颐信科技有限公司

电子认证业务规则

ECCA Certification Practice Statement

(CPS)

版本 V5.1

发布日期：2019年10月18日

生效日期：2019年11月03日

颐信科技有限公司

版本修订表

版本号	发布日期	说明
V1.3	2005 年 10 月	参考有关规定和技术文档制订
V2.0	2007 年 10 月 20 日	依据《电子签名法》和《电子认证服务管理办法》，参照信息产业部《电子认证业务规则规范（试行）》进行修订
V3.0	2009 年 2 月 24 日	依据升级系统技术文档及有关规定修订
V4.0	2014 年 6 月 3 日	依据《电子认证服务管理办法》和《电子签名法》结合业务系统支持SM2椭圆曲线密码算法进行修订
V4.5	2016年3月25日	1、明确鉴别证书变更请求者身份的方式 2、修改职责分割的岗位描述 3、完善进行私钥的销毁处理的描述 4、明确根私钥被攻破、需要作废或被作废情况下的应变流程 5、明确赔付监督机制
V5.0	2018年6月29日	1、明确设备证书的鉴别方法 2、第三方鉴别的策略 3、明确证书在线更新的鉴别方式
V5.1	2019年10月18日	1、进一步完善2018年6月29日修订的3点问题 2、修改《电子认证服务许可证》编号 3、明确认证信息发布的网址 4、处理日志的周期中对监控录像保存周期进行修改 5、电子认证服务机构密钥更替中明确根证书有效期 6、增加证书扩展项的自定义扩展项3个自定义OID 7、CRL 和 CRL 条目扩展项明确了CRL的颁发者

版权声明

颐信科技有限公司享有并保留颐信数字证书认证中心（简称颐信CA）提供的全部软件及证书产品的一切知识产权，包括所有权、名称权和利益分享权等。

所有由颐信 CA 颁发的数字证书、提供的软件、技术文档、协议合同、司法文件等均属于颐信科技有限公司的知识产权范围。

颐信 CA 网站上公布的一切信息，未经颐信 CA 书面允许，他人不得转载用于商业行为。

用来表示目录中颐信 CA 域中的实体的甄别名（以下简称 DN）以及该域中颁发给终端实体的证书，均为颐信 CA 的财产。

在没有获得颐信 CA 书面授权时，任何人不能使用或接受任何颐信 CA 使用的名称、商标、交易形式或者可能与之相混淆的名称、商标、交易形式。

证书申请人（接受申请时即为用户）声明并保证：其交付给颐信CA 和相关证书颁发机构用于证书签发的辨识名称和其它所有相关申请资料，不得在任何管辖区域内干预或侵犯第三方的商标、服务标志、商标名称、公司名称或其它知识产权等权利，包括侵害商业利益、不公平竞争、损害他人信誉及干扰或误导他人。

目录

1 概括性概述

1.1 概述

1.1.1 颐信科技有限公司

颐信数字证书认证中心（以下简称颐信CA）是由颐信科技有限公司负责管理和运营的权威、公正的第三方电子认证服务机构。2004 年建成并开始试运营，2005年分别获得国家商用密码管理局颁发的电子认证服务密码使用许可证（编号：0019）和中华人民共和国工业和信息化部颁发的电子认证服务许可证（编号ECP11010815012），获准在全国范围内开展电子认证服务业务。

颐信 CA 作为第三方电子认证服务机构，主要是按《电子签名法》、《电子认证服务管理办法》等国家法规、政策，为用户提供以数字证书技术为基础的身份认证和信任服务，包括证书的颁发、存档、查询、废止等，颐信CA 采用“双中心”、“双密钥”、“双证书”的认证体系，签发的证书符合 X.509C V3 标准，可以广泛应用于电子政务、电子商务及其它网上交易系统的安全认证。

1.2 文档名称与标识

《颐信科技有限公司电子认证业务规则》（以下简称颐信CPS）是对颐信 CA 提供的认证业务整个过程的全面和综合性描述，是颐信 CA 在数字证书、密钥生命周期管理及证书服务设施维护管理过程中应遵循的操作标准。

本 CPS 适用于颐信 CA 信任体系范围内的所有实体，包括颐信CA自身、颐信CA授权的 RA 中心、证书受理点、电子签名依赖方以及所有被颐信 CA 支持的服务提供者，各参与方必须完整理解和执行本 CPS 的所有条款，并承担相应的责任和义务。

本 CPS 由颐信 CA 信息安全管理委员会根据相关法律、政策以及颐信 CA 的具体业务要求，负责修订和发布。颐信CA 拥有本 CPS 的完全版权，本CPS 通过颐信CA 网站对外发布，自发布之日起十五日后生效，对具体机构和个人不再另行通告。

任何机构或个人如对本 CPS 有任何质疑，都可来信来函咨询。

颐信科技有限公司联系方式：

通信地址：北京市朝阳区万红西街 2 号燕东大厦 C 座 401

邮政编码：100015

网站地址：http://www.ecca.com.cn

电话号码：010－84505959

颐信 CA 的标识为：

颐信数字证书认证中心（ EcGuard Certification Authority）简称为颐信CA，有时也称为颐信 CA 中心，英文缩写为 ECCA，因此，“颐信 CA”、“颐信 CA 中心”、“ECCA”都是颐信数字证书认证中心的合法标识。颐信数字证书认证中心的

标准图标为：颐信数字证书认证中心 EcGuard Certification Authority

1.3 电子认证活动参与者

电子认证活动参与者包括：电子认证服务机构、注册机构、订户、依赖方以及其它关联机构，所有这些参与者共同构成一个信任体系，颐信CA 及其授权的 RA注册中心、证书受理点、订户、依赖方共同形成颐信 CA 的信任体系。

1.3.1 电子认证服务机构

颐信 CA 是依据《电子签名法》设立的第三方电子认证服务机构。颐信 CA 作为颁发证书的实体，按照“双证书”技术体系标准和规范，负责为用户产生加密证书的密钥对（签名证书的密钥对在客户端由证书载体产生），为用户签发证书，为用户提供证书储存、查询、注销等证书管理服务。

1.3.2 注册机构

注册机构负责用户的证书申请和资料审核，对证书申请者进行身份标识和鉴别。注册机构可分为 RA 注册中心和证书受理点两级。

根据业务的需要，颐信 CA 可以授权建立远程 RA 注册中心和证书受理点。授权 RA 注册中心和受理点必须严格遵循颐信 CPS。

1.3.3 订户

订户是从颐信 CA 接收数字证书的实体，包括已经申请并拥有颐信 CA 签发的证书的个人、企业、组织、机构、网站、服务器等各类主体和实体。

在电子签名应用中，订户即为电子签名人。

1.3.4 依赖方

依赖方是信任证书真实性的实体，依赖方可以是、也可以不是一个订户。

颐信 CA 承诺，颐信CA 和所有授权的 RA 注册中心、证书受理点都严格遵循本CPS 的规范进行操作，保证订户的证书中信息是真实的，在颐信 CA 信任体系内部，依赖方应该（也必须）信任颐信 CA 的根证书（也即是颐信 CA 的根密钥对）。而依赖方对于用户证书（被执行注销、冻结等废止操作的除外）及对应的签名的信任，是建立在通过颐信CA 提供的认证服务的基础上。

1.3.5 其他参与者

在颐信 CA 信任体系中，其他参与者包括提供其它相关服务的实体和接受颐信CA 认证服务的实体，如证书认证系统和密钥管理系统提供商及需要颐信 CA 提供证据的司法部门等。

1.4 证书应用

1.4.1 颐信 CA 数字证书种类

颐信 CA 数字证书类型包括以下几种：

证书类型	证书的用途
个人身份证书	个人身份证书包含证书订户的个人身份信息、公钥及颁发机构的数字签名，用于网络通讯中标识个人用户身份。用于文档签名、文档加密、网上交易等
企业身份证书	企业身份证书包含证书订户的企业身份信息、公钥及颁发机构的数字签名，用于网络通讯中标识企业用户身份，如在网络申报系统中向服务器端证明用户的真实身份。 用于文档签名、网上工商事务、网上招标投标、网上签约、安全网上公文传送、网上缴费、网上缴税、网上购物和网上报关等
服务器身份证书	服务器身份证书用于网络通讯中标识和验证服务器的身份。 服务器证书中包含服务器域名、服务器相关信息、公钥以及颁发机构的数字签名。
安全邮件证书	安全邮件证书中包含用户的邮箱地址信息和颁发机构的数字签名，用于对电子邮件进行加密和数字签名处理，保证电子邮件的安全。
代码签名证书	代码签名证书为软件开发商或个人提供了一个理想的解决方案，使得软件开发者能对其软件代码进行数字签名 通过对代码的数字签名来标识软件来源以及软件开发者 的真实身份，保证代码在签名之后不被恶意篡改。使用户在下载已经签名的代码时，能够有效的验证该代码的可信度。

1.4.2 适合的证书应用

从数字证书的功能上讲，颐信 CA 签发的证书可以实现以下功能：

1. 确保证书持有者身份或者数据信息发送者的身份的真实性；
2. 保证信息的完整性；
3. 防止操作双方对操作过程进行抵赖和否认；
4. 提供和支持保证信息机密性功能（颐信 CA 采用双证书，为订户提供加密证书）。

证书可以用来对《电子签名法》未限制使用的民事活动中的合同或者其他文件、单据等进行数字签名的验证，可以应用于电子政务、电子商务、网上在线交易、企业信息化等应用领域。

具体的证书类型包括个人身份证书、单位身份证书、邮件证书、 WEB 服务器证书等，证书申请人可以根据实际需要，决定选用哪种证书类型。

1.4.3 限制的证书应用

在《电子签名法》规定禁止使用电子签名的下列情况，不得使用颐信CA 签发的数字证书：

（一）涉及婚姻、收养、继承等人身关系时；

（二）涉及土地、房屋等不动产权益转让时；

（三）涉及停止供水、供热、供气、供电等公用事业服务时；

（四）法律、行政法规规定的不适用电子文书的其他情形。

另外，在有可能损害国家安全等违法犯罪情况时，订户不得使用颐信CA 签发的数字证书，由此造成的法律责任和后果全部由订户负责。

1.5 策略管理

1.5.1 CPS 文档管理机构

本 CPS 的管理机构是颐信 CA 信息安全管理委员会，由颐信 CA 信息安全管理委员会负责本 CPS 的起草、审批、注册、发布、更新等事宜。

本 CPS 由颐信 CA 拥有完全版权，所有旧版本由颐信 CA 统一归档管理。

本 CPS 接受信息产业部电子认证管理办公室监督。

1.5.2 联系方式

颐信 CPS 由“颐信 CA 信息安全管理委员会 ”负责管理，任何有关颐信 CPS的问题、建议、质疑，都可以与“颐信 CA 信息安全管理委员会”联系。
联系地址：北京市朝阳区万红西街 2 号燕东商务大厦 C 座 4 层（100015）
电话号码：86-010-84505959
传真号码：86-010-84505912

1.5.3 CPS 批准程序

由颐信 CA 信息安全管理委员会负责组织和指定专人编写颐信 CPS 草案，CPS草案编写完成后，由颐信CA 信息安全管理委员会进行评审和审批，如果不能通过评审，将再次进行修改，直至最后通过，通过颐信CA 信息安全管理委员会审批后，CPS在颐信 CA 的网站上对外公布。

本 CPS 经颐信 CA 信息安全管理委员会审批通过后，从对外公布之日起三十日内向信息产业部备案。

1.6 定义和缩写

（1）颐信 CA

颐信 CA 是颐信数字证书认证中心的简称，是专门从事基于 PKI/CA 技术的电子认证服务的第三方电子认证服务机构，由颐信科技有限公司负责管理和运营。

（2）CPS（Certification Practice Statement）

“电子认证业务规则”的英文简称。明确规定颐信CA 在审批、签发、发布和废止证书等证书生命周期管理以及相关的业务应遵循的各项操作规范。

（3）PKI（Public Key Infrastructure ）

即公开密钥基础设施。支持公开密钥体制的安全基础设施，提供身份鉴别、加密、完整性和不可否认性服务。

（4）CA（Certification Authority）

认证机构的英文简称。CA 是网络身份认证的管理机构，是网上安全电子交易中具有权威性和公正性的可信赖的第三方机构。CA 为电子商务的各参与方签发标识其身份的数字证书，并对数字证书进行更新、废止等一系列管理。

（5）RA（Registration Authority）

注册机构的英文简称。RA 是 CA 认证体系的一个功能组件，负责对数字证书申请进行资格审核，并决定是否同意给该申请者发放数字证书，承担因审核错误而引起的一切后果。

（6）CRL（Certificate Revocation List）

证书撤消列表的英文简称。CRL 中记录所有在原定失效日期到达之前被废止或冻结的数字证书的序列号，供数字证书使用者在认证对方数字证书时查询使用。CRL 通常又被称为数字证书黑名单。内容通常还包含列表颁发者、颁发日期、下次废止列表的预定发行日期和废止的数字证书序列号，并说明废止的时间与理由。

（7）LDAP（Lightweight Directory Access Protocol）

即轻量级目录访问协议,用于查询、下载数字证书以及数字证书废止列表(CRL)。

（8）OCSP（Online Certificate Status Protocol）

即在线数字证书状态查询协议，用于支持实时查询数字证书状态。

（9）EKey

EKey 是一种集智能卡和读写器于一体的 USB 设备，因此有时也称为USB-KEY。因为其体积小、重量轻、便于携带，又称“智能密码钥匙”或“电子令牌”，可以实现身份认证、数据加密/解密、数字签名、数据安全存储等功能，是现代计算机

网络中很好的客户端信息安全产品。它可应用到电子政务、电子商务、电子业务的各领域中，为建立系统的安全平台提供快捷、安全的客户端解决方案。

（10）X.509 标准

是国际电信同盟认证体系的证书标准。

（11）信息安全管理委员会

颐信 CA 信息安全管理委员会，负责制定颐信 CA 证书认证体系的策略，监督和管理认证体系策略的实施。为规范颐信数字证书认证中心的管理，保障认证体系的可靠，维护颐信CA 数字证书认证的权威性，为互联网络的安全交易提供支持，颐信 CA 信息安全管理委员会制订了证书策略，对颐信 CA 数字证书认证体系，管理要求，运行要求和系统与设施要求等内容做出了相关的规定。

（12）认证（Certification ）

不同实体在进行网上操作时，通过可信赖的、中立的第三方（如CA 认证中心）对身份进行审核，并由第三方出具证明证实其身份的可靠性和合法性的过程。

（13）数字签名（Digital Signature）

利用公开密钥算法等方法保证信息传输过程中信息的完整性、发送者的身份认证和不可抵赖性的一种技术。

（14）私钥（Private Key）

是一种不能公开、由持有者秘密保管的数字密钥，用于创建数字签名，就相对应的公开密钥加密的文件或信息予以解密。

（15）公钥（Public Key）

可以公开的数字密钥，用于验证相应的私人密钥签名的报文，也可以用来加密报文、文件，由相应的私人密钥解密。

（16）密钥对

私钥加上对应的公开密钥。

（17）数字证书

数字证书又称为数字标识(Digital Certificate，Digital ID)。它提供了一种在 Internet 上身份验证的方式，是用来标志和证明网络通信双方身份的数字信息文件，与司机驾照或日常生活中的身份证相似。在网上进行电子商务活动时，交易双方需要使用数字证书来表明自己的身份，并使用数字证书来进行有关交易操作。通俗地讲，数字证书就是个人或单位在 Internet 上的身份证。

（18）订户

个人、集体、公司、服务器或者其他拥有任何颐信 CA 证书的人或实体。

2 信息发布与信息管理

2.1 认证信息的发布

颐信 CA 通过网站（www.ecca.com.cn）公布与认证服务相关的信息，通过网站公布的内容主要包括：颐信CA 的业务规则（CPS）、安全产品和服务项目、颐信CA 的发展状况和动态等，只有颐信 CA 有权对这些信息进行更新、修改以及删除等操作。

颐信 CPS 由颐信 CA 信息安全管理委员会负责制定、修改、发布，颐信CPS必须经信息安全管理小组审批通过后，才能通过颐信 CA 网站或其它途径对外公布。

颐信 CA 签发的证书、 CRL 以及证书状态信息等都是通过专用目录服务系统（LDAP）和在线证书状态查询系统（OCSP）进行发布的，同时，颐信CA 授权的 RA 注册中心可以保留颐信 CA 签发的证书、CRL 以及证书挂起信息的副本，证书用户可通过网址（www.ecca.com.cn）公布的目录服务系统（LDAP）和在线证书状态查询系统（OCSP）链接地址,查询并下载数字证书、下载CA 根证书、 CRL等信息。

2.2 发布的时间与频率

颐信 CA 网站上的信息由颐信 CA 根据实际情况决定，随时可能对有关信息进行更新和调整。

颐信 CPS 将不定期进行更新和公布。由颐信CA 信息安全管理委员会每年度至少对 CPS 进行一次审核和评估,确定 CPS 与国家法律、政策以及颐信 CA 的认证服务业务是否相符合，并确定是否需要对 CPS（或部分内容、条款）进行修订、修改和调整。若需要修改，则由信息安全管理小组起草修改草案，并进行最终审批，审批通过后将通过颐信 CA 的网站重新发布新版本 CPS。

专用目录服务中发布的用户证书一直保持不变，用户也可以通过 LDAP 协议，访问 LDAP 系统，实时查看和获得某一证书的状态，包括是否有效。

颐信 CA 的 CRL 每 24 小时更新发布一次，授权的 RA 中心可以及时同步更新。

2.3 信息库访问控制

对于公开发布的 CPS、证书、CRL 等信息，颐信 CA 允许公众自行通过网站和目录服务器进行查询和访问。

颐信 CA 对部分重要信息内容实行授权访问控制，只有授权的颐信 CA 工作人员才能编写、修改和删除颐信 CA 在线发布的信息资料，同时颐信 CA 在必要时可自主选择是否实行信息的授权访问，以确保只有证书用户才有权查阅受颐信CA控制的信息资料。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

颐信 CA 依照特定的签发流程，保存与证书注册过程有关的特定记录，对特定对象进行身份鉴别，以区别于其它申请者，这一命名过程中出现的名称，包括甄别名和用户唯一标识符，是一组能辨别真实实体的数据。

按照 X.509 标准的规定，每个证书订户对应一个可分辨的名称，该名称由甄别名和用户唯一标识符组成。甄别名包含于每张证书的主题中，用户唯一标识符是一项独立的证书基本域，名称应唯一标识证书订户的身份。

颐信 CA 要求甄别名在不同实体中不可重用，证书的唯一标识符未被使用。

每个订户对应一个甄别名（Distinguished Name，简称DN）。颐信CA 签发的数字证书中的主体名称，采用 X.500 DN 的方式。

3.1.2 对名称意义化的要求

订户的甄别名（DN）必须具有一定的代表意义。

证书主体名称表示本证书所对应的最终实体的特定名称，描述了与主体中的公钥绑定的实体信息。

3.1.3 订户的匿名或伪名

颐信 CA 证书服务体系中，不支持订户（证书申请人）使用匿名或伪名。

3.1.4 理解不同名称形式的规则

颐信 CA 签发的证书的 DN 的具体内容依次由以下六个部分组成：
CountryName(国家名，简称 C)
StateOrProvince （省份，简称S）
LocalcityName(地市 ， 简称L) L)
OrganizationName(组织名称，简称O)
OrganizationalUnitName(机构名称，简称为 OU)
CommanName(用户名称，简称为 CN)

3.1.5 名称的唯一性

在颐信 CA 证书服务体系中，证书主体名称必须是唯一的，对应一个真实的实体。

颐信 CA 要求甄别名在不同实体中不可重用。

颐信 CA 唯一标识符未被使用，申请者的唯一标识符在证书基本域中不可见。

当订户因为主体名称相同而发生纠纷时，颐信 CA 没有权力和义务进行裁决，用户可以向相关主管部门提出申请和裁决。

3.1.6 商标的识别、鉴别和角色

证书订户使用商标作为标识名称，应向颐信CA 提供商标注册方所有权的证明文件。

颐信 CA 在证书签发过程中，将按规定对用户身份真实性进行鉴别，但不对用户提供的标识符是否拥有知识产权进行验证和确认，也不保证这种权利的唯一性。

对于因商标、标识等归属问题造成的纠纷，颐信CA 不承担调解和仲裁的责任，颐信 CA 没有这种权力和义务。

3.2 初始身份的确认

3.2.1 证明拥有私钥的方法

颐信 CA 采用“双证书”体系，为每个证书订户产生签名证书和加密证书。

签名证书的密钥对是由订户的证书载体自行产生，而且签名私钥由载体保存，不会离开载体,公钥和订户的身份信息通过私钥签名后，一起传递到颐信CA 认证系统，认证系统需要对此签名信息以及订户的身份信息、公钥和私钥的正确性、合法性和唯一性进行验证，如果通过验证，则证明该用户拥有签名私钥，才能给订户签发证书。

加密证书的密钥对是由颐信 CA 的密钥管理系统产生的，当认证系统为用户签发“签名证书”时，自动到密钥管理系统申请用于数据加密的密钥对，并且给订户签发一个“加密证书”。由于此密钥对是由密钥管理系统产生的，公钥和私钥的正确性、合法性和唯一性已经通过密钥管理系统的验证，可以保证密钥对的安全。同时，此“加密证书”的密钥对还要在密钥管理系统中进行备份和归档保存。

3.2.2 组织机构身份的鉴别

对于组织机构身份的鉴别，颐信CA 需要严格验证该组织机构的合法证件。组织机构申请者身份的鉴别流程，会根据申请证书种类的不同而不同，颐信CA 可以按照

每种证书相应的要求进行不同的验证。如通过证明 e-mail 的有效性、查询可信的数据库验证真实性、面对面鉴别身份材料其它可以获得申请者明确的身份信息的方式等；相应的证书申请流程规定了不同的鉴别程序。证书申请表上有申请者本身或被充分授权的证书申请者代表的签字。

在申请组织机构证书时，申请者应指定证书申请代表，并对其合法授权，证书申请代表在证书的申请表上签字表示接受证书申请的有关条款，并承担相应的责任。颐信 CA 及其证书服务机构审核单位证书申请者的代表人是否符合要求。

对组织机构的身份鉴别按以下方式进行：

颐信 CA 或其注册机构、受理点等证书服务机构必须检查申请者所递交的文件，申请者需向颐信CA 提供单位或服务器确实存在的有效证明，包括但不限于工商营业执照、企事业单位组织机构代码证等；证明文件的复印件须加盖申请单位的公章，申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。颐信 CA 可以通过查询第三方数据库或咨询相应的政府机构等方式，来对申请者及其申请材料进行验证。颐信 CA 可以通过从第三方得到的电话号码等其他联络方式，用某种方式与申请机构进行联络以确认某个信息（例如，验证代理人的职位或者验证申请表中的某个人是否是申请人）。如果颐信CA 无法从第三方得到所有需要的信息，可要求第三方进行调查，或要求证书申请者提供额外的信息和证明材料。

如果颐信 CA 或其注册机构、受理点等证书服务机构已经预先明确了证书申请单位的身份，那么颐信 CA 和其授权的证书服务机构可以信赖申请者提供的证明。

组织身份的份鉴别，通常是通过现场鉴别的方式进行。对于包括邮递、传真、在线更新等非现场方式进行的身份鉴别，颐信 CA 将会要求申请者提供额外的身份鉴别资料和证明，通过电话、邮件、第三方调查、邮政地址调查、在线电子付款账户实名匹配验证、可信任第三方数据库等颐信 CA 以为合理的方式辅助进行鉴别。

颐信 CA 和其授权的证书服务机构在规定期限内保存组织机构的全部申请材料，这个规定期限由法律、政策、主管部门的要求或者颐信 CA 自行决定。

3.2.3 个人身份的鉴别

个人申请者身份的鉴别流程，会根据申请证书种类的不同而不同，颐信CA可以按照每种证书相应的要求进行不同的验证。如通过证明e-mail 的有效性、查询可信的数据库验证真实性、面对面鉴别身份材料以及其它可以获得申请者明确的身份信息的方式等；相应的证书申请流程规定了不同的鉴别程序。证书申请表上有申请者本身或被充分授权的证书申请者代表的签字。

1．证明e-mail 的有效性。通过审核和验证证书持有者的e-mail 地址真实存在性来识别和鉴定个人的身份。
2．查询可信的信息数据库。通过核对和证实可信的数据库内必要的个人特征,识别和鉴定个人身份。由颐信CA 来选择和决定可信的数据库，包括现存的颐信CA数据库和其它第三方的数据库。

3．面对面鉴定。个人申请者的识别和鉴别可以通过以下方法中的一种来进行：

颐信 CA 和其授权的证书服务机构将申请者本人和两份身份证明（原件和复印件）进行比较，对申请资料的原件和复印件真实性进行审核，身份证明文件必须是有效的中华人民共和国居民身份证、军官证、港澳台居民身份证、护照及外国人永久居住证等。

如果颐信 CA 或受理点已经明确确认申请者个人的身份，那么颐信CA 或其授权的证书服务机构可以信任现有的证明。

4、颐信 CA 提供个人证书在线更新身份鉴别，可以通过从第三方获取的信息来验证该申请者个人的身份，如果颐信 CA 无法从第三方得到所有所需的信息，可要求第三方进行调查或要求申请者提供额外的信息和证明材料。

申请者必须承担材料真实性的责任，颐信CA 和其授权的证书服务机构在进行了法律规定的有限审查以后，不承担对申请者的身份证明文件（如身份证等）进行合法性甄别的义务。

个人的身份鉴别，通常通过通过现场鉴别的方式进行。对于包括邮递、传真在线更新等非现场方式进行的身份鉴别，颐信 CA 将会要求申请者提供额外的身份鉴别资料和证明，通过电话、第三方调查、邮件、邮政地址调查、在线电子付款账户实名匹配验证、可信任第三方数据库等颐信 CA 认为合理的方式辅助进行鉴别。

批准申请后，颐信CA 或注册机构将保留复印件，并与证书申请表一并存档保存。

3.2.4 设备证书订户身份的鉴别

申请者提交设备证书请求文件，需要包含服务器签名公钥，颐信CA 不负责服务器签名公私钥对的产生。

如果证书名称为域名（或 IP 地址），申请者需提交相关证明材料确认服务器已经申请了有效的域名或IP 地址（加盖公章）。

申请者填写书面申请表（一式三份），经过单位授权代表的签署及单位盖章后，携带相关资料(同§3.2.2)到颐信CA 授权的发证机构进行身份审核及办理交费手续；颐信 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表面审查，并进行批准或拒绝的操作。

申请设备证书需要提供：a、证书申请表 b、公钥或CSR文件；c、营业执照副本复印件加盖公章；d、互联网接入合同或域名使用权证书及对应域名管理邮箱信息；

关于域名或IP的查询验证，域名管理邮箱可通过whois查询，也可以使用admin@domain.com等通用域名管理员邮箱。

查询whois的地址：http://www.domaintools.com/ 通过输入域名或者IP即查询！还可能会有反钓鱼审查。一般审核流程需要1-2个工作日即可。

申请者必须承担材料真实性的责任，颐信CA 和其授权的证书服务机构在进行了法律规定的有限审查以后，不承担对申请者的身份证明文件（如身份证等）进行合法性甄别的义务。

目前，颐信CA 主要通过第三种方式进行订户身份鉴别。对于包括邮递、传真、邮件等非现场方式进行的身份鉴别颐信 CA 将会要求申请者提供额外的身份鉴别资料和证明，通过电话、第三方调查、邮政地址调查、可信任第三方数据库等颐信CA 以为合理的方式辅助进行鉴别。

对于设备证书，颐信CA不提供在线更新设备证书的鉴别服务，设备证书更新需用户重新提交申请，颐信CA 或注册机构对设备证书更新订户进行查验与鉴别，鉴别要求同本CPS §3.2.2 及 §3.2.4。

批准申请后，颐信CA 或注册机构将保留复印件，并与证书申请表一并存档保存。

3.2.5 没有验证的订户信息

颐信 CA 不要求申请者提供 §3.2.2 、 §3.2.3 和 §3.2.4中规定的初始注册时必须提交的身份证明文件以外的其它信息。如果申请者提供了其它信息，颐信 CA 将不会验证，也不会保证这些信息的真实性和正确性，但可以以书面形式，与申请者必须提供的信息一并归档保存。

3.2.6 授权确认

为确保办理人具有特定的许可，代表组织机构获取数字证书，需要出具组织机构授权其为该组织机构办理颐信 CA 数字证书事宜的授权文件。颐信 CA 及授权的 RA 注册中心还需要审核申请代表人的身份和资格，并且可以通过电话等方式与其所代表的组织机构进行核实确认，以确定其是否真正获得了授权许可。

如果颐信 CA 经过调查，无法确认其是否确实获得了该组织机构的授权，可以要求申请者提供额外的准确信息，颐信 CA 和授权的 RA 中心也有权拒绝为该申请者办理数字证书。

3.2.7 互操作准则

互操作可能是交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的 CA 中心之间建立相互信任关系，从而使双方的订户可以实现相互认证。

颐信 CA 将根据业务需要，在遵循《电子认证业务规则》的各项控制要求的基础上，与颐信CA 证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。但交叉认证并不表示颐信 CA 批准了或赋予了其他 CA 中心或电子认证服务机构的权力。

颐信 CA 将严格按国家法规、政策在交叉认证方面的标准和要求执行。

3.3 密钥更新请求中的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

颐信 CA 颁发的证书有效期为一年（颐信 CA 也可以根据协议确定证书的有效期），订户的密钥有效期与订户数字证书有效期相同。在有效期即将结束前，订户需要重新更新证书，将重新产生新密钥对。证书订户持原证书载体可到颐信 CA或其注册机构填写《业务申请表》，由颐信CA 相应机构服务处理用户的密钥更新。

3.3.2 注销后密钥更新的标识与鉴别

对于注销后的证书，不对其进行密钥更新操作。订户必须重新进行身份鉴别和注册，并生成新的密钥对，向颐信 CA 申请重新签发证书。

3.4 注销请求中的标识与鉴别

如果订户本人申请证书注销时，其身份的标识和鉴别，使用与原始身份验证相同的流程，详见§3.2.2 组织机构身份鉴别和§3.2.3 个人身份鉴别。用户也可以通过

电话的方式向颐信 CA 或授权的 RA 注册中心申请注销，此时，颐信CA 或 RA中心先进行冻结操作，等完成对用户身份和申请的审核之后再正式注销。

如果是因为订户违反了本 CPS 的规定，或者是国家司法和其它主管部门要求注销某订户的证书，颐信CA 将按照相关程序进行审核并直接注销该证书。颐信CA可根据实际需要，向证书订户进行通报。

4 证书生命周期操作要求

证书生命周期的概念：证书生命周期包括数字证书申请、审核、签发、证书注销、证书更新、证书冻结、证书解冻、证书补办、查询、归档等维护工作的整个周期。

4.1 证书申请

颐信 CA 提供离线申请方式。根据订户申请的证书类型，颐信CA 采用不同的申请注册程序，但都应遵守证书申请操作所规定的步骤。

4.1.1 证书申请实体

证书申请相关实体有颐信 CA、颐信CA 授权的 RA 注册中心和证书受理点以及证书申请者，证书申请者包括个人和具有独立法人资格的组织机构（包括行政机关、事业单位、企业单位、社会团体、人民团体等）。

4.1.2 注册过程与责任

证书申请者根据申请的证书种类，按照颐信CA 的要求提交申请表格。申请表可以从颐信 CA 的网站下载或到颐信 CA 和其授权的证书服务机构领取。证书申请表格的填写内容，依照申请证书类型的不同而不同。

1、个人身份证书

颐信 CA 的个人身份证书是经颐信 CA 签名的包含个人身份信息的证书，它用于标志自然人在进行信息交换、电子签名、电子政务、电子商务等网络活动中的身份，并且保障信息在传输中的安全性和完整性，可以存储在 EKey 、IC 卡等介质中。

申请者申请个人身份证书，需要递交以下资料：

a) 申请者按照要求填写并签字的书面申请表

b) 个人身份证（或军官证、护照等其它有效的身份证明文件）原件和复印件；如果颐信CA 或受理点已经通过电话、邮递、第三方验证或者其他方式明确确认申请者个人的身份，申请人可以通过传真、邮递等方式递交身份证明文件的复印件，而不必递交身份证明文件的原件。

c) 如果是委托办理，需同时递交申请人和被委托人的上述证件及复印件，以及申请委托人亲笔签名的书面授权书。

2、机构证书

颐信 CA 的机构证书是经颐信 CA 签名的包含单位身份信息的证书，用于标志单位身份证书持有人在进行信息交换、电子签名、电子政务、电子商务等网络活动中的身份，颁发给企事业单位、政府部门、社会团体等各类组织机构。

申请机构证书，需要递交以下资料：

a) 申请者填写并签字盖章的书面申请表；

b) 申请者的企事业单位组织机构代码证的原件（正本或者副本）及复印件；

c) 申请者的营业执照原件（正本或者副本）及复印件，如果没有营业执照，则提供书面申请表上可选的其他有效证件原件（正本或者副本）及复印件；目前认可的有效证件如下：工商营业执照、事业单位法人登记证、税务登记证、组织机构代码证、社会团体登记证以及其他国家法律承认有效的证明文件。如果颐信 CA 或受理点已经通

过电话、邮递、第三方验证或者其他方式明确确认单位申请者的身份，申请人可以通过传真、邮递等方式递交证明文件的复印件，而不必递交证明文件的原件；

d) 受托申请人的身份证（或军官证、或学生证或护照等有效证明文件）原件与复印件

e) 申请者对受托申请人的书面委托授权书（需加盖公章）。

3、安全邮件证书，颐信 CA 的邮件证书是经颐信 CA 签名的，用于标志申请者电子邮件（E-mail）的身份。证书持有人可以在电子邮件中对信件内容进行加密和签名操作。

颐信 CA 没有义务也没有必要确认申请者提供的 E-mail 地址是否为申请者所有，只保证受理的申请者信息只能用于该E-mail 证书的申请，以及这些信息和该 E-mail 证书信息的对应关系。如果因为E-mail 归属而产生纠纷，颐信CA 不会也不应予以解决，颐信 CA 会根据有处理职能的相关部门的要求提供有关帮助，但这不是一种义务性的承诺。

安全邮件证书的申请者可以是个人或组织机构，邮件证书需要递交的资料与申办个人身份证书和机构证书的要求相同。

4、设备证书

（1）SSL 服务器证书，Web 服务器证书和网站的 IP 地址、域名绑定，它可以保证网站的真实性和不被人仿冒，通过在用户端浏览器和 Web 服务器之间建立 SSL安全通道，保证用户在网络通讯中的安全性。

申请 Web 服务器证书，需要递交以下资料：

a) 申请者填写并签字（或盖章）的书面申请表

b) 申请者（个人或组织机构）的身份证明材料原件和符合条件的复印件（具体要求同前述个人和单位证书的要求）。

c）申请者必须书面填写关于该域名（或者IP 地址）的归属性声明文件，以表明该域名（或者 IP 地址）属于申请者所有。

d）如果是委托办理，需同时递交申请者和受托人的身份证明文件及复印件，以及申请者亲笔签名的书面授权委托书。

（2）应用服务器证书，实现应用服务器的身份标识和应用的加解密、电子签名等。应用服务器证书可以存放在硬盘、IC 卡、加密机、加密卡等各类设备上。

申请应用服务器证书，需要递交以下资料：

a）申请者填写并签字（或盖章）的书面申请表

b）申请者（个人或组织机构）的身份证明材料原件和符合条件的复印件（具体要求同前述个人和单位证书的要求）。

c）申请者必须书面填写关于该应用服务器的归属性声明文件，以表明该应用服务器属于申请者所有。

d）如果是委托办理，需同时递交申请者和受托人的身份证明文件及复印件，以及申请者亲笔签名的书面授权委托书。

证书申请流程：

a）证书申请者携带相关证明到各注册机构或受理点，填写相关申请表，由注册录入员将申请信息录入系统。

b）各注册机构或受理点审核申请者的相关身份资料的真实性，如果身份鉴别未通过，将拒绝为用户发放证书，并将未通过的信息存档。

c）如果身份鉴别通过，各注册机构或受理点通过服务系统录入、审核证书申请信息，将信息递交给注册机构 RA，由其转交给 CA 认证机构。

d) CA 认证机构根据证书请求签发证书。

e) 各注册机构或受理点将签发的证书写入存储介质。

f) 各注册机构或受理点向证书申请者发放证书和密码信封等。
g) 申请者接受证书。

5、代码签名证书

颐信CA签发的代码签名证书为软件开发商提供了一个理想的解决方案，使得软件开发商能对其软件代码进行数字签名。通过对代码的数字签名来标识软件来源一级软件开发者的真实身份，保证代码在签名后不被恶意篡改。使用户在下载已经签名的代码时，能够有效的验证该代码的可信度。

申请代码签名证书，需要递交的资料与申办个人身份证书和机构证书的要求相同。

颐信 CA 在证书注册过程中的职责是：建设安全可靠的电子认证服务系统并保证其可靠运行，设立结构合理的证书注册机构，以及制订符合法律规定和产业政策的电子认证业务规则。

作为颐信 CA 授权的 RA 注册中心、证书受理点需要承担向订户说明证书办理流程、解释证书办理的要求、回答订户的各项咨询的职责，负责对证书申请人的身份进行鉴别，负责对申请者提供的证明文件进行检查和核实。

证书申请人需要按照本 CPS 的规范和要求，正确填写证书申请表，准备相关身份证明材料。证书申请者必须保证申请资料的真实性、准确性和完整性。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

颐信 CA 或授权的 RA 注册中心、证书受理点依照本 CPS 的规范，按照身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见 §3.2.2 组织机构身份鉴别、§3.2.3 个人身份的鉴别和§3.2.4 设备证书订户身份鉴别。

4.2.2 证书申请批准和拒绝

颐信 CA 或授权 RA 注册中心根据本 CPS 的规范，对证书申请人身份进行识别与鉴别后，将根据鉴别结果，决定批准或者拒绝用户的证书申请。

如果颐信 CA 或授权的 RA 注册中心批准证书申请，将会为证书申请人签发和制作数字证书。

证书申请人未能通过身份鉴别，颐信 CA 或授权 RA 注册中心将拒绝申请人的证书申请，并通知申请人。被拒绝的证书申请人可以在准备正确的材料后，再次提出证书申请。

4.2.3 处理证书申请的时间

颐信 CA 及授权的注册机构将尽快确认证书申请信息，注册机构收到所有必须的相关信息后，将在 24 小时之内处理证书申请。

注册机构能否在上述时间期限内处理证书申请，取决于证书申请人是否真实、完整、准确地提交了相关信息和是否能够及时响应颐信 CA 的管理要求。

4.3 证书签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

注册机构确认了用户的申请后，将录入用户的身份信息，并向颐信CA 上传证书申请信息。

颐信 CA 在接收到注册机构上传的证书申请之后，将会为用户签发证书，其中签名证书的公钥来自用户载体，加密证书的公钥来自密钥管理中心。证书的签发意味着电子认证服务机构最终完全正式批准了证书的申请。

4.3.2 电子认证服务机构和注册机构对订户的通告

电子认证服务机构通过注册机构对订户的通告有以下几种方式：

1．通过面对面的方式，通知订户到注册机构或受理点领取数字证书，注册机构把密码信封和证书等直接提交给订户，来通知订户证书信息已经正确生成；

2．通过电子邮件（e-mail）方式通知；

3．邮政信函通知；

4．其他颐信 CA 认为安全可行的方式。

4.4 证书接受

4.4.1 构成接受证书的行为

数字证书签发和制作完成后，注册机构将数字证书及密码信封和其它相关资料当面交给证书申请者，证书申请者从得到数字证书起，就被视同为同意接受证书。订户接受证书后，应妥善保管或及时更改与证书对应的 PIN 码。

4.4.2 电子认证服务机构对证书的发布

颐信 CA 在签发完证书后，最迟于 24 小时内将证书发布到目录服务器中。

颐信 CA 采用主、从目录服务器结构来发布所签发的证书。签发完成的数据直接写入主目录服务器中，然后通过主从映射，将主目录服务器的数据自动发布到从目录服务器中，供订户和依赖方查询和下载。

4.4.3 电子认证服务机构对其他实体的通告

其他实体可以通过目录服务器查询到颐信 CA 已经签发的数字证书。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户提交证书申请并接受颐信 CA 所签发的证书后，被视为已经同意遵守颐信 CPS 及其它与颐信 CA 相关实体签定的权益、责任和义务保护条款。订户接收数字证书后，应妥善保存证书及证书对应的私钥。任何人使用证书时都必须验证证书的有效性和合法性，包括证书是否被注销、是否还在有效期内、是否由颐信CA签发等。

在使用与颐信 CA 所签发的证书有关的签名及经过签名的信息时，参与方（颐信 CA、证书订户和依赖方等）按本 CPS 的规定享有相应的权利和应尽的义务。参与方均视为已被通知并同意遵守本 CPS 以及颐信 CA 与各方签署的协议、规范中条款。任何超出本 CPS 规定的证书及私钥的使用范围，颐信 CA 将不承担由此带来的任何后果。

颐信 CA 签发的各类证书，仅用于表明证书持有者在申请证书时所要标识的身份和验证证书持有者用该证书所对应的私钥做出的签名。这样，通过签名和签名验证，保证证书持有者的身份真实性、信息的完整性和行为的不可抵赖性。如果证书持有人将该证书用于其它目的，颐信 CA 将不承担由此产生的任何责任。

订户只有在接受了相关证书之后才能使用对应的私钥，只能在指定的应用范围内使用私钥和证书，并且在证书到期或注销之后，订户应停止使用该证书对应的私钥。

4.5.2 依赖方公钥和证书的使用

如果证书中的某些字段明确了证书的使用范围和用途，那么该证书只被允许在这一范围内进行使用。依赖方必须对此做出合理的判断，任何对超出证书所标明的适用范围的行为的信赖，都将由依赖人独立承担责任，颐信CA 对此不承担任何责任和义务。

依赖方获得对方的证书和公钥后，可以通过CRL 或 OCSP 服务器，对该证书进行有效性验证，获取对方证书的基本状况和对方的身份，并通过公钥验证对方电子签名的真实性。验证证书的有效性通常包括三个方面的内容：

1. 用颐信 CA 根证书验证颐信 CA 所签发证书中的颐信 CA 的签名，确认该证书是颐信 CA 签发的，并且证书的内容没有被篡改。

2. 验证证书的有效期，确认该证书在有效期之内。

3. 查询证书序列号是否在 CRL 列表中，或者查询证书状态，确认该证书没有进行注销、冻结等废止操作。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

4.6 证书更新

4.6.1 证书更新的情形

出现以下情形，经证书订户申请，颐信CA 及其授权的注册机构可以为订户更新证书：

1. 为保证证书及其密钥对的安全可靠，颐信 CA 颁发的证书有效期通常为一年，在证书的有效期即将结束时。

2. 证书订户的基本身份信息（关键信息）发生了变化，如果继续使用该证书，可能会对身份识别产生影响。

3. 证书订户的密钥出现问题。

另外，还有一种情况就是如果证书认证机构的主体信息、密钥、目录服务地址等发生变化，影响到对用户证书的认证时，需要电子认证服务机构主动对用户证书进行更新。

4.6.2 请求证书更新的实体

所有持有颐信 CA 和其授权的证书服务机构签发的证书订户，包括个人、企业单位、事业单位、政府机构、社会团体等各类组织机构等，在其证书的有效期未到前，由于证书有效期将到期或其它安全原因，均可以请求更新其持有的各类证书。

4.6.3 证书更新请求的处理

对于证书信息发生改变的订户，订户需采取离线更新的方式，需要订户亲自到证书注册机构办理证书更新。

对于证书信息未发生改变的订户，订户可以采取离线更新及在线更新两种方式。订户在线办理证书更新时，需订户在线填写更新请求，并需要按照颐信 CA 的要求，用当下的私钥对更新请求信息签名，交纳相应的费用，递交给发证机构，颐信 CA 注册机构在收到订户的更新请求后，对用户的身份信息和交费情况进行审核，审核通过后为其签发新的证书。订户既可在注册机构现场取得操作人员制作的新证书，也可以通过网络下载新的证书。

注册机构对申请证书更新的订户进行查验与鉴别，鉴别要求参考本 CPS 规范的§3.2.2 、§3.2.3和§3.2.4。

4.6.4 颁发新证书时对订户的通告

离线更新方式，对订户的通告有以下几种方式：

1. 通过面对面的方式，通知订户证书更新已完成，新证书已颁发；
2. 通过电子邮件（e-mail）方式通知；
3. 邮政信函通知；
4. 其他颐信 CA 认为安全可行的方式。

4.6.5 构成接受更新证书的行为

不管是证书订户提出的更新请求，还是电子认证服务机构主动进行的证书更新，当订户在注册机构面对面收到操作员制作的新证书，或者从网上成功下载新证书，即表示订户接受了新证书。

4.6.6 电子认证服务机构对更新证书的发布

颐信 CA 在签发更新证书后，最迟于 24 小时内将更新证书发布到目录服务器中，对外进行发布。

4.6.7 电子认证服务机构对其它实体的通告

其它实体可以通过目录服务器查询已经更新的数字证书。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

出现以下情况，需要进行密钥更新：

1．证书的有效期即将到期，需要进行证书更新。

2．密钥失效。

3．怀疑私钥泄漏或者被其他人窃取。

此外，凡是在颐信CA架构内部使用的证书，包括CA、RA、操作员的证书，到期后，必须进行证书密钥更新。

证书即将到期的订户，出于安全考虑，应尽量采取证书密钥更新，来获得新的证书。

4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体同§4.6.2。

4.7.3 证书密钥更新请求的处理

证书密钥更新请求的处理同§4.6.3。

4.7.4 颁发新证书时对订户的通告

颁发新证书给订户的通告同§4.6.4。

4.7.5 构成接受密钥更新证书的行为

正式接受密钥更新证书的行为同§4.6.5。

4.7.6 电子认证服务机构对密钥更新证书的发布

颐信 CA 对密钥更新证书的发布同§4.6.6。

4.7.7 电子认证服务机构对其他实体的通告

颐信 CA 在颁发证书时对其他实体的通告同§4.6.7。

4.8 证书注销和冻结

4.8.1 证书注销的情形

证书在有效期内，如果出现下列情况之一的（包括但不限于下面列出的情况），订户应当申请注销数字证书：

1. 怀疑数字证书私钥泄漏。
2. 数字证书中的信息发生重大变更。

3. 由于证书不再需要用于原来的用途而要求终止。

4. 认为本人不能履行或需要终止履行数字证书认证业务规则。

发生下列情形之一的，颐信 CA 可以直接注销其签发的数字证书：
1. 户申请注销数字证书。
2. 订户在申请注册时提供不真实的信息。
3. 订户没有履行双方合同规定的义务。
4. 数字证书的安全性得不到保证。
5. 法律、行政法规规定的其他情形。

4.8.2 请求证书注销的实体

只有证书订户本人或者其授权的委托代理人，以及电子认证服务机构及其授权的服务机构、法院、政府主管部门及其他公权力部门等，才有权力提出证书注销的请求。

4.8.3 注销请求的流程

证书注销请求的处理采用与原始证书签发相同的过程：

1. 证书注销的申请人到颐信 CA 网站下载或到颐信 CA 授权的注册机构书面填写《业务申请表》，并注明注销原因。

2. 颐信 CA 授权的注册机构根据§3.2 的要求对订户提交的注销请求进行审核。

3. 颐信 CA 注销订户证书后，注册机构将当面通知订户证书被注销，并在 24 小时内通过 CRL，向外界公布订户证书注销信息。

4. 强制注销是指颐信 CA 或授权的 RA 注册中心确认订户违反本 CPS 时，对订户证书进行强制注销，注销后将立即通知该订户，并在 24 小时内通过 CRL 向外界公布证书注销信息。

4.8.4 注销请求宽限期

如果出现私钥泄漏等事件，注销请求必须在发现泄漏或有泄漏嫌疑 8 小时内提出。其他注销原因的注销请求必须在48 小时内提出。如果在宽限期内，因订户未及时提出注销请求而产生的任何损失和责任，颐信 CA 并不承担。

4.8.5 电子认证服务机构处理注销请求的时限

发证机构接到注销请求后 24 小时内处理完毕，颐信CA 每日签发一次 CRL （24 小时生效），OCSP 即时生效，并将最新的CRL 发布到目录服务器和 OCSP 服务器指定的位置，提供下载和证书状态查询。

4.8.6 依赖方检查证书注销的要求

在具体应用中，依赖方必须使用以下两种功能之一来进行证书状态的查询：

LDAP 查询：利用证书中标识的LDAP 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。

在线证书状态查询（OCSP）：服务系统接受证书状态查询请求，并将查询结果经过签名后，返回给请求者。

注意:依赖方要验证CRL 的可靠性和完整性,确保是经颐信CA 发布并且签名的。

4.8.7 CRL 发布频率

颐信 CA 可采用实时或定期方式发布 CRL。发布CRL 的频率根据证书策略确定,一般为 24 小时定期发布。

4.8.8 CRL 发布的最大滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.8.9 在线状态查询的可用性

颐信 CA 提供 7*24 小时的在线证书状态查询服务。即在网络允许的情况下,订户能够实时获得证书状态查询服务。

4.8.10 在线状态查询要求

依赖方是否进行在线状态查询完全取决于应用的安全要求。很多应用本身建有用户帐户数据库并给予用户帐户进行应用控制,数字证书在此只起身份鉴别的作用,在这种情况下,在线状态查询不一定是必须的。对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用,依赖方在信赖一个证书前必须通过证书状态在线查询检查该证书的状态。

4.8.11 注销信息的其他发布形式

主要通过 X.509 V2 格式的 CRL 发布注销信息。除CRL 外,目前暂不提供其它发布形式。

4.8.12 密钥损害的特别要求

无论是最终订户还是颐信 CA、授权的注册机构，发现证书密钥受到安全损害时应立即注销证书。

4.8.13 证书冻结的情形

当证书仍然处于有效期，为了保留订户的证书使用权利，而不申请注销该证书，当出现下列情况时，可以进行证书冻结：

1. 证书订户要求暂停使用该证书一段时间

2. 订户未能履行与颐信 CA 签订的协议中应尽的义务，但向颐信 CA 和其授权的服务机构提出申请并获得批准后

3. 除证书订户（或者其授权的委托代理人）外的其他实体，如电子认证服务机构及其授权的服务机构、法院、政府主管部门及其他公权力部门，向颐信 CA 和其授权的服务机构提出冻结证书请求并获得批准

4.8.14 请求证书冻结的实体

只有证书订户本人或者其授权的委托代理人，以及电子认证服务机构及其授权的服务机构、法院、政府主管部门及其他公权力部门等，才有权力提出证书冻结的请求。

4.8.15 冻结请求的流程

首先是证书订户提出申请，再由注册机构核实申请者的身份，然后注册机构实施证书冻结操作。

4.8.16 冻结的期限限制

实施证书冻结操作后，证书一直就处于冻结状态，直至订户发出其它申请，如证书解冻或者证书注销等。

如果订户没有发出下一步申请，到证书有效期结束后，自动注销该证书。

4.8.17 冻结证书的恢复

证书冻结原因消除以后，订户打算继续使用该证书，并且证书还处在有效期以内的，订户可以申请解冻证书，使其成为有效且可用的证书。

4.9 证书状态服务

4.9.1 操作特征

颐信 CA 通过目录服务器和 OCSP 服务器为订户和依赖方提供证书状态查询服务，包括 CRL 查询和 OCSP 查询。

4.9.2 服务可用性

颐信 CA 提供 7*24 小时的 CRL 列表下载和 OCSP 查询服务。即在网络允许的情况下，订户能够实时获得证书状态查询服务。

4.9.3 可选特征

除了 CRL 列表下载、LDAP 查询和 OCSP 在线证书状态查询以外，颐信CA 暂时不提供其它证书查询方式。

4.10 订购结束

订购结束是指当证书有效期满或证书注销后，该证书的服务时间结束。

订购结束包括以下两种情况：

1.证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户可以终止订购；

2.在证书有效期内，证书被注销后，即订购结束。

一旦用户在证书有效期内终止使用颐信 CA 的认证服务，颐信 CA 在批准其终止请求后，将实时把该订户的证书注销，并按照 CRL 发布策略进行发布。

4.11 密钥生成、备份和恢复

4.11.1 密钥生成、备份与恢复的策略与行为

订户的签名密钥对由订户的密码设备（如智能 USB KEY 或智能 IC 卡）生成，加密密钥对由密钥管理中心生成。

签名密钥由订户的密码设备产生和储存，颐信CA 不负责用于签名的私钥的保管和恢复。

密钥恢复是指加密密钥的恢复。密钥恢复分为两种情况：订户密钥恢复和司法取证密钥恢复。

1．订户密钥恢复：当订户的密钥损坏或丢失后，某些密文数据将无法解密还原，此时订户可申请密钥恢复。订户在颐信 CA 授权的注册机构申请，经审核后，通过颐信 CA 向密钥管理系统提出请求；密钥恢复模块接受订户的恢复请求，恢复订户的密钥并下载于订户证书载体中。

2．司法取证密钥恢复：司法取证人员向密钥管理中心申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

具体策略在§6.1 和§6.2 中详细描述。

4.11.2 会话密钥的封装与恢复的策略与行为

会话密钥的封装采用数字信封技术，发送者使用信息接收者的公钥对会话密钥进行加密，接收者用自己的私钥解密而获得会话密钥。

颐信 CA 并不保管和储存用户的会话密钥。

5 认证机构设施、管理和操作控制

颐信 CA 机构设施符合国家相关规范和标准，所有作业人员均经过严格审查和考评，满足任职要求，且人员控制管理严格，只有经过授权的操作人员，才可以根据有关的安全操作规范进入相应的管理区域进行操作；操作过程规范有序，操作行为会有记录日志，所有这些为开展电子认证服务业务打下了坚实可靠的基础。

5.1 物理控制

颐信 CA 位于安全可靠的建筑物内，满足防火、防水、抗震等安全要求。核心机房采用全电磁屏蔽机房，达到屏蔽机房最高等级标准，主要安装核心的证书认证系统。在主机房外还部署了各类配套设施和监控系统。

颐信 CA 的主机房（屏蔽机房）是专门针对电子认证服务业务高安全性要求设计的，严格按照电信级机房的标准施工，采用防静电地板，机柜统一接地，全部固定在楼板中，有特殊的消防、监控及入侵检测设备。在电力、空调、门禁和防火设施方面达到了电信级机房的标准。工作人员进入机房必须经过电子（磁卡）及生物（指纹）验证，并制定了严格门禁安全管理策略。

5.1.1 场地位置、设计标准和环境条件

颐信 CA 位于北京市朝阳区万红西街 2 号燕东大厦 B 座四层，依据敏感程度的不同整个区域由低到高划分为 7 个物理安全区域，第一区、第二区和第三区为初级敏感区，第四区为敏感区，第五区、第六区和第七区为高度敏感区。

颐信 CA 每个安全区域入口通过不同颜色标识：灰色（一区：大厅）、蓝色（二区：市场部）、紫色（三区：系统部办公区、研发部办公区、会议室）、绿色（四区：管理区）、黄色（五区：服务区）、橙色（六区：过渡区、七区：CA/KM 核心区）。

主机房是全屏蔽机房，面积约为 110 ㎡，根据证书系统的不同功能模块，又分隔为核心区、过渡区、服务区、管理区等四个部分。核心区包括 CA 机房和 KM机房，CA 机房放置证书签发系统及主 LDAP 和 OCSP 系统， KM 机房放置密钥管理系统，KM 审计管理终端；服务区放置RA 注册系统及从 LDAP 和 OCSP 系统，CA 审计管理终端；管理区放置审计管理终端及安全监控系统。

机房的安装、装修设计遵循国家相关标准和技术规范。

5.1.2 物理访问

颐信 CA 根据七道不同安全等级的门禁划分为不同的安全区域，通过门禁系统及其它管理措施严格控制人员的进出。针对物理场地的访问和管理，颐信CA 专门制定了《颐信CA 场地访问管理办法》、《颐信数字证书认证中心门禁管理条例等访问控制条例。

外部人员必须经过相关主管领导批准，由指定专人陪同才能进入。内部人员根据部门和职责的不同，必须利用门禁卡才能进入到规定的区域。客户接待区和市场部、技术部、系统部等办公区域采用感应卡识别模式门禁，工作人员只能进入各自相应的部门区域，主机房的管理区和服务区只有系统部管理人员才能进入，而过渡区采用双人感应卡识别模式门禁，核心的 CA 室和 KM 室采用双人感应卡加指纹识别模式门禁，必须至少两名具有权限的管理人员在场才能进入。所有授权人员的进出，门禁系统都会有相应的记录。

5.1.3 电力与空调

（1）电源供电系统

电源供电系统按照供配电设计规范，采取高标准设计和高标准建设，确保提供纯净、无谐波干扰、不间断的稳定电源，保证机房所有系统设备和配套设施能够安全和可靠地不间断运行。另外，还考虑了预留备用容量，能充分满足未来系统扩充和业务拓展所需要的电力。

主机房（屏蔽机房）采用两路电源供电，一路为三相市电（380/220V 三相五线制），另一路为自备105KW 康明斯伟力 DY105C 型柴油发电机。两路电源均接至自动

切换配电柜，自动切换配电柜实时检测供电状况，自动完成电源的切换工作，确保机房电源供应不中断。

自动切换配电柜再给 50KVA 大容量在线 UPS 供电，由 UPS 通过低压配电柜向屏蔽机房中的系统设备、辅助设备、空调、照明等设施提供高质量的电源。

（2）空调通风系统

颐信 CA 屏蔽机房的空调系统分两种类型：

一种是专业精密空调，采用意大利海洛斯 Hirose 公司模块化机房专用空调8LU，为 KM 室和 CA 室提供恒温恒湿的洁净空气。该精密空调采用全封闭防尘、防静电设计，采用上送风、下回风的方式，保证核心机房内恒温、恒湿，空气清新。

第二种是普通空调，为主机房服务区和管理区提供恒温恒湿环境。

5.1.4 水患防治

颐信 CA 机房在进行装修时也考虑了水患防治，机房内没有任何给、排水管线，也没有任何水源储存设备。装修材料选用防水产品，门窗进行密封处理。机器设备均放置在机柜之中。通过采用这些处置措施，能够彻底防止水患侵害。

5.1.5 火灾防护

颐信 CA 的普通办公区域，由燕东大厦统一安装有消防报警系统，采用高灵敏度的温度、烟雾感应探头，保证第一时间发现火灾事故。同时，各房间配置有相应的消防灭火器具。

在主机房（屏蔽机房）内设有专业的气体消防报警灭火系统。在屏蔽室顶部，通过消防过壁装置，引入温感、烟感双路感应报警和监控信号，并设置消防气体喷头。根据屏蔽室的面积和高度，在两个屏蔽室内各设置一个温感报警器和一个烟感探头，通过火灾报警传递器引到值班室，与独立火警主机相连，当温感、烟感探头同时报警时，气体消防灭火系统启动，消防气体喷头自动在屏蔽室内喷射灭火气体。

其它火灾防护措施还有：机房装修时所有材料均采用不可燃材料；成立专门的消防小分队，定期检查消防设施，定期查检消防制度的落实情况，从而彻底消除火灾隐患。

整个消防系统和管理措施经过了公安消防部门的检验，并颁发了合格证书。

5.1.6 介质存储

颐信 CA 的各种存储介质包括硬盘、磁带、光盘等，处在防磁、防静电干扰的环境中，得到了安全可靠的保护，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。并由专人管理，受访问控制策略的保护，只有授权人员可以访问。

5.1.7 废旧物品处理

按照规定，颐信CA 认证系统使用的硬件设备、存储设备或其它重要配件等，在确认废弃不再使用时，需要由专人保管，定期集中统一销毁，确保敏感信息和机密信息不被泄露。

对于过期或作废的纸质文档、资料等，定期进行清理，集中销毁。

所有销毁行为必须履行手续，登记造册，以备日后检查核对。

5.1.8 异地备份

颐信 CA 对认证系统的数据库核心数据，采用同城异地的方式进行备份，为此，专门制定了异地备份管理制度。按规定每月由专人将完全备份的备份介质送到同城异地专用的保险柜中保存。

5.2 程序控制

5.2.1 可信角色

颐信 CA 中有权管理、配置、使用或操作认证系统（包括其中任何部分或其附属系统），能够完成系统的维护、管理、设置、审计或者是完成证书的证书新办、证书更新、证书注销、证书冻结、证书解冻，证书补办等操作的所有员工、合约人或者顾问人员，在本 CPS 中均视作可信角色。

颐信 CA 的可信角色包括：

信息安全管理委员会

备份根密钥管理人员

CA 管理小组
CA 超级管理员
CA 审计管理员
CA 业务管理员
KM 管理小组
KM 超级管理员
KM 审计管理员
KM 业务管理员
KM 业务操作员
RA 管理小组
RA 超级管理员
RA 审计管理员
RA 业务管理员
RA 业务操作员

根据本 CPS 和其它授权协议，颐信 CA 授权的下级 RA 中心或代理 RA 中心的 RA 管理小组人员均视为可信角色，必须接受本 CPS 和其它相关政策的约束。

5.2.2 每项任务需要的人数

颐信 CA 根据任务的性质和重要程度不同，每项任务分配的人员是不同的。为了保证系统的安全，任何一个人都不可以完成所有的任务，每个角色都有明确的分工，而且相互牵制和相互监督。

颐信 CA 信息安全管理委员会由 5 人组成，主要负责颐信CA 安全策略的制订、监督执行、安全事件的处置，每人管理一个根密钥的备份卡。

颐信 CA 的根密钥用 LaGrange 插值多项式构造一个（3，5）门限方案，将密钥分割成 5 个成份，分别加密存放在五个备份 USBKEY 上，任意 3 个成份(即 3 个备份 USBKEY)就可以通过 CA 系统恢复密钥。颐信CA 的根密钥采用 3of5 的管理策略，即根密钥由 5 人共同管理，必须至少 3 人以上在场才能完成恢复、更新、废止根密钥的任务。

证书业务操作员分成用户信息录入、用户信息审核和证书制作三种不同的角色，包括录入员、审核员、制证员，一般每个证书受理点需要配置 3 人，每人担任不同的角色。

CA 管理小组包括 CA 超级管理员、CA 业务管理员、CA 审计管理员 3 类不同的角色，每人只能担任一种角色，不能兼任。

KM 管理小组包括 KM 超级管理员、KM 业务管理员、KM 审计管理员、KM 业务操作员 4 类不同的角色每人只能担任一种角色，互相不能兼任。

RA 管理小组包括 RA 超级管理员、RA 业务管理员、RA 审计管理员、RA 业务操作员 4 类不同的角色每人只能担任一种角色，互相不能兼任。

CA 管理小组、KM 管理小组、本地RA 管理小组主要由颐信 CA 系统部人员担任。而远程 RA（颐信 CA 授权的下级 RA 中心或代理 RA 中心）管理小组人员可以根据业务需要由远程 RA 中心人员担任。

5.2.3 每个角色的识别与鉴别

颐信 CA 各安全区域的进入，都需要门禁卡及指纹的识别，所有能够完成系统管理、操作、审计以及可以颁发用户证书的可信角色，都需要配发以EKEY 为载体的数字证书，可信角色凭数字证书实现身份的识别和鉴别，只有正确通过识别的角色，才能登录到系统中，完成自己相应的任务。所有可信角色的操作都会在系统中形成系统日志，以备日后检查和审计。

5.2.4 需要职责分割的角色

颐信 CA 的安全策略就是要保证不能有任何一个人能够完成所有的任务，角色之间可以相互牵制和监督。重要任务，如根密钥的管理、管理员卡的制作、密钥恢复操作等，必须由多人共同承担，只能多数人同时在场才能完成这样的任务。

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，任何证书生命周期操作都要由注册、审核、签发 3个可信角色来完成。系统管理员、业务管理员、系统审计员、密钥管理员分别由不同的可信人员担任，进行权限与职责分割，共同完成对电子认证系统的管理。

5.3 人员控制

5.3.1 资格、经历和无过失要求

由于 CA 的安全性要求较高，所以其工作人员必须具有相应的任职资质、安全意识和业务技能，颐信CA 对所有员工都必须经过严格审查，然后进行相关PKI/CA认证技术的培训，经考核合格后，方能录用。员工与公司要签署工作合同和保密协议。

5.3.2 背景审查程序

颐信 CA 员工的录用必须履行严格的程序。

首先由用人部门提出申请，由人事管理部门进行初选，包括应聘者的工作履历、社会背景、思想道德状况，对其可靠信程度进行评估，对重要岗位人员可安排到原单位走访调查。初选合格者再安排业务部门进行业务素质考核。对考核合格者再安排不少于 3 个月的试用。重要岗位的至少需要在公司工作一年以上，核心岗位的员工需要在公司工作两年以上。根据需要，颐信CA 会对员工定期和不定期进行履行职责情况进行综合考核，并根据考核情况进行合理调配。

颐信 CA 对于下级 RA 中心或授权 RA 中心的关键员工进行同样要求，需要进行思想道德水平和工作业务能力进行综合考核，从而保证整个认证体系的安全可靠。

5.3.3 培训要求

颐信 CA 根据政策和业务的需要以及员工的实际情况，合理安排培训。

培训内容主要包括以下几个方面：

1. 国家的法律、政策以及行业的发展动态；

2. 电子认证技术的进步和发展以及数字证书的应用技术；

3. 公司安全管理和保密制度；

4. 市场业务技术和客户服务能力；

5. 个不同职能岗位的具体岗位内容培训。

对于培训工作，由颐信 CA 人事行政部制定计划，统一组织和实施，并保留完整的培训档案。

5.3.4 再培训周期和要求

颐信 CA 根据政策要求以及运营策略调整等情况，至少每半年对市场部、客服务部进行一次法规政策、相关技术、业务技能以及安全管理等方面的培训。对于系统部系统运行管理人员则根据实际情况，如认证系统更新升级、新的应用系统投入使用、密码和认证技术发展等，都需要根据实际情况及时安排培训。

5.3.5 工作岗位轮换周期和顺序

颐信 CA 会根据工作的需要、人员的业务技能和性格等综合情况，对工作人员进行合理调配。

在系统部内部，根据工作需要和人员变动情况，可能需要对人员工作岗位进行轮换。

5.3.6 未授权行为的处罚

颐信 CA 不论是系统管理操作，还是系统运营操作（如证书颁发），业务人员都必须具有相应的证书才能完成操作，对于某些特别重要操作，还专门规定必须至少两人同时进入现场，相互监督完成工作，并且所有操作都会在系统日志中保留痕迹，通过日志审计，能够发现操作人员进行了哪些操作。因此，在颐信 CA，一般不可能发生未授权操作行为。

当一旦发现工作人员进行未授权操作行为，将立即终止该员工所有的系统管理和操作权限，禁止该员工进入系统运行环境，并视情节严重程度进行适当处理，若严重损害颐信 CA 和客户利益，将根据法律和颐信 CA 的相关政策，提交司法机构处理。

5.3.7 独立合约人的要求

颐信 CA 对于不属于CA内部的工作人员，但从事CA有关业务的人员等独立签约者（如注册机构的工作人员），CA机构的统一要求如下：

a)正规劳务公司派遣人员；

b)具有相关业务的工作经验；

c)必须接受CA的岗前培训。

5.3.8 提供给员工的文档

颐信 CA 给员工提供其业务工作所需的所有文档、资料，并要求其妥善保管。系统部门员工的文档包括：系统运行维护手册、系统备份手册以及应急处理和灾难恢复手册等；

市场部、客服部员工的文档包括：产品技术方案、产品白皮书等。

研发部门员工的文档包括：证书应用接口开发手册等。

5.4 审计日志程序

5.4.1 记录事件的类型

颐信 CA 必须记录与认证系统相关的事件。这些记录，无论是采用纸质的或者是电子的，必须包含事件日期、事件时间段、事件内容、事件相关的实体等。包括：

1．证书订户服务申请和注销的信息，如申请表、协议、身份资料和其它相关信息等。

2．认证系统自身密钥的生成、变更等记录。

3．认证系统日常运行产生的日志记录文件。

4．进出颐信 CA 控制区的申请表格和相关记录，机房工作日志、系统日常维护记录、录像监控信息等。

5．系统软硬件设备的更换、安装、拆除和变化等。

6．认证机构、注册机构和受理点之间的协议、规范和相关工作记录。

7、。其它与认证系统相关的事件，如物理通道的参观、设备维护保养以及人事变动等信息。

5.4.2 处理日志的周期

颐信 CA 对系统运行、证书发放方面的记录每月审计一次。

系统值班日志每月审计一次。

监控录像信息系统自动保存三个月，对于重要活动录制成光盘长久保存。

客户信息资料每季度检查一次。

5.4.3 审计日志的保存期限

用户信息资料在用户证书失效后至少继续保存 5 年。

系统运行日志保存 1 年，故障处理情况保存 3 年。

5.4.4 审计日志的保护

颐信 CA 执行严格的分级分类管理制度，确保只有授权的人员才能接触这些审计记录。这些记录处于严格的保护状态，并且关键数据信息采取异地备份，严格禁止未授权的人员接触、阅读、修改和删除审计日志记录。

5.4.5 审计日志备份程序

颐信 CA 保证所有的审计记录和审计检查都按照颐信 CA 备份标准和程序进行。根据记录的性质和要求，定期备份，采用在线和离线方式进行备份。

5.4.6 审计收集系统

颐信 CA 审计收集系统涉及以下几个方面：

证书签发系统；

密钥管理系统；

RA 注册系统；

网站、数据库安全保障系统；

系统安全防护系统；

网络和操作系统部分；

其它有必要审查的部分。

5.4.7 对导致事件实体的通告

在认证系统运行中出现影响安全控管措施的时候，必须通知安全管理人员，并及时采取紧急应对措施。

颐信 CA 进行系统安全审计，如发现有安全攻击行为时，在法律和技术许可的前提下追溯攻击者，根据攻击者的行为和造成的后果，采取包括切断对攻击者开放的服务、提交司法机构处理等措施。是否通知攻击者，由颐信 CA 自行决定。

5.4.8 脆弱性评估

在认证系统运行时，应该从内部和外部对系统潜在的风险和威胁进行评估，并根据日志的审计情况和监督情况，及时调整和升级与系统运行密切相关的安全控制策略，以便将系统的运行风险降低到最低程度。

5.5 记录归档

5.5.1 归档记录的类型

颐信 CA 对以下记录归档保存：

1. 颐信 CA 的认证系统建设和升级文档。

2. 颐信CA 的认证系统自身密钥对的生成、内置、变更等成功和失败的纪录。

3. 颐信 CA 的认证系统日常运行产生的日志记录文件。

4. 证书申请信息、证书服务审批记录、与证书订户的协议、证书等。

5．颐信 CA 的认证系统和证书服务的审计数据、认证系统密钥升级和更新信息等。

6．进出敏感区域的纪录、机房工作日志、系统日常维护记录、录像带监控录像等。

7．系统软硬件设备更换、安装、拆除、变化等的纪录。

8．电子认证服务规则、证书策略、服务规范和动作协议等。

5.5.2 归档记录的保存期限

除法律法规和电子认证服务主管机构规定的保存期限外，颐信CA 制定的有关归档记录保存期如下：

1．电子认证服务业务规则、用户申请信息表格和相关协议、订户的申请、更新、注销、挂起的证书和过期证书，至少保存到证书有效期结束后 5 年。

2.证书用户的申请、查询、注销证书的服务记录，至少保存到证书有效期结束后 5 年。

3．订户证书和密钥的相关变动信息，至少保存 5 年。

4．认证机构的证书和密钥，以及变动的相关信息，至少保存 20 年。

5．在不违反法律法规和有关政策的前提下，可以与证书用户协商确定归档记录的保存时限。

5.5.3 归档文件的保护

归档文件既有物理安全措施的保证，也有密码技术的保证，以保证归档文件能够长期有效保存。存档文件以物理隔离或逻辑隔离的方式保存，只有经过授权的业务人员按照特定的安全方式才能接触和获取。除了法律和认证操作规范的需求，任何人不得获得。

颐信 CA 保存的申请者和证书订户的基本信息资料和身份鉴别信息，除非经过政府主管机构或具有特殊权力的司法机构经过合法途径予以申请，任何无关的第三方均不能获得相关资料。

5.5.4 归档文件的备份程序

颐信 CA 的归档文件备份程序按照颐信 CA 相关政策和策略规定执行：

首先由相关部门进行整理，经审计无差错后，提交信息安全总监签批，然后再采取适当的安全措施进行保存。档案介质采用物理安全方式进行保护，并且保留严格限制的权限和口令，只有相关的业务管理员可以访问。

当系统因为异常情况导致无法正常运营时，按照颐信CA 的灾难恢复策略，利用这些归档保存的数据进行系统的恢复。

5.5.5 记录时间戳要求

颐信 CA 的归档文件和记录，都有时间标识，有些是系统自动记录，有些可以是业务人员手动增加。

5.5.6 归档收集系统

颐信 CA 的归档文件和资料，全部由颐信 CA 内部工作人员或者是内部的管理系统，按照预先约定的程序，手动或自动产生和收集，并由具有相关权限的人员进行管理和分类。

5.5.7 获得和检验归档信息的程序

颐信 CA 归档文件或资料由专人进行保管和保存，按照要求，定期要对归档文件和资料进行检验和清理。内部工作人员如果需要使用归档文件和资料，只有在具有正当和合法的使用要求时，经过主管领导批准并履行合法手续后，才能获得和使用。

5.6 电子认证服务机构密钥更替

颐信 CA 的根密钥在 CA 系统初始化时由加密机生成，根私钥以加密的形式保存。为了保证系统安全性，采用秘密共享算法进行分散安全保管与m/n 恢复机制，颐信 CA 是采用“3 of 5”的原则，将根密钥通过一定的算法分割成五个部分，分别加密存放在五个智能密码钥匙——根备卡中。通过其中任意三个根备卡都能合成根密钥，可以用来签发/撤销特权卡、安全审计员卡和恢复根密钥。

颐信 CA 的根证书有效期截止到2033年3月22日，在证书到期前，颐信CA 将对根证书进行更新，为了保证根证书的更新不影响认证机构的正常运行，颐信CA 采取以下方式进行更新：

首先由根 CA 生成新的密钥对，生成新根证书，然后分别使用新证书（ new）和老证书 (old)进行互签，生成 New With Old、Old with New、New with New，连同原来的 Old With Old 共四种证书持有状态，一并通过 LDAP 服务器发布。证书认证系统根据用户的持有根证书的状态，选取相应的认证方式。

5.7 损害和灾难恢复

为了在出现异常或灾难情况时，能够在最短时间内重新恢复认证系统的运行，颐信 CA 制订了可靠的灾难恢复计划和应急管理办法。

5.7.1 事故和损害处理程序

颐信 CA 认证系统遇到攻击，发生通信网络资源毁坏、计算机设备系统不能正常提供服务、系统被破坏、数据库系统被篡改等灾难时，颐信CA 将按灾难恢复计划实施恢复。具体可参见颐信 CA 灾难恢复管理办法。

5.7.2 计算资源、软件和/或数据的损坏

当认证系统使用的数据或其它信息出现异常损坏时，可以依照颐信CA 的系统备份与恢复操作手册，根据系统内部备份的资料，或者异地备份的资料，执行系统恢复操作，使认证系统能够尽快重新正常运行。

当认证系统使用的硬件设备出现毁坏时，可以依照颐信CA 的系统备份与恢复操作手册，启动备份硬件设备以及相关的备份操作系统和认证系统，重新恢复系统运行。

5.7.3 实体私钥损害处理程序

颐信 CA 的根私钥出现损毁、遗失、泄露、破解、被篡改，或者有被三者窃取时，颐信 CA 应该：

1. 立即向电子认证服务管理办公室和其它相关政府主管机构报告，并立即注销所有已经签发的证书，更新 CRL 和 OCSP 服务信息，供证书订户和依赖方查询。同时，立即更新生成新的根密钥，并自签发新根证书。

2. 新根证书签发后，按照本 CPS 关于证书签发的规定，重新签发下级证书。

3. 新根证书签发后，立即通过颐信 CA 信息库、目录服务器和其它方式进行发布。

证书订户的私钥出现遗失、泄露、破解、被篡改、或者是怀疑可能被第三方窃取时，订户按照本 CPS 的规定，首先提出证书注销，并按照规定重新申请新证书。

5.7.4 灾难后的业务连续性能力

为避免由于突发灾难造成的业务停顿，颐信CA 制订了一套完整的异地业务恢复计划，并且，根据需要每年至少开展一次灾难恢复计划演练，并根据实际情况的变化，及时更新恢复计划和灾难恢复文件，并保存相应的归档记录，从而保证在出现灾难时，颐信 CA 认证系统能够在 24 小时内恢复系统的运行和提供认证服务。

5.8 电子认证服务机构或注册机构终止

如果颐信 CA 因故计划终止服务和经营，颐信 CA 会按相关的法律规定，向主管部门报告，并按规定程序进行操作。

1．在法律规定的期限前，向主管部门、证书持有者和其它相关实体进行及时通告。

2．按照规定，安排业务承接。

3．认证服务相关运营资料，包括证书、用户信息、系统文件、CPS、规范和协议等。

4．停止有关的运营服务。

5．清除系统根密钥。

当颐信 CA 授权的证书服务机构因故终止服务时，颐信 CA 将按照与其签定的相关协议处理有关业务承接事宜和其它事项。

6 认证系统技术安全控制

颐信 CA 证书认证系统采用双密钥、双证书体系，任何证书订户都有两对密钥，分为签名密钥对和加密密钥对，密码设备采用经过国家商用密码管理局鉴定的产品，密码算法采用国家商用密码管理局指定的算法。

6.1 密钥对的生成和安装

密钥对是电子签名安全的关键，颐信CA 对密钥对的产生、管理、传输都制定了特殊规定和要求，以保证密钥对的安全性、唯一性和完整性。

6.1.1 密钥对的生成

1、颐信 CA 根密钥的产生

颐信 CA 根密钥对是由国家商用密码管理局鉴定和许可的密码设备生成的。

颐信 CA 的顶级根密钥对在 CA 初始化时首先生成的，在这个过程中，保证必须至少 3 名具有权限的密钥管理和操作人员在场，同时操作加密机完成根密钥的产生。任何人无法单独完成根密钥的产生。私钥在加密机中保存，通过专用 3/5密钥分隔算法，把备份出来的根密钥（由密码机同步密钥加密）分隔成不同的 5份根密钥备份 USBKEY，根密钥备份 USBKEY 用于保存根密钥任意 3 份就可以恢复完整密钥。应用中任何与私钥有关的签名运算操作都在加密机内部进行，私钥不能以明文或者密文的方式输出到加密机外。

颐信 CA 数字证书升级系统生成二级根密钥操作是在二级 CA 初始化时完成的，会提示要求生成根密钥。根密钥备份USBKEY 管理人员数量也在系统初始化时指定（可为 1、3、5），目前系统中设置为5 个。生成二级根密钥操作具有非常高的安全要求，操作时必须三人以上同时在场。颐信 CA 二级根密钥的生成是 CA 服务器端的应用程序驱动密码机在密码机内部生成，保存在密码机加密模块中，通过专用 3/5 密钥分隔算法，把根密钥（由密码机同步密钥加密）安全导出通过数字信封技术加密后传送到 CA 管理端（线路加密使用CA 管理端 USBKEY 临时产生的加密密钥制作数字信封），根密钥数字信封下传到CA 管理端后 CA 管理端调用 USBKEY解密后将根密钥按 LaGrange 插值方式拆成五份，备份到十个 USBKEY 中（每一份均做一次重复备份）整个过程不落地。应用中任何与私钥有关的签名运算操作都在加密机内部进行，私钥不能以明文或者密文的方式输出到加密机外。CA 根密钥是整个 CA 系统的信任源，对 CA 根密钥的保护关系到整个 CA 系统的安全。颐信 CA 升级版证书认证系统采用"签名运算在密码机内部执行及密钥分隔备份与恢复管理机制“二项主要措施来保护 CA 根密钥。

2、证书订户签名密钥对的产生

每个证书订户，可以自主选择国家商用密码管理局批准许可的设备生成签名密钥对，如加密机、加密卡、USB KEY、智能 IC 卡等产品。用户在选择这类产品和设备时，应事先咨询颐信 CA 有关系统的兼容和接受事宜，颐信 CA 并不承诺接受所有此类密码产品和设备。

为了保证签名私钥的唯一性，颐信 CA 不为证书订户生成签名密钥对，因此，证书订户的签名私钥都是通过证书载体在客户端产生的，用户必须进行安全、可靠的保存，防止此密钥的遗失、泄露。如果因客户的保管不慎，造成用户签名私钥被盗用，颐信 CA 不承担任何责任和义务。

3、证书订户加密密钥对的产生

证书订户的加密密钥对是由颐信密钥管理中心产生，通过密钥管理中心的密钥生成服务器控制随机数发生器产生随机数序列，经强素数生成算法可按需求生成RSA 1024比特长度密钥对、RSA 2048比特长度密钥对和SM2 256比特长度密钥对，在验证密钥对正确性后将密钥对加密保存在备用密钥库中作为证书订户加密密钥对的来源。当CA 向 KM 申请加密密钥对，KM 从其备用库中取一公私钥对放入在用库中，同时对该密钥对解密使用用户签名公钥重新制作数字信封发给 CA 通过安全的通道最后传递到客户端，下载到客户的证书载体中。加密钥对在颐信 CA 密钥管理系统中进行备份保存。

4、证书订户必须承担保护私钥安全的责任和义务，并承担由此带来的法律责任。

6.1.2 私钥传送给订户

由于加密密钥对于数据加密的重要性，且加密密钥必须通过网络在密钥管理中心、CA 中心和用户终端间传送，所以必须采取严密措施确保加密密钥对的安全传送（包括保密性、完整性和不可抵赖性）。在物理结构中使用了两个网段，一个是用于密钥管理系统内部通信的通道，另一是为外界提供服务的通道。

CA 签名服务器通过专用网络与密钥管理系统连接，并通过防火墙进行隔离。认证系统向密钥管理系统申请密钥，以及 KM 向 CA 发送密钥是按安全协议进行不落地传送的。KM 把加密公/私密钥数字信封发送给 CA，CA 验证 KM 证书，取出公钥，签发加密证书，然后把签名证书、加密证书、加密私钥数字信封打包送给客户端。

具体过程：认证系统 CA 签名服务器向 KM 密钥管理系统申请加密密钥对，KM 从其备份库中取一公私钥对放入在用库中，同时对该密钥对脱密使用用户签名公钥重

新制作数字信封发给 CA 签名服务器，CA 签名服务器接收 KM 返回的数据并制作加密证书，CA 签名服务器将制作好的证书及 KM 制作的数字信封打包发给 CA 管理服务器，CA 管理服务器接收并验证后重新打包发到 RA 服务器，RA 服务器接收验证后向 CA 管理服务器发送成功回执并将数据下传到制证岗，制证岗调用用户签名私钥解数字信封并验证 KM 的签名后将证书及加密密钥下载到本地 USBKEY 载体中。CA 签名服务器通过 CA 管理服务器收到 RA 的成功回执后，向LDAP 和 OCSP 发布新签发的证书。

6.1.3 公钥传送给证书签发机构

证书订户在向颐信 CA 申请签发证书时，必须向颐信CA 传递自己的签名公钥，该公钥将与用户的身份信息一起，用订户的签名私钥进行签名，并且通过安全可靠的方式进行传递。颐信CA 认证系统接收到这个信息之后，需要进行验证。验证通过后，才能给用户签发证书。

证书签发成功后的回复信息，得到电子签名和信息完整性的保护，并采用安全可靠的方式进行传递。

注册中心(RA)受理用户新办证书请求，对用户信息及申办资格审核后交制证岗。制证岗登录系统后调取被审核过的待制证用户数据，插入一格式化的USBKEY，点击制证按钮开始制证。待制 USBKEY 在其内部生成一签名公私钥对并将公钥送出，制证员对用户数据及送出的公钥签名后提交到 RA 服务器，RA 服务器验证签名并将用户数据及用户签名公钥制作 CMP 包发到 CA 管理服务器，CA 管理服务器接收并验证后重新打包发到 CA 签名服务器，CA 签名服务器接收并验证后使用用户签名公钥制作签名证书。

6.1.4 电子认证服务机构公钥传送给依赖方

颐信 CA 的公钥包含在颐信 CA 的自签发的根证书中，通过颐信CA 的网站（www.ecca.com.cn）进行发布。颐信CA 支持在线传递公钥或者从颐信 CA 的网站下载公钥。

6.1.5 密钥的长度

颐信CA目前支持的密钥算法为RSA算法和SM2算法。

RSA算法的密钥长度支持1024位和2048位，SM2算法的密钥长度是256位。符合国家商用密码管理局相关要求。伴随国家商用密码管理局的要求提高，颐信CA将根据管理部门的要求及时进行技术调整。

6.1.6 公钥参数的生成和质量检查

公钥参数必须使用国家商用密码管理局批准许可的加密设备生成，例如密码机、加密卡、 USB KEY 和 IC 卡等，并遵循这些设备的生成规范和标准。颐信 CA认为这些设备内置的协议、算法等已经具备足够的安全等级要求。

对于参数质量的检查，同样由通过国家商用密码管理局批准许可的加密设备进行生成，例如密码机、加密卡、 USB KEY 和 IC 卡等，颐信 CA 认为这些设备内置的协议、算法等已经具备足够的安全等级要求。

6.1.7 密钥使用目的

颐信 CA 的私钥用于签发自身的证书、系统的设备和管理员证书、CRL 列表以及下级单位的证书。颐信 CA 的公钥证书用于验证颐信 CA 的私钥的签名。

订户的签名密钥和加密密钥用于提供安全服务，如身份认证、数据签名和数据加密等。签名证书对应的密钥用法为：Digital Signature，Non-Repudiation；加密证书对应的密钥用法为：Key Encipherment，Data Encipherment。在颐信CA认证体系中，密钥的用途和证书类型密切相关。如果颐信CA 在其签发标准扩展项内指明了用途，证书订户必须按照指明的用途使用。

颐信 CA 证书密钥使用目的会在证书的Key Usage（密钥用法）扩展域及Extended Key Usage（增强密钥用法）指明：

Key Usage（密钥用法）：表示本证书的公钥能够支持的功能和服务。它的值包括：digital signature, non-repudiation, key encipherment, dataencipherment, keyagreement,certificatesignature,CertificationRevocation List (CRL) signature, encipher only 和 decipher only 等。其中，certificatesignature,CertificationRevocationList(CRL)signature 只能是 CA 证书才能具有的密钥用法。在进行证书验证的时候，如果不进行密钥用法的检查，就可能会出现攻击者使用合法申请的证书，签发新的证书，而这张证书在进行证书验证时，能够追溯到根CA 的情况。这是我们特别要注意的。

因此，虽然扩展域是可选项，但是在安全上，这一扩展域又是不可或缺的。

Extended Key Usage （增强密钥用法）：包含一系列的OID 值，表示本证书中的公钥的特定用法。尽管 X.509 标准没有明确地定义这些目的的标识符，但是在 RFC3280 中说明了一些与此扩展相关的 OID,包括：Transport Layer Security(TLS) server authentication, TLS client authentication, code signing,e-mailprotection,timestamping,and OnlineCertificateStatusProtocol (OCSP) signing。

所有密钥的使用，必须遵照本 CPS 的规定执行。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

颐信 CA 使用国家商用密码管理局批准许可的密码产品,因此,密码模块的标准、使用和控制都符合国家有关规定。

6.2.2 私钥多人控制（m 选 n）

颐信 CA 采用多人控制策略来激活、使用、停止其根私钥。

颐信 CA 的根私钥采用 5 人控制的策略，需要其中至少3 人同时在场来共同执行生成和分割程序。颐信CA 认证系统在技术上已经建立了相应的安全机制，对生成操作进行限制。具有权限的密钥管理人员和操作人员，分别持有的一段密码。所有与私钥相关的信息，如 USB KEY、PIN 码等，分别由不同的管理人员来控制。

6.2.3 私钥托管

颐信 CA 只提供证书订户加密私钥的托管，而不提供签名私钥的托管。对用户加密私钥的托管，由颐信KM 管理中心完成，加密私钥的保护、管理、存档、备份等，按照国家相关的规范和标准进行。

用户必须妥善管理自己的加密和签名私钥，如果用户的加密私钥丢失、损坏，可以通过颐信 CA 申请恢复。若是签名私钥丢失、损坏，则不能申请恢复，只是申请证书作废，重新申请新的签名证书。

6.2.4 私钥备份

颐信 CA 的证书订户的加密私钥都由颐信密钥管理中心自动进行存档、备份。订户的签名私钥由订户自行保管，颐信 CA 不备份订户的签名私钥。

6.2.5 私钥归档

颐信 CA 的私钥经过加密后按照严格的安全措施保存。在私钥有效期结束后，仍将采取同样的安全保密机制进行保存，并遵循颐信 CA 规定。

对于颐信密钥管理中心托管的订户加密证书私钥，颐信CA 提供过期私钥归档保存服务，并遵循颐信 CA 规定。

6.2.6 私钥导入、导出密码模块

颐信 CA 的私钥，严格按照颐信CA 的规定的程序和策略进行备份，除此之外，任何导入导出操作都是不允许的。

颐信 CA 不提供从硬件密码模块中导出私钥的方法，也禁止此类操作。

6.2.7 私钥在密码模块的存储

颐信 CA 使用国家商用密码管理局批准许可的密码设备及密码模块进行私钥的存储。

6.2.8 激活私钥的方法

颐信 CA 的根密钥存储在认证系统内部的密码机模块中，必须经过至少三个授权的管理人员共同操作，才能激活。除此之外，没有办法可以激活颐信CA 的根私钥。

对于颐信 CA 信任体系内部证书订户的私钥，都是存在于证书的载体中，只有通过密码验证后，方可激活其私钥，并由应用系统进行调用。

6.2.9 解除私钥激活状态的方法

一旦私钥被激活，除非这种状态被解除，私钥总是处于活动状态。在某些使用中，私钥被激活，只能进行一次操作，如果需要进行第二次操作，需要再次激活。

颐信 CA 解除用户私钥激活状态的方式包括退出、断电、断开 USB KEY 或 IC 卡设备。

6.2.10 销毁私钥的方法

颐信 CA 的私钥不再被使用，或者与私钥相对应的公钥到期或者被注销后，加密设备必须清空，同时，所有用于激活私钥的 PIN 码等也必须被销毁或收回。颐信CA 在进行用户密钥销毁时，需要多个具有销毁私钥权限的工作人员通过身份认证后方可进行。密钥销毁操作完成后，对数据库中密钥的备份进行销毁。销毁过程将按照软硬件密码设备生产厂商制定操作流程实施。

证书订户的私钥如果不再被使用，或者与私钥相对应的公钥到期或者被注销后，由订户决定其销毁办法，订户必须保证有效销毁其私钥，并承担有关责任。涉及到密钥到期后的保存与归档的，参照本 CPS 执行。

6.2.11 密码模块的评估

颐信 CA 使用国家商用密码管理局批准许可的密码产品，接受其颁布的各类标准、规范、评估结果、评价证书等各项要求。

6.3 密钥对管理的其它方面

6.3.1 公钥归档

公钥的归档，其操作过程、安全措施、保存期限以及保存策略与证书保持一致。

6.3.2 证书操作期和密钥对使用期限

公钥和私钥的使用期限与证书的有效期相关，但却有所不同。

对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了验证在证书有效期内签名的信息，公钥的使用期限可以在证书的有效期限以外。当私钥受到损坏或密钥对存在被破解的风险后，签名证书的公钥在技术上仍然可以用于验证数字签名，但这种验证在法律上不一定是有效的。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

6.4 激活数据

6.4.1 激活数据的产生和安装

颐信 CA 产生的激活数据，包括用于下载口令（以密码信封等形式提供）、USBKEY、IC 卡的登录口令等，都是在安全可靠的环境中，由相关硬件设备随机产生。这些激活数据，都通过安全可靠的方式，例如采用离线当面递交的方式交给订户。

对于非一次性使用的激活数据，颐信 CA 建议用户自行进行修改。

6.4.2 激活数据的保护

订户激活数据必须进行妥善保管，或者记住以后进行销毁，不可被第三方所获取。如果有书面保留需要时，必须进行安全可靠的保存。

6.4.3 激活数据的其他方面

考虑到安全因素，对于订户激活数据的生命周期，规定如下：

用于保护私钥或者 IC 卡、USB KEY 的口令，建议订户根据业务应用的需要，定期进行修改。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

颐信 CA 认证系统的信息安全管理，按照国家商用密码管理局公布的《电子认证系统密码及其相关安全技术规范》、信息产业部公布的《电子认证服务管理办法》以及其它相关的标准和规范实施和执行。

主要的安全技术和控制措施包括：

1. 身份识别和验证管理

2. 资源和信息存取权限控制

3. 安全审计和日志

4. 资料备份和保存的安全管理

5. 人员职责分权、对 CA 工作角色进行分类，建立安全分散和牵制机制

6. 内部操作程序控制

7. 信息传递加密机制

6.5.2 计算机安全评估

颐信 CA 认证系统，通过了国家商用密码管理局、解放军信息安全测评中心的检测和审查、认证。

6.6 生命周期安全控制

6.6.1 系统开发控制

颐信 CA 证书认证系统采用“颐信密钥管理系统（V2.0）”、“电子认证服务系统（V2.0）”及“SJY42-C密码机”等国家密码管理局批准和许可的系统、设备进行建设。

颐信 CA 负责系统的运营、管理和维护，一般不再对系统进行开发和改造。

如果由于国家密码政策和电子认证管理办法进行调整，涉及颐信CA 证书认证系统必须进行改造，则由国家信息安全工程技术研究中心按照国家相关政策、标准和程序进行研制开发、升级改造。

开发、升级和改造过程中，颐信CA 会及时向有关主管部门和信任体系实体成员进行报告和通报。

6.6.2 安全管理控制

颐信 CA 认证系统的信息安全管理控制，严格遵循信息产业部、国家商用密码管理局等主管部门的规范进行操作。

颐信 CA 认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行安装和使用，任何升级都会记录在案并进行版本控制、功能测试。颐信 CA 还对认证系统进行定期和不定期的检查和测试。

颐信 CA 采用严格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。

硬件设备在采购和接收时，会进行安全性检查，用来识别设备是否被入侵、是否存在安全漏洞等。加密设备的采购和安装，必须按照国家商用密码管理局的相关政策进行，采取更加严格的安全控制机制，进行检验、安装和测试。

颐信 CA 认证系统所有软硬件系统和设备升级以后，废弃设备必须确认不含有涉及颐信 CA 认证系统安全性的信息存在。

6.6.3 生命周期的安全控制

颐信 CA 认证系统的软硬件设备具备可持续的升级能力，其中软、硬件生命周期的控制，以保证其安全性和可靠性。

6.7 网络安全控制

颐信 CA 认证系统采用严格的网络安全控制机制，确保认证系统的安全性和可靠性。

认证系统只有授权的管理人员和操作人员，通过配发的 USB KEY 证书，才能完成对认证系统的维护管理和操作使用，并且所有操作都会在系统保留操作日志。

另外，为了确保网络系统安全，颐信CA 认证系统安装部署了入侵检测、防火墙、病毒防护等安全系统和设备，以加强对认证系统的防护和保护。

6.8 时间戳

根据对系统安全管理和控制的需要，颐信CA 会决定是否使用时间戳。根据不同数据对时间的敏感性、严密性和逻辑关系的要求，颐信CA 将确定是否采用时间戳或为用户提供时间戳服务。

颐信 CA 目前不提供时间戳服务。

7 证书、证书注销列表和在线证书状态协议

7.1 证书

证书由基本证书域、签名算法域和签名值域三个部分构成。

基本证书域包括以下属性：

序号	项目名称	描述
1	Version	版本号
2	SerialNumber	序列号
3	Signature	签名算法
4	Issure	颁发者
5	Validity	有效期
6	Subject	主体名称
7	SubjectPublicKeyInf	主体公钥信息
8	Extensions	扩展项

7.1.1 版本号

颐信 CA 签发的数字证书，采用X.509C v3 格式，版本号信息存放在证书基本域中的版本属性栏内。

7.1.2 证书扩展项

颐信 CA 签发的数字证书包含有扩展项，标准的扩展域可能包括以下属性：

序号	名称	描述
1	authorityKeyIdentifier	机构密钥标识符
2	subjectKeyIdentifier	主体密钥标识符
3	keyUsage	密钥用法
4	extKeyUsage	扩展密钥用途或增强密钥用法
5	CRLDistributionPoints	CRL 分布点
6	authorityInfoAccess	机构信息访问

自定义扩展项：

序号	名称	描述
1	IdentifyCardNumber	个人身份证号码
2	InuranceNumber	个人社会保险号
3	ICRegistrationNumber	企业工商注册号
4	OrganizationCode	企业组织机构代码
5	TaxationNumber	企业税号
6	Identify Code	个人身份标识码
7	SubjectUniqueID	实体唯一标识符
8	Uniform Social Credit Code	统一社会信用代码

7.1.3 算法对象标识符

证书的签名算法域中保存颐信 CA 对证书签名时采用的算法，其标识符为：SignatureAlgorithm。

7.1.4 名称形式

颐信 CA 签发的证书，其名称形式的格式和内容符合X.501 甄别名格式。主要由证书的主体名称（Subject）和主体唯一标识符确定。在特定的应用系统中，任何用户的主体唯一标识不能重复或者相同。而证书的主体名称（Subject）由 CountryName(国家名，简称C)、StateOrProvince （省份，简称S ）、LocalcityName(地市，简称L)、OrganizationName(组织名称，简称O)、OrganizationalUnitName(机构名称,简称为 OU)、CommanName(用户名称,简称为 CN)等六个部分组成。

7.1.5 名称限制

颐信 CA 签发的单位身份证书、个人身份证书、代码签名证书，其识别名称不许使用匿名或者伪名，必须是具有确定含义的识别名称。

颐信 CA 保留对特殊应用，证书的识别名称可以采用匿名或者伪名（即证书的识别名称可以是特殊的自定义编号）的权力。

7.1.6 证书策略对象标识符

未使用。

7.1.7 策略限制扩展项的用法

未使用。

7.1.8 策略限定符的语法和语义

未使用。

7.2 证书注销列表

颐信 CA 定期签发和发布 CRL，供用户下载和查询。

7.2.1 版本号

颐信 CA 目前签发的 CRL 的版本号是 X.509 V2，此版本号保存在 CRL 版本格式栏目中。

7.2.2 CRL 和 CRL 条目扩展项

1. CRL

颁发者

CN = RSARootCA

OU = ECCA

O = ECCA.COM.CN

S = Beijing

C = CN

颁发者：

CN = SM2RootCA

OU = ECCA

O = ECCA.COM.CN

S = Beijing

C = CN

CRL 发布：

颐信 CA 每隔 24 小时自动发布最新的完全CRL。

签名算法：

颐信 CA 签发 CRL，分别采用 SHA1withRSA 签名算法和SM2签名算法。

2. 颐信 CA 使用 CRL 的条目扩展项，具体请参阅颐信 CA 证书格式规范。

7.3 在线证书状态协议

颐信 CA 提供 OCSP 服务（在线证书状态查询），实时发布证书状态，OCSP 可以方便证书订户和依赖方及时查询证书状态信息。

7.3.1 版本号

颐信 CA 的 OCSP 服务目前采用 OCSP V1 版本。

7.3.2 OCSP 扩展项

目前未使用。

8 认证机构审计和其它评估

8.1 评估的频率或情形

1．根据《电子签名法》、《电子认证服务管理办法》等法律、政策的要求，颐信 CA 每年一次接受上级主管部门的评估和检查。

2.颐信CA 每年至少进行一次内部的评估、审核，包括颐信CA 下级 RA 中心、授权 RA 中心和其它关联的服务机构。

3．颐信 CA 可以委托或接受其它第三方权威和专业机构的审计和评估。

8.2 评估者的资质

1．颐信 CA 无条件接受国家信息产业部组织的审核、评估和检查，评估者是信息产业部或由信息产业部组织，包括信息产业部认可的专家和相关机构等。

2．颐信 CA 进行内部的审计、评估，评估者必须具有相关的专业技术和业务能力，包括颐信CA 的主管领导和业务骨干。进行内部评估之前，需要制定相应的评估内容、评估标准和评估实施办法等。

3．第三方机构的评估和审计。第三方机构必须是国家相关主管部门批准的具有相应资质的专业评审机构。

8.3 评估者与被评估者之间的关系

1．外部评估者（信息产业部或其它专业机构）和颐信 CA 之间是相互独立的关系，没有任何的业务、财务往来或者其它利益关系，足以影响评估的客观性，评估者应以独立、公正、客观的态度对颐信 CA 进行评估和审计。

2. 颐信 CA 内部评估者，与被评估者之间，也应该是互相独立的关系，没有任何的利益关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对被评估者进行评估和审计。

8.4 评估内容

1.颐信 CA 按照信息产业部提出的评估标准和规范,接受其任何内容的评估和审计；

2.颐信 CA 的 CPS 及执行情况；

3. 服务的完整性：密钥和证书生命周期的安全管理、证书注销和冻结的操作、业务系统的安全操作、业务操作标准等；

4. 物理环境和网络安全的控制：信息安全管理、人员安全管理、软硬件设备设施的安全控制、系统和网络的安全控制、系统开发和维护的安全控制、系统备份和灾难恢复、归档和审计的安全管理。

8.5 对问题与不足采取的措施

1. 信息产业部评估完成后，颐信 CA 必须根据评估结果检查缺失和不足，根据其提出的整改要求,提交修改措施和整改计划书,并接受其对整改计划的审查和再次评估；

2. 颐信 CA 完成内部评估后，评估人员需要列出所有问题项目的详细清单，由评估人员和评估对象共同讨论有关问题，并将结果书面通知颐信CA 相关主管领导和主管部门，并根据评估结果进行后续处理。

8.6 评估结果的传达与发布

1. 信息产业部检查和评估之后，颐信CA 将根据信息产业部要求，通过颐信CA的网站或其它公告形式对外发布；

2．颐信 CA 内部评估结果在与被评估者交流讨论后，将视为机密资料进行处理，只有评估者和被评估者以及颐信 CA 主管领导了解。

3．第三方专业机构的评估结果，颐信 CA 会及时向信息产业部或其它有关单位报告和通报，对确认的不足和缺失，颐信 CA 会及时进行整改和升级。

9 法律责任和其它业务条款

9.1 费用

颐信 CA 主要是以服务费（每年）的形式收取证书费用，其它证书服务收费项目包括证书更新、注销、挂失、恢复等操作的手续费。

颐信 CA 根据不同的数字证书应用项目，向证书订户或其他授权签约方、关联机构收取的证书服务费也会有所差别，具体费用由双方协商，在合作协议中明确规定。证书订户及其他授权签约方、关联机构有责任和义务，按照颐信CA 对外公布的价目或协议约定的标准向颐信 CA 交纳相关费用。

9.1.1 证书签发和更新费用

颐信 CA 不单独另收证书签发费。

对于在有效期内的证书，如果用户信息发生变化，需要更新证书的，经颐信CA 审核后，可以对证书进行更新，颐信CA 收取证书更新手续费。证书更新后，证书的有效期保持不变。

9.1.2 证书查询费用

颐信 CA 目前不单独收取证书查询费。
颐信 CA 保留对特殊应用系统收取证书查询费的权力。

9.1.3 证书注销或状态信息的查询费用

根据实际情况，颐信 CA 可以注销订户的证书。颐信 CA 对证书注销和相关的证书查询不收取费用。

9.1.4 其他服务费用

颐信 CA 关于证书的其它费用包括（但不局限于）以下内容：

1. 由于订户的原因，申请的证书注销、冻结、恢复等操作，颐信 CA 可收取一定的手续费。

2. 颐信 CA 针对特约授权或关联机构，由于提供超出证书管理范围的特殊服务，可能会根据实际情况，收取一定的费用。

3. 针对其它可能占用颐信CA 资源的服务，颐信CA 可能会根据实际情况收取费用。其它服务收费问题，颐信 CA 会及时通过相关渠道发布或直接与用户进行协商，以协议的形式进行约定。

9.1.5 退款策略

颐信 CA 通常是以服务费（每年）的形式收取证书费用，因此，一旦证书成功签发，颐信 CA 将不会给订户退还服务费。颐信 CA 保证在证书有效期内为证书订户提供本 CPS 规定或与颐信 CA 约定的所有服务。

由于颐信 CA 的自身原因，导致证书颁发出错和用户证书不能使用的，而且用户不再申请和申办证书，由用户提供退款请求，经过鉴定和审批后，颐信CA 可以给证书订户退还部分或全部服务费。

用户申请退款并不影响订户申请其它赔偿。

9.2 财务责任

颐信科技有限公司作为颐信 CA 的总公司，负责颐信 CA 的管理和运营。颐信科技有限公司具有足够的经济实力，确保颐信CA 的正常运行，能够保障客户的合法权益，承担对证书订户、依赖方等造成的责任风险，并依据本 CPS 规定，履行对客户的赔偿承诺。

根据需要，颐信CA 可以提供国家主管部门颁发的资质证书文件，或者委托第三方对资产、财务进行审计和评估。

9.2.1 保险范围

颐信 CA 承诺，对于以下情况，颐信 CA 承担相应的赔偿责任：

1．由于颐信CA 的根私钥泄露或管理不善，导致其它第三方以颐信CA 的名义，伪造合法订户的证书，并且利用此证书给合法订户造成损失。

2．非订户的责任，导致订户的私钥被破解，并且其它第三方以破解的私钥假冒证书订户的签名，给用户带来损失。如果由于订户的管理不善，导致订户的证书被盗用，则不属于此列。

3．由于颐信CA 的责任，导致不能为用户提供及时的服务，造成用户的损失。

9.2.2 对最终实体的保险或担保

颐信 CA 对证书用户（包括订户和依赖方）提供的保险和担保范围，不超出本CPS 的规定和声明。

9.3 业务信息保密

9.3.1 保密信息范围

以下信息应视为颐信 CA 的保密信息范畴：

1．颐信 CA、授权的RA 中心、其它关联机构以及证书订户相互之间的协议、来往公函及商务合同等。法律有明确规定或者双方以书面的形式声明可以公开的，则不属于保密范围。

2．与证书持有者公钥配对的私钥属于保密信息，订户须妥善保管。其它第三方不得试图进行破解和盗用。如因用户管理不善，导致私钥泄露或被盗用，用户应自行承担责任。

3．涉及证书订户个人隐私方面的信息，如通信联系方式、财务状况等。

4．对颐信 CA 或关联的实体进行的审计和评估报告，属于保密内容。但是按照国家政策规定必须公开的内容除外。

5．由于公开而可能导致颐信CA 认证系统受到攻击或者风险增加的，如颐信 CA 认证系统中的某些重要技术、配置、参数等信息。

6．颐信 CA 内部审计记录，包括：本地日志、服务器日志、归档日志的信息，只有审计员和业务管理员可以查看。

7．颐信 CA 的业务发展规划和商务计划等。

8．颐信 CA 有关系统和产品研发的规划、设计、方案以及技术资料和文档等。

9.3.2 不属于保密的信息

以下信息可视为不保密信息：

1．与证书办理相关的申请流程、申请手续和操作手册，颐信CA 的 CPS、证书策略等。

2．证书订户可以公开的基本身份信息。

3．颐信 CA 发布的证书和 CRL，包括证书的公钥、订户的基本信息和其它的扩展项信息。

4．证书被注销、注销、挂起的信息，颐信 CA 通过目录服务公布这些信息，供其它第三方验证和查询。

9.3.3 保护保密信息的责任

颐信 CA 及其信任体系中的任何授权机构和关联机构，以及证书订户和依赖者等各方对以上规定的保密信息内容都应承担妥善保管的责任。

除本 CPS 的规定外，颐信 CA 还可通过颐信 CA 的网站或双方的协约，对承担信息保密的责任进行声明和约定。

当信息保密责任人出于某种原因，公布或泄露某些保密信息，给其它有关方造成影响或损失，颐信 CA 有权追究其法律责任。

9.4 个人隐私保密

9.4.1 隐私保密方案

颐信 CA 将按照国家相关法律和政策规定，切实加强订户隐私的保护。

1．对属于用户隐私的信息（包括电子的和纸质的），颐信CA 指定专人负责保管，并定期进行清理和归档。

2．属于订户隐私的信息，绝对不能对外公布或泄露给其它第三方机构，但对于公安机关或其它国家权威部门进行案件调查除外。

3．禁止利用客户的隐私信息，开展与电子认证无关的其它应用和业务。

9.4.2 作为隐私处理的信息

作为用户隐私处理的信息包括：用户的通信地址、财务状况、信用情况、司法状况，对于个人用户还包括年龄、婚姻、身体健康状况等，对于企业用户还包括企业的结构和人员组成、企业发展历程、客户关系、业务经营范围等。

9.4.3 不被视为隐私的信息

作为证明和识别证书订户身份的基本信息，将不视为隐私信息，如个人用户的姓名、身份证号码，企业用户的名称、机构代码、工商登记证号码等。

9.4.4 保护隐私的责任

颐信 CA 及其授权的 RA 中心和其它关联机构都必须承担保护证书订户隐私的责任。任何一方如因违反本 CPS 的规定而导致用户隐私泄露，必须承担相应的责任。

9.4.5 使用隐私信息的告知与同意

颐信 CA 承诺不把用户的隐私信息用于与证书认证无关的业务。

对于特殊情况，如用于司法取证等，颐信CA 将履行必须的手续，同时将按照法律和政策规定，向用户进行通报。

对于授权机构和其它关联机构，如果需要使用所属订户的隐私信息，须向客户进行说明（如使用隐私的内容、目的和范围等），并得到客户的书面同意和授权，同时，还需要把详细情况向颐信 CA 进行通报。

9.4.6 依法律或行政程序的信息披露

对于以下情况，颐信CA 需要向国家司法和行政管理部门或机构披露订户的有关信息：

1. 国家法律规定，并经主管部门通过合法授权程序提出申请。

2. 公安机关或司法部门处理因使用证书产生的纠纷，通过合法程序提出的申请。

3. 具有合法司法管辖权的仲裁机构，通过合法程序提出的申请。

9.4.7 其他信息披露情形

颐信 CA 没有责任和义务披露除用户证书及证书认证需要的基本身份信息之外的任何信息。

9.5 知识产权

颐信科技有限公司作为颐信 CA 的总公司，享有并保留颐信 CA 提供的全部系统和软件的一切知识产权，包括所有权、名称权和利益分享权等。颐信CA 有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。

按本 CPS 的规定，所有由颐信 CA 签发的证书和提供的软件、系统、文档中，使用、体现和相关的一切版权、商标和其他知识产权均属于颐信科技有限公司，这些知识产权包括所有相关的文件、CPS、规范文档和使用手册等。颐信 CA 授权的 RA 注册中心和其它关联机构征得颐信 CA 的书面同意，可以使用相关的文件和手册，并有责任和义务提出修改意见和建议。

9.6 陈述和担保

本 CPS 对颐信 CA 的电子认证服务业务规则进行总体描述和说明，颐信 CA 及授权的 RA 中心、其它关联机构、证书订户和电子认证依赖方须遵循本CPS 的规定。但这并不影响颐信 CA 与用户、证书订户、电子认证依赖方等实体签定业务合同和协议。如果本 CPS 的条款与业务合同、协议不相一致，以具体合同、协议为准。

9.6.1 电子认证服务机构的陈述与担保

颐信 CA 的陈述和担保如下：

1. 在本 CPS 的规范范围之内，严格按照本 CPS 的各项规定，提供完备的基础设施和认证服务。

2. 建立安全机制，确保颐信 CA 根私钥的安全。

3. 颐信 CA 所提供的所有认证服务业务均符合法律、法规和主管部门的规定。

9.6.2 注册机构的陈述与担保

RA 中心按照程序获得颐信 CA 的授权之后，将保证：

1. 遵循颐信 CPS、颐信 CA 的授权协议以及其它颐信 CA 公布的规范和流程，接受并处理证书订户的证书申请，并依据授权设置、管理各类下级证书服务机构。

2. RA 中心遵循颐信 CA 制定的服务受理规范、系统运作和管理要求，根据本CPS 及颐信 CA 公布的规范，RA 中心有权决定是否为申请者提供相应的服务。

3. 按照颐信 CA 的要求和规范，确定下属证书服务受理机构的设置方式、管理方式和审核方式，这些方式将以书面的形式进行公布。

4. 依据本 CPS 的规定，确保其运营系统处在安全的物理环境中，并具备相应的安全管理和隔离措施。 RA 中心必须能够提供证书服务全部的数据资料及备份，并按照颐信 CA 的要求，保证其下属证书服务机构间的信息传输安全。RA 中心承诺严格履行所有针对证书用户的隐私保护义务，并承担由此而带来的法律责任。

5. 承认颐信 CA 对所有证书服务申请者的服务请求拥有最终处理权。

6. 不得拒绝任何来自颐信 CA 的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加及删减等。

7. 为证书订户提供必要的技术咨询和服务保障，使订户顺利地申请和使用证书。

9.6.3 订户的陈述与担保

证书订户应当了解办理数字证书的责任和义务，按照证书申办流程，履行相关手续，办理数字证书。证书订户一旦接受发证机构所签发的证书，即表示订户知悉并接

受颐信 CA 的 CPS 中所有条款及协议。自接受之时起至证书有效期结束，如证书订户不另行通知，将视为订户向颐信CA 信任体系及所有合理依赖方作出如下保证：

1. 在证书申请表中所填内容和信息必须是真实、完整、准确的，可供颐信 CA 及其授权的证书服务机构审查和核实，并且愿意承担任何由于提供虚假、伪造信息而引起的法律责任；

2. 如果通过中间代理人办理证书，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知颐信 CA 或者其授权的证书服务机构；

3. 订户将按照本 CPS 的规定，只将证书用于经过授权的或其它合法的使用目的；

4. 订户应当妥善保管和正确使用证书及其对应的私钥。使用证书所对应的私钥进行签名时，证书订户应确认证书为有效证书（证书在有效期内，没有被注销、注销、冻结等），并且每次签名都是订户自己主观认可的签名，订户愿意承担由此签名而产生的法律责任。如果是利用无效证书对应的私钥进行签名，订户须承担由此假冒签名而引起的法律责任；

5. 订户向发证机构陈述的所有包含在证书中的信息是真实的。如果订户发现证书中某些信息存在错误，但并没有及时通知发证机构，那么，发证机构将视为上述订户承诺的信息都是真实的；

6. 订户不得拒绝任何来自颐信 CA 的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务内容的增加及删减等。

9.6.4 依赖方的陈述与担保

任何颐信 CA 及授权机构的依赖方，如果信任颐信 CA 及其签发的证书，就意味着作出如下保证：

1. 依赖方熟悉和理解本 CPS 的条款和规定，了解证书的使用目的和要求；

2. 依赖方了解和认可证书认证技术原理和证书应用流程，在信任颐信 CA 颁发的证书时，已经通过安全可靠的途径、办法对证书进行了验证，包括通过颐信 CA 的根证书、LDAP 和 OCSP 服务等方式，检查证书的有效性，是否过期，是否被注销、注销或者冻结，以及其它需要确认的证书主体信息；

3. 一旦由于疏忽或者其它原因，违背了上述合理检查条款，依赖方愿意承担因此而产生的后果；

4. 依赖方接受本 CPS 的所有条款，尤其是了解和接受有关免责、拒绝和限制义务条款。

9.7 担保免责

颐信 CA 声明：在下列情况下，颐信 CA 免于承担责任

1. 由于意外或其他不可抗力造成的操作失败或延迟，并由此任何损失、损坏或赔偿责任；

2. 由于非颐信 CA 所能控制和预见的原因、事件而引起的设备故障、线路中断，致使颐信 CA 及其证书服务机构签发证书错误、延误或者无法签发证书、无法提供证书认证服务等，颐信 CA 不负任何赔偿责任；

3. 颐信 CA 不承担任何用户证书认证业务之外的损失和责任。如果证书订户故意或者恶意提供虚假信息，而颐信 CA 按正常程序履行了审核责任，但是并未查出虚假信息内容，因而给订户颁发了证书，证书订户利用此类通过虚假信息获得的证书给第三方造成的损失，颐信 CA 无须承担。由此引起的法律问题、经济纠纷以及其它责任全部由证书订户承担。颐信 CA 不承担认证业务以外的法律和经济责任，但是会根据其它方面的请求，提供司法方面的协查和举证帮助；

4. 颐信 CA 不承担任何未经授权而以颐信 CA 名义编撰、发表或散布不可信消息而引起的法律责任和经济责任；

5. 颐信 CA 对签发的各类证书的适用范围和用途有明确规定，对由于超越适用范围和用途而造成的损失不承担任何责任。

9.8 偿付责任限制

赔偿上限：

1. 颐信 CA 的赔偿上限不超过电子签名人购买该证书实际价格（不含证书介质费）的 2 倍；

2. 颐信 CA 对所有当事实体（包括但不限于电子签名人和电子签名依赖方）的合计责任不超过证书适用的责任上限；

3. 颐信 CA 对任何特定证书的合计责任限制在不超出赔偿责任上限的范围内。每张证书的责任均有上限而不考虑电子签名和交易处理等有关的其他索赔的数量。当责任超过上限时，可用的责任上限将首先分配给最早得到索赔解决的一方。颐信 CA 没有责任为每个证书支付高出责任上限的赔偿，而不管责任上限的总量在索赔提出者之间如何分配；

4. 同一个证书首次发生了安全事故后，电子签名人或者电子签名依赖方须及时告知颐信 CA。如电子签名人继续使用或者电子签名依赖方继续信任有问题的证书而导致再次出现安全事故，颐信 CA 只受理其首次安全事故，对首次安全事故以后的事故，颐信 CA 不仅不承担法律责任和赔偿责任，而且按相关条款，颐信 CA 及相关当事人可以追究电子签名人或者电子签名依赖方的法律责任和赔偿责任；

5. 颐信 CA 只在证书有效期限内承担损失或损害赔偿；

6. 赔偿根据电子签名人或者电子签名依赖方的类别、所受损失的具体情况，按照颐信 CA 赔偿标准依法赔付；

7. 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；

8. 颐信 CA 保留根据国家法规或政策对赔偿上限进行适当调整的权力。颐信 CA 如果对赔偿上限进行了调整，将通过网站等途径及时通报调整情况。针对具体的证书应用项目，颐信 CA 可以与合作方协商制定赔偿上限，并在双方合作协议中明确规定。

9.9 赔偿

9.9.1 赔偿责任和范围

在认证活动中产生的赔偿，除法律法规或商务协议另有规定外，都以本 CPS的规定作为处理依据。

赔偿责任认定包括以下几种情况：

1. 事故责任明确认定为电子认证服务提供者的，由颐信 CA 承担赔偿责任。电子签名人或者电子签名依赖方利用电子认证服务提供者提供的电子签名认证服务从事民事活动时，因电子认证服务提供者的电子签名认证技术、产品等服务致使电子签名人或者电子签名依赖方遭受损失，经权威鉴定机构和专家评定 ,责任确实属于颐信 CA 的，电子签名人和电子签名依赖方有权要求颐信 CA 承担相应的赔偿责任。以下几种情况，颐信 CA 须赔偿用户的损失：

1.1 由于颐信 CA 的根私钥泄露或者被盗用，致使其他人可以假冒颐信 CA 的名义为用户签发证书，并用此伪造的证书从事电子认证服务，导致用户出现各种损失；

1.2 由于非用户的管理责任，致使用户证书对应有私钥被攻破、解密，而造成用户的损失；

1.3 由于颐信 CA 认证系统的原因，导致对用户证书的认证、识别、鉴定等出现错误，从而导致用户或其他方损失；

1.4 签发证书时，由于人为原因，未按照本 CPS 的规定办理证书签发、注销、注销、冻结等请求，而造成证书订户损失的。

由颐信 CA 承担赔偿责任的，颐信 CA 将按照《颐信数字证书认证中心赔偿办法》的相关受理程序处理。

2.事故责任明确认定为电子签名人或者电子签名依赖方的，由电子签名人或者电子签名依赖方承担相应的法律责任和赔偿责任。

出现以下情况之一，电子签名人或电子签名依赖方应赔偿认颐信 CA 的损失：

2.1 未向颐信 CA 提供真实、完整和准确的信息，而导致颐信 CA 或有关各方损失；

2.2 在知悉证书密钥已经失密或者可能失密时，未及时告知颐信 CA 并终止使用该证书，而导致颐信 CA 或有关各方损失；

2.3 证书的非法使用，即违反颐信 CA 对证书使用的规定，造成了颐信 CA 或有关各方的利益受到损失；

2.4 其它不符合颐信 CA 要求和规定的行为，给颐信 CA 或有关各方造成损失。如果事故责任方之间无法解决问题和争端，须按照相关规定由权威机构或仲裁机构评定和仲裁。提交仲裁机构的，根据仲裁条例在时效内裁决，仲裁的决定是终决性的，对每个当事人都有约束力。仲裁的议程应采用中文记录，而且仲裁决定应由有司法权的法院来判定，或者申请法院对其判决或执行命令时予以司法许可范围内的配合。

9.9.2 赔偿处理流程

1．理赔

当明确了安全事故责任后,事故责任明确认定为电子认证服务提供者颐信 CA承担的,由颐信 CA 承担法律责任并按法律规定及颐信 CA 赔偿办法予以赔偿。由颐信 CA 的负责人及客户服务部工作人员上门慰问受损当事人,在双方谈判商定理赔额度后,以约定方式及时赔付。

2．索赔

事故责任明确在电子签名人或者电子签名依赖方的，由电子签名人或者电子签名依赖方承担相应的法律责任和赔偿责任，颐信 CA 根据具体情况依法索赔。

3．登记备案

由颐信 CA 客户服务部对事件全程进行记录、登记和备案。

4．上报

出现重大安全事故的，颐信CA 按规定上报上级主管部门，除理赔外，还要接受上级主管部门的处罚。

5．赔付监管

颐信CA 赔付监管职责有运营总监执行，负责这个赔付流程的审定、管理与监督。。

9.10 有效期和终止

9.10.1 有效期限

本 CPS 在文档中将详细注明版本号以及发布日期和生效日期（若无生效日期，则自发布之日起十五日后生效），当新版本发布生效之后，旧版本将自动失效。

9.10.2 终止

如颐信 CA 需要终止本 CPS 或者其中某些部分时，须通过有效途径，提前向有关方面通报。

9.10.3 效力的终止与保留

在本 CPS 中涉及审计、保密信息、隐私保护、归档、知识产权的条款，以及涉及颐信 CA 赔偿及有限责任的条款，在本 CPS 终止以后仍继续有效。

9.11 对参与者的个别通告与沟通

本 CPS 作为颐信 CA 提供电子认证报务的一般原则和总体规范，对于颐信 CA 所有业务均适用，因此，颐信CA 主要采用网站或者其它途径对外公布本 CPS，一般不对某些用户或个别订户进行单独通告。

如由于本 CPS 的修改、调整，对部分用户影响较大，颐信CA 应当与之充分协商，并通过其它协议的方式进行解决。

任何人或机构如果对本 CPS 中提及的服务、规范、操作等有疑问，或希望提出修改意见，均可以书面形式，提交颐信 CA。颐信 CA 经过研究，如认为确有必要的，可以单独与之进行交流和沟通。为了保证通信过程的法律效力，书面通信须以快递、挂号邮件的方式进行。

9.12 修订

颐信 CA 有权根据国家法律、政策的规定及颐信CA 自身业务的需要，对本CPS 进行修订和调整，从而产生新版本的 CPS。

9.12.1 修订程序

颐信 CA 信息安全管理委员会在每个年度，将对颐信 CPS 进行至少一次审查，确保其符合国家法律法规和主管机构的要求，符合颐信CA 认证服务业务的实际需要。

颐信 CA 信息安全管理委员会如果确定 CPS 需要修订，则指定专人起草修订稿，然后再提交信息安全管理小组讨论，经讨论后确定为正式稿，正式稿须包括发布日期和生效日期等。修订后的正式稿要及时提交信息产业部予以备案，颐信CA还要对旧版本进行归档处理。

9.12.2 通知机制和期限

颐信 CA 有权在适当的时候修改和调整 CPS 中的任何术语、条件和条款，而且无需预先通知任何一方。

如颐信 CPS 的修订和调整，对于某些订户或电子签名依赖方确实影响较大，颐信 CA 会及时采取正式途径与之沟通。

9.12.3 必须修改业务规则的情形

出现下列情况，颐信 CA 必须对本 CPS 进行修订：

1. 国家法律、政策对电子认证服务进行重大调整，本CPS 与新法律、政策有明显不一致的地方；
2. 国家有关电子认证服务的标准、规范进行更新，本 CPS 有不相符的条款；
3. 国家密码技术、标准有重大发展，颐信CA 认证系统必须进行更新和升级；
4. 颐信 CA 开创新的业务模式，与本 CPS 有较大冲突。

9.13 争议处理

当颐信 CA 与其他各方因电子认证服务产生争议时，首先是以友好协商的方式进行解决，若协商不成，则提交双方信任的权威机构进行鉴定、评估和协调，若仍然不成，则按照双方的协议约定，提交具有司法管辖权的仲裁机构或司法部门进行裁决。

9.14 管辖法律

本 CPS 服从《电子签名法》、《电子认证服务管理办法》等中国法律的管辖和解释。

9.15 与适用法律的符合性

所有电子认证活动参与方，均须遵守《电子签名法》、《电子认证服务管理办法》以及其它相关的法律法规。

9.16 一般条款

9.16.1 完整协议

本 CPS 直接影响颐信 CA 的权利、义务的条款和规定，除非通过受到影响的当事人发出经过鉴定的信息或文件，或者在此另有其他规定，否则不能进行口头上的修正、放弃、补充、修改或终止。

本 CPS 与其它规则、规范或协议发生冲突时，所有认证活动参与方都将受到本 CPS 规定的制约，但以下所示的协议除外：

1. 在本 CPS 的生效日期以前签定；

2. 该合同明确表示替代本 CPS 处理相关各方事务，或本 CPS 的规定被法律禁止执行。

9.16.2 转让

无论是各方明示的或暗示的转让人或受让人，本 CPS 均保证其权益，并对其有约束力。各方可根据法律转让本 CPS 详述的权利和义务。

9.16.3 分割性

本 CPS 的任何条款或其应用，不论何种原因导致无效或不能执行，都不会影响其它条款继续生效和执行。

9.16.4 强制执行

无论出于何种原因，一方未执行本 CPS 的某个条款或某项规定，并不意味其将来可以不再执行该项条款或规定。

9.16.5 不可抗力

颐信 CA 信任体系范围内任何一方，可以不对由于以下超越其控制能力的不可抗力事件造成的对本 CPS 规定的担保责任的违反、延误或无法履行的行为承担责任。

不可抗力是指不能预见、不能避免且不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象，也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规致使合同无法履行，或者是战争、罢工、骚乱等社会异常事件。