天津滨海CA电子认证服务系统

证书策略

V 2.0

天津市滨海数字认证有限公司

二o二二年八月

电子认证服务系统证书策略

天津市滨海数字认证有限公司版权所有

版权声明

地址：天津空港经济区西七道26号

邮编：300308

电话：400-872-5550

电子邮件：tjbhca@tjbhca.com

注意：《天津滨海CA电子认证服务系统证书策略》服从中国的法律法规，包括且不限于《中华人民共和国电子签名法》、《电子认证服务管理办法》以及其他相关法律、行政法规。对任何已经或即将涉嫌犯罪而影响天津市滨海数字认证有限公司认证服务的组织、单位和个人，天津市滨海数字认证有限公司将保留依法追诉的权利。

目 录

第一章 概括性描述

1.1 概述

1.1.1 天津市滨海数字认证有限公司概述

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市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。

1.1.2 电子认证服务系统证书策略

天津滨海 CA 电子认证服务系统是由天津滨海 CA 建设、运营的一个公开密钥基础设施，提供基于数字证书的电子认证服务。天津滨海 CA 是依照《中华人民共和国电子签名法》设立的第三方电子认证服

务机构，致力于创建和谐的网络信任环境，向互联网用户提供安全、可靠、可信的电子认证服务。

天津滨海 CA 电子认证服务系统的证书策略（Certificates Policies,以下简称“CP”）符合国家电子认证服务主管机构发布的相关规定，适用于所有由天津滨海 CA 签发和管理的数字证书。

本 CP 作为天津滨海 CA 中数字证书最高策略，为整个电子认证服务系统内的数字证书提供管理、操作和规范的依据，以及为天津滨海 CA 各参与方的权利义务关系确定一个限制范围和基本条款，明确了天津滨海 CA 数字证书和相关服务的操作流程框架，以及为安全、完整地实施这些流程所应采取的业务、技术和法律方面的要求。

天津滨海 CA 作为一个电子认证服务机构（CA），在本 CP 的约束下生成和运营天津滨海 CA 根证书及签发用户证书。天津滨海 CA 的电子认证业务规则（CPS）接受本 CP 的约束，详细阐述了天津滨海 CA 作为电子认证服务机构提供的证书服务、如何提供证书服务及相应的管理、操作和保障措施。所有天津滨海 CA 证书的用户及依赖方必须参照本 CP 及相关的 CPS 的规定，决定对证书的使用和信任。

1.2 文档名称与标识

1.2.1 名称

本文档名称为《天津滨海 CA 电子认证服务系统证书策略》，简称“天津滨海 CA 证书策略”或直接简称“CP”。

1.2.2 版本

变更时间	变更版本	备注
2016 年 12 月 28 日	版本为 V1.0	创建
2017 年 6 月 6 日	版本为 V1.1	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》，将此内容更新至 CP。
2018 年 3 月 19 日	版本为 V1.2	2018 年 3 月，修订了一些细节，如，吊销改注销、增加证书标准扩展项、微调证书生命周期相关业务规则等。
2021 年 11 月 8 日	版本为 V1.3	1、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
2022 年 8 月 1 日	版本为 V2.0	最新版本 证书生命周期操作要求中,增加了线上业务相关内容

1.2.3 发布

天津滨海 CA 通过网站发布，网站地址：

https://www.tjbhca.com

1.3 电子认证活动参与者

1.3.1 证书管理中心（CA）

天津滨海 CA 是根据《中华人民共和国电子签名法》《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构。

天津滨海 CA 的证书管理中心（CA）是颁发证书的实体，负责证书的签发、运营和管理，由天津滨海 CA 建设和运营。CA 的主要职责包括：

- 证书的签发和管理
- 管理和发布证书、证书注销列表（CRL）
- 管理和运营证书信息库
- 证书相关策略、CPS 等规范的制定和发布

1.3.2 注册机构

注册机构（RA）作为电子认证服务机构授权的下属机构，负责证书用户信息的申请、审核、整理汇总、统计分析，是 CA 数字认证体系的一个组成部分，在 CA 的统一领导和集中管理下开展业务活动。

注册机构可以由天津滨海 CA 自建或授权的第三方机构建立。当注册机构由第三方机构建立时，天津滨海 CA 必须与其签订协议，明确双方的权利和义务。

1.3.3 注册分支机构

注册分支机构与注册机构功能类似。当注册机构服务的群体超过一定程度时，在注册机构下面设注册分支机构。注册分支机构的上级是注册机构，下级是受理点。注册分支机构由天津滨海 CA 授权建立或撤消。注册分支机构是可选项，即根据客户数量决定是否设立。

1.3.4 证书持有者（证书用户）

证书持有者，也称为证书用户，指接受并持有天津滨海 CA 颁发的各类证书且持有与列示于证书中的公钥相对应的私钥的人物对象或单位组织，包括个人、企业和组织机构等。

1.3.5 依赖方

依赖方，是指使用证书里的公钥来验证电子签名有效性的实体。依赖方可以是证书用户，也可以不是证书用户。

在天津滨海 CA 认证服务体系之内，依赖方作为依赖于证书真实性的实体，在电子签名应用中，是电子签名依赖方。

在天津滨海 CA 认证服务体系之内，依赖方作为实体，信任天津滨海 CA 证书，可以对使用天津滨海 CA 证书机制进行的数字签名进行验证，也可以使用其他天津滨海 CA 证书用户的公钥加密信息。

1.3.6 其他参与者

其他参与天津滨海 CA 认证服务体系提供相关服务的其他实体或个人。

1.4 证书应用

1.4.1 证书类型及应用范围

数字证书可确保互联网上信息传递双方身份的真实性、信息的保

密性和完整性、以及网上交易的不可否认性。

天津滨海 CA 数字证书后续预计会在社会管理和公共服务、电子交易、电子办公、电子公证、公共服务及电子政务相关方面等领域应用，为建设互联网络的信任环境开展基础性的服务。根据证书的功能以及后续的实际应用，天津滨海 CA 依据本 CP 签发的证书在不违反相关法律法规的前提下，适用于以下类型：

1）个人证书：个人包括自然人或特定身份的人员，如公务员、企业员工等。此类证书通常用于数字签名、加密解密、安全电子邮件以及网上身份认证等；

2）机构证书：机构包括企事业单位、政府机关、社会团体等。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；

3）设备证书：设备包括服务器、防火墙、路由器等，此类证书通常用于网上设备的身份认证。

1.4.2 证书禁止使用的情形

天津滨海 CA 发放的数字证书禁止在任何违反国家法律法规或破坏国家安全的情形下使用，否则由此造成的法律后果由用户自己承担。

1.5 证书策略

1.5.1 策略文档管理机构

管理本文档的机构是：天津滨海 CA 安全策略（管理）委员会。

1.5.2 联系人

天津滨海 CA 将对电子认证服务系统证书策略文档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

1.5.3 决定 CP 符合策略的机构

天津滨海 CA 安全策略（管理）委员会作为最高策略管理机构，负责决定本 CP 的符合性和可用性。

1.5.4 CP 批准程序

本 CP 批准主要分为计划、编写（修订）、审议和发布四个阶段。编写组根据相关法律政策和运营策略提出 CP 编写（修订）计划，再由编写组完成具体条款编写工作，编写（修订）后的 CP 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，并按要求向工业和信息化部备案。

1.6 定义和缩写

1.6.1 定义

1）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。

2）注册机构（RA）

注册机构（Registration Authority，简称 RA）是负责用户证书的申请、审批和证书管理部分工作，面向证书用户的机构。

3）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。

4）证书策略（CP，Certificate Policy）

证书策略（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。

5）电子认证业务规则（Certificate Practice Statement ，简称 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、注销和密钥以及证书更新的操作规范等事务文档。

6）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。

7）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。

8）证书注销列表（CRL）

证书注销列表(Certificate Revocation List，简称 CRL)，是一种包含注销的证书列表的签名数据结构。CRL 是证书注销状态的公布形式，就像信用卡的黑名单，它通知其他证书用户某些电子证书不再有效。

9）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。

1.6.2 缩略语

DN Distinguished Name 唯一甄别名

LDAP Lightweight Directory Access Protocol 轻量目录访问

协议

RA Registration Authority 注册机构

PIN Personal Identification Number 个人识别码

PKI Public Key Infrastructure 公钥基础设施

第二章 信息发布与信息管理

2.1 认证信息的发布

天津滨海 CA 需要发布的信息包括证书策略、电子认证业务规则，证书使用和服务相关的协议、证书、证书注销列表（CRL）、证书在线状态查询（OCSP）等。

天津滨海 CA 提供明确的访问位置和方法，通过在线的方式对外发布证书、证书注销列表、证书在线状态查询，这种信息的发布通常是证书服务的一部分。

此外，天津滨海 CA 在其网站的固定位置发布证书策略、电子认证业务规则、相关协议等。

2.2 发布的时间或频率

天津滨海 CA 安全策略（管理）委员会批准本证书策略文档（CP）和相关电子认证业务规则文档（CPS）后将立即公布至信息库。

天津滨海 CA 至少 24 小时发布一次用户证书的证书注销列表（CRL）。

发布更改的信息即时生效，并对一切仍有效的数字证书的使用者、新的数字证书及相关业务的申请者均具备约束力。

2.3 信息库访问控制

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。

对于天津滨海 CA 对外公开发布的信息库，不对包括 CP、CPS、证书、证书在线状态信息、CRL 的访问进行限制，天津滨海 CA 保留设置访问控制措施以防止恶意访问的权利。

第三章 身份识别与鉴别

3.1 命名

3.1.1 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 签发的证书，其命名规则和要求必须被记录在按照本 CP 制定的 CPS 中。证书的甄别名必须包含通用名（Common Name，CN=）内容，经过验证的通用名应当包含人员姓名、组织机构名、域名等内容。

3.1.2 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，包含主题识别名称。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，并且可以被依赖方识别。

3.1.3 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。

3.1.4 理解不同名称形式的规则

依 X.500 甄别名命名规则解释。

3.1.5 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。

3.1.6 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。

3.2 初始身份确认

3.2.1 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。

3.2.2 组织机构身份的鉴别

天津滨海 CA 支持向组织机构提供证书申请服务。在对组织机构身份进行鉴别时，鉴别流程应当明确记录在 CPS 中。鉴别流程须包含对组织机构申请者身份信息、经办人身份信息的鉴别。

天津滨海 CA 授权的发证机构的审核人员须合理、审慎地核对申请资料的原件与复印件，严格进行身份鉴别。

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。

3.2.3 个人身份鉴别

天津滨海 CA 支持向个人提供证书申请服务。在对个人身份进行鉴别时，鉴别流程应当明确记录在 CPS 中。鉴别流程须包含对申请人本人或被委托人身份信息的鉴别。

天津滨海 CA 授权的发证机构的审核人员须合理、审慎地核对申请资料的原件与复印件，严格进行身份鉴别。

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。

3.2.4 设备身份的鉴别

天津滨海 CA 支持设备证书申请服务，其鉴别流程应当明确记录在 CPS 中。鉴别流程除包含对申请者身份信息、经办人身份信息的鉴别外，对于证书名称为域名（或 IP 地址）的申请，还须包含对其使用权证明的鉴别。

天津滨海 CA 授权的发证机构的审核人员须合理、审慎地核对申请资料的原件与复印件，严格进行鉴别工作。

3.2.5 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。

3.2.6 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。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

随着密钥使用时间的增加，其可能遗失或遭破解的风险也随之增加，用户应定期更新密钥，以确保相关密钥的安全性。

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。

3.3.2 注销后密钥更新的标识与鉴别

注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，详见第 3.2.2 节组织机构身份的鉴别、第 3.2.3 节个人身份的鉴别和 3.2.4 设备身份的鉴别。

3.4 注销请求的标识与鉴别

在天津滨海 CA 的证书业务中，证书注销请求可以来自用户，也可以来自天津滨海 CA。天津滨海 CA 提供证书注销请求服务，其标识与鉴别流程应当明确记录在 CPS 中。

第四章 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

组织机构代表人或其授权的代理人、个人或其授权的代理人可以作为提交证书申请的提交者。

4.1.2 注册过程与责任

天津滨海 CA 接受线下和线上两种方式的证书申请。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，又称“临柜”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。

天津滨海 CA 应当在 CPS 中明确证书申请的注册过程和责任。

申请者应事先了解用户协议、本 CP 及相应 CPS 等文件约定的事项，特别是其中关于证书适用范围、权利、义务和担保的相关内容。

申请者应向天津滨海 CA 递交证书申请表及相应证明文件，此行为即意味着申请者已经了解和接受上述内容。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

天津滨海 CA 授权的发证机构遵循第三章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。

4.2.2 证书申请批准和拒绝

完成 4.2.1 执行识别与鉴别后，如果用户满足相应要求，则视为天津滨海 CA 已经批准该证书请求，申请人即成为天津滨海 CA 的证书用户；否则应拒绝证书申请。

如果法律法规明确禁止某个申请，或天津滨海 CA 认为批准该申请具有高风险性，天津滨海 CA 应拒绝该申请。

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。

4.2.3 处理证书申请的时间

在在申请者提交的资料齐全且符合要求的情况下，对于离线申请，天津滨海 CA 或授权的发证机构将在 1 个工作日内对证书申请者提交的证书信息进行识别，并完成证书申请受理。对于线上申请，天津滨海 CA 或授权的发证机构将在 3 个工作日内对证书申请者提交的证书信息进行识别，并完成证书申请受理。

4.3 证书签发

4.3.1 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。

4.3.2 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。

4.4 证书接受

4.4.1 构成接受证书的行为

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；

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。

4.4.2 电子认证服务机构对证书的发布

一旦证书用户接受证书，天津滨海 CA 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。

4.4.3 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。

4.5 密钥对和证书的使用

4.5.1 证书使用者私钥和证书的使用

证书持有者必须妥善保管和存储与证书相关的私钥，避免遗失、泄露、被篡改或者被盗用。证书持有者按本 CP 及依照本 CP 制定的 CPS 的规定享有相应的权利和应尽的义务，如果证书持有人将该证书用于其它用途，天津滨海 CA 将不承担任何由此产生的责任和义务。如果证书中的某些字段明确了证书的使用范围和用途，那么该证书也只被允许在这一范围内使用。任何超出证书所标明的适用范围内的行为，都将由行为人独立承担责任。

4.5.2 依赖方公钥和证书的使用

在信任证书和签名前，依赖方要独立地作出应有的努力和合理的判断。假定证书是被恰当的使用，那么依赖方应当利用合适的软件、硬件去进行数字签名验证或者其它想要进行的加解密操作，作为依赖证书的条件。这些操作包括识别证书链和验证证书链中所有的数字签名。

4.6 证书更新

4.6.1 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。

天津滨海 CA 应当在 CPS 中描述可能发生证书更新的情况。

4.6.2 请求证书更新的实体

持有天津滨海 CA 颁发的未到有效期限的证书用户可以作为请求证书更新的实体。证书用户也可授权给代理人，由代理人代为申请证书更新。

4.6.3 证书更新请求的处理

处理证书更新请求，天津滨海 CA 必须对申请者身份进行鉴别，通过后才能进行证书更新操作。天津滨海 CA 应当在 CPS 中明确证书更新请求处理的细节，包括身份鉴别、证书更新操作和证书发放等。

4.6.4 签发新证书时对证书持用者的通告

同本 CP 第 4.3.2 之规定。

4.6.5 构成接受更新证书的行为

同本 CP 第 4.4.1 之规定。

4.6.6 电子认证服务机构对更新证书的发布

同本 CP 第 4.4.2 之规定。

4.6.7 电子认证服务机构对其他实体的通告

同本 CP 第 4.4.3 之规定。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

天津滨海 CA 应当在 CPS 中描述可能发生证书密钥更新的情况，例如密钥泄露、证书到期等。证书密钥更新，其具体操作同证书更新。

4.7.2 请求证书密钥更新的实体

持有天津滨海 CA 颁发的未到有效期限的证书用户可以作为请求证书密钥更新的实体。

4.7.3 证书密钥更新请求的处理

同本 CP 第 4.6.3 之规定。

4.7.4 签发新证书时对证书使用者的通告

同本 CP 第 4.3.2 之规定。

4.7.5 构成接受密钥更新证书的行为

同本 CP 第 4.4.1 之规定。

4.7.6 电子认证服务机构对密钥更新证书的发布

同本 CP 第 4.4.2 之规定。

4.7.7 电子认证服务机构对其他实体的告知

同本 CP 第 4.4.3 之规定。

4.8 证书变更

4.8.1 证书变更的情形

证书变更指改变证书中除用户公钥之外的信息而签发新证书的情形，证书的有效期未变更。用户证书只有在有效期内，才可能发生证书变更的情况。天津滨海 CA 应当在 CPS 中列明发生证书变更请求的常见原因。

4.8.2 请求证书变更的实体

用户本人或其授权代表。

4.8.3 证书变更请求的处理

对于要求证书变更的，需确认证书变更请求是被用户或用户授权的代表提出的，并对其身份进行鉴别。证书处理过程同本 CP 第 4.6.3 之规定。

4.8.4 签发新证书时对证书持有者的通告

同本规则 4.3.2 之规定。

4.8.5 构成接受变更证书的行为

同本规则 4.4.1 之规定。

4.8.6 电子认证服务机构对变更证书的发布

同本规则 4.4.2 之规定。

4.8.7 电子认证服务机构对其他实体的通告

同本规则 4.4.3 之规定。

4.9 证书注销

4.9.1 证书注销的情形

发生下列情形的，用户证书可以注销：

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）用户不能履行电子认证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 采取的临时注销措施，也可以是用户申请注销证书时填写的其他原因。

4.9.2 请求证书注销的实体

请求证书注销的实体包括：

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）依赖方的授权代表。

4.9.3 注销请求的流程

由证书用户提出的证书注销请求，天津滨海 CA 应首先对其进行

身份鉴别。通过鉴别后才能受理该请求。天津滨海 CA 应当在 CPS 中明确证书注销请求的鉴别要求。

对于强制注销，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注销，注销后必须立即通知该证书用户。

当依赖方提出证书注销申请时，如证书仅用于依赖方的系统，可以不经过证书持有者本人同意，予以注销证书，注销后必须立即通知该证书持有者。

被注销的用户证书在 24 小时内通过 CRL 向外界公布。

4.9.4 注销请求宽限期

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

4.9.5 电子认证服务机构处理注销请求的时限

发证机构在接到用户挂失、注销等数字证书注销申请时，应及时受理。在受理后 24 小时内保证数字证书注销操作正式生效。

证书持有者在正式提出证书注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注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注销相关手续前及发证机构受理用户证书注销相关申请时起到证书注销生效时 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。

4.9.6 依赖方检查证书注销的要求

依赖方在信任天津滨海 CA 签发的证书前，需要检查该证书的状态信息，包括查询证书注销列表（CRL）、查询证书在线状态（OCSP）等。

4.9.7 CRL 发布频率

天津滨海 CA 至少每 24 小时签发和公布一次 CRL，在发布的同时对原有内容进行更新。

4.9.8 CRL 发布的最大滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.9.9 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）。

4.9.10 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。

4.9.11 注销信息的其他发布形式

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

4.9.12 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注销证书。

4.10 证书冻结

天津滨海 CA 暂不提供证书冻结和解冻服务。若要提供冻结和解冻服务，天津滨海 CA 将及时修订本 CP 和 CPS 文档、按要求发布 CP 和 CPS 文档并按要求向工业和信息化部备案。

4.11 证书状态服务

4.11.1 操作特征

证书状态可以通过 CRL、LDAP 目录查询或 OCSP 查询服务获得。

4.11.2 服务可用性

天津滨海 CA 提供 7*24 小时的证书目录查询服务。

4.11.3 可选特征

无。

4.12 证书持有终止

以下三种情形将被视为证书持有终止：

1）证书持有者在证书到期后没有提出对证书密钥进行更新，将被视为证书持有终止；

2）在证书有效期内，证书持有者主动提出对证书进行注销视为证书持有终止；

3）被动注销视为证书持有终止。

4.13 口令解锁

当证书持有者忘记电子钥匙口令时，使用者提供有效身份或单位证明，填写业务申请表，申请口令解锁。

处理口令解锁请求，天津滨海 CA 必须对申请者身份进行鉴别，通过后才能进行口令解锁新操作。天津滨海 CA 应当在 CPS 中明确口令解锁请求处理的细节，包括身份鉴别、口令解锁操作等。

4.14 密钥生成、备份与恢复

4.14.1 密钥生成、备份与恢复的策略和行为

证书持有者的签名密钥对由证书持有者的密码设备（如智能 USB KEY）生成与保存，加/解密密钥（简称“加密密钥”）由国家设立的密钥管理机构生成。

用户证书的加密密钥由天津市国家密码管理局托管备份。

密钥恢复是指加密密钥的恢复，是一种严格受控的过程，密钥恢复只有在必须的情况下才进行，并且申请要提出充分的理由和提供有关文件、材料才可进行。

天津滨海 CA 不保留用户签名证书的私钥备份。用户必须妥善保管签名私钥，由于签名私钥遗失所造成的损失由证书用户自己承担，天津滨海 CA 不负责。

4.14.2 会话密钥的封装与恢复的策略与行为

会话密钥是指用户在使用证书建立加密通道时临时生成的加密密钥，该密钥由应用环境来决定使用，电子认证服务机构不对其进行保存和恢复。

第五章 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

天津滨海 CA 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。CA、RA 的操作都应在受到物理保护的建筑环境内进行，可以阻止并检测对敏感信息或系统进行的未经授权的使用、访问或披露。天津滨海 CA 应当在 CPS 中简要描述场地物理设施等情况。

5.1.2 物理访问

在物理安全方面，天津滨海 CA 保证对每一间机房的访问都可被审计和可控，确保每一间机房都只有经过授权的人员可以访问。

5.1.3 电力与空调

CA 和 RA 的安全设施应配备主备电源确保持续、不间断的电力供应。此外，还应配备空调系统以控制温度和相对湿度。

5.1.4 水患防治

CA 和 RA 的安全设施应通过建筑、设备装配和可行措施等防止洪

水或其它水患造成的损害。

5.1.5 火灾防护

CA 和 RA 的安全设施应通过建筑、设备装配和可行措施等防止和扑灭火灾或其它烟雾、火苗造成的损害。火灾防护措施应当符合国家消防规定的要求。

天津滨海 CA 机房安装了火灾自动报警系统和自动气体灭火系统，火灾探测系统能够同时通过检测温度和烟雾发现火灾的发生，且火灾报警系统与自动气体灭火系统联动。

5.1.6 介质存储

CA 和 RA 应保护备份关键系统数据或敏感信息的磁性存储免受水、火或其他物理因素的损害，并采取保护措施以阻止、检测和预防对这些介质未经授权的使用、访问或披露。

5.1.7 废物处理

CA 和 RA 应执行废物（纸张、介质或其它任何废物）处理流程，以防止对包含机密或隐私信息的废物进行未经授权的使用、访问和披露。

5.1.8 异地备份

CA 和 RA 应采取安全的异地方式保持对关键数据或任何其它敏感

信息的备份。

5.1.9 注册机构物理控制

下属的注册机构的物理场地也需要有足够的安全措施，保证只有授权的人员才能进入，只有授权的人员才能接触系统进行证书管理。

5.2 程序控制

5.2.1 可信角色

被指定为管理基础设施可信性的员工、承包商和顾问等应当被视为在可信岗位上的可信人员，成为可信人员必须满足本 CP 的筛选要求。可信人员包括有权执行、访问或控制如身份鉴别、密钥操作等可能会造成重大影响的所有员工、承包商和顾问。

天津滨海 CA 应当在 CPS 中列举可信人员的名称。

5.2.2 每项任务需要的人数

CA 和 RA 必须建立、保持和执行严格的控制程序，以确保基于工作职责进行的任务分割，并且确保由多名可信人员共同完成敏感操作。必须制定政策或控制措施以确保基于工作职责进行的任务分割。最敏感的任务，例如访问和管理 CA 密码设备或相关的密钥存储设备，必须要求多个可信人员进行操作。

这些内部控制流程必须被严格设计、以确保最少要求由两个可信人员拥有物理或逻辑访问控制权限。CA 密码设备的访问在其整个生

命周期内必须严格确保由多个可信人员共同进行，包括从最初的接收到最后的逻辑或物理的破坏。一旦用于密钥操作的模块被激活，进一步的访问控制必须被启用，以便对设备物理和逻辑访问都保持分割控制。

5.2.3 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。进入机房需要使用门禁卡、密码和指纹识别；进入系统需要使用 USB Key 存储的数字证书进行身份鉴别。天津滨海 CA 将独立完整地记录其所有的操作行为。

5.2.4 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。任何密钥恢复的操作，都需要五位管理员中的半数以上管理员同时来完成。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。

5.3 人员控制

5.3.1 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。

5.3.2 背景审查程序

天津滨海 CA 证书服务人员需要根据背景审查规范进行身份背景审查、业务能力调查等。通过审查后才能任职。背景调查必须符合法律法规的要求。

天津滨海 CA 应当在 CPS 中明确背景审查相关流程。

5.3.3 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）CP 和 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。

5.3.4 工作岗位轮换周期和顺序

根据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。

5.3.5 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 相关的管理规范执行。

5.3.6 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》。

5.3.7 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。

5.4 审计日志程序

5.4.1 记录事件的类型

CA 和 RA 必须记录一些审计事件，无论是手动生成或者是系统自动生成，都应该包含事件发生的日期或时间、导致事件发生的实体身

份。天津滨海 CA 应当在 CPS 中明确所记录的日志和事件的类型。

5.4.2 处理日志的周期

天津滨海 CA 应定期检查审计日志，以便发现重要的安全和操作事件，对发现的安全事件采取相应的措施，并对审计行为进行备案。

天津滨海 CA 应当在 CPS 中明确对于不同类型的审计日志的处理周期。

5.4.3 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。

5.4.4 审计日志的保护

所有的审计日志应当采取保护机制，防止未授权的浏览、修改、读取、删除或篡改等。

5.4.5 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。

5.4.6 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。

5.4.7 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。

5.4.8 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。

5.5 记录归档

5.5.1 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。

5.5.2 归档记录的保存期限

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、注销、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，自证书期满或注销之日起，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。

5.5.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。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。

5.5.4 归档文件的备份程序

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。

5.5.5 记录的时间戳要求

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。

5.5.6 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。

5.6 电子认证服务机构密钥更替

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（管理）委员会授权，五位加密机管理员、一位加密机操作员同时在场，共同启动密钥管理程序，执行密钥更新指令，由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。

5.7 事故与灾难恢复

5.7.1 事故和损害处理流程

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。

5.7.2 计算机资源、软件、数据的损坏

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、软件和(或)数据。

5.7.3 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 或注册机构注销其证书。天津滨海 CA 按第 4.9 节发布证书注销信息。

2）当天津滨海 CA 的证书出现私钥损害时，天津滨海 CA 将立即注销 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。

5.7.4 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。

5.8 电子认证服务机构或注册机构的终止

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，并在终止服务六十日前向国务院信息产业主管部门报告,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：

1）起草 CA 终止声明；

2）通知与 CA 停止相关的实体；

3）关闭从目录服务器；

4）证书注销；

5）处理存档文件记录；

6）停止认证中心的服务；

7）存档主目录服务器；

8）关闭主目录服务器；

9）处理加密密钥；

10）处理和存储敏感文档；

11）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。

第六章 认证系统技术安全控制

6.1 密钥对的生成和安装

由于密钥对是安全机制的关键，所以在电子认证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。

6.1.1 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；

天津滨海CA在技术、流程和管理上保证密钥对产生的安全性。

6.1.2 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。

6.1.3 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。

6.1.4 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。

6.1.5 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。

6.1.6 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。

6.1.7 密钥的使用

在天津滨海 CA 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 证书和证书注销列表（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。

6.2 私钥保护和密码模块工程控制

6.2.1 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。

6.2.2 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、注销、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。

6.2.3 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。

6.2.4 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。

6.2.5 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。

6.2.6 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。

6.2.7 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。

6.2.8 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。

6.2.9 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。

6.2.10 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。

6.2.11 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。

6.3 天津滨海 CA 密钥的保管

6.3.1 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。

6.3.2 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。

6.4 激活数据

6.4.1 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。

6.4.2 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。

6.4.3 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 计算机安全控制

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。所有授权用户必须有合法的安全令牌，并且通过密码验证。

天津滨海CA根据法律法规和主管部门的规定，按照国家计算机安

全等级的要求，实现安全等级制度。

为了保证认证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，制定操作规范。另外，本系统采用对关键主机设备双机热备和增加冗余资源的方法，使系统在发生故障时仍能正常工作。

对于计算机有一套完整的保管和维护制度：

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）制定设备维修计划，建立满足正常运转最低要求的易损坏备件库；

4）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。

另外对特别的计算机主机进行了安全漏洞扫描和安全优化，安装了防病毒系统。

6.6 生命周期技术控制

6.6.1 系统开发控制

系统开发采用先进的安全控制理念，同时应兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

6.6.2 安全管理控制

天津滨海CA对系统的维护保证操作系统、网络设置和系统配置安全。通过日志检查系统与数据完整性和硬件的正常操作。认证系统只开放与业务相关的功能，只有天津滨海CA授权的员工能够进入天津滨海CA的系统或设备。

6.6.3 生命期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过了主管部门鉴定，使用了基于标准的强化安全通信协议确保了通信数据的安全，在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，在开发完成后进行严格的安全测试，整个系统安全可靠。

6.7 网络的安全控制

天津滨海CA网络安全的主要目标是保障网络基础设施、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、数据备份、灾难恢复等安全防护措施。

6.8 时间戳

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。

第七章 证书、证书注销列表和在线证书状态协议

7.1 证书

7.1.1 证书格式标准

天津滨海CA签发的证书均符合国家标准证书格式，遵循X.509 V3规范，并可以提供支持证书扩展的能力。

7.1.2 证书标准项

证书序列号：即证书参考号码。

证书有效期：证书的起止时间。

主题：为用户申请证书时所填写的申请信息，即用户的甄别名。

颁发者：为天津滨海CA。

证书标准项一览表

项目名称		值	说明
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	

	O	TJCA	
	C	CN	
有效期从			有效开始日期
到			有效结束日期
使用者	C	CN	所属国家
	S		省份
	L		城市
	O		组织机构
	OU		机构名称
	CN		使用者主体
	E		电子邮箱
公钥		ECC	
公钥参数		1.2.156.10197.1.301	
基本扩展项			
自定义扩展项			
指纹算法		SHa1	
指纹		签名值	摘要

7.1.3 证书扩展项

证书扩展项一览表

类目	OID	对应项目	备注
标准扩展项	1.2.156.10260.4.1.1	身份标识码	如:居民身份证号码、军官证号码、护照号码等
	1.2.156.10260.4.1.3	企业工商注册号	
	1.2.156.10260.4.1.4	企业组织机构代码	
	1.2.156.10260.4.1.5	企业税号	
自定义扩展项	1.2.86.21.1.3	信任服务号	

7.1.4 算法对象标识符

天津滨海CA签发的证书符合X.509 V3，签名算法采用基于SM3的SM2，为1.2.156.10197.1.501。

7.1.5 名称形式

天津滨海CA的证书通过DN来命名。

国家：Country（C）

省份：State or Province（S）

地市：Locality (L)

组织：Organization（O）

机构：Organizational Unit（OU）

用户名称：Common Name（CN）

电子邮箱：E-mail （E）

7.1.6 名称限制

天津滨海CA签发的证书,其识别名称不允许为匿名或者伪名,必须具有确定含义的识别名称。

7.1.7 证书策略对象标识符

证书策略由天津滨海CA制定并对外发布，作为本机构的证书策略的标识，代表本机构提供证书服务的相关策略。另一方面，只有用户同意该证书策略，才可以从天津滨海CA申请和获得证书。

7.1.8 策略限制扩展项的用法

规定在CA体系中的各层CA使用相同的CP以及是否和其他CA体系互相信任。目前，天津滨海CA未使用本扩展域。

7.1.9 策略限定符的语法和语义

Certificate Policies CA证书策略

Policy Mappings 策略映射

Basic Constraints 基本制约

7.1.10 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。

7.2 证书注销列表

7.2.1 版本号

天津滨海CA定期签发CRL（证书废除列表），其所签发的CRL遵循RFC 3280标准。采用X.509中的CRL V2 格式。

7.2.2 CRL 和 CRL 条目扩展项

CRL扩展项：颁发机构密钥标识符(Authority Key Identifier)。

CRL条目扩展项：不使用CRL条目扩展项。

7.3 在线证书状态协议

7.3.1 版本号

天津滨海CA为证书持有者提供OCSP（在线证书状态查询服务），OCSP 为CRL 的有效补充，方便证书持有者及时查询证书状态信息。天津滨海CA OCSP 服务遵循RFC 2560标准。

天津滨海CA使用OCSP 版本1（OCSP V1）。

7.3.2 OCSP 扩展项

天津滨海CA目前未使用OCSP扩展项。

第八章 认证机构审计和其他评估

8.1 评估的频率或情形

天津滨海CA的评估根据情况而定，有年度评估、运营前评估、安全事件发生后的评估和随时进行评估。天津滨海CA本身需要对其关联单位（包含天津滨海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CP和相应CPS的规定，其频率可由天津滨海CA决定或由法律制定的监管机构决定。

8.2 评估者的资质

在进行外部审计时，天津滨海CA应选择具有国家或国际上认可资质的专业审计评估机构，在业界享有良好的声誉，具备丰富的实际操作经验。

天津滨海CA的内部审计，由安全运维部负责组织实施，要求评估人员至少具备认证机构、信息安全审计相关知识，并且熟悉本CP和相关CPS的规范，以及应具备计算机、网络、信息安全等方面的知识和实际工作经验。

8.3 评估者与被评估者的关系

外部评估者与天津滨海CA之间是独立的关系，没有任何业务、财务往来或其它利害关系足以影响评估的客观性。

天津滨海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

8.4.1 安全管理

物理环境的安全控制、数据和信息的安全管理、人员的安全控制、建筑设施的安全控制、软硬件设备和存储介质的安全控制、系统和网络的安全控制、系统开发和维护的安全控制、灾难恢复和备份系统的管理、审计和归档的安全管理等。

8.4.2 操作的规范性

是否制订和公布CP/CPS；是否按照CP/CPS来制订相关的操作规范和运作协议；是否按照CP/CPS及相关操作规范和运作协议开展业务。

8.4.3 服务的完整性

密钥和证书生命周期的安全管理、证书注销操作、业务系统的安全操作、业务操作标准审查、用户资料的保密和存储管理、售后服务的标准和规程等。

8.5 对问题与不足采取的措施

完成内部和外部审计后，天津滨海CA必须根据评估的结果检查缺失和不足，提出修改和预防措施，并跟踪改善情况。

天津滨海CA根据需要可就整改情况开展后续跟踪评估。

天津滨海CA应当在CPS中简要描述具体流程和要求。

8.6 评估结果的传达与发布

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

第九章 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

根据天津滨海CA的价目确定。

9.1.2 证书查询费用

根据天津滨海CA的价目确定。

9.1.3 证书注销或状态信息的查询费用

根据天津滨海CA的价目确定。

9.1.4 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。

9.1.5 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。

9.2 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，并依据本CP和相关CPS规定的方式进行赔偿。

9.3 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。

9.3.1 保密信息范围

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）用户信息

- 用户的注册信息；
- 用户系统、应用访问CRL、OCSP的记录（时间、频度）；
- 用户与认证机构、注册机构签订的协议。

9.3.2 不属于保密的信息

1）本CP、CPS、证书申请流程、手续、申请操作指南、证书注销列表等；

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。

9.3.3 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。

9.4 个人隐私保密

9.4.1 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。

9.4.2 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。

9.4.3 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。

9.4.4 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。

9.4.5 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。

9.4.6 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，必须披露本CP和相应的CPS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。

9.4.7 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。

9.5 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 保留对本规则的所有知识产权；

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。

9.6 权利和责任

9.6.1 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》及相关法律的规定，接受工业和信息化部的业务监督和指导，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本CP和相关CPS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将及时注销证书，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。

9.6.2 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CP和相关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。

9.6.3 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本CP和相关CPS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CP的条例和与相关CPS的条例，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。

9.6.4 证书依赖方的权利和责任

依赖方必须熟悉本CP的条款以及相应的CPS的条款，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CP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。

9.6.5 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。

9.7 有限责任与免责条款

9.7.1 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签发的数字证书方面，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承诺在现有的技术条件下，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。

9.7.2 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、被注销的数字证书；

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。

9.8 赔偿

一、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：（1）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）由于天津滨海CA的原因，使得证书中出现了错误信息。（3）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：

1）个人证书1000元；

2）机构证书4000元；

3）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。

二、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。

三、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注销。

9.9 本 CP 的有效期与终止

本CP自发布之日起正式生效。本CP中将详细注明版本号及发布日期。最新版本的本CP请访问天津滨海CA网站以获得，对具体个人不做另行通知。当新版本的CP正式发布生效，旧版本的CP将自动终止。

9.10 本 CP 的修订

9.10.1 修订

当出现以下情形时，天津滨海CA将对本CP进行修订：

1）因相关法律法规要求而引起本CP发生改变；

2）因相关技术条件变化而引起本CP发生改变；

3）因其它原因而引起本CP发生改变。

9.10.2 修订流程

1）CP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CP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 网站或其它方式发布，同时按照《电子认证服务管理办法》的要求，自公布之日起三十日内向工业和信息化部备案。

9.11 争议解决

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。

9.12 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》和《中华人民共和国合同法》等。

9.13 与适用法律的符合性

无论在任何情况下，本CP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。

9.14 一般条款

9.14.1 完整协议

本CP将替代先前的、与主题相关的书面或口头解释。

9.14.2 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。

9.14.3 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。

9.14.4 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。

9.15 各种规范的冲突

若本CP与其它规定、指导方针相互抵触，用户必须接受CP的约束，除非本CP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CP。

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CP的规定执行；对协议中不同于本CP内容的约定，按双方协议中约定的内容执行。

9.16 其他条款

天津滨海CA对本CP具有最终解释权。

单位名称:天津市滨海数字认证有限公司
地址：天津空港经济区西七道26号
客服电话：400-872-5550
E-mail：tjbhca@tjbhca.com
公司网址：https：//www.tjbhca.com