶段

天津滨海 CA 根据应用系统的大小以及集成内容复杂度难易度，成立专门需求分析小组。

天津滨海 CA 需求分析方式一般为电子邮件、电话、网络远程以及现场会议沟通等方式。根据应用系统项目所在地、应用系统大小以及集成内容难易等因素，综合考虑采用以上那种或那几种沟通方式。

需求分析小组与系统开发商和最终用户沟通后，形成需求分析说明书，并纸质说明书或者邮件的形式再次与开发商和用户确认需求是否存在遗漏是否存在不明确之处，完成最终的《用户需求分析说明书》。

B. 解决方案阶段

天津滨海 CA 成立专门解决方案小组，根据集成项目难易度决定解决方案由几位集成经验丰富的人员组成。方案小组分析《用户需求分析说明书》每个需求点，整理每个需求点中可能遇到的情况。确定使用关键技术以及集成方式。对分析后每种情况都制定合理的方案以及备选方案，最终完成《解决方案说明书》。将《解决方案说明书》与《用户需求分析说明书》一起提交给质量管理和测试、技术支持部等部门。

C. 方案评审阶段

技术项目部根据集成项目的复杂程度来组织方案评审会，质量管理和测试、技术支持部等相关部门共同参与，项目评审小组在方案评审会中依据 CMMI 过程域的评审规定对集成项目的可行性、风险性以及应对风险的方案进行评审，形成评审报告。

D. 方案集成阶段

应用系统部分集成工作一般由应用系统开发商来完成。技术项目部将《集成方案说明书》、所需关键技术资料(jar 包、dll 库、com 组件等)、集成示例等交予应用系统开发商，应用系统开发商按照集成方案说明书将天津滨海 CA 的产品集成到应用系统中，升级应用系统，在此期间，天津滨海 CA 技术人员对集成开

发商进行技术协助，包含接口调试、问题解决以及必要的技术培训。

E. 方案测试阶段

根据需求分析说明以及项目集成方案说明书编写全面测试说明书。包括集成测试用例 CASE、测试方式、测试用户等，依据测试说明书对集成项目中涉及 CA 应用部分进行测试，保证集成后的应用系统能够正常使用。

F. 系统实施阶段

系统实施中涉及天津滨海 CA 的安全产品，例如签名验证服务、电子签章服务器等由天津滨海 CA 提供技术人员来完成服务器的部署，业务系统升级由开发商完成。

网络拓扑结构部分由网络部署商来完成。按照项目集成方案说明书，服务器部署完成后，需服务器拓扑到原有网络中并且能够与天津滨海 CA 证书目录服务器通信，在拓扑过程中如果涉及到原网络防火墙的设置等对原网络产生影响时网络部署商协助拓扑。

G. 运行维护阶段

应用系统使用过程中的维护，天津滨海 CA 提供 7*24 小时免费电话支持。遇到电话无法解决的情况时天津滨海 CA 提供在线远程协助或上门问题解决的服务。

6.3 信息服务规范

6.3.1 服务内容

A. 证书信息服务

天津滨海 CA 系统中签发、更新、重签发的数字证书，可通过 CRL 信息服务、OCSP 信息服务等实现实时、定时与电子政务信息系统进行数据同步，数据包括业务类型、CA 身份标识、用户基本信息、用户证书信息等。

B. CRL 信息服务

CRL 在天津滨海 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，发布的数据包括业务类型、CA 身份标识、CRL 文件、同步时间等。

C. 服务支持信息服务

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

D. 决策支持信息服务

天津滨海 CA 面向电子政务应用单位、政府监管机构提供的决策支持信息，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。

6.3.2 服务管理规则

天津滨海 CA 制定了相关信息的隐私保障机制，对用户信息进行妥善保护。

A.天津滨海 CA 只在进行证书签发和管理时收集私有信息。除了有特殊要求外，天津滨海 CA 不收集更多私有信息；

B.天津滨海 CA 在某项业务中开展证书应用而获得的私有信息，在使用时，会首先得到该业务应用单位的许可；

C.允许的个人信息发布，天津滨海 CA 会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；

D.在特别紧急情况下，天津滨海 CA 会经管理机构的同意，发布私有信息。任何特定的私有信息发布将严格遵照相关法律和政策；

E.在以下情况下，天津滨海 CA 可以将私有信息发给获得相应授权的人员：

1）司法程序；

2）经私有信息所有者同意；

3）按照明确的法定权限的要求或许可。

F.天津滨海 CA 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；

G.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；

H.对问责程序需要进行的信息访问，严格审核相应的问责人员身份及授权文件，无误后进行问责举证；

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

6.3.3 服务方式

天津滨海 CA 的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。

A. 证书信息同步服务

天津滨海 CA 的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。

B. CRL 信息同步服务

天津滨海 CA 的 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。

C. 服务支持信息服务

1）天津滨海 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.证书生命周期服务流程及相关费用；

c.证书用户操作手册；

d.证书常见问题解答（FAQ）；

e.获得证书帮助联系方式：

客户服务热线电话：400-872-5550；

办公地址：天津市东丽区空港经济区西七道 26 号；

邮政编码：300308；

投诉电话：022-58211300。

f.其他应该发布的相关信息。

2）天津滨海 CA 通过 WEB 网站面向电子政务应用系统集成商发布如下信息：

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：

技术支持电话：022-58211310；

办公地址：天津市东丽区空港经济区西七道 26 号；

邮政编码：300308；

投诉电话：022-58211300。

e.其他应该发布的相关信息。

3）认证机构通过 WEB 网站（www.tjbhca.com）面向电子政务应用系统发布如下信息：

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）。

D. 决策支持信息服务

天津滨海 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：提供面向业务的服务效率分析信息，如处理时间、服务接通率等。

6.4 使用支持服务操作规范

6.4.1 服务内容

A. 面向证书持有者的服务支持

1）数字证书管理

包含数字证书的导入、导出，一级客户端证书管理工具的安装、使用、卸载等。

2）数字证书的应用

在数字证书用于身份认证、电子签名、加解密等应用的操作过程中出现的如：证书无法读取、签名失败、证书验证失败等各类异常问题。

3）证书存储介质硬件设备使用

包含证书存储介质在使用过程中出现的如：口令锁死、驱动安装、介质异常等。

4）电子认证系统使用

包含对证书的申领、补办、变更、解锁、更换、撤销、冻结、查询、更新、密钥更新等。

5）电子政务认证服务支持平台使用

为用户提供在天津滨海 CA 的数字证书在线服务平台中使用的如：证书更新失败、下载异常、无法提交撤销申请等各类问题，可在天津滨海 CA 官网

http://www.tjbhca.com/上查看问题解决或者在线联系客服等。

B. 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。

6.4.2 服务方式

A. 座席服务

天津滨海 CA 设置有客户服务中心：400-872-5550，用户可以通过拨打服务热线，客服专员会根据用户的问题请求，查询知识库系统，协助用户处理。

B. 在线服务

天津滨海 CA 为用户提供自助信息查询、网络实时通讯、远程终端协助，以及在线帮助与传统模式相结合的服务，用以满足客户多方位服务帮助的需求。

1）自助信息查询

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已知条件在网站：http: //www.tjbhca.com/信息系统上

进行记发式的检索，查找目标问题的答案。

2） 网络实时通讯

用户通过网站：http://www.tjbhca.com/在线帮助远程发起支持请求，客服人员能够第一时间同登录网站的访客取得联系，进行交流。

3）远程终端协助

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服服务人员发起协助请求。由专业技术人员通过远程终端控制功能，实时监测用户的软件硬件环境，通过同屏显示指导、帮助用户解决应用故障。

4）在线帮助与传统模式的结合

将在线服务系统与电话服务、短信及邮箱反馈相结合，客服人员可以通过多种方式为客户提供服务帮助和反馈，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。

C. 现场服务

根据用户的实际需求，由客服人员帮客户预约技术支持工程师，上门现场为用户处理数字证书应用中存在的问题。

D. 满意度调查

以调查问卷的模式，通过电话、WEB 网站、邮件系统、短信平台、传真等多种用户可以接受的调查方式进行客户回访，全面开展用户满意调查，分析调查结果，改善服务。在满意度调查过程中发生的所有相关文件及文档全部归档保存。

E. 投诉受理

通过电话：022-58211300、网站平台：http://www.tjbhca.com/、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，并将结果解释反馈给用户。将投诉受理中产生的相关文件及文档进行归档保存。

F. 培训

培训方式由天津滨海 CA 与客户双方约定的形式开展。

培训内容主要包含：电子政务电子认证服务基础性技术知识、服务规范、数字证书应用集成规范及相关帮助文档、常见问题解答、操作使用手册等。

6.4.3 服务质量

A.在线服务、现场服务

以上服务时间做到充分满足各类用户的需要，服务时间是至少 5 天*8 小时。

B.热线电话服务

以上服务时间是 7 天*24 小时服务。

C.天津滨海 CA 设有专门的投诉热线受理和客户满意度调查，保证优质的客服服务质量。

D.客服问题、应对技术问题和技术故障

按照类别、严重程度依次以一般事件、严重事件、重大事件依次进行分类登记和处理，制定响应处理流程和工作机制，以确保服务的及时性和连续性，各类响应时间按双方协议为准，或以不影响客户使用数字证书为准则。

6.5 安全保障规范

6.5.1 认证机构设施、管理和操作控制

6.5.1.1 物理控制

A. 场地位置与建筑

天津市滨海数字认证有限公司坐落在天津市滨海新区空港经济区东软软件园内，CA 机房位于大楼 1 层东部，中心区域占地面积 100 平方米,功能间由外到内划分为公共区、管理区、服务区、缓冲区、核心区五个部分。机房采用高安全性的监控技术，包括视频实时监测、指纹、身份识别卡等安全防护技术，以确保物理通道的安全。天津滨海 CA 机房实行 24 小时监控。

B. 物理访问

1）门禁管理方面我们采用 2 人分别持卡和输入密码的认证方式，并且当门打开状态超过 15 秒后门禁系统自动开启声光报警提醒工作人员及时关闭大门；

2）机房的核心区域，采用密码和指纹验证结合的方式控制；

3）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；

4）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；

5）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；

6）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。

C. 电力与空调

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独立供

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。

天津滨海 CA 系统采用双路电源供电，在单路电源中断时，仍可以维持系统正常运转。同时，使用不间断电源（UPS）的稳压功能避免电压波动危害。

天津滨海 CA 机房采用的是符合国家标准的机房专用恒温精密空调作为主设备，保持机房恒湿恒温。

D. 水患防治

天津滨海 CA 在机房建设时已切断了进入机房区的所有水源，并采取了屋顶，地面防渗、防水处理、气体灭火等相应措施，以防止水对机房区的侵蚀，充分保障系统安全。

E. 火灾防护

天津滨海 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。

F. 介质存储

天津滨海 CA 对存储系统程序、用户数据、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。

G. 废物处理

天津滨海 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运维部审批通过后，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滨海 CA 的相关处理要求进行，所有处理行为将记录在案。

H. 异地备份

天津滨海 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备份。在异地备份时按照策略和流程由专人送交到异地保险柜。以上所有操作流程均记录在案。

I. 入侵侦测报警系统

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。

6.5.1.2 操作过程控制

A. 可信角色

电子认证服务机构、注册机构、依赖方等组织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。

B. 每个角色的识别与鉴别

天津滨海 CA 的在职人员，按照所担任角色的不同进行身份鉴别。对进入 CA 中心的人员进行严格的限制，实行严格的登记制度，一些重要的部门如机房绝对禁止非相关人员进入。工作人员进入机房需要使用门禁卡和密码识别，进入核心区需密码及指纹识别，并通过监控系统及系统日志随时记录各个人员的操作行为；进入证书系统需要使用 USB Key 存储的数字证书进行身份鉴别，且其操作将完整的记录在系统日志中。天津滨海 CA 将独立完整地记录其所有的操作行为。

C. 要求职责分割的角色

为保证系统安全，遵循可信角色分离、操作和管理分离的原则，天津滨海 CA 的可信角色由不同的人员担任。要求职责分割的角色包括（但不限于）以下几种：安全管理员、系统管理员、网络管理员、操作员、审计管理员，其中审核员与其他操作员不能兼任，审计管理员与运营人员、业务人员均不能兼任。

天津滨海 CA 制定了规范和策略，严格控制任务和职责的分割。对于最敏感的操作，例如访问和管理 CA 的加密设备及其密钥，需要 3 个可信角色。其它操作，例如发放证书，需要至少 2 个可信角色。

6.5.1.3 人员控制

A. 资格、经历和无过失要求

可信角色的人员必须提供相关的背景、资历证明，并具有足以胜任其工作的相关经验，且没有相关的不良记录。

B. 背景审查程序

在雇佣人员担任可信任角色前，会依据以下流程对其进行审查：

1）应聘者提交的个人资料

最高学历毕业证书、学位证书、资格证及有效身份证件原件等相关的有效证明和履历。

2）应聘者个人身份的确认

人力资源部门通过电话、信函、网络、走访、调阅档案等形式对其提供材料的真实性进行鉴定。

3）六个月的试用期考核

通过现场考试、日常观察、情景考验等方式对其考察。

以上三方面的审查结果必须符合资格、经历和无过失的要求。

C. 培训要求

天津滨海 CA 对员工根据其岗位和角色安排不同的培训，培训内容主要有：

1）系统软硬件安装、运行和维护；

2）密码技术、PKI 体系结构和天津滨海 CA 系统建设方案；

3）CA 系统安全管理以及系统的备份与恢复；

4）CA 中心的运行管理以及应用软件的运行与维护；

5）证书的生成、签发和管理以及产品质量控制体系；

6）机房消防、门禁和监控系统安全管理；

7）天津滨海 CA 可信任角色岗位职责、安全令牌管理办法和保密制度；

8）《天津滨海 CA 电子政务电子认证服务业务规则》（CPS）；

9）天津滨海 CA 内部管理制度、政策、规定、标准和程序；

10）其他国家和地方相关法律、法规、管理办法等。

D. 工作岗位轮换周期和顺序

根据员工轮岗管理制度及具体工作情况安排并制定员工工作岗位的轮换周期与顺序。

E. 未授权行为的处罚

员工一旦被发现执行了未经授权的操作时，将被立即终止工作并受到纪律惩罚，其处理办法根据天津滨海 CA 对未授权行为进行处罚的规定执行。

F. 提供给员工的文档

为使系统正常运行，必须提供给具有权限的相关人员各种文档，详细请参考《天津市滨海数字认证有限公司管理制度汇编》。

G. 独立合约人的要求

对不属于天津滨海 CA 内部的员工，但从事天津滨海 CA 有关业务的人员等独立签约者，天津滨海 CA 的统一要求如下：

1）人员档案进行备案管理；

2）具有相关业务的工作经验；

3）必须接受天津滨海 CA 组织的岗前培训。

6.5.1.4 审计日志程序

天津滨海 CA 严格按照电子政务 CPS 开展业务，并通过对日志的审计程序保证业务开展。

A. 记录事件的类型

1）CA 密钥申请及使用统计的管理事件；

2）RA 系统记录的证书持有者身份信息，包括机构名称、个人姓名、证件号码、地址、邮箱、联系人等信息；

3）证书生命周期中的各项操作，包括证书申请、证书批准、证书密钥更新、证书撤销等事件；

4）系统、网络安全记录，包括入侵检测系统的记录、系统日常运行产生的日志文件、系统故障处理工单、系统变更工单等；

5）人员访问控制记录；

6）系统巡检记录；

7）天津滨海 CA 中心物理环境巡检记录；

8）事故处理记录。

上述日志信息包括记录时间、序列号、记录的实体身份、日志种类等。

B. 审计周期

对于 CA 和用户证书生命周期内的管理事件日志，天津滨海 CA 将每年进行一次内部检查、审计。

对物理设施的访问日志，天津滨海 CA 将每周进行一次检查、处理。

对于系统安全事件和系统操作事件日志，天津滨海 CA 每月进行一次检查、

处理。

C. 审计日志的保存期限

审计日志每月形成新的归档文件，交由相关部门保存归档，审计跟踪文档至少保存二年，密钥和证书信息档案至少保存到证书失效后五年。

D. 审计日志的保护

建立完善的管理制度，并采取物理和逻辑的控制方法确保只有经天津滨海 CA 授权的人员才能对审计日志进行操作。审计日志处于严格的保护状态，并且有异地备份，严禁未经授权的任何操作。

E. 审计日志备份程序

所有文档包括最新的审计跟踪文档需储存在磁盘中并存放在安全的文档库内并进行备份。根据记录的性质和要求，采用在线和离线的各种备份工具，有每天、每周、每月和每年等各种形式的备份。

F. 审计收集系统

天津滨海 CA 可以审计天津滨海 CA 认证体系内任何其认为有必要监控和审计的系统。

G. 对导致事件实体的告知

导致事件主要包括攻击和非授权行为。

天津滨海 CA 对审查中发现的攻击现象将做详细记录，在法律许可的范围内追溯攻击者，并保留采取相应对策措施的权利，如：切断对攻击者已经开放的服务、递交司法部门处理等措施。

天津滨海 CA 对审查中发现的未授权行为将上报安全策略（管理）委员会，隔离该员工，并对未授权行为进行评估，确认风险，做出相应处理。

H. 脆弱性评估

根据审计记录，天津滨海 CA 和 RA 要定期进行系统、物理设施、运营管理、人事管理等方面的信息安全脆弱性评估，并根据评估报告采取措施。

6.5.1.5 记录归档

A. 归档记录的类型

天津滨海 CA 会定期存档，间隔时间由天津滨海 CA 自行决定，存档的内容包括天津滨海 CA 发行的证书、审计数据、证书申请相关材料等。

B. 归档的保存期限

除了法律法规和主管部门提出的保存期限以外，天津滨海 CA 制订的有关天津滨海 CA 架构内电子认证服务运营信息的归档保存期限至少应该如下:

1）用户服务申请的信息，如申请表、协议、身份资料和其他相关信息的记录，一般为 5 年，重要记录为 10 年；

2）认证系统日常运作产生的日志记录等文件保存 5 年；

3）机房进出记录、认证系统日常维护记录、系统软硬件设备更换、安装、拆除、配置变化等的记录、监控系统记录、系统的故障处理记录等保存 5 年；

4）用户申请、更新、撤销、挂起的证书和过期证书，永久保存；天津滨海 CA 的证书和密钥，以及相关的变动信息，自证书期满或撤销之日起，其记录至少保存 5 年；

5）人员变更记录等保存 10 年；

6）与法律政策的规定不一致的，选择两者中较长的期限予以保存。

C. 档案的保护

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。天津滨海 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。

D. 档案备份程序

系统定期对证书信息、审计数据等进行备份，该备份数据采用物理隔离方式，与外界不发生信息交互。

E. 对记录加盖时间戳的要求

天津滨海 CA 认证系统的各种系统日志、操作日志有对应的记录时间，采用标准的时间戳请求、时间戳应答及时间戳编码格式。

F. 获得和检验归档信息

只有被授权的可信人员能够访问归档记录。天津滨海 CA 将每年组织专人检验归档信息的完整性。

G. 独立的数据库、系统

档案管理系统拥有独立的数据库、系统，通过内部网络登录，天津滨海 CA 对访问档案系统的用户权限有严格要求，只授权相关人员浏览相关档案，通过管理员权限随时监控登录者动态。

H. 定期对档案备份进行比较

天津滨海 CA 由两个人分别来对数据的进行备份，并且为了确保档案信息的准确，定期对异地备份的数据与本地备份的数据进行比较。

6.5.1.6 认证机构密钥更替

天津滨海 CA 根密钥需要更替时，采取与系统根密钥初始化生成相同的流程和方法进行。

新旧密钥更替期间，天津滨海 CA 有效保证了认证机构根密钥及信任链验证的有效性。操作过程为：集齐五名加密机管理员，一名加密机操作员同时在场；3 名加密机管理员依次通过卡的密码验证后，才能启动对加密机的操作；操作加密机时需插入操作员卡并登录，该操作员卡片由密钥管理员负责。新旧根证书过渡期，采用新私钥为旧公钥签名证书、旧私钥为新公钥签名证书、新私钥为新公钥签名的证书方式，以保证用户和依赖方能够可靠地验证天津滨海 CA 根证书以及确保证书信任链的有效性。

6.5.1.7 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。

A. 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。

B. 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。

目前阶段，通过系统设置，每日 23：00 数据库自动进行增量备份，每日定时将前一晚的增量数据拷贝至专用的移动设备。每周日 23：00 数据库进行全备份，每周一将前一天新的全备份数据拷贝至专用的移动设备。增量备份文件存放

在专用文件夹内。全备份文件存放在专用文件夹内。每月第一个工作日进行上一月度备份数据光盘刻录。

C. 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。对认证系统的操作日志进行备份，目前采取认证系统安装目录的拷贝方式进行，主要包括：CA 系统安装目录、RA 系统安装目录。

目前阶段，手动进行认证系统操作日志备份。每周一用专用移动设备拷贝相关安装目录。这些安装目录统一放在一个上级文件夹内。每月进行上一个月度备份数据光盘刻录。

D. 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。

E. 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。

F. 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，每日导出前一日数据进行备份，备份采用专用移动设备，存储于专用文件夹。

视频监控数据本地保存至少三个月。所有录像资料在硬盘录像机中进行双机备份，以备查询。

G. 其他

以上六条涉及的备份事件，需至少两人同时在场，以确保备份数据真实完整可靠。

以上六条涉及的备份事件，刻录光盘备份文件时需至少两人同时在场，以确保刻录的数据真实完整可靠。

以上第一条至第三条刻录光盘一式两份，一份本地保存，一份异地保存。其他刻录光盘一份，本地保存。本地保存的数据备份，涉及认证系统的核心数据和日志，存储于机房保险柜中，不得出机房。本地保存的门禁日志和监控数据由安全运维部负责保管。异地保存的数据定期由机房管理员交接给安全管理员和审计人员，并由安全管理员和审计人员送往异地保险柜地点。

对于刻录的光盘，进行检查，确认数据可读无损。对于光盘损毁不可读的需及时补刻。

6.5.1.8 损害和灾难恢复

A. 损害处理过程

天津滨海 CA 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，并进行了本地及异地备份。应针对影响认证业务正常运营的故障与意外事件，如黑客攻击、网络系统瘫痪、病毒、系统数据破坏或丢失，系统严重故障、水灾、停电或电力系统故障等，制定应急处理预案。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、软件和(或)数据。

当天津滨海 CA 遭到攻击、发生通讯网络故障、计算机设备不能正常提供服务、软件遭破坏、数据库被篡改等情况下或因不可抗力造成天津滨海 CA 主中心机房无法正常提供服务时，天津滨海 CA 将依据灾难恢复方案实施修复。

1）数据抢救

灾难发生时，需在保证人身安全的情况对公司的重要数据进行抢救，抢救的范围主要包括：记录公司重要信息的文件、资料，存储公司重要数据的光盘，存放重要数据的硬盘、服务器。此过程需由安全策略（管理）委员会进行统筹指挥，按照既定的计划执行，公司员工必须服从统一调度和指挥。

2）损坏评估及启动应预案

灾难发生后由安全策略（管理）委员会根据情况成立应急小组，记录损失情况，损坏信息应包括:

a.公司重要生产、监视测量、办公系统及设备；

b.拥有在可以执行计划之内的关键性功能的员工；

c.保存公司重要数据的介质；

d.网络、通讯设备。

根据损坏信息情况进行应急预案启动，如选举临时领导、使用备份服务器、备份通讯设备进行替代等。

3）业务恢复计划

业务恢复计划总体可划分为以下几个阶段:

a. IT 基础设施恢复阶段：

此阶段主要的目标是将对于保存数据的基础设施、业务系统所在的主机、公司网络架构进行恢复。首先分析可继续利用的 IT 基础设施，如供电设施、交换机、服务器、防火墙等。若有不可用的设备，需及时同代理商进行沟通借用或新购相应设备。

b.系统恢复阶段：

系统恢复主要针对关键服务器。为节约时间需同时针对各个服务器系统进行快速恢复。

c.网络恢复阶段：

网络恢复阶段的主要针对以下几点进行：关键商业应用系统的内部局域网，网络设备的支持外部广域网和电信服务待恢复系统和终端用户（公司同事）间的通讯。

d.业务平台恢复阶段：

主要围绕日常工作常用的业务平台进行，包括业务系统数据恢复、业务系统

重搭建。

业务系统重搭建：由于一些业务系统的特殊性，需尽快与相应平台的供应商接口人取得联系，并申请临时可用的加密、许可文件等。各技术应急人员需在短时间内进行重搭建。

业务系统数据恢复：首先须对业务系统的数据进行恢复，需要寻找相应的恢复设备完成此操作，目前我们主要利用备份光盘和可正常工作的服务器进行数据恢复工作。需要将抢救出或异地备份的光盘和硬盘接连在对应设备上恢复出数据，并测试可行性。

B. 实体私钥损害处理程序

对于实体私钥的损害，天津滨海 CA 有如下处理要求和程序：

1）当天津滨海 CA 或注册机构或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，并立即通知天津滨海 CA 或注册机构撤销其证书。天津滨海 CA 按证书撤销章节发布证书撤销信息。

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

a.根证书是天津滨海 CA 提供电子认证服务的信任链的起始点，拥有最高级别的安全要求；

b.确认根私钥受损情况发生后，第一时间由安全策略（管理）委员会启动根私钥受损应变程序，指定部门分别负责备案和撤销工作；

c.指定安全运维部负责向国家密码管理局报告情况、备案；

d.指定营业管理部负责撤销签发的所有证书，并手动更新证书撤销列表（CRL）；

e.系统自动更新目录服务器（LDAP）、证书在线状态查询服务（OCSP），并由工作人员以抽检的方式验证更新结果；

f.完成以上工作后，需向安全策略（管理）委员会报告和确认；

g.安全策略（管理）委员会授权重新生产密钥；

h.加密机管理员、加密机操作员、系统管理员、安全管理员共同根据安全策略（管理）委员会的要求，遵循《根私钥保护机制》中规定的五选三的秘密分担要求，完成根密钥生产和备份工作；

i.安全运维部负责电子认证服务系统初始化工作，签发测试根证书；

j.安全运维部负责向国家密码管理局商用密码检测中心申请互联互通测试；

k.通过互联互通测试后，安全运维部负责完成正式入根工作；

l.入根并完成验证后，需向安全策略（管理）委员会报告。

C. 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，天津滨海 CA 能够在出现灾难后最短时间内恢复其业务能力。天津滨海 CA 目前正计划建立省际异地灾难恢复中心，灾难恢复中心的建立，将进一步增强天津滨海 CA 的灾后业务存续能力。

D. 业务连续性计划的保障

1）建立了业务连续性计划，并进行经常检查和更新，确保其持续有效；

2）制订了应急演练预案，并经常进行演练，确保流程操作的有效性；

3）定期测试备份设备、设施、后备电源等，确保其可用性；

4）制订了《终止操作规范》，对 CA 中心终止服务时的告知及业务承接作出计划；

5）一般工作机不安装软驱和光驱，如有安装软驱和光驱的计算机，每次使用磁盘都要用杀毒软件检查；

6）对于联网的计算器，任何人在未经批准的情况下，不得向电脑内拷入软件或文件；

7）数据库和系统由专员定期进行备份，并同时存放在本地机房保险柜和异地银行保险柜，且只有授权人员才可接触备份；

8）光盘等在使用前，必须确保无病毒；

9）电脑一经发现病毒，应立即通知安全运维部人员处理；

10）系统运营管理人员密切监视并定时检查主机系统、网络系统、外围设备、及附属设备的运行状况；

11）安全管理员、物理环境安全管理员配合物业安保部门定时对机房物理设施进行巡查，包括供电系统、UPS、消防系统、监控系统、空调、通风系统等；

12）为每个操作人员签发一张数字证书并建立相应的访问控制权限表；

13）操作人员在离开办公桌前应对办公机锁屏，下班前应退出系统并关机；

14）任何人未经操作员本人同意，不得使用他人的计算机；

15）所有连接内网的办公电脑不得上互联网；

16）不要随便运行或删除电脑上的文件或程序；

17）对公司辞职人员的电脑由负责人立即更改电脑密码，保密电脑内文件；

18）定期对有关人员进行安全方面的培训，对安全方面出现的问题以及处理办法及时通知给相关操作人员。

6.5.1.9 认证机构或注册机构终止

当天津滨海 CA 打算终止经营时，会在终止经营前三个月给天津滨海 CA 授权的发证机构、垫付商和证书持有者书面或 Email 通知，并在终止服务四十五日前向国家密码管理局和工业和信息化部报告,按照相关法律规定的步骤进行操作。天津滨海 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：

A. 起草 CA 终止声明；

B. 通知与 CA 停止相关的实体；

C. 关闭从目录服务器；

D. 证书撤销；

E. 处理存档文件记录；

F. 停止认证中心的服务；

G. 存档主目录服务器；

H. 关闭主目录服务器；

I. 处理加密密钥；

J. 处理和存储敏感文档；

K. 销毁 CA 主机硬件。

根据天津滨海 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滨海 CA，要完成相似的操作，唯一的不同在发送天津滨海 CA 终止通知的时间限制上；由于密钥受损原因终止天津滨海 CA，要求天津滨海 CA 通知用户的过程尽快完成；由于非密钥受损的原因终止天津滨海 CA，在通知所有用户后，采取适当的步骤减轻天津滨海 CA 终止对用户的影响。

6.5.2 认证系统技术安全控制

6.5.2.1 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，确保密钥对的生成、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。

A. 密钥对的生成

1）加密密钥对：由中华人民共和国国家密码管理局许可的、天津滨海 CA 证书签发系统申请的、天津市密码管理局所属的 KMC 的加密机设备生成的；

2）签名密钥对：证书申请者可使用国家密码管理局认可的、天津滨海 CA 证书签发系统支持的介质生成签名密钥对。签名私钥存储在介质中不可导出，保证无法复制。

B. 私钥传送给证书使用者

用户的加密私钥是在天津市国家密码管理局的商用密码密钥管理中心（KMC）产生，该私钥只保存在 KMC 和用户介质中。在加密私钥从 KMC 到用户的传递过程中采用国家密码管理局许可的对称密钥算法加密。天津滨海 CA 无法获得，保证了用户的密钥安全。

C. 公钥传送给证书签发机构

天津滨海 CA 从 KMC 取得用户公钥后为其签发证书，在此过程中采用国家密码管理局许可的对称密钥算法加密，保证传输中数据的安全。

D. 电子政务电子认证服务机构传送给依赖方

天津滨海 CA 的根公钥包含在天津滨海 CA 的根证书中。用户可以通过天津滨海 CA 网站（www.tjbhca.com）下载天津滨海 CA 根证书。

E. 密钥的长度

为了保证加密和解密的安全性，天津滨海 CA 所使用的密钥对长度为 256 位。如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，天津滨海 CA 将会完全遵从。

F. 公钥参数的生成和质量保证

公钥参数由国家密码管理局鉴证许可、天津滨海 CA 证书签发系统申请、天津市国家密码管理局的硬件产生，符合国家密码管理部门的要求。

G. 密钥的使用

在天津滨海 CA 电子政务电子认证服务体系中的密钥用途和证书类型紧密相关。CA 证书的签名密钥用于签发 RA 证书和证书撤销列表（CRL）；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；加密密钥用于对需在网络上传送的信息进行加密，保证信息除发送方和接收方外不被其他人窃取、篡改。

6.5.2.2 私钥保护和密码模块工程控制

A. 密码模块标准和控制

天津滨海 CA 使用国家密码管理局许可的产品，密码模块的标准符合国家规定和要求。

天津滨海 CA 的根密钥使用加密机密码模块，加密机安置在核心区，且对加密机的任何操作必须在核心区进行。加密机的数据包括两方面的内容：管理员口令卡、CA 私钥的备份。加密机备份操作时，必须五位管理员中的半数以上管理员同时到场才能进行。加密机恢复操作时，必须五位管理员中的半数以上管理员同时在场才能进行。

天津滨海 CA 私钥的备份数据存放在保险柜中，如有特殊情况需要使用，必须经过天津滨海 CA 安全策略（管理）委员会批准。

B. 私钥多人控制

天津滨海 CA 采用多人控制策略进行根私钥的生成、更新、撤销、备份和恢复等操作，秘密分担采用“五选三”算法，CA 加密机采取“五管一操”模式进行管理，即五张管理员卡一张操作员卡。各秘密份额保存在不同的加密机管理员卡中。天津滨海 CA 的 CA 系统在技术上建立了相应安全机制，对生成操作进行限制。

C. 私钥托管

KMC 可以根据客户和法律的需要，对用户证书的加密密钥进行托管。签名私钥不进行托管，以保证其不可否认性。

D. 私钥备份

用户的签名私钥天津滨海 CA 和 KMC 都不备份。加密私钥由 KMC 备份，备份数据以密文形式存在。

E. 私钥归档

天津滨海 CA 根证书失效后，必须将失效的根密钥及根证书归档并妥善保存。在证书失效至少 5 年后，方可销毁归档的根密钥。

F. 私钥导入、导出密码模块

天津滨海 CA 可以采用软件将私钥安全导入到加密机中，私钥无法从硬件密码模块中导出。

G. 私钥在密码模块的存储

天津滨海 CA 的私钥存储在硬件密码设备中，并在该设备中使用。

H. 激活私钥的方法

在激活 CA 私钥时，必须五位管理员中的半数以上管理员同时在场才能进行。

I. 解除私钥激活状态的方法

在解除私钥激活状态时，必须五位管理员中的半数以上管理员同时在场才能进行。

J. 销毁私钥的方法

在销毁根私钥时，必须五位管理员同时在场才能进行。

天津滨海 CA 根私钥不再使用时，必须将私钥从加密设备中删除，并将加密设备初始化。同时用于激活私钥的管理员卡必须收回。

K. 密码模块应达到的标准

天津滨海 CA 使用国家密码主管部门批准和许可的密码产品。

6.5.2.3 密钥对管理的其他方面

A. 公钥归档

用户证书中的公钥包括签名证书中的公钥和加密证书中的公钥。它们由天津滨海 CA 和天津市国家密码管理局的密钥管理中心定期归档。

B. 证书和密钥对使用期限

所有证书使用者的证书有效期和其对应的密钥对的有效期是一致的。

6.5.2.4 激活数据

A. 激活数据的产生和安装

激活数据是私钥保护密码，证书存储介质（如：智能 USB Key）出厂时设置了缺省的 PIN 值，从而激活了证书存储介质的 PIN。

B. 激活数据的保护

用户的激活数据必须进行妥善保管，或者记住以后进行销毁，不可被他人获悉。为了配合业务系统的安全需要，应该经常对激活数据进行修改。

C. 激活数据的其他方面

只有在拥有证书介质并知道证书介质的 PIN 值时才能激活证书存储介质，从而使用私钥。

6.5.2.5 计算机安全控制

A. 访问管理

在天津滨海 CA，只有经过严格授权的 CA 管理员可以访问 CA 数据库中的数据；只有经过严格授权的 RA 管理员可以访问存储在 RA 服务器数据库中的数据。用户可以访问天津滨海 CA 目录服务器中的公开信息，没有权限访问 CA 和 RA 数据库中的数据。

天津滨海 CA 有防火墙以及其他访问控制机制保护，其配置只允许已授权的机器访问。只有经过授权的天津滨海 CA 员工才能够进入天津滨海 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。所有授权的员工的口令必须符合安全要求，8 位口令中至少包含一个小写字母、一个字符、一个数字、一个大写字母。

B. 安全控制

为了保障认证机构的网络基础设施、主机系统、应用系统及数据库运行的安全，天津滨海 CA 采用防火墙、病毒防治、入侵检测、漏洞扫描等安全防护措施。

在整体网络系统中，将网络划分为：核心区、管理区、服务区等。各分区之间采用不同的防火墙产品进行保护。采用多层防火墙保护方案提高系统安全性，既限制外部对系统的非授权访问，也限制内部对外部的非授权访问，同时还限制内部系统之间特别是安全级别低的系统对安全级别高的系统的非授权访问。防火墙系统屏蔽所有常用的网络访问如 Telnet、FTP、SMTP、RPC、NFS 等。管理员定期查看防火墙访问日志。同时对防火墙的管理员权限严格控制。

在服务区防火墙后配置了一套入侵检测系统，对渗透过防火墙的攻击与内部的恶意攻击进行报警，实时对进出天津滨海 CA 系统网络的通信以及内部网络系统进行实时监视。管理员能够时刻掌握正在进行的连接和访问情况。系统运用协议分析和模式匹配方法，有效地识别各种网络攻击和异常现象，如拒绝服务攻击、

非授权访问尝试、预攻击探测等。

除此之外，对于计算机设备管理如下：

1）专人负责设备的领取和保管，做好设备的领用、进出库和报废登记；

2）对设备定期进行检查、清洁和保养维护；

3）对设备进行维修时，必须记录维修的对象、故障原因、排除方法、主要维修过程及与维修有关的情况等。

6.5.2.6 生命周期安全控制

A. 认证系统运行管理

天津滨海 CA 制定了认证系统运行的安全保障机制，确保了在系统运行、维护过程中的安全。建立了监控和检查机制，确保系统网络运行环境的安全性。

1）天津滨海 CA 对认证系统的操作建立了技术档案，由专人管理，所有对认证系统的维护操作都严格按照运维管理制度和操作手册进行。

2）按照运维管理制度，任何人不得随意修改系统及网络的各种配置，任何对系统、网络配置的变更（如防火墙配置更改、新建数据库、添加新账号、更新 WEB 内容、添加删除软件等），任何对配置的修改需要经过天津滨海 CA 安全运维部负责人的同意，并填写相应表单，配置修改后需要进行新配置文档的归档。

3）依据运维制度，应用和操作系统软件只有在全面正确的测试后才能安装，测试包括实用性、安全性、在其他系统上的有效性。测试在独立的系统上完成。

4）根据运维管理制度要求，天津滨海 CA 的测试系统、运营系统、网络设施等，具有专门的操作维护人员，并有相应明确的授权。

5）依据运维管理制度，天津滨海 CA 的运行维护操作人员定期检查系统及网络的稳定性、安全性及容量，确保符合服务水平。

6）天津滨海 CA 使用可靠厂商的病毒防治软件，配置一台防病毒服务器安装防病毒软件的服务端，在认证系统网络内所有服务器与终端 PC 安装防病毒软件的客户端，并统一配置管理中心地址为防病毒服务端地址，服务端每日对客户端自动进行软件及病毒库等版本更新，保障认证系统运行的安全可靠。

7）根据运维管理制度，对认证系统进行监控及时发现系统中可能存在的隐患，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。

8）天津滨海 CA 依据运维管理制度对认证系统相关媒介由专人进行妥善保管，严密了领取和归还流程，避免了非授权的访问。

B. 认证系统的访问管理

1）天津滨海 CA 制定了安全管理制度，对认证系统的访问进行角色和权限的授权，避免权力过于集中，权力的分散便于互相制约。《内部审计制度》要求对人员进行认证及鉴别，以确认其行为是否符合规定。根据根私钥保护机制对密钥操作人员严格把控（如密钥生成时 3 选 2 控制）。

2）天津滨海 CA 建立了系统控制管理制度，严格管控认证系统访问人员角色职能，确保合理的职责分割和权限控制，并明确了授权及取消授权的操作流程和策略。

3）天津滨海 CA 建立了安全保障规范、电子认证系统网络部署策略，根据要求控制网络访问。

4）天津滨海 CA 建立了安全管理制度，对人员访问操作系统及认证系统软件的安全访问进行控制。

5）天津滨海 CA 建立了《内部审计制度》对各种对认证系统的访问拥有严格的审计措施。

C. 认证系统的开发和维护

1）按照运维管理制度，任何人不得随意修改系统的各种配置，任何对系统的变更、添加删除软件，任何对配置的修改需要经过天津滨海 CA 安全运维部负责人的同意，并填写相应记录表，配置修改后需要进行新配置文档的归档。

2）天津滨海 CA 严格控制对 CA 系统的源代码及测试数据的访问，禁止一切违规操作，一经发现将严格处置。

3）依据运维管理制度，应用和操作系统软件只有在全面正确的测试后才能安装，测试包括实用性、安全性、在其他系统上的有效性。测试在独立的系统上完成。

4）依据运维管理制度在认证系统中，购买、使用或修改的软件，进行严格检查，避免“特洛伊木马”等攻击。

6.5.2.7 网络安全控制

A. 网络访问顺序

外网—服务区防火墙--服务区—管理区防火墙—管理区—核心区防火墙—

核心区

B. 系统中的防火墙安全策略

1）服务区防火墙

默认所有端口阻断，服务区防火墙对 ocsp 服务器做地址转换，开放相应端口。

2）管理区防火墙

从管理区访问服务区不做限制，从服务区访问管理区默认所有端口阻断，管理区防火墙对 RA 服务器做地址转换，开放防病毒服务器端口、RA 服务端口。

3）核心区防火墙

从核心区访问管理区不做限制，从管理区访问核心区默认所有端口阻断，核心区防火墙对 CA 服务器做地址转换，开放 CA 服务端口。

4）核心区 VPN 防火墙

默认所有端口阻断，允许 VPN 通道内互相访问。

C. 系统中的入侵检测安全策略

1）解决方案

本策略应用于天津滨海 CA 认证系统。该策略用于定义检测入侵者和当发现同样行为时应采取的各种行为。同时该策略也定义了 IDS 规则库的相关应用。

a.本公司安全运维部网络管理员负责管理、维护和监控 IDS，定期备份 IDS 日志。

b.对于天津滨海 CA 认证系统的系统软件、应用软件及相关数据库的入侵行为，导致相关敏感数据被窃取的，以及导致网络中断造成公司业务无法正常进行的，均被视为一级入侵行为；对于未引起公司业务中断，但造成了业务支撑系统性能下降的，导致相关非关键数据信息被窃取的入侵行为，视为二级入侵行为。对于进行了物理攻击，但未造成伤害的，进行了渗透试探但未能得逞的入侵行为，视为三级入侵行为。

c.如发生入侵行为，由网络管理员以报告形式通知公司主管领导，组织安全评估小组，进行该行为的危险评估，属于一级和二级入侵行为的，及时上报天津市公安局。

d.网络管理员每月进行 IDS 规则库的升级，升级办法为直接从厂商技术支持网站下载升级包升级，如需系统升级则与设备供应商联系。

2）系统配置说明

该设备配置在服务区，对服务区交换机和管理区交换机进行监控，单独配置一台 PC 为 IDS 的管理终端和日志存储终端。

D. 系统中的漏洞扫描安全策略

使用可靠厂商的漏洞扫描设备定期对认证系统网络进行漏洞扫描，及时发现系统漏洞及补丁修复，保障认证系统运行的安全可靠。

E. 系统中的病毒防治安全策略规划

使用可靠厂商的病毒防治软件，配置一台防病毒服务器安装防病毒软件的服务端，在认证系统网络内所有服务器与终端 PC 安装防病毒软件的客户端，并统一配置管理中心地址为防病毒服务端地址，服务端每日对客户端自动进行软件及病毒库等版本更新，保障认证系统运行的安全可靠。

6.5.2.8 时间戳

时间戳系统基于国家标准时间源，采用 PKI 技术，为应用系统提供精准、安全和可信时间认证服务。该系统是一套高性能、高稳定性，具备跨平台、易扩展和快速部署能力的软硬件集成化网络安全系统。

时间戳系统能够通过 HTTP 协议申请严格遵循国际标准（RFC3161）和（RFC2630）两种时间戳协议的时间戳，采用标准的时间戳请求、时间戳应答以及时间戳编码格式，具有良好的兼容性能。

该系统可以广泛应用有可信时间需求的电子政务和电子商务活动中，为业务提供可信时间服务。

时间戳服务系统对外提供应用开发接口，应用系统通过调用接口的方式完成打时间戳和验时间戳业务功能，有效的减少应用系统的重复开发，减少工作量、缩短项目周期。

目前，时间戳系统已稳定应用于天津滨海 CA 电子认证服务系统，在系统关键业务运行日志、操作日志等日志中，使用了时间戳服务。

除此以外，天津滨海 CA 还应用时间戳系统，通过互联网向广大客服提供可信时间源，以及安全可靠的、防篡改、防抵赖的可信时间服务。

7. 电子政务电子认证服务中的法律责任及相关要求

7.1 要求

天津滨海 CA 在开展电子认证服务时，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。

天津滨海 CA 在《天津滨海 CA 电子政务电子认证服务业务规则》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，具体应涵盖的内容见“7.2 内容”。

7.2 内容

7.2.1 费用

A. 证书签发和更新费用

根据天津滨海 CA 的价目确定。

B. 证书查询费用

根据天津滨海 CA 的价目确定。

C. 证书撤销或状态信息的查询费用

根据天津滨海 CA 的价目确定。

D. 其他服务费用

天津滨海 CA 可根据证书持有者的要求，订制各类通知服务，具体服务费用，由天津滨海 CA 与用户在签订的协议中另行约定。

E. 退款策略

在实施证书操作和签发证书的过程中，天津滨海 CA 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，天津滨海 CA 将不办理退证、退款手续。如果用户在证书服务期内退出数字证书服务体系，天津滨海 CA 将不退还剩余时间的服务费用。

7.2.2 财务责任

天津滨海 CA 保证具有维持、运作和履行其责任的财务能力。天津滨海 CA 有能力承担对用户、依赖方等造成的责任风险，并依据电子政务电子认证服务业务规则规定的方式进行赔偿。

7.2.3 业务信息保密

天津滨海 CA 有信息保密制度，保护自身和用户的敏感信息、商业秘密。

A. 保密信息范围

1）系统方面：

a.认证系统结构、配置，包括系统、网络、数据库等；

b.认证系统安全策略和方案；

c.系统操作、维护记录；

d.各类系统操作口令。

2）运营管理方面

a.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；

b.密钥管理策略与操作记录；

c.CA 或 RA 批准或拒绝的申请纪录；

d.可信人员名单；

e.内部安全管理策略与制度；

f.审计记录。

3）用户信息

a.用户的注册信息；

b.用户系统、应用访问 CRL、OCSP 的记录（时间、频度）；

c.用户与认证机构、注册机构签订的协议。

B. 不属于保密的信息

1）天津滨海 CA 电子认证业务规则、电子政务电子认证服务业务规则、证书申请流程、手续、申请操作指南、证书撤销列表等；

2）在提供方披露数据和信息之前，已被接收方所持有的数据和信息；

3）其他可以通过公共、公开渠道获得的信息。

C. 保护保密信息的责任。

天津滨海 CA 有各种严格的管理制度、流程和技术手段来保护机密信息并保证不泄露给第三方的责任，包括但不限于商业机密、客户信息等。天津滨海 CA 的每个员工都要接受信息保密方面的培训。各方有保护自己和其他人员或单位的机密信息并保证不泄露的责任。

7.2.4 个人隐私保密

A. 隐私保密方案

天津滨海 CA 制定有隐私保护制度，保证证书用户的个人信息不被滥用、未授权使用或出售，同时采取必要措施防止客户资料被遗失、盗用与篡改。

B. 作为隐私处理的信息

天津滨海 CA 在管理和使用证书持有者提供的相关信息时，除了证书中已经包括的信息以及证书状态信息外，该证书持有者的基本信息以及证书申请人提供的不构成数字证书内容的资料将被视为隐私处理，只有经证书持有者同意或有关法律法规、公共权力部门根据合法的程序要求，才可以公开。

C. 不视为隐私的信息

用来构成证书内容的信息，证书相关信息是可以公开的，通过天津滨海 CA 目录服务、Web 服务、OCSP 方式向外公布。

D. 保护隐私的责任

除非执法、司法方面的强制需要，天津滨海 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。

E. 使用隐私的告知与同意

使用隐私信息，须告知并获得隐私所有人或机构的同意。

F. 依法律或行政程序的信息披露

天津滨海 CA 不会将证书持有者的保密信息提供给其他个人或第三方机构。当天津滨海 CA 在法律、法规或规章条款的要求下，或在司法机关的要求下，必须披露电子政务电子认证服务业务规则中具有保密性质的信息时，天津滨海 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。

G. 其它信息披露情形

天津滨海 CA 对其他信息的披露受制于法律、法规和用户协议。

7.2.5 知识产权

1）天津滨海 CA 享有并保留对证书以及天津滨海 CA 提供的全部软件、系统的一切知识产权，包括所有权、名称权和利益分享权等；

2）天津滨海 CA 保留对本 CPS 的所有知识产权；

3）证书所有者拥有其证书相关的密钥对的知识产权；

4）证书申请者保留申请中所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。

7.2.6 陈述和担保

A. 天津滨海 CA 的权利和责任

1）天津滨海 CA 遵守《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子政务电子认证服务管理办法》及相关法律的规定，接受国家密码管理局的监督和指导，对所签发的数字证书承担相应的法律责任。

2）天津滨海 CA 保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。

3）除非通过天津滨海 CA 证书库发出了天津滨海 CA 的私钥被破坏或被盗的通知，天津滨海 CA 保证其私钥是安全的。

4）天津滨海 CA 签发给用户的证书符合天津滨海 CA 电子政务电子认证服务业务规则规定的所有实质性要求。

5）天津滨海 CA 将向证书用户通报任何已知的、将在本质上影响证书的有效性和可靠性事件。

6）天津滨海 CA 将及时撤销证书，并发布到 CRL 上供用户查询。

7）证书公开发布后，天津滨海 CA 向证书依赖方证明，除未经验证的用户信息外，证书中的其他用户信息都是准确的。

B. 天津滨海 CA 下属 RA 的权利和责任

1）RA 应遵守由天津滨海 CA 制定的所有运营政策、操作管理规范、规定登记程序和安全保障措施，天津滨海 CA 有权根据情况修改有关内容。

2）RA 有责任验证申请人提供信息的准确性和可靠性，验证过程由 RA 审核执行，通过天津滨海 CA 制定的审核步骤，确定颁发的证书的有效性和真实性。

3）承担发布 CRL 并保证 CRL 准确性与及时性的责任。

4）RA 应使用天津滨海 CA 确定的信息传输协议和标准，与天津滨海 CA 交换信息。

5）RA 应承担因在本 CPS 规定的用途外使用 RA 管理员证书所造成的损失和责任。

6）对于天津滨海 CA 提供的属于天津滨海 CA 专有的技术、软件开发包只有使用权，并对其承担保密义务；无权将未经天津滨海 CA 授权的属于天津滨海 CA 独有的技术/产品以任何方式让第三方知道和使用，并应对泄密承担相应责任。

C. 证书持有者的权利和责任

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

2）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的或者由天津滨海 CA 推荐使用的安全措施；

3）证书持有者需熟悉本 CPS 的条例和与证书相关的证书政策，遵守证书使用方面的有关限制；

4）如果发生任何可能导致安全性危机的情况，例如遗失私钥、遗忘或泄密以及其他情况，证书持有者应立刻通知天津滨海 CA 或天津滨海 CA 授权的发证机构，申请采取挂失、废除等处理措施。

D. 证书依赖方的权利和责任

依赖方必须熟悉本 CPS 的条款以及和用户数字证书相关的证书政策，并确保本身的证书只用于申请时预定的目的。

依赖方在信赖其他用户的数字证书前，必须采取合理步骤，查证用户数字证书及数字签名的有效性。

证书依赖方对证书的信赖行为就表明他们已阅读并知悉本 CPS 的所有条款，并同意承担证书依赖方有关证书使用的相关责任和义务。

E. 其他参与者的权利和责任

具有与依赖方同样的权利和责任。

7.2.7 担保免责

A. 有限责任

天津滨海 CA 根据与用户签订的合同承担相应的有限责任，且责任仅限于涉

及由天津滨海 CA 颁发的数字证书方面，但对于因用户或依赖方的原因造成的损害天津滨海 CA 不承担任何责任。

天津滨海 CA 承诺在现有的电子政务电子认证服务业务下，天津滨海 CA 签发的数字证书不会被伪造、篡改；如果由于天津滨海 CA 的私钥管理问题造成数字证书被伪造、篡改，天津滨海 CA 将承担相应有限责任。

在与用户和依赖方签定的协议中，对于因用户或依赖方的原因造成的损害不具有赔偿义务。

B. 免责条款

如有下列情形之一，应当免除天津滨海 CA 的责任：

1）用户应当提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息。

2）用户应当妥善保管天津滨海 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。

3）用户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。

4）用户知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知天津滨海 CA 及相关各方，并终止使用该电子签名制作数据。

5）用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，不得将数字证书在天津滨海 CA 规定使用范围之外的其他任何用途使用。

6）用户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、被撤销的数字证书。

7）用户应当根据规定按时向天津滨海 CA 及当地业务受理点缴纳服务费用。

8）自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、台风、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。

7.2.8 偿付责任限制

对于由如下原因造成的用户或依赖方损失，天津滨海 CA 对用户或依赖方进行赔偿：

A. 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；

B. 由于天津滨海 CA 的原因，使得证书中出现了错误信息；

C. 因天津滨海 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。天津滨海 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滨海 CA 视情况重新制定，天津滨海 CA 会将重新制定后的情况立刻通知相关当事人。

天津滨海 CA 所颁发数字证书的赔付责任上限如下：

A. 个人证书 1000 元；

B. 机构证书 4000 元；

C. 设备证书 12000 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，天津滨海 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。

7.2.9 赔付责任

A. 以下情况，用户对自身原因造成的天津滨海 CA、依赖方损失承担责任：

1）用户在证书申请中对事实的虚假或错误描述；

2）在证书申请中用户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）用户没有使用可信系统保护私钥，或者没有采取必要的措施来防止用户私钥的安全损害、丢失、泄漏、修改或非授权的使用；

4）用户使用的名字（包括但不限于通用名、域名和 e-mail 地址）破坏了第三方的知识产权法；

5）证书的非法使用，即违反天津滨海 CA 对证书使用的规定，造成了天津滨海 CA 或有关各方的利益受到损失。

B. 在如下情况，依赖方对自身原因造成的天津滨海 CA 损失承担责任：

1）依赖方没有执行依赖方的职责义务；

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。

7.2.10 有效期和终止

天津滨海 CA 的本 CPS 自发布之日起正式生效。本 CPS 中将详细注明版本号及发布日期。最新版本的本 CPS 将在服务范围内予以发布，对具体个人不做另行通知。当新版本的 CPS 正式发布生效，旧版本的 CPS 将自动终止。

7.2.11 对参与者的个别通告与沟通

电子认证服务活动中某一参与方与另一参与方进行通信时必须以函件的方式进行通讯，相关文件需要签名或者单位公章，如果委托办理，还需提供委托授权书，还可以通过数字签名与签名验证的技术手段进行通讯，以使其通信过程在法律上有效。

7.2.12 修订

A. 修订

当出现以下情形时，天津滨海 CA 将对本 CPS 进行修订：

1）因相关法律法规要求而引起天津滨海 CA 本 CPS 发生改变；

2）因其它原因而引起天津滨海 CA 本 CPS 发生改变。

B. 修订流程

1）本 CPS 修订小组提出修订意见，征询各方的建议，包括用户和依赖方；

2）搜集各方意见并进行研究讨论；

3）在本 CPS 修订小组进行修改并提交天津滨海 CA 决策层批准；

4）再次进行审议和生效，并通过天津滨海 CA 在服务范围内予以发布，同时按照《电子政务电子认证服务管理办法》的要求，向国家密码管理局备案。

7.2.13 争议处理

当天津滨海 CA 与用户或依赖方出现争议并未能达成一致意见时，可通过法律途径解决。电子政务电子认证服务监管部门，或者其他的争端解决机制。

7.2.14 管辖法律

天津滨海 CA 在各方面都服从《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子政务电子认证服务管理办法》、《电子认证服务密码管理办法》和《中华人民共和国合同法》等。

7.2.15 与适用法律的符合性

无论在任何情况下，本 CPS 的执行、解释、翻译和有效性均应遵守和适应中华人民共和国的相关法律和法规。如有不符之处，应以中华人民共和国的相关法律和法规为准。

7.2.16 一般条款

A. 完整协议

本电子政务电子认证服务业务规则将替代先前的、与主题相关的书面或口头解释。

B. 分割性

对于法庭或其他仲裁机构判定某条款非法和不可执行而导致协议无法执行的情况，保留采用法律解决的权利。

在法律允许的范围内，天津滨海 CA 用户协议、依赖方协议和其他用户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。

C. 强制执行

合同一方或几方不履行合同条款的，其它方可以要求强制执行。

D. 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、恐怖行动、罢工、自然灾害、供货商或代理商倒闭、互联网或其它基础设施无法使用等，造成天津滨海 CA 无法提供正常的服务时，不承担由此给客户造成的损失。但各方都有义务建立灾难恢复和业务连续性机制。

E. 各种规范的冲突

若本电子政务电子认证服务业务规则与其它规定、指导方针相互抵触，用户必须接受本电子政务电子认证服务业务规则的约束，除非本电子政务电子认证服务业务规则的规定在法律禁止的范围之内，或有关规定、指导方针明确地言明优于本电子政务电子认证服务业务规则。

在天津滨海 CA 与包括用户在内的其它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，均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；对协议中不同于本电子政务电子认证服务业务说明内容的约定，按双方协议中约定的内容执行。

7.2.17 其他条款

天津滨海 CA 对本 CPS 具有最终解释权。