
亚洲诚信 CA

电子政务证书策略及电子认证业务规则

(CP&CPS)

V1.0.2

亚数信息科技（上海）有限公司

发布日期：二〇二五年十二月

历史版本

版本号	更新内容	生效日期
V1.0	发布初版	2024. 11. 11
V1.0.1	调整了密钥使用期限	2025. 1. 23
V1.0.2	文档清理	2025. 12. 22

目录

1.	概括性描述	1
1.1	概述	1
1.1.1	公司介绍	1
1.1.2	文档名称和标识	1
1.2	电子政务电子认证业务范围	1
1.2.1	服务内容	1
1.2.2	证书类型	1
1.3	电子政务电子认证活动参与者	2
1.3.1	电子政务认证机构	2
1.3.2	注册机构	2
1.3.3	订户	2
1.3.4	依赖方	2
1.3.5	其他参与者	2
1.4	电子政务电子认证策略管理	2
1.4.1	管理机构	2
1.4.2	联系方式	3
1.4.3	批准程序	3
1.5	定义和缩写	3
1.5.1	缩写及其含义一览表	3
1.5.2	定义一览表	4
1.6	策略与信息发布与管理	5
1.6.1	策略与信息的发布	5
1.6.2	策略与信息发布时间与频率	5
1.6.3	策略与信息访问控制	5
2.	身份标识与鉴别	6
2.1	数字证书命名与格式	6
2.1.1	证书命名	6
2.1.2	证书版本	6
2.1.3	证书扩展项	6
2.2	身份标示与鉴别	7
2.2.1	证明拥有私钥的方法	7
2.2.2	组织机构身份鉴别	7
2.2.3	个人身份鉴别	7
2.2.4	政府部门个人身份鉴别	8
2.3	密钥更新请求的标识与鉴别	8
2.3.1	常规密钥更新的标识与鉴别	9
2.3.2	撤销后密钥更新的标识与鉴别	9
2.4	撤销请求的标识与鉴别	9
3.	数字证书服务操作规范	10
3.1	证书申请	10
3.1.1	证书申请流程	10
3.1.2	证书申请实体	10
3.1.3	注册过程与责任	10

3.2	证书申请处理.....	11
3.2.1	执行识别与鉴别功能.....	11
3.2.2	证书申请批准和拒绝.....	11
3.2.3	处理证书申请的时间.....	12
3.2.4	告知证书申请的结果.....	12
3.3	证书签发.....	12
3.3.1	证书签发中注册机构和认证机构的行为.....	12
3.3.2	认证机构和注册机构对用户的通告方式.....	12
3.3.3	证书获取方式.....	12
3.4	证书接受.....	12
3.4.1	构成接受证书的行为.....	12
3.4.2	认证机构对证书的发布.....	13
3.5	密钥对和证书的使用.....	13
3.5.1	用户私钥和证书的使用.....	13
3.5.2	信赖方公钥和证书的使用.....	13
3.6	密钥更新.....	13
3.6.1	密钥更新的情形.....	13
3.6.2	证书更新的情形.....	14
3.6.3	更新申请的提交.....	14
3.6.4	更新申请的鉴别.....	14
3.6.5	密钥更新方式.....	14
3.6.6	通知证书持有者密钥更新.....	15
3.6.7	构成接受密钥更新的行为.....	15
3.6.8	认证机构对密钥更新的发布.....	15
3.7	证书变更.....	15
3.7.1	证书变更的情形.....	15
3.7.2	证书变更的申请.....	15
3.7.3	证书变更的鉴别.....	15
3.7.4	证书变更受理方式.....	15
3.7.5	通知证书持有者证书变更.....	15
3.7.6	构成接受证书变更的行为.....	15
3.7.7	认证机构对证书变更的发布.....	15
3.8	证书撤销.....	15
3.8.1	证书撤销的情形.....	16
3.8.2	可以发起请求撤销证书的实体.....	17
3.8.3	证书撤销的申请.....	17
3.8.4	证书撤销的鉴别.....	17
3.8.5	证书撤销受理方式.....	17
3.8.6	认证机构处理撤销请求的时限.....	18
3.8.7	通知证书持有者证书撤销.....	18
3.8.8	构成接受证书撤销的行为.....	18
3.8.9	认证机构对证书撤销的发布.....	18
3.8.10	CRL 发布频率.....	18
3.8.11	CRL 发布的最大滞后时间.....	18
3.8.12	在线状态查询的可用性.....	18
3.8.13	在线状态查询要求.....	18
3.9	密钥生成、备份与恢复.....	19

3.9.1	证书持有者密钥恢复.....	19
3.9.2	问责取证密钥恢复.....	19
3.10	证书挂起.....	19
3.10.1	证书挂起的情形.....	19
3.10.2	请求挂起的实体.....	19
3.10.3	证书挂起请求的鉴别.....	19
3.10.4	挂起请求的流程.....	20
3.10.5	证书挂起的限制.....	20
4.	应用集成支持与信息服务操作规则.....	22
4.1	服务策略和流程.....	22
4.2	应用接口.....	22
4.2.1	密码设备调用接口.....	22
4.2.2	密码模块安全技术接口.....	22
4.2.3	通用密码服务接口.....	22
4.3	集成内容.....	22
4.4	信息服务内容.....	22
4.4.1	证书信息服务.....	22
4.4.2	CRL 信息服务.....	23
4.4.3	服务支持信息服务.....	23
4.4.4	决策支持信息服务.....	23
4.5	信息服务管理规则.....	23
4.6	信息服务方式.....	24
4.6.1	证书信息同步服务.....	24
4.6.2	CRL 信息同步服务.....	24
4.6.3	服务支持信息服务.....	24
4.6.4	决策支持信息服务.....	24
5.	使用支持服务操作规则.....	25
5.1	服务内容.....	25
5.1.1	面向证书持有者的服务支持.....	25
5.1.2	面向应用提供方的服务支持.....	25
5.2	服务方式.....	25
5.2.1	座席服务.....	25
5.2.2	在线服务.....	25
5.2.3	现场服务.....	26
5.2.4	满意度调查.....	26
5.2.5	投诉受理.....	26
5.2.6	客户培训.....	26
5.3	服务质量.....	26
6.	认证机构设施、管理和操作控制.....	27
6.1	物理控制.....	27
6.1.1	场所区域与建筑物.....	27
6.1.2	物理访问.....	27
6.1.3	电力和空调.....	27
6.1.4	水患防治.....	27
6.1.5	火灾预防和保护.....	28
6.1.6	介质存储.....	28
6.1.7	废物处理.....	28

6.1.8	异地备份	28
6.2	操作过程控制	28
6.2.1	可信角色	28
6.2.2	角色的识别与鉴别	29
6.2.3	角色职责分离设置	29
6.3	人员控制	29
6.3.1	可信人员要求	29
6.3.2	可信人员背景审查	29
6.3.3	人员培训及再培训	30
6.3.4	工作岗位轮换周期和顺序	30
6.3.5	违规行为处罚	30
6.3.6	外包服务人员及要求	30
6.3.7	提供给员工的文档及保密策略	30
6.4	审计日志程序	30
6.4.1	审计事件的类型	30
6.4.2	审计日志的处理周期	31
6.4.3	审计日志记录的保存期限	31
6.4.4	审计日志的保护措施	31
6.4.5	审计日志的备份程序	32
6.4.6	审计收集系统	32
6.4.7	对导致事件实体的通告	32
6.5	记录归档要求	32
6.5.1	记录归档的类型	32
6.5.2	记录归档的保存期限	32
6.5.3	记录归档的保护措施	32
6.5.4	记录归档的备份程序	32
6.5.5	记录归档时间戳要求	32
6.5.6	记录归档收集系统	33
6.5.7	记录归档检验机制	33
6.6	认证机构密钥更替	33
6.7	数据备份	33
6.7.1	数据备份计划	33
6.7.2	异地备份中心	33
6.8	损害与灾难恢复	33
6.8.1	事件和损害的列表	33
6.8.2	计算资源、软件或数据的损坏	34
6.8.3	实体私钥损害处理程序	34
6.8.4	灾难后的业务连续性能力	34
6.8.5	业务连续性计划	34
6.9	认证机构或注册机构的终止	34
7.	认证系统技术安全控制规则	35
7.1	密钥对的生成和安装	35
7.1.1	密钥对的生成	35
7.1.2	私钥传送给用户	35
7.1.3	公钥传送给证书签发机构	35
7.1.4	认证机构公钥传送给依赖方	35
7.1.5	密钥的算法	35

7.1.6	公钥参数的生成和质量检查	36
7.1.7	密钥使用目的	36
7.2	私钥保护和密码模块工程控制	36
7.2.1	在 CA 私钥保护方面的要求	36
7.2.2	用户私钥保护方面的要求	36
7.3	密钥对管理的其他方面	36
7.3.1	公钥归档	36
7.3.2	证书操作期和密钥对使用期限	36
7.4	激活数据	37
7.4.1	激活数据的产生和安装	37
7.4.2	激活数据的保护	37
7.4.3	激活数据的其他方面	37
7.5	系统安全控制	38
7.5.1	安全技术要求	38
7.5.2	安全技术措施	38
7.6	生命周期技术控制	38
7.6.1	CA 系统运行管理	38
7.6.2	CA 系统访问管理	38
7.6.3	CA 系统的开发和维护	38
7.7	网络的安全控制	39
7.8	时间戳	39
8.	法律责任和其他业务条款	40
8.1	费用	40
8.1.1	证书签发和密钥更新费用	40
8.1.2	其他服务费用	40
8.1.3	退款策略	40
8.2	财务责任	40
8.2.1	责任担保范围	40
8.2.2	其他资产	40
8.3	业务信息保密	40
8.3.1	保密信息范围	40
8.3.2	不属于保密的信息	41
8.3.3	保护保密信息的信息	41
8.4	个人隐私保密	41
8.4.1	保护隐私的责任	41
8.4.2	使用隐私信息的告知与同意	41
8.4.3	依法律或行政程序的隐私信息的使用	41
8.4.4	不被视为隐私的信息	41
8.5	知识产权	41
8.6	陈述与担保	42
8.6.1	认证机构的陈述与担保	42
8.6.2	注册机构的陈述与担保	42
8.6.3	订户的陈述与担保	42
8.6.4	依赖方的陈述与担保	42
8.6.5	其他参与者的陈述与担保	43
8.7	担保免责	43
8.8	偿付责任限制	43

8.9	赔偿责任.....	43
8.10	有效期限与终止.....	44
8.10.1	有效期限.....	44
8.10.2	终止.....	44
8.10.3	效力的终止与保留.....	44
8.11	对参与者的个别通告与沟通.....	44
8.12	修订.....	44
8.12.1	修订程序.....	44
8.12.2	通知机制和期限.....	45
8.12.3	必须修改业务规则的情形.....	45
8.13	争议处理.....	45
8.14	管辖法律.....	45
8.15	与适用法律的符合性.....	45
8.16	一般条款.....	45
8.16.1	完整协议条款.....	45
8.16.2	转让条款.....	45
8.16.3	分割性条款.....	45
8.16.4	强制执行条款.....	46
8.16.5	不可抗力条款.....	46
8.17	其他条款.....	46

1. 概括性描述

1.1 概述

1.1.1 公司介绍

亚数信息科技（上海）有限公司（TrustAsia Technologies, Inc, 中文简称“亚洲诚信”，英语简称“TrustAsia”）成立于2013年4月。2020年12月，亚洲诚信通过国家密码管理局组织的商用密码的资格审查，获得由国家密码管理局颁发的《电子认证服务使用密码许可证》（许可证号：0060）。2021年11月，TrustAsia获得国家工业和信息化部颁发的《电子认证服务许可证》（许可证编号：ECP31010421056）。

亚洲诚信获得由中国质量认证中心（简称“CQC”）颁发的《ISO9001质量管理体系认证》、《ISO27001信息安全管理体系统认证》、《ISO22301业务连续性管理体系认证》和《ISO27701隐私信息管理体系》，均被中国合格评定国家认可委员会（简称“CNAS”）认可。

亚洲诚信是国内杰出网络信息安全数字证书及安全监测解决方案提供商，旗下“亚洲诚信”是亚数信息科技（上海）有限公司的信息安全领域品牌，专业提供国际知名品牌数字证书及网络信息安全管理解决方案，深受网络信息安全领域认可和信赖。

我们将以国际化的运营管理和服务水平，为各行各业对通信和信息安全方面有需求的用户提供全球化的电子认证服务。

1.1.2 文档名称和标识

此文档称作《亚洲诚信电子政务证书策略及电子认证业务规则》，简称《亚洲诚电子政务 CP&CPS》，并在亚洲诚信网站发布，网址：
<https://www.trustasia.com>。

1.2 电子政务电子认证业务范围

1.2.1 服务内容

亚洲诚信按照《电子政务电子认证服务管理办法》所规定的服务内容及要求，面向电子政务活动中的政务部门和企事业单位、社会团体、社会公众等电子政务用户提供证书申请、证书签发、证书更新、证书撤销以及密钥生成、备份和恢复等服务。

1.2.2 证书类型

亚洲诚信可提供以下类型的数字证书：

对象	OID
设备证书	1.2.156.115224.1
个人证书	1.2.156.115224.2
机构证书	1.2.156.115224.3

以上各类数字证书格式应遵循 GM/T 0015，在标识实体名称时，应保证实体身份的唯一性，且名称类型应支持 X.500、RFC-822、X.400 等标准协议格式。

1.3 电子政务电子认证活动参与者

1.3.1 电子政务认证机构

电子认证服务机构（Certification Authority，简称 CA）指所有得到授权能够签发公钥证书的实体。

亚洲诚信是依法设立的电子认证服务机构，通过给从事电子交易活动的各方主体签发数字证书、提供数字证书验证服务等手段，成为电子认证活动的参与主体。

亚洲诚信作为多个 CA 的运营商，执行与公钥操作相关的功能，包括接收证书请求、签发、撤销和更新数字证书，以及维护、签发和发布 CRL 和 OCSP 响应。

1.3.2 注册机构

注册机构 (Registration Authority，简称 RA)代表 CA 建立起证书注册过程，确认证书申请者(订户)的身份，批准或拒绝证书申请，批准订户的证书撤销请求或直接撤销证书，批准订户证书更新请求。

亚洲诚信可以授权外部机构作为注册机构，外部注册机构需符合：

1. 与亚洲诚信签订相关合同并明确双方的权利和义务以及所承担的法律
责任。
2. 遵守本CPS。
3. 遵守亚洲诚信的注册机构管理制度。

1.3.3 订户

订户是指从亚洲诚信获得证书的所有最终用户，可以是个人、机构。订户通常需要同亚洲诚信签订合约以获得证书，并承担作为证书订户的责任

1.3.4 依赖方

依赖方是基于对亚洲诚信签发的证书和（或）数字签名的信赖而从事有关活动的实体。依赖方可以是、也可以不是一个订户。

1.3.5 其他参与者

为亚洲诚信的电子认证活动提供相关服务的其他实体。

1.4 电子政务电子认证策略管理

1.4.1 管理机构

亚洲诚信安全策略委员会是亚洲诚信所有策略的最高管理机构，负责制定、批准、发布、实施、更新、废止本 CP&CPS。

亚洲诚信的安全策略委员会由来自于公司管理层、主管运营安全、技术安全、客户服务和人员安全等合适代表组成。

本策略文档的对外咨询服务等日常工作由策略部门负责。

1.4.2 联系方式

1.4.2.1 CPS 联系人

如对本 CP&CPS 有任何疑问，请联系：

部门：策略部

电话：021-58895880（转 CP&CPS 咨询）

传真：021-51861130

邮件：cps-cn@trustasia.com

地址：上海市徐汇区桂平路 391 号 B 座 32 楼（200233）

1.4.2.2 证书撤销、挂起联系人

如遇证书问题报告及证书撤销、证书挂起请求，须通过以下方式之一提交：

邮件：revoke-cn@trustasia.com

电话：400-880-8600（转证书撤销）

书面材料：前往亚洲诚信现场受理

备注：证书撤销、证书挂起请求，必须提交书面材料。

1.4.3 批准程序

本 CP&CPS 由亚洲诚信安全策略委员会组织“CPS 编写组”编制，该小组完成编制后提交安全策略委员会审核，经该委员会审批同意后，正式在亚洲诚信官方网站上发布。

所有正式发布的 CP&CPS 版本从对外发布之日起的三十日之内向上海市密码管理局备案。

1.5 定义和缩写

1.5.1 缩写及其含义一览表

CA	Certification/Certificate Authority	电子认证服务机构
CAA	Certification Authority Authorization	认证机构授权
ccTLD	Country Code Top-Level Domain	国家顶级域名
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
CRL	Certificate Revocation List	证书撤销列表
CSR	Certificate Signing Request	证书请求文件
DBA	Doing Business As	商业名称
DNS	Domain Name System	域名系统
EV	Extended Validation	扩展验证/增强验证
FIPS	(US Government) Federal Information Processing Standard	(美国政府) 联邦信息处理标准
FQDN	Fully Qualified Domain Name	完全限定域名
gTLD	Generic Top-Level Domain	通用顶级域名
IANA	Internet Assigned Numbers Authority	互联网编码分配机构
ICANN	Internet Corporation for Assigned Names and Numbers	互联网名字与编号分配机构
KM	Key Management	密钥管理
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议

LRA	Local Registration Authority	本地注册机构
OCSP	Online Certificate Status Protocol	在线证书状态协议
OID	object identifier	对象标识符
OSCCA	State Cryptography Administration Office of Security Commercial Code Administration of China	中国国家商用密码管理办公室
PIN	Personal Identification Number	个人身份识别码
PKCS	Public KEY Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公钥基础设施
RA	Registration Authority	注册机构
RFC	Request For Comments	请求评注标准(一种互联网建议标准)
SSL	Secure Sockets Layer	安全套接字
TLS	Transport Layer Security	传输层安全
TTL	Time to Live	IP 包的生存时间
X.509	The ITU-T standard for Certificates and their corresponding authentication	ITU-T 证书标准及其相应的认证

1.5.2 定义一览表

术语	定义
安全策略委员会	认证服务体系内的最高策略管理监督机构和 CP&CPS 一致性决定机构
电子认证服务机构 (CA)	证书认证机构, 是签发证书的实体, 负责建立, 签发, 撤销及管理证书的某个机构。该术语适用于根 CAs 及中级 CAs。
注册机构 (RA)	负责处理证书申请者 and 证书订户的服务请求, 并将之提交给认证服务机构, 为最终证书申请者建立注册过程的实体, 负责对证书申请者进行身份标识和鉴别, 发起或传递证书撤销请求, 代表电子认证服务机构批准更新证书或更新密钥的申请。
证书策略 (CP)	一套命名的规则集, 用以指明证书对一个特定团体或者具有相同安全需求的应用类型的适用性。例如, 一个特定的 CP&CPS 可以指明某类证书适用于鉴别从事企业到企业交易活动的参与方, 针对给定价格范围内的产品和服务。
认证业务规则 (CPS)	电子认证服务机构在签发、管理、撤销或更新证书、密钥过程中所采纳的业务实践的通告。
认证路径 (Certification Path)	一个有序的证书序列 (包含路径中起始对象的公钥), 通过处理该序列可获得末端对象的公钥。
策略限定符 (Policy qualifier)	依赖于策略的信息, 可能与 CP&CPS 标识符共同出现在 X.509 证书中。该信息可能包含可用 CP&CPS 或依赖方协议的 URL 地址, 也可能包含证书使用条款的文字。
数字证书	使用数字签名绑定公钥和身份的电子文档
电子签名	具有识别签名人身份和表明签名人认可签名数据功能的技术手段。
数字签名	通过使用非对称密码加密系统对电子记录进行加密、解密变换来实现的一种电子签名。
电子签名人	是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的人。
电子签名依赖方	是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的人。
公钥基础设施 (PKI)	一组包括硬件、软件、人员、流程、规则及责任的合集, 用于实现基于公钥密码的密钥及证书的可信创建、签发、管理及使用的功能。
证书撤销列表 (CRL)	一个经电子认证服务机构数字签名的列表, 它标出了一系列证书颁发者认为无效的证书。
密钥对	私钥和关联的公钥

私钥(电子签名制作数据)	密钥对的密钥, 由密钥对的持有者保密, 在电子签名过程中, 用于创建数字签名和(或)解密用相应公钥加密的电子记录或文件。
公钥(电子签名验证数据)	密钥对的密钥, 可以由相应私钥的持有者公开披露, 并且由依赖方用于验证使用持有者的相应私钥创建的数字签名和(或)加密消息。它们只能使用持有人相应私钥解密。
订户	从电子认证服务机构接收证书的实体, 也被称为证书持有人。在电子签名应用中, 订户即为电子签名人。
订户协议	申请人在收到证书前必须阅读和接受的证书的签发和使用的协议。
依赖方	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、也可以不是一个订户。
依赖方协议	在验证、依赖或使用证书或访问或使用亚洲诚信信息库之前必须由依赖方阅读和接受的协议。
WHOIS	通过 RFC 3912 中定义的协议, RFC 7482 中定义的注册表数据访问协议, 或 HTTPS 网站直接从域名注册商或注册管理执行机构取得的信息。

1.6 策略与信息发布与管理

1.6.1 策略与信息的发布

亚洲诚信的信息库可通过亚洲诚信的官网 (www.trustasia.com) 访问, 是一个对外公开的、面向订户及证书应用依赖方提供信息服务的信息库, 该信息库包括但不限于以下内容:

1. 证书信息服务

亚洲诚信严格按照《电子政务电子认证服务业务规则规范》和本 CP&CPS 的要求, 向订户提供数字证书的申请、签发、存档、查询、撤销等服务。

2. CRL 信息服务

亚洲诚信通过目录服务器 (LDAP) 发布订户的 CRL, 订户或依赖方可以通过 CRL 站点查获已被撤销了的证书的信息。

3. 服务支持信息服务

亚洲诚信以页面和接口的形式提供查询服务, 接口符合《电子政务数字证书应用接口规范》要求。

4. 决策支持信息服务等

亚洲诚信证书信息可为政府主管部门提供科学管理和决策可靠依据。

1.6.2 策略与信息发布时间与频率

对于 CP&CPS, 在完成第 1.4.3 章节所述的批准流程后立即发布到亚洲诚信网站上, 并确保 7x24 小时可访问。

对于订户证书的 CRL 至少 24 小时发布一次; 对于子 CA 证书的 CRL 至少 12 个月发布一次, 且 CRL 有效期不超过 12 个月, 如果有子 CA 证书撤销的情况, 则在 24 小时之内更新发布 CA 证书的 CRL。

在紧急情况下, 信息库其他内容的发布时间和频率, 由亚洲诚信独立做出决定, 这种发布应是即时高效的, 并且是符合国家法律的要求的。

1.6.3 策略与信息访问控制

亚洲诚信信息库中的信息以只读的方式对外提供查询和获取。

亚洲诚信通过网络安全防护、系统安全设计、安全管理制度确保这些信息只有授权人员才能进行信息库的增加、删除、修改、发布等操作。

2. 身份标识与鉴别

2.1 数字证书命名与格式

2.1.1 证书命名

亚洲诚信签发的证书格式符合 GM/T 0015-2012 数字证书格式规范，不得使用匿名或假名。

2.1.2 证书版本

亚洲诚信签发的证书符合 X.509 V3 版证书格式，版本信息存放在证书版本格式栏内。

2.1.3 证书扩展项

亚洲诚信除了使用证书标准项和标准扩展项以外，还使用亚洲诚信规定的自定义扩展项。

1. 证书扩展项

密钥用途

	用途	0	1	2	3	4	5	6	7	8
设备证书	加密	×	×	√	√	√	×	×	×	×
	签名	√	√	×	×	×	×	×	×	×
个人证书	加密	×	×	√	√	√	×	×	×	×
	签名	√	√	×	×	×	×	×	×	×
机构证书	加密	×	×	√	√	√	×	×	×	×
	签名	√	√	×	×	×	×	×	×	×
CA 证书	-	×	×	×	×	×	√	√	×	×

用途说明:

0 digitalSignature	1 nonRepudiation	2 keyEncipherment
3 dataEncipherment	4 keyAgreement	5 keyCertSign
6 cRLSign	7 encipherOnly	8 decipherOnly

其它类型证书的密钥用途遵守 RFC5280，按需进行设置。

证书策略

亚洲诚信签发的证书策略，符合 X.509 证书格式，这一策略信息存放在证书策略属性栏内。

基本限制

用于鉴别证书持有者身份，如最终用户等。

扩展密钥用途

	设备证书	身份认证证书	身份认证证书
服务器验证 1.3.6.1.5.5.7.3.1	√	×	×
客户端验证 1.3.6.1.5.5.7.3.2	√	√	√
安全电子邮件 1.3.6.1.5.5.7.3.4	×	√	√

其它类型证书的扩展密钥用途遵守 RFC5280，按需进行设置。

CRL 发布点

CRL 分发点扩展项包含可以获取 CRL 的 URL，用于验证证书状态。

序列号

亚洲诚信签发的证书采用随机序列号。

2. 自定义扩展项

有关自定义扩展项的内容，请参考本 CP&CPS 附录中关于证书自定义扩展项说明。

2.2 身份标示与鉴别

2.2.1 证明拥有私钥的方法

证书申请者必须证明其正当地持有与包含在证书中的公钥相对应的私钥，其证明方法是提交经过数字签名的 PKCS#10 格式证书签名请求 (CSR)。

亚洲诚信在为订户签发证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断订户拥有私钥。

2.2.2 组织机构身份鉴别

任何组织机构（政府机构、企事业单位等），在以组织名义申请机构类证书时，应进行严格的身份鉴别，如通过查询可信数据库验证其真实性、鉴别申请者提交的身份材料以及其他可以获得申请者明确的身份信息的方式等。机构类订户的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（公章）表示接受证书申请的有关条款，并承担相应的责任。

组织机构在申请证书前应指定并授权证书的申请代表，由证书申请代表前往亚洲诚信受理点当场提交组织机构的有效身份证件及其复印件（包括但不限于工商营业执照、事业单位法人证书、统一社会信用代码证书等）、证书申请表、组织机构授予证书申请代表的授权书以及证书申请代表的有效身份证件，并当场签署数字证书服务协议。

亚洲诚信将通过查询签发有效身份证件的权威第三方数据库以确认组织是真实存在的、合法的实体；将通过申请表获取的组织联系方式，以电话或电子邮件等方式与组织进行联络，以确认申请代表所提供的信息的真实性。

此外，必要时，亚洲诚信还可以要求申请者提供额外的信息及证明材料。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。亚洲诚信不确认、不担保所签发的证书中除验证信息以外的其他身份信息是真实的、可靠的、属于申请者本人的。

对于亚洲诚信签发的订户证书，亚洲诚信会建立评估标准用于识别存在潜在高风险欺诈情况的证书请求。对于被鉴别为“高风险”的证书请求，亚洲诚信可直接予以拒绝。亚洲 CA 在复核并验证申请相关的申请材料后，会根据验证结果决定批准、拒绝申请或要求申请者补充递交相关材料。批准申请的，将保留相关证明材料的复印件，与申请资料一并存档保存。证书申请的现场全过程将由录音录像设备记录保存。

2.2.3 个人身份鉴别

如果申请者的身份是自然人，亚洲诚信将会审核申请者的姓名、地址以及证书申请的真实性等相关必要信息。申请者需要证明其对请求中包含的某些身份属性有控制权，例如其包含在证书请求中证书涉及的电子邮箱地址或域名。申请者还可能被要求提交有效的政府签发的带照片的证件（如居民身份

证、护照、驾驶证、军官证或其他同等证件)的清晰副本。亚洲诚信会验证证件的副本是否与所请求的名称匹配,以及其他相关信息是否正确。

个人证书申请者须前往亚洲诚信受理点当场出示有效身份证件并提供其复印件(包括但不限于居民身份证、护照、驾驶证、军官证等其他同等证件)、证书申请表,并当场签署数字证书服务协议。当由他人代表本人申请时,须同时出示代理人及被代理人的有效身份证件,以及被代理人签发给代理人的授权书。

亚洲诚信将通过检查申请者所提交的证件副本是否有任何篡改或伪造的痕迹,必要时通过查询权威第三方数据库等可靠的方式对申请者提供的身份信息进行核实验证,以确保申请者所提供的信息与核查结果一致。若申请者委托他人代理申请证书时,亚洲诚信将通过申请表获取的申请者联系方式,以电话或电子邮件等方式与其进行联络,以确认申请代表所提供的信息的真实性。亚洲诚信不确认、不担保所签发的证书中除验证信息以外的其他身份信息是真实的、可靠的、属于申请者本人的。

当申请信息包含组织信息时,亚洲诚信将启动组织身份鉴别机制,要求申请人按组织身份鉴别规则提供相关申请材料。

对于亚洲诚信签发的订户证书,亚洲诚信会建立评估标准用于识别存在潜在高风险欺诈情况的证书请求。对于被鉴别为“高风险”的证书请求,亚洲诚信可直接予以拒绝。亚洲CA在复核并验证申请相关的申请材料后,会根据验证结果决定批准、拒绝申请或要求申请者补充递交相关材料。批准申请的,将保留相关证明材料的复印件,与申请资料一并存档保存。证书申请的现场全过程将由录音录像设备记录保存。

2.2.4 政府部门个人身份鉴别

当证书申请者为政府部门中的个人时,证书申请者还需额外提交由所属政府部门签章的证明文件(如录用/任职证明文件等),证明文件需明确显示组织及部门的名称并证明申请者属于该部门。其他申请资料同组织身份鉴别规则。

亚洲CA将通过检查申请者所提交的证明文件是否有任何篡改或伪造的痕迹,并通过查询权威第三方数据库以确认政府部门是真实存在的、合法的实体;通过申请表获取的政府部门联系方式,以电话或电子邮件等方式与政府部门进行联络确认申请者是否是该部门成员,以确保申请者所提供的信息与核查结果一致。证书中的通用名称将登记证书申请者的真实姓名。亚洲诚信不确认、不担保所签发的证书中除验证信息以外的其他身份信息是真实的、可靠的、属于申请者本人的。

对于亚洲诚信签发的订户证书,亚洲诚信会建立评估标准用于识别存在潜在高风险欺诈情况的证书请求。对于被鉴别为“高风险”的证书请求,亚洲诚信可直接予以拒绝。亚洲CA在复核并验证申请相关的申请材料后,会根据验证结果决定批准、拒绝申请或要求申请者补充递交相关材料。批准申请的,将保留相关证明材料的复印件,与申请资料一并存档保存。证书申请的现场全过程将由录音录像设备记录保存。

2.3 密钥更新请求的标识与鉴别

在证书到期之前,订户可以请求证书更新或变更,亚洲诚信会为每一张更新或变更证书更新密钥。在收到证书更新或变更请求后,亚洲诚信将创建一个含有新公钥但证书主题内容与原证书相同的新证书,并且可选择地延长证书

有效期。亚洲诚信可根据实际情况选择对申请者进行重新确认，或者依赖之前提供或获得的信息。

密钥更新会造成使用原密钥对加密的文件或数据无法解密，因此，订户在申请密钥更新前，必须确认使用原密钥对加密的文件或者数据已经解密，由此造成的损失，亚洲诚信将不承担责任。

2.3.1 常规密钥更新的标识与鉴别

亚洲诚信支持在有效期内的证书订户进行密钥更新或变更请求，亚洲诚信会生成一个新的密钥来替换正在使用的密钥对或即将到期的密钥对。密钥更新分为以下三种情况，亚洲诚信会根据不同情形做相应的标识与鉴别：

1. 证书变更

当订户提交证书信息变更申请后，亚洲诚信会对证书信息进行重新审核。审核通过后，亚洲诚信将重新签发新的证书。变更证书的有效期与原证书有效期一致。

2. 证书补发

当订户需要补发证书时，应主动向亚洲诚信提出证书补发申请。亚洲诚信会对证书信息进行重新审核。审核通过后，亚洲诚信将重新签发新的证书。补发证书的有效期与原证书有效期一致。

3. 证书换发

当订户证书需要换发时，应主动向亚洲诚信提出证书换发的申请。亚洲诚信会对证书信息进行重新审核。审核通过后，亚洲诚信将重新签发新的证书。新证书有效期将从证书换发之日起至原证书到期为止再另加一个证书有效周期。

关于密钥更新的鉴别

亚洲诚信会对证书信息进行重新验证，若原证书的验证可用且时效未过期（验证有效期为 398 天），则可以参考原证书验证方式审核验证，若原验证信息不可用或已超期，则亚洲诚信会按照初次申请证书流程和要求进行审核验证。但无论原验证是否可用，订户都必须提交相应申请资料并接受亚洲诚信的面对面审核。审核通过后，亚洲诚信将重新签发新的证书。

2.3.2 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。

2.4 撤销请求的标识与鉴别

在亚洲诚信的证书业务中，证书撤销请求可以来自订户，也可以来自亚洲诚信。另外，当亚洲诚信有本 CP&CPS 3.8.1 所述理由需要撤销订户的证书时，有权发起撤销订户证书。

订户需要前往受理点提交书面申请资料向亚洲诚信提交请求，亚洲诚信通过与证书保障级别相应的方式来确认要撤销证书的人或组织确实是订户本人，或者其授权者。依据不同的情况，确认方式可以采用下面的一种或几种：域名控制权验证、电话、传真、e-mail、邮寄或快递服务。

3. 数字证书服务操作规范

3.1 证书申请

3.1.1 证书申请流程

电子政务活动中的个人和具有独立法人资格的组织机构在电子政务活动中进行基于数字证书的身份鉴别、需要采用数字签名及实现信息加密时，可以向亚洲诚信提出证书申请，申请流程如下：

1. 个人证书申请者可以本人前往亚洲诚信受理点当场提交资料提出申请，也可以委托持有申请者授权书的代理人代理；机构证书申请者应指定并授权证书的申请代表，由证书申请代表前往亚洲诚信受理点当场提交资料提出申请；
2. 亚洲诚信会对申请者当场提交的资料进行受理并要求申请者本人或申请代表当面签署接受服务协议；
3. 亚洲诚信将依据本 CP&CPS 第 2.2 章节的鉴别要求对申请者提供的资料信息进行审核，检查资料的充分性，验证申请信息的完整性，确认授权的合法性；
4. 亚洲 CA 在复核并验证申请相关的申请材料后，会根据验证结果决定批准、拒绝申请或要求申请者补充递交相关材料；
5. 亚洲诚信批准申请的，将保留相关证明材料的复印件，与申请资料一并存档保存。

3.1.2 证书申请实体

证书申请实体包括电子政务活动中的个人和具有独立法人资格的组织机构（国家机关、事业单位、社会团体和人民团体等）。申请实体或被组织机构授权代表的申请的个人可以提交证书申请。申请实体对其或被授权代表人向亚洲诚信提供的任何数据负责。

3.1.3 注册过程与责任

1. 注册过程
 - 提交证书申请；
 - 生成密钥对；
 - 接受亚洲诚信的审核；
 - 同意适用的订户协议以及 CP&CPS；
 - 支付任何适用的费用。
2. 责任
 - 订户即申请证书的实体，应事先了解并书面接受本 CP&CPS 及订户协议等文件约定的事项，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。
 - 订户有责任向亚洲诚信提供真实、完整和准确的证书申请信息和资料。根据《中华人民共和国电子签名法》的规定，申请者未向亚洲诚信提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、亚洲诚信造成损失的，订户应承担相应的法律及赔偿责任。
 - 订户有责任保护其拥有的证书私钥安全。

-
- 亚洲诚信应妥善保管证书订户申请信息。
 - 亚洲诚信有责任对订户提供的证书申请信息和身份证明材料进行检查和审核。

3.2 证书申请处理

3.2.1 执行识别与鉴别功能

亚洲诚信接收到订户的证书申请后，亚洲诚信验证团队会按本 CP&CPS 第 2.2 章节的要求，对订户的身份进行识别与鉴别。亚洲诚信会维护系统和流程，以便根据 CP&CPS 充分验证申请人的身份。通过电话、传真或电子邮件进行沟通的内容将与申请者通过面对面直接提供资料信息一起安全存储。在证书申请者提交证书申请后，亚洲诚信将依据本 CP&CPS 第 2.2 章节的鉴别要求对申请者提供的资料信息进行审核，检查资料的充分性，验证申请信息的完整性，确认授权的合法性以及申请者对服务协议的接受。验证完成后，亚洲诚信验证团队会对所有证书申请信息及相关文件进行复核，并根据验证结果决定批准、拒绝申请或要求申请者补充递交相关材料。亚洲诚信将对申请材料进行保密，对于批准申请的申请材料妥善保存；确保身份鉴别材料或电子数据具备不可篡改和抗抵赖性，私密信息不被泄露。在证书签发前，若亚洲诚信根据本 CP&CPS 第 2.2 章节指定来源获得的数据或证明文件不超过 398 天且该信息未发生变化，则亚洲诚信可使用该数据或证明文件，核实证书中的信息。

3.2.2 证书申请批准和拒绝

3.2.2.1 证书申请的批准

亚洲诚信成功完成了证书申请所必需的确认步骤后，通过颁发正式证书来批准证书申请。

如果符合下述条件，亚洲诚信可以批准证书申请：

1. 该申请完全满足 CP&CPS 第 2.2 章节关于订户身份的识别和鉴别的规定；
2. 订户接受或者没有反对订户协议的内容和要求；
3. 订户已经按照规定支付了相应的费用。

3.2.2.2 证书申请的拒绝

如果发生下列情形，亚洲诚信有权拒绝证书申请：

1. 申请不满足 CP&CPS 第 2.2 节的规定；
2. 订户不能根据要求提供所需的身份证明材料；
3. 订户不接收或申明反对订户协议的内容；
4. 订户未按照规定支付和相关费用；
5. 申请的证书含有 ICANN (The Internet Corporation for Assigned Names and Numbers) 考虑中的新 gTLD (顶级域名)；
6. 订户证书的使用途径不符合其所在地的法律法规；
7. 亚洲诚信认为批准该申请将会对亚洲诚信带来争议、法律纠纷或者损失。
8. 提交申请的公钥长度、算法或其他存在不安全因素。

对于拒绝的证书申请，亚洲诚信将会及时告知订户证书申请失败并告知其原因。

3.2.3 处理证书申请的时间

证书处理的时间很大程度上取决于订户何时提供完成验证所需的详细信息和文档以及是否及时地响应亚洲诚信的管理要求。证书申请请求会持续有效直至被拒绝。在申请者提交的资料齐全且符合要求的情况下，亚洲诚信处理证书申请的时间不超过 2 个工作日。

3.2.4 告知证书申请的结果

亚洲诚信成功完成了证书申请所必需的确认步骤后，通过颁发正式证书来批准证书申请。

对于拒绝证书申请的，亚洲诚信将会当面告知或邮件通知订户证书申请失败并告知其原因。亚洲诚信拒绝证书申请的原因如同本 CP&CPS 第 3.2.2.2 章节所述。

3.3 证书签发

3.3.1 证书签发中注册机构和认证机构的行为

亚洲诚信在签发之前确认证书请求的来源。

在签发过程中，RA 管理员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发往 CA 的证书签发请求信息须有 RA 的身份鉴别与信息保密措施，并确保请求发到正确的 CA 证书签发系统。CA 证书签发系统在获得证书签发请求后，对来自 RA 的信息进行鉴别与解密。

3.3.2 认证机构和注册机构对用户的通告方式

亚洲诚信在发布后的合理时间内以任何安全的方式提供证书。通常，亚洲诚信会在订户申请审核通过后，对订户的通告有通过以下几种方式：

1. 面对面告知，亚洲诚信把密码和数字证书等直接提交给订户，办理现场领取数字证书；
2. 电话通知；
3. 电子邮件通知；
4. 其他亚洲诚信认为安全可行的方式通知订户并交付证书。

3.3.3 证书获取方式

证书申请批准后，亚洲诚信将证书以安全的方式交付给申请者，申请者可以通过一下任意一种方式获取证书：

1. 由亚洲诚信将证书下载至数字证书载体，面对面交付；
2. 通过专门的亚洲诚信证书服务网站，自助下载证书。

3.4 证书接受

3.4.1 构成接受证书的行为

订户全权负责在订户的计算机或硬件安全模块上安装已颁发的证书。订户被认为接受已颁发的证书的行为包括但不限于：

1. 订户自行访问专门的亚洲诚信证书服务网站，将证书下载至数字证书载体中，并下载完毕。

-
2. 亚洲诚信在订户允许下，代替订户下载证书，并把证书通过安全载体发送给订户。
 3. 证书获取通知发送给订户后，订户通过该通知下载证书。
 4. 订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容。

3.4.2 认证机构对证书的发布

亚洲诚信按照订户协议把证书交付给订户视为证书的发布。

3.5 密钥对和证书的使用

3.5.1 用户私钥和证书的使用

订户在接受到亚洲诚信签发的证书后，应采取合理措施妥善保管密钥对并控制其使用授权，避免未经授权的使用。

订户应按协议规定、法律法规、CP&CPS 的范围内使用密钥对。对于签名证书，其私钥可以用于数字签名；对于加密证书，其私钥可用于数据解密。在证书到期或被撤销后，必须停止使用该证书。

3.5.2 信赖方公钥和证书的使用

依赖方应在依赖证书前考虑总体情况和损失风险。

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

1. 获得数字签名对应的证书及信任链；
2. 确认该签名对应的证书是依赖方信任的证书；
3. 通过查询CRL或OCSP确认该签名对应的证书是否被撤销；
4. 检查、验证证书有效期；
5. 证书的用途适用于对应的签名；
6. 使用证书上的公钥验证签名。
7. 考虑本CP&CPS或其它地方规定的其它信息。

以上条件不满足的话，依赖方有责任拒绝签名信息。

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。

3.6 密钥更新

3.6.1 密钥更新的情形

证书密钥更新一般有两种情况：补发和换发。

1. 证书补发

补发是指证书在有效期内，订户申请更新证书的操作。

以下情况订户需要申请证书补发：

- 1) 订户证书（文件）丢失或损坏或订户认为原有证书和密钥不安全；
- 2) 订户一张证书多处部署，需要使用不同的密钥对；
- 3) 订户需要增加域名（仅限于设备证书用于SSL/TLS服务器证书）；
- 4) 其他经亚洲诚信认可的原因。

2. 证书换发

换发是指在证书将要过期的 30 日（含）内，订户申请更新证书的操作。

在订户证书到期前的 30 日（含）内，亚洲诚信将通过适当的方式通知订户对证书进行换发操作。

若订户提交证书更新请求时不变更证书主体甄别名及相关身份信息，若原证书的验证可用且时效未过期（验证有效期为 398 天），则可以参考原证书验证方式审核验证，若原验证信息不可用或已超期，则亚洲诚信将按照初次申请证书流程和要求进行审核验证。

若订户提交证书更新请求时需要变更部分证书信息或原证书的验证时效已超过验证期限（验证有效期为 398 天），则亚洲诚信将按照证书初次申请的流程及要求进行验证。

若订户原来证书已过期，再次申请证书时按证书初次申请的流程及要求进行验证。证书撤销后不能进行密钥更新。

无论订户原证书的验证时效是否过期，订户在提交更新申请时都必须提交相应的申请资料并接受亚洲诚信的面对面审核。

3.6.2 证书更新的情形

同本 CP&CPS 第 3.6.1 章节。

3.6.3 更新申请的提交

已经申请过亚洲诚信证书且其证书未过期的证书持有者或证书持有者的授权代表可以向亚洲诚信提交证书更新申请，证书更新申请的提交方式同新申请。

3.6.4 更新申请的鉴别

对于证书更新，其处理过程包括申请识别和鉴别、证书信息验证及签发证书。

1. 对于申请的识别和鉴别须基于以下几个方面：
 - 1) 订户的原证书存在并且由亚洲诚信所签发；
 - 2) 证书更新请求在许可期限内；
 - 3) 订户能提交能够识别原证书的足够信息，如订户甄别名、证书序列号等。
2. 对于证书信息验证的处理过程，亚洲诚信将按照本 CP&CPS 第 2.3.1 章节之规定进行处理；亚洲诚信也可以根据订户证书更新的具体申请情况，选择按一般初次证书申请流程进行验证。
3. 以上鉴别和验证全部通过后，亚洲诚信才可以批准签发证书。

3.6.5 密钥更新方式

密钥更新分为以下三种情况，亚洲诚信会根据不同情形对证书做相应更新：

1. 证书变更
当订户提交证书信息变更申请后，亚洲诚信会对证书信息进行重新审核。审核通过后，亚洲诚信将重新签发新的证书。变更证书的有效期与原证书有效期一致。
2. 证书补发
当订户需要补发证书时，应主动向亚洲诚信提出证书补发申请。亚洲诚信会对证书信息进行重新审核。审核通过后，亚洲诚信将重新签发新的证书。补发证书的有效期与原证书有效期一致。
3. 证书换发
当订户证书需要换发时，应主动向亚洲诚信提出证书换发的申请。亚洲诚信会对证书信息进行重新审核。审核通过后，亚洲诚信将重新签发新

的证书。新证书有效期将从证书换发之日起至原证书到期为止再另加一个证书有效周期。

3.6.6 通知证书持有者密钥更新

同本 CP&CPS 第 3.3.2 章节。

3.6.7 构成接受密钥更新的行为

同本 CP&CPS 第 3.4.1 章节。

3.6.8 认证机构对密钥更新的发布

同本 CP&CPS 第 3.4.2 章节。

3.7 证书变更

3.7.1 证书变更的情形

证书变更是指订户的证书在其有效期内，证书扩展信息的备用名称发生变更而重新签发新的证书。

亚洲诚信不接受订户变更证书机构名称的请求，如需变更机构名称，订户需重新申请新的证书。

3.7.2 证书变更的申请

同本 CP&CPS 第 3.6.3 章节。

3.7.3 证书变更的鉴别

当订户提交证书信息变更申请后，亚洲诚信会对证书信息进行重新验证，若原证书的验证可用且时效未过期（验证有效期为 398 天），则可以参考原证书验证方式审核验证，若原验证信息不可用或已超期，则亚洲诚信会按照初次申请证书流程和要求进行审核验证。但无论原验证是否可用，订户都必须提交相应申请资料并接受亚洲诚信的面对面审核。审核通过后，亚洲诚信将重新签发新的证书。变更证书的有效期与原证书有效期一致。

3.7.4 证书变更受理方式

同证书新申请的受理方式。

3.7.5 通知证书持有者证书变更

同本 CP&CPS 第 3.3.2 章节。

3.7.6 构成接受证书变更的行为

同本 CP&CPS 第 3.4.1 章节。

3.7.7 认证机构对证书变更的发布

同本 CP&CPS 第 3.4.2 章节。

3.8 证书撤销

3.8.1 证书撤销的情形

3.8.1.1 订户证书撤销的情形

若出现以下情况的一种或多种，亚洲诚信将在 24 小时之内撤销证书，适当情况下将此类投诉转发给执法部门：

1. 订户以书面形式请求撤销证书；
2. 订户通知亚洲诚信最初的证书请求未得到授权且不能追溯到授权行为；
3. 亚洲诚信获得了证据，证明与证书公钥对应的订户私钥遭到了损害；
4. 亚洲诚信获得证据，证书中所包含的域名或IP地址的控制权验证已不再可靠；
5. 亚洲诚信获得了证书遭到误用的证据；
6. 亚洲诚信获悉订户违反了订户协议、CPS 中的一项或多项重大责任；
7. 亚洲诚信获悉任何表明 FQDN 或 IP 地址的使用不再被法律许可（例如，某法院或仲裁员已经撤销了域名注册人使用域名的权力，域名注册人与申请人的相关许可及服务协议被终止，或域名注册人未成功更新域名）；
8. 亚洲诚信获悉证书中所含信息出现重大变化；
9. 亚洲诚信获悉证书的签发未能符合亚洲诚信的CP&CPS；
10. 亚洲诚信认为任何出现在证书中的信息不准确、不真实或具有误导性；
11. CP&CPS中职责的履行被延迟或受不可抗力的阻碍；自然灾害；计算机或通信失败；法律、规章或其它法律的改变；政府行为；或其它超过个人控制的原因并且对他人信息构成威胁的；
12. 亚洲诚信已经履行催缴义务后，订户仍未缴纳服务费。
13. 证书的技术内容或格式对应用程序软件供应商或依赖方构成不可接受的风险（如，可能会确定已弃用的加密/签名算法或密钥大小会带来不可接受的风险，因此应将此类证书在给定的时间内撤销）。

3.8.1.2 中级 CA 证书撤销的原因

若出现以下情况中的一种或多种，亚洲诚信应在 7 天之内撤销中级 CA 证书：

1. 中级证书颁发机构正式书面申请撤销；
2. 中级证书颁发机构发现并通知亚洲诚信初始证书请求未经过授权且不能追溯到授权行为；
3. 亚洲诚信获得了证据，证明与证书公钥对应的中级 CA 私钥遭到了损害；
4. 亚洲诚信获得了证书遭到误用的证据；
5. 亚洲诚信获悉中级证书的签发未能符合CP&CPS；
6. 亚洲诚信认为任何出现在中级CA证书中的信息不准确、不真实或具有误导性；
7. 亚洲诚信由于任何原因停止运营，且未与另一家CA达成协议以提供证书撤销服务；
8. 证书的技术内容或格式给应用软件供应商或依赖方带来了不可接受的风险（如，可能确定不赞成使用的加密/签名算法或密钥大小带来不可接受的风险。

3.8.2 可以发起请求撤销证书的实体

请求证书撤销的实体可为订户、亚洲诚信、或经司法机构授权的司法人员。此外，依赖方、应用软件提供商，防病毒机构或其他第三方可以提交证书问题报告，告知亚洲诚信有合理理由撤销证书。

3.8.3 证书撤销的申请

3.8.3.1 订户主动提出撤销申请

订户可通过向亚洲诚信提交撤销证书申请表及相关身份证明材料，申请表中需说明撤销原因。

3.8.3.2 订户被强制撤销证书

1. 当亚洲诚信有充分的理由确信出现本 CP&CPS第 3.8.1 章节中会导致订户证书被强制撤销的情形时，亚洲诚信将通过内部流程申请撤销证书；
2. 当亚洲诚信的根证书或中级 CA证书相对应的私钥出现安全风险时，经国家电子认证服务主管部门批准后可直接发起内部流程申请撤销证书；
3. 依赖方、司法机构、应用软件提供商、防病毒机构等第三方可以前往受理点当场提交证书问题报告并提出撤销申请。

3.8.4 证书撤销的鉴别

3.8.4.1 订户主动提出撤销申请的鉴别

1. 亚洲诚信按本CP&CPS第2.4章节的规定进行证书撤销请求的鉴别；
2. 亚洲诚信进行撤销请求鉴别后，一并确认订户所需撤销的证书是否为亚洲诚信所发放，证书是否在有效期内，撤销理由是否属实，若均通过则对证书进行撤销。

3.8.4.2 订户被强制撤销证书的鉴别

1. 当亚洲诚信有充分的理由确信出现本 CP&CPS第3.8.1 章节中会导致订户证书被强制撤销的情形时，亚洲诚信将通过内部流程申请撤销证书并提供相关证明材料，经过复审鉴别后完成撤销；
2. 在亚洲诚信的根证书或中级 CA证书相对应的私钥出现安全风险时，经国家电子认证服务主管部门批准后可直接发起内部流程申请撤销证书并提供相关证明材料，经过复审鉴别后完成撤销；
3. 当依赖方、司法机构、应用软件提供商、防病毒机构等第三方提出证书撤销申请时，亚洲诚信将组织调查并根据调查结果来决定是否撤销证书，并告知其结果。

3.8.5 证书撤销受理方式

亚洲诚信只接受受理点现场提交的证书撤销书面申请。

订户或其授权代表（机构证书必须指定授权代表）需前往亚洲诚信受理点提交证书撤销申请表、授权书以及身份证明材料。

依赖方、司法机构、应用软件提供商、防病毒机构等第三方需要申请撤销证书的须提交书面证书问题报告。

3.8.6 认证机构处理撤销请求的时限

亚洲诚信将在收到撤销请求或证书问题报告后的 24 小时内展开调查，以决定是否撤销证书或采取其它合理处置方式。

3.8.7 通知证书持有者证书撤销

当订户主动提出证书撤销申请并且证书被撤销后，亚洲诚信会以电子邮件等适当方式通知证书持有者，若未能联络到证书持有者，在必要情况下，亚洲诚信可以通过网站进行公告被撤销的证书。

当订户证书被强制撤销后，亚洲诚信将通过适当的方式，包括邮件、电话等，通知证书持有者已被撤销及被撤销的理由；若未能联络到证书持有者，在必要情况下，亚洲诚信可以通过网站进行公告被撤销的证书。

3.8.8 构成接受证书撤销的行为

证书撤销列表 CRL 作为公开的信息，没有读取权限的安全设置，依赖方可以自由的根据需要进行查询，包括查询证书撤销列表、通过亚洲诚信指定网站查询证书状态、通过在线证书状态协议（OCSP）方式查询等。

依赖方在信任此证书前，应根据亚洲诚信最新公布的 CRL 主动检查证书的状态，同时还需验证 CRL 的可靠性和完整性，以确认证书的有效性。

3.8.9 认证机构对证书撤销的发布

亚洲诚信完成撤销工作后将及时将其发布到证书撤销列表。

证书撤销列表 CRL 作为公开的信息，没有读取权限的安全设置，依赖方可以自由的根据需要进行查询，包括查询证书撤销列表、通过亚洲诚信指定网站查询证书状态、通过在线证书状态协议（OCSP）方式查询等。

依赖方在信任此证书前，应根据亚洲诚信最新公布的 CRL 主动检查证书的状态，同时还需验证 CRL 的可靠性和完整性，以确认证书的有效性。

3.8.10 CRL发布频率

对于订户证书的 CRL 发布周期至少 24 小时发布一次。

对于中级证书的 CRL 发布周期至少 12 个月发布一次，若对中级证书有撤销行为 CRL 应在至少 24 小时内发布更新。

3.8.11 CRL发布的最大滞后时间

亚洲诚信 CRL 生成后会自动发布至公网，一般情况下 1 小时内生效，最长在 24 小时内生效。

3.8.12 在线状态查询的可用性

亚洲诚信的 OCSP 查询服务符合 RFC2560 和 RFC6960 标准，服务 7X24 小时可用，且 OCSP 的响应数据由被查询证书的上级 CA 证书签名或由被查询证书上级 CA 签发的 OCSP 响应者证书签名。

3.8.13 在线状态查询要求

亚洲诚信提供的 OCSP 服务支持 POST 和 GET 两种请求方式，订户可自由进行在线状态查询。

亚洲诚信若收到未签发证书的 OCSP 请求，不会响应“good”状态。

3.9 密钥生成、备份与恢复

3.9.1 证书持有者密钥恢复

订户的签名证书密钥由订户自行管理，亚洲诚信不提供密钥恢复。加密证书的密钥则由订户的签名证书的公钥进行加密，订户使用签名证书的私钥进行密钥恢复。亚洲诚信对加密后的密钥进行备份管理，依照相关的管理规定进行密钥恢复。

3.9.2 问责取证密钥恢复

1. 亚洲诚信对密钥备份进行记录与归档；
2. 亚洲诚信对备份密钥恢复事件保留记录；
3. 密钥由订户生成的公钥信息加密。

3.10 证书挂起

3.10.1 证书挂起的情形

出现以下情形之一，亚洲诚信可将订户证书暂时挂起：

- 1) 订户请求挂起证书；
- 2) 经授权的司法人员、依赖方、应用软件提供商、防病毒机构等相关第三方有充分合理理由并递交书面证明材料，申请挂起订户证书；
- 3) 亚洲诚信发现订户的征信或经营状态出现重大问题；
- 4) 亚洲诚信发现订户证书申请资料存在虚假信息，不能满足证书签发条件；
- 5) 亚洲诚信发生或怀疑发生私钥泄露、认证系统存在安全隐患威胁用户证书安全；
- 6) 亚洲诚信有理由相信订户未履行订户协议下的义务、陈述或保证；
- 7) 亚洲诚信 CPS 要求或有相关法律法规要求挂起订户证书。

3.10.2 请求挂起的实体

请求证书挂起的实体可为订户、亚洲诚信 CA、或经司法机构授权的司法人员。此外，依赖方、应用软件提供商，防病毒机构或其他的第三方可以提交证书问题报告，告知亚洲诚信 CA 有合理理由挂起证书。

3.10.3 证书挂起请求的鉴别

在亚洲诚信 CA 的证书业务中，证书挂起请求可以来自订户，也可以来自亚洲诚信 CA。另外，当亚洲诚信 CA 有以下所述理由需要挂起订户的证书时，有权发起挂起订户证书：

出现以下情形之一，亚洲诚信可将订户证书暂时挂起：

- 1) 订户请求挂起证书；
- 2) 经授权的司法人员、依赖方、应用软件提供商、防病毒机构等相关第三方有充分合理理由并递交书面证明材料，申请挂起订户证书；
- 3) 亚洲诚信发现订户的征信或经营状态出现重大问题；
- 4) 亚洲诚信发现订户证书申请资料存在虚假信息，不能满足证书签发条件；
- 5) 亚洲诚信发生或怀疑发生私钥泄露、认证系统存在安全隐患威胁用户证书安全；

6) 亚洲诚信有理由相信订户未履行订户协议下的义务、陈述或保证；

7) 亚洲诚信 CPS 要求或有相关法律法规要求挂起订户证书。

订户需要前往受理点提交书面申请资料向亚洲诚信 CA 提交请求，亚洲诚信 CA 通过与证书保障级别相应的方式来确认要挂起证书的人或组织确实是订户本人，或者其授权者。依据不同的情况，确认方式可以采用下面的一种或几种：域名控制权验证、电话、传真、e-mail、邮寄或快递服务。

3.10.4 挂起请求的流程

3.10.4.1 订户主动提出挂起申请

- 1) 订户可通过向亚洲诚信CA提交挂起证书申请表及相关身份证明材料；
- 2) 亚洲诚信CA按本CP&CPS第3.10.3章节的规定进行证书挂起请求的鉴别；
- 3) 亚洲诚信CA进行撤销请求鉴别后，一并确认订户所需挂起的证书是否为亚洲诚信CA所发放，证书是否在有效期内，挂起理由是否属实，若均通过则对证书进行挂起；
- 4) 亚洲诚信CA完成挂起工作后应及时将其发布到CRL及OCSP上；
- 5) 证书被挂起后，亚洲诚信CA会以电子邮件等适当方式通知订户，若未能联络到订户，在必要情况下，亚洲诚信CA可以通过网站进行公告被挂起的证书；
- 6) 亚洲诚信CA提供7*24小时的证书挂起申请服务，订户主动申请证书挂起的，必须提交书面申请资料。
- 7) 亚洲诚信CA在鉴别挂起请求有效后，于2个工作日内完成证书挂起。

3.10.4.2 订户被强制挂起证书

- 1) 当亚洲诚信CA有充分的理由确信出现本CP&CPS第3.10.1章节中会导致订户证书被强制挂起的情形时，亚洲诚信CA将通过内部流程申请撤销证书；
- 2) 当依赖方、司法机构、应用软件提供商、防病毒机构等第三方提请证书问题报告时，亚洲诚信CA应组织调查并根据调查结果来决定是否挂起证书，若决定挂起将告知其结果；
- 3) 在证书被挂起后，亚洲诚信CA将通过适当的方式，包括邮件等，通知最终订户证书已被挂起及被挂起的理由；若未能联络到订户，在必要情况下，亚洲诚信CA可以通过网站进行公告被挂起的证书；
- 4) 亚洲诚信CA提供7*24小时的证书问题报告及处理服务，相关方可通过本CP&CPS第1.4.2章节中所提供的联系方式进行问题报告。
- 5) 亚洲诚信CA于2个工作日完成证书挂起。

3.10.5 证书挂起的限制

订户证书一旦被挂起将处于挂起状态直至：

订户通过提交申请表、身份证证件证明文件以及授权书要求解除冻结自己的证书或者直接撤销自己的证书，经亚洲诚信 CA 审核后，决定解除冻结或撤销证书，并将结果以适当方式（包括邮件等）通知订户；

当证书被动挂起时，订户可在收到挂起通知后 3 个工作日内向亚洲诚信 CA 提出申辩并提交相关证明材料，亚洲诚信 CA 对申辩评估后，认定其证据合理充分后，解除冻结证书，并将结果及理由以适当方式（包括邮件等）通知相关方；

当证书被动挂起的原因消除后，订户可以通过提交申请表、身份证证件证明文件、授权书及相关证明材料要求解除冻结证书，经亚洲诚信 CA 审核后，决定解除冻结证书，并将结果及理由以适当方式（包括邮件等）通知相关方；当被挂起的证书到期时，亚洲诚信 CA 内部可以发起证书撤销流程，并于 2 个工作日内将结果及理由以适当方式（包括邮件等）通知相关方。

4. 应用集成支持与信息服务操作规则

4.1 服务策略和流程

1. 针对不同政府行业的业务背景，亚洲诚信根据行业提供区分性的证书模板和接口文档，具体到每个项目再对业务系统进行充分调研，指导或参与业务系统证书应用部分的开发和实施；
2. 制定项目管理制度，规范系统和程序开发行为；
3. 制定安全控制流程，明确人员职责；
4. 实施证书软件发布版本管理，并进行证书应用环境控制；
5. 项目开发程序和文档等资料妥善归档保存。

4.2 应用接口

4.2.1 密码设备调用接口

密码设备应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的底层应用接口。

服务器端密码设备的底层应用接口符合 GM/T 0018 的要求；客户端证书介质的底层应用接口符合 GM/T 0016 和 GM/T 0017 的要求。

4.2.2 密码模块安全技术接口

亚洲诚信采用新模式与新技术密码模块安全技术接口，符合 GM/T 0028 和 GM/T 0054 的要求。

4.2.3 通用密码服务接口

通用密码服务接口为各类密码服务层和应用层提供统一的通用密码服务接口，符合 GM/T 0019 的要求。

4.3 集成内容

亚洲诚信为电子政务应用单位提供证书应用接口程序集成工作。集成工作提供以下服务：

1. 证书应用接口的开发包（包括客户端和服务器端）；
2. 接口说明文档；
3. 集成演示Demo；
4. 集成手册；
5. 证书应用接口开发培训和集成技术支持；
6. 协助应用系统开发商完成联调测试工作。

4.4 信息服务内容

4.4.1 证书信息服务

亚洲诚信提供证书的申请、撤销、证书更新、密钥更新等服务。证书主要分为身份标识证书以及服务器证书，证书格式符合 GM/T 0015 标准。

4.4.2 CRL信息服务

亚洲诚信提供CRL服务，同3.8.10以及3.8.11。

4.4.3 服务支持信息服务

4.4.3.1 服务内容

1. 亚洲诚信提供证书售后服务，包括证书申请、证书撤销、证书重签发、证书部署等场景的协助以及证书产品培训。
2. 亚洲诚信提供证书售前服务，包含信息系统需要证书的场景的建议、CPS解答、价格咨询等服务。
3. 亚洲诚信提供接口服务。

4.4.3.2 服务能力

1. 亚洲诚信提供5*8小时在线支持服务。
2. 受理方式包含工单系统、电子邮件等方式，内容包含专业服务、满意度调查、知识库、投诉受理等

4.4.3.3 服务质量

1. 亚洲诚信对支持服务提供及时的响应
2. 提供多种服务渠道，包含IM工具、电话、远程软件等
3. 落实投诉的处理承诺

4.4.4 决策支持信息服务

亚洲诚信运营依照国家相关管理规定进行实施。

4.5 信息服务管理规则

亚洲诚信在提供信息服务时，将确保做好相关信息的隐私保障机制，实现对用户的信息保护承诺。

1. 私有信息类型的敏感度
以下信息属于私有信息：

- 1) 个人隐私信息；
- 2) 商业机密；
- 3) 政府部门的敏感信息和工作秘密。

证书申请过程中涉及的用户申请信息是敏感信息，而发布的证书和CRL信息不是敏感信息，证书发布根据用户要求进行公布与不公布。

2. 允许的私有信息采集
亚洲诚信仅允许在进行证书发放和管理时才能收集CPS声明的私有信息。
3. 允许的私有信息使用
亚洲诚信只使用CA或者RA收集的私有信息。
4. 私有信息的安全存储
亚洲诚信采取安全手段对用户私有信息进行安全存储，确保用户私有信息不发生泄露、未授权访问等安全事件。
5. 允许的个人信息发布
亚洲诚信仅能面向证书应用单位发布与之相关的私有信息，以协助证书应用单位进行证书业务管理。
任何特定的私有信息发布应遵照相关法律和政策实行。

-
6. 所有者纠正私有信息的机会
亚洲诚信允许用户在其证书生命周期内对其私有信息进行更正。
 7. 对司法及监管机构发布私有信息
亚洲诚信在以下情况下，可以执行将私有信息提供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。

4.6 信息服务方式

4.6.1 证书信息同步服务

亚洲诚信根据用户提交的材料，通过录入员将信息同步至电子政务系统中。电子政务系统将签发的证书同步到系统的 web 服务，以供订户下载；另外也提供接口的方式来同步证书。

4.6.2 CRL信息同步服务

签发的证书扩展中，包含 CRL 地址，亚洲诚信确保此 CRL 的信息同步，并且对此 CRL 进行数字签名。

4.6.3 服务支持信息服务

同 4.4.3

4.6.4 决策支持信息服务

亚洲诚信在信息库中公布面向电子政务用户相关的决策信息。

5. 使用支持服务操作规则

5.1 服务内容

5.1.1 面向证书持有者的服务支持

1. 数字证书管理
数字证书的导入、导出，以及客户端证书管理工具的安装、使用、卸载等。
2. 数字证书使用
基于数字证书的身份认证、电子签名、加解密等应用过程中出现的各种异常问题，如：证书无法读取、签名失败、证书验证失败等。
3. 证书存储介质硬件设备使用
包括证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。
4. 电子认证服务支撑平台使用
在认证机构的数字证书在线服务平台中使用的各类问题，如：密钥更新失败、下载异常、无法提交注销申请等。

5.1.2 面向应用提供方的服务支持

1. 电子认证软件系统使用
提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用支持问题，如证书信息无法查询、数据同步失败、服务无响应等。
2. 电子签名服务中间件的应用
解决服务中间件在集成时出现的各种情况，如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

5.2 服务方式

5.2.1 座席服务

亚洲诚信提供 7*24 热线服务，服务热线：400-880-8600。

5.2.2 在线服务

1. 自助信息查询系统
将知识库信息按照不同的类型、属性、层次等方式、结构进行分类存储，用户可以按照咨询问题或者已知条件在信息查询系统上进行启发式的检索，查找目标问题的答案。
2. 网络实时通讯系统
用户可以通过官网上的实时通讯工具与亚洲诚信网络客服人员取得联系，进行交流。
3. 远程终端协助系统
用户通过安装远程终端软件，可以通过互联网或者局域网向客户服务人员发起协助请求。由服务人员通过远程终端控制功能，实时检测用户的软硬件环境，通过同屏显示指导、帮助用户解决应用故障。
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结合，方便用户既可以打电话、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。

5.2.3 现场服务

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

5.2.4 满意度调查

通过多种用户可接受的多种调查方式，如电话、邮件系统、满意度表单等，进行客户回访来收集用户满意度调查报告。

亚洲诚信将用户回访中产生的相关文档进行归档、保存。

5.2.5 投诉受理

用户可通过 400-880-8600 热线电话、电子邮件等方式进行投诉。

亚洲诚信将启动投诉处理流程，在受理过程中记录投诉问题，将投诉受理中产生的相关文档进行归档、保存，并将结果及时反馈给用户。

5.2.6 客户培训

培训方式可以由亚洲诚信与用户双方约定的形式开展。

培训内容主要包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答（FAQ）、操作手册等。

5.3 服务质量

亚洲诚信的热线服务（400-880-8600）为 7*24 小时服务；

亚洲诚信的在线服务、现场服务为 5*8 小时服务；在有应急服务需求的特殊情况下，将提供及时的服务响应。

亚洲诚信对技术问题和故障按照一般事件、严重事件、重大事故进行分类，并制定了响应处理流程和机制，确保服务的及时性和连续性。技术支持响应时间以最大程度不影响客户使用为准则。

同时，亚洲诚信接受国家密码管理局和省部密码管理部门组织开展的服务质量评估检查。

6. 认证机构设施、管理和操作控制

6.1 物理控制

6.1.1 场所区域与建筑物

亚洲诚信的运营机房位于上海市浦东新区锦绣东路 4819 号，进入机房实行分层访问管理，依次为公共区、管理服务区、缓冲区、CA 核心区（屏蔽机房）、KM 核心区（屏蔽机房）。

亚洲诚信机房具备抗震、防火、防水、恒湿温控、独立供电、备用发电、门禁控制、视频监控等功能，可保证认证服务的连续性和可靠性。机房和系统建设遵循下列标准实施：

- 1) 《计算机场地技术要求》（GB 2887-89）
- 2) 《电子信息系统机房设计规范》（GB 50174- 2008）
- 3) 《建筑内部装修设计防火规范》（GB50222-95）
- 4) 《低压配电设计规范》（GBJ50054-95）
- 5) 《处理涉密信息的电磁屏蔽室的技术要求和测试方法》C 级（BMB3-1999）
- 6) 《电子计算机场地通用规范》（GB/T 2887-2011）
- 7) 《建筑物防雷设计规范》（GB/50057-2010）

6.1.2 物理访问

亚洲诚信 CA 机房的门禁系统可实现对各层门进出的控制，具备以下功能：

- 采用门禁卡和指纹鉴别的控制方式控制每个区域的进入；
- 进出每一道门都有日志记录；
- 每个区域整个区域还有视频监控系统，对场地内外的重要通道实行 7*24 小时不间断录像。所有录像资料至少保留 6 个月，以备查询。
- 管理服务区和核心区的门都设有强开报警和超时报警；
- 整套门禁系统连接 UPS，在市电中断时由 UPS 提供紧急供电。

亚洲诚信可信人员自进入亚洲诚信 CA 机房公共区后，均须经过双人指纹认证加门禁授权卡身份认证。

针对外来人员进入楼内，需经过亚洲诚信审核通过后，且在亚洲诚信可信人员的陪同进入。

6.1.3 电力和空调

亚洲诚信有安全、可靠的电力供电系统及电力备用系统双路供电，以确保系统 7*24 小时正常供电及在出现供电系统出现供电中断是能够提供正常的服务。另外，还采用专用柴油机，可满足新建机房所有机架满载可续航 12 小时以上。

机房内具有空调系统控制运营设施中的温度和湿度，功率按各机房机柜数量、设备满载情况配置

6.1.4 水患防治

亚洲诚信 CA 机房高于地面 1.45 米并部署有漏水报警系统，一旦发生水患系统将立即报警，通知有关人员采取应急措施。

6.1.5 火灾预防和保护

亚洲诚信 CA 机房消防报警系统采用柜式七氟丙烷自动灭火装置。系统通过设置在机房的温感和烟感采集消防数据，同时供系统实时处理用户火灾自动报警终端的报警数据和系统运行状态数据。系统管理分手动模式和自动模式两种，实现网络系统实时检测、监测和系统的手动、自动控制模式的设定，并完成了系统设计的有关各种联动动作。

6.1.6 介质存储

亚洲诚信对审计、归档、备份信息的介质保存在安全的设施中，使用物理访问控制进行保护，只允许授权人员访问且需要至少 2 名可信人员在场，并采取介质使用登记进行记录介质情况，以防止重要信息的泄露和损坏。

6.1.7 废物处理

亚洲诚信对不在使用的纸张文件和数据光盘进行粉碎处理，使信息无法恢复；
对于涉密介质在作废处理前要根据生产商的指导做归零处理；
对于加密设备在作废处理前根据设备制造商提供的方法将期初始化并进行特例销毁。
在处理作废内容时，应经过审批，至少 2 名可信人员在场，并记录过程。

6.1.8 异地备份

亚洲诚信采用了完全备份与增量备份相结合的方式对生产系统数据和信息进行备份。制定了备份数据收集、保管、押运、恢复管理策略，确保备份数据的安全，防止泄露和未经授权使用。
对关键数据、审计日志数据使用离线介质进行备份并运送到异地保存，保存设施满足 6.1.6 章节介质存储的描述。并会定期检查备份系统和设备的可靠性和可用性，定期检查备份介质可靠性和数据完整性。

6.2 操作过程控制

6.2.1 可信角色

亚洲诚信在提供电子认证服务过程中，将能从本质上影响证书的签发、使用、管理和撤销等涉及密钥操作的职位都视为可信角色。这些角色包括但不限于：

- 鉴别和客服人员：负责订户信息录入、审核数字证书申请信息、完成鉴别、审批和撤销等操作，并提供相关支持服务；
- 密钥与密码设备管理人员：负责维护 CA 密钥和证书生命周期，负责管理加密设备；
- 系统维护人员：负责对 CA 系统的硬件和软件实施日常维护，并监控和排查故障；
- 安全管理人员：负责场地安全、日常安全管理工作；
- 安全审计人员：负责对业务操作行为进行审计；
- 人力资源管理人員：负责对关键岗位人员实施可信度背景调查、安全管理等工作。

6.2.2 角色的识别与鉴别

亚洲诚信在允许所有人员访问并执行其受信任角色所必需的系统之前，都需要向 CA 和 RA 系统进行身份验证。例如：

- 对于可信人员的物理访问，通过门禁卡和指纹识别进行鉴别，并确定相应的权限。
- 对于进行订户证书生命周期管理的可信人员，通过使用相应的数字证书访问系统，完成证书管理工作。
- 对于系统维护人员，他们使用各自的帐户和密码通过堡垒机登录系统进行维护工作。

6.2.3 角色职责分离设置

为保证系统安全，遵循可信角色分离的原则，即亚洲诚信的可信角色由不同的人担任。亚洲诚信 CA 涉及职责分离的角色主要有：

- 鉴证服务岗；
- 财务管理岗；
- 系统运维岗；
- 密钥管理岗。

6.3 人员控制

6.3.1 可信人员要求

亚洲诚信对承担可信角色的工作人员的资格要求如下：

1. 具备良好的社会和工作背景。
2. 遵守国家法律、法规，无违法犯罪记录。
3. 遵守亚洲诚信有关安全管理的规范、规定和制度。
4. 具有认真负责的工作态度和良好的从业经历。
5. 具备良好的团队合作精神。
6. 关键和核心岗位的工作人员必须具备相关的工作经验，或通过亚洲诚信相关的培训和考核后方能上岗。

6.3.2 可信人员背景审查

亚洲诚信依据有关材料，通过公司自主背调方式完成对可信人员的工作背景调查。

所有的可信员工和申请调入的可信员工都必须同意对其进行背景调查。背景调查必须符合法律法规的要求，调查内容、调查方式和从事调查的人员不得有违反法律法规的行为。背景调查应使用合法手段，尽可能地通过相关组织、部门进行人员背景信息的核实。

背景调查分为：基本调查和全面调查。基本调查包括对工作经历，职业推荐，教育，社会关系方面的调查。全面调查除包含基本调查项目外还包括对犯罪记录，信用记录方面的调查。对于公开信任证书业务的关键岗位必须进行全面调查。

人事部门调查程序包括：

- 对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。
- 通过电话、网络等形式对其提供的材料的真实性进行鉴定。

-
- 完成调查后，将结果上报主管相关工作的领导进行批准。
 - 亚洲诚信与员工签订保密协议，以约束员工不许泄露 CA 证书服务的所有保密和敏感信息。同时，对所有承担可信角色的在职人员进行职位考察，以便能够持续验证这些人员的可信程度和工作能力。

6.3.3 人员培训及再培训

亚洲诚信根据可信角色的职位需求，给予相应的岗前培训，将员工参加培训的情况形成记录并存档，培训内容包括但不限于：

- 基本公钥基础设施（PKI）知识；
- CP&CPS 及相关标准和程序；
- 身份认证和验证政策和程序；
- 安全管理策略和机制；
- 灾难恢复和业务连续性程序；
- 国家关于电子认证服务的法律、法规及标准、程序；
- 其他需要进行的培训等。

对于充当可信角色或其他重要角色的人员，每年至少进行一次相关技能和知识培训。此外，亚洲诚信将根据机构系统升级、策略调整等要求，不定期的要求人员进行继续培训。

6.3.4 工作岗位轮换周期和顺序

亚洲诚信将依据本机构的内部策略而制定在职人员的工作岗位轮换周期和顺序。

6.3.5 违规行为处罚

当出现在职人员未经授权或超出权限使用亚洲诚信 CA 系统操作认证业务等情况时，一经确认，将立即撤销该人员的登录证书、同时终止其系统访问权限，并视该人员未授权行为的情节严重性实执行相关惩罚措施。

6.3.6 外包服务人员及要求

对于雇用与亚洲诚信 CA 业务有关工作的独立合约人，会要求提供身份证、学历证书、资格证书等有效证明，并需签署保密协议。

6.3.7 提供给员工的文档及保密策略

亚洲诚信向其员工提供完成其工作所必须的文档。

6.4 审计日志程序

6.4.1 审计事件的类型

亚洲诚信支持其 CA 的所有基本事件审核功能以记录下列事件。如果亚洲诚信 CA 的应用程序无法自动记录事件，会实施手动程序以满足要求。这些事件包括但不限于以下类型：

- CA 密钥生命周期内的管理事件，包括：
 - 密钥生成、备份、存储、恢复、使用、撤销、归档、销毁、私钥泄露等；
- 密码设备生命周期内的管理事件，包括：
 - 设备接收、安装、卸载、激活、使用、维修等；

-
- 证书申请事件，包括：
 - 订户接受订户协议，申请资料验证、申请及验证资料保存等；
 - 证书生命周期内的管理事件，包括：
 - 证书的申请、批准、更新、撤销等；
 - 成功或失败的证书操作；
 - 系统安全事件，包括：
 - 成功或不成功访问 CA 系统的活动，
 - 对于 CA 系统网络的非授权访问及访问企图，
 - 对于系统文件的非授权的访问及访问企图，
 - 安全、敏感文件或记录的读、写或删除，
 - 系统崩溃，硬件故障和其他异常；
 - 防火墙和路由器记录的安全事件；
 - 系统操作事件，包括：
 - 系统启动和关闭，
 - 系统权限的创建、删除，设置或修改密码；
 - CA 设施的访问，包括：
 - 授权人员进出 CA 设施，
 - 非授权人员进出 CA 设施及陪同人和安全存储设施的访问；
 - 可信人员管理记录，包括：
 - 网络权限的帐号申请记录，
 - 系统权限的申请、变更、创建申请记录，
 - 人员情况变化。

上述日志记录一般包含记录的时间、序列号、做日志记录的实体身份、记录内容的描述。

6.4.2 审计日志的处理周期

对于系统的自动日志和操作人员的手工记录，每月进行一次检查。

对系统安全日志，每月进行一次跟踪处理，检查违反策略和规范的重大事件。

对于系统审计，其对象包括与认证业务有关的软件与硬件设备，包括但不限于证书认证系统、密钥管理系统、应用软件系统、数据库系统、密码设备、防火墙、路由器、防病毒系统等。这些操作都有相应的系统审计日志。

对于系统运行日志应该每周审计一次。

6.4.3 审计日志记录的保存期限

亚洲诚信所有审计日志在证书失效后至少保存 10 年。

6.4.4 审计日志的保护措施

亚洲诚信的审计日志储存在数据库里并备份，其中包括有关文档中的审计信息和事件记录。

亚洲诚信执行严格的物理和逻辑访问控制措施，以确保只有授权人员才能接近这些审查记录，严禁未授权的访问、阅读、修改和删除等操作。

对于书面形式的归档记录文件，设有专门的文件柜，由专人对书面档案进行妥善保存，并有相应的查阅制度，确保只有经批准的人员方可访问书面归档记录。

6.4.5 审计日志的备份程序

亚洲诚信的系统日志进行定期备份；电子记录备份到备份服务器，手工纸质记录归档保存到专门的文件柜内。

6.4.6 审计收集系统

应用程序、网络和操作系统等都会自动生成审计数据和记录信息。

6.4.7 对导致事件实体的通告

当亚洲诚信发现被攻击时，将记录攻击者的行为，在法律许可的范围内追溯攻击者，保留采取相应对策措施的权利。亚洲诚信有权决定是否对事件相关实体进行通知。

6.5 记录归档要求

6.5.1 记录归档的类型

亚洲诚信对以下几类事件进行归档记录，包括但不限于：

1. 证书信息，证书服务批准和拒绝信息；
2. 证书申请信息、相关资料、相关证明文件及审核操作数据；
3. 证书更新、撤销及挂起请求信息及相关资料、证明文件及审核操作数据；
4. 审计记录；
5. CP&CPS；
6. 员工资料，包括但不限于背景调查、录用、培训等资料；
7. 各类外部、内部评估文档。

6.5.2 记录归档的保存期限

1. 对订户证书生命周期内的管理事件的归档，保留 10 年以上。
2. 对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生命周期。
3. 订户证书的归档保留期限不少于证书失效后 10 年。
4. CA 证书和密钥的归档在其生命周期之外，额外保留 10 年

6.5.3 记录归档的保护措施

亚洲诚信对电子、纸质形式的归档文件有安全的物理和逻辑保护，同时有严格的管理程序，确保归档文件不会被损坏，防止非授权访问、修改删除等行为的发生。

6.5.4 记录归档的备份程序

对系统生成的电子记录进行定期备份，备份以离线介质形式进行异地存放；对手工生成的电子记录，归档以备份服务器进行备份。
对纸质资料，不需要进行备份，但采取严格的安全措施保证其安全性，防止非授权访问、修改删除等行为的发生。

6.5.5 记录归档时间戳要求

亚洲诚信所有归档文件均有时间记录，由操作人员手工或系统自动添加。

6.5.6 记录归档收集系统

对于系统生成的电子记录，实时同步到日志服务器，且每周备份到异地。
对于手工生成的电子记录，由备份服务器完成收集备份工作。
对于书面的归档资料，收集归档到文件柜中。

6.5.7 记录归档检验机制

亚洲诚信采取了物理和逻辑的访问控制方法，以确保只有授权人员才能接近这些归档信息，严禁未授权的访问、阅读、修改和删除等操作。当归档信息被恢复后会对其进行完整性检验。

6.6 认证机构密钥更替

亚洲诚信的根证书有效期最长不超过 20 年，任何由其签发的证书，包括 CA 证书和订户证书，其失效时间不超过根证书的失效时间，任何由 CA 证书签发的订户证书，其失效时间不超过 CA 证书的失效时间。

CA 证书对应的密钥对，当其寿命超过本 CPS 规定的最大生命期时，亚洲诚信将启动密钥更新流程，替换已过期的 CA 密钥对。密钥变更按如下方式进行：

1. 上级 CA 的私钥到期时间在下级 CA 密钥的生命期之前，停止签发新的下级 CA 证书(“停止签发日期”)。
2. 在“停止签发证书的日期”之后，对于批准的下级 CA 或订户的证书请求，将采用新的 CA 密钥签发证书。
3. 产生新的密钥对，签发新的上级 CA 证书。
4. 上级 CA 继续利用原来的 CA 私钥签发 CRL 直到利用原私钥签发的最后的证书过期为止。

6.7 数据备份

6.7.1 数据备份计划

亚洲诚信建有完善的《数据备份管理规定》，根据数据备份策略定期进行数据备份。

6.7.2 异地备份中心

亚洲诚信设有同城容灾数据备份系统，按照业务连续性计划中所制定的流程响应。

6.8 损害与灾难恢复

6.8.1 事件和损害的列表

当发生业务系统故障、网络通讯故障、网络设备故障、数据库故障等情况时，亚洲诚信将根据制定的《业务连续性管理规定》等相关制度采取合理措施。

6.8.2 计算资源、软件或数据的损坏

亚洲诚信对业务系统及其他重要系统的资源、软件及数据进行了备份，并制定了相应的应急处理流程。当发生网络通信资源毁坏、计算机设备不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，亚洲诚信 CA 将按照《业务连续性计划》实施恢复。

6.8.3 实体私钥损害处理程序

亚洲诚信制定了根私钥泄露的应急预案，其中明确规定了根私钥泄露的内部处理流程、人员分工及对外通知处理流程。

6.8.4 灾难后的业务连续性能力

一旦物理场地出现重大灾难，亚洲诚信将根据相应的《业务连续性计划》可确保灾难后的在 48 小时内恢复查询服务，并尽快全面恢复认证业务。

6.8.5 业务连续性计划

亚洲诚信制订了相应的《业务持续计划》，确保 CA 业务的可持续性。

6.9 认证机构或注册机构的终止

当亚洲诚信拟终止电子认证业务时，将严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》及行业主管部门中对电子认证机构终止电子认证服务的规范要求相关工作。

7. 认证系统技术安全控制规则

7.1 密钥对的生成和安装

7.1.1 密钥对的生成

7.1.1.1 CA 签名密钥的生成

CA 密钥对必须在安全的物理环境中，使用国家密码主管部门批准和许可的密码设备中生成。加密机采用密钥分割或秘密共享机制进行备份。

在生成 CA 密钥对时，亚洲诚信按照加密机密钥管理办法，执行详细的操作流程控制计划，选定并授权 5 个密钥管理员，密钥管理员凭借口令和智能 IC 卡对密钥进行控制。在审计人员见证下，由 5 名中的 3 名密钥管理人员同时到达亚洲诚信屏蔽机房进行 CA 密钥生成操作。密钥对生成过程和操作均需全程录像记录并保存。

7.1.1.2 订户密钥的生成

订户密钥对由订户自身的服务器或其它设备内置的密钥生成机制生成。订户应确保其密钥产生的可靠性，并负有保护其私钥安全的责任和义务，并承担由此带来的法律责任。如果订户申请时提交的是一个包含弱算法的 PKCS#10 申请文件，亚洲诚信会拒绝该申请，并建议用户生成新的密钥对。

对于证书订户的加密密钥对，由亚洲诚信的密钥管理中心生成，并通过安全的方式传输给订户。

7.1.2 私钥传送给用户

订户的签名私钥由订户自己生成，将不会进行传送。订户的加密密钥由亚洲诚信密钥管理系统生成，并通过安全的方式传输给订户。

7.1.3 公钥传送给证书签发机构

作为证书申请流程的一部分，订户生成密钥对，并在 CSR 中将公钥提交给亚洲诚信。

7.1.4 认证机构公钥传送给依赖方

亚洲诚信的公钥包含在亚洲诚信自签发的根 CA 证书和中级 CA 证书中，订户和依赖方可从亚洲诚信官网下载。

7.1.5 密钥的算法

亚洲诚信遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求。目前，为保证密钥的安全强度，亚洲诚信不同类型的证书密钥遵循以下标准：

证书类型	根证书	中级证书	订户证书
签名算法	SM3WithSM2	SM3WithSM2	SM3WithSM2
公钥算法	SM2	SM2	SM2

7.1.6 公钥参数的生成和质量检查

对于使用硬件密码模块的证书订户，公钥参数必须使用国家密码管理局许可资质的加密设备和硬件介质生成。对于参数质量的检查，由于使用获得国家密码管理局许可资质的加密设备和硬件介质生成和存储密钥，已经具备足够的安全等级要求。

7.1.7 密钥使用目的

亚洲诚信签发的 X.509 v3 证书包含了密钥用法扩展项，其用法与 RFC 5280 标准相符。对于亚洲诚信在其签发证书的密钥用法扩展项内指明了的用途，证书订户必须按照该指明的用途使用密钥。

根 CA 密钥一般用于签发以下证书和 CRL：

1. 代表根 CA 的自签名证书；
2. 中级 CA 的证书、交叉证书；
3. 基础设施的证书，如 OCSP 响应验证证书。

中级 CA 密钥一般用于签发以下证书和 CRL：

1. 订户证书；
2. 特定用途的 PKI 体系功能证书(如 OCSP 证书)；
3. 订户 CRL。订户的密钥可以用于提供安全服务，如信息加密和签名等。

订户的密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等；加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

7.2 私钥保护和密码模块工程控制

7.2.1 在CA私钥保护方面的要求

亚洲诚信私钥以加密的形式分段存放在符合国家密码主管部门的要求硬件密码模块中，且私钥的使用也在硬件密码模块中进行。

7.2.2 用户私钥保护方面的要求

亚洲诚信使用签名证书的公钥对加密证书的私钥进行加密，并在验证用户身份后，通过加密信道将加密后私钥传递订户。

7.3 密钥对管理的其他方面

7.3.1 公钥归档

亚洲诚信公钥归档参考第 6.7 章节

7.3.2 证书操作期和密钥对使用期限

类型	私钥使用期限	证书期限
公开信任的根 CA	不超过证书有效期	25 年

公开信任的子 CA	不超过证书有效期	20 年
设备证书	签名私钥:不超过证书有效期	1185 天
	加密私钥:无规定	
个人证书	签名私钥:不超过证书有效期	1185 天
	加密私钥:无规定	
机构证书	签名私钥:不超过证书有效期	1185 天
	加密私钥:无规定	

7.4 激活数据

7.4.1 激活数据的产生和安装

亚洲诚信私钥的激活数据按照加密设备制造商提供的操作规范，在至少半数以上的密钥管理员在场且许可的情况下，由加密设备产生。

订户私钥的激活数据，包括用于下载证书的口令(以密码信封等形式提供)、USB Key、IC 卡的登陆口令等，都必须在安全可靠的环境下产生。这些激活数据，都是通过安全可靠的方式，例如离线当面递交、邮政专递等方式交给订户。对于非一次性使用的激活数据，亚洲诚信建议用户自行进行修改。

如果订户证书私钥的激活数据是口令，这些口令必须：

1. 至少 8 位字符
2. 至少包含一个小写字母
3. 不能包含很多相同的字符
4. 不能和操作员的名字相同
5. 不能使用生日、电话等数字
6. 不能包含用户名信息中的较长的子字符串

7.4.2 激活数据的保护

CA 私钥的激活数据（智能 IC 卡、PIN 码），亚洲诚信按照可靠的方式由可信人员自己掌管。所有可信人员都被要求记住而不是记下他们的密码或与其他人分享，且须签署协议来确认他们知悉所承担的责任。

订户的激活数据必须在安全可靠的环境下产生，必须妥善保管，或记住以后进行销毁，不可被他人所获悉。如果证书订户使用口令或 PIN 码保护私钥，订户应妥善保管，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户应注意防止其生物特征被人非法窃取。

7.4.3 激活数据的其他方面

订户的密钥对应应在合规的硬件介质中生成，存储密钥对的介质口令应由订户自行设置。证书签发完成后，当场交给订户。

当私钥的激活数据进行传送时，应保护他们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢失、偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或者全部。比如记录有口令的在纸页必须粉碎。

考虑到安全因素，对于申请证书的订户激活数据的生命周期，规定如下：

1. 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随时予以变更，使用期限超过 3 个月后就应进行修改。

7.5 系统安全控制

7.5.1 安全技术要求

CA 系统的信息安全管理，按照国标《证书认证系统密码及其相关安全技术规范》、工业和信息化部公布的《电子政务电子认证服务管理办法》，参照 ISO27001 信息安全管理体系要求，以及其他相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。主要的安全技术和控制措施包括：身份识别和验证、逻辑访问控制、网络访问控制等。

7.5.2 安全技术措施

对每位拥有系统（包括 CA 系统、RA 系统）业务操作权限的可信人员实行严格的双因素验证机制，即访问时同时采用用户名、口令以及数字证书双因素登录方式。

对系统运维人员，通过堡垒机或专用终端登录系统实施操作，确保 CA 软件和数据文件安全可信，不会受到未经授权的访问。

核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。这种分离可以阻止未授权的网络访问。使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。只有 CA 系统操作与管理组中的、有必要工作需要、访问系统的可信人员可以通过口令访问 CA 数据库。

7.6 生命周期技术控制

7.6.1 CA系统运行管理

亚洲诚信通过内部变更控制流程来控制 CA 系统，确保该系统正常运行。

7.6.2 CA系统访问管理

亚洲诚信已制定了各种安全策略、管理制度与流程对认证系统进行访问管理。CA 系统的访问管理，严格遵循国家密码管理局的有关运行管理规范进行操作。

亚洲诚信定期对系统进行安全检查，用来识别设备是否被入侵，是否存在安全漏洞等。

7.6.3 CA系统的开发和维护

亚洲诚信的软件设计和开发过程遵循以下原则：

1. 制定公司内部的升级变更申请制度，并要求工作人员严格按照流程执行；
2. 制定公司内部的采购流程及管理制度；
3. 开发程序必须在开发环境进行严格测试成功后，再申请部署于生产环境；
4. 变更部署前进行有效的在线备份；
5. 第三方验证和审查；
6. 安全风险分析和可靠性设计。

亚洲诚信会定期对 CA 系统进行备份维护。

7.7 网络的安全控制

亚洲诚信的认证系统采用防火墙进行系统的访问控制，采用 IDS/IPS 实施对网络攻击的防御，使用堡垒机对远程登录进行权限管理，使用路由器进行网络分层控制。

认证系统应仅对指定的服务或人员开放，且只开放最小的访问权限。

认证系统应定期进行安全漏洞扫描、安全设备配置审核，并对相关日志进行审计。

7.8 时间戳

亚洲诚信计算机上的系统时间应使用网络时间协议 (NTP) 进行更新，以使系统时钟至少每 24 小时同步一次。

亚洲诚信维护一个内部的 NTP 服务器，与外部资源同步，并将其时钟的精确度保持在一秒或更少。

此外，亚洲诚信的一个专门的权威时间戳机构 (TSA) 正在运作，以提供符合 RFC 3161 的时间戳服务。

8. 法律责任和其他业务条款

8.1 费用

8.1.1 证书签发和密钥更新费用

亚洲诚信可根据提供的电子认证相关服务向本机构的证书订户收取费用，具体收费标准根据市场和管理部门的规定自行决定。

如果亚洲诚信签署的协议中指定的价格和亚洲诚信公布的价格不一致，以协议中的价格为准。

8.1.2 其他服务费用

如果亚洲诚信向订户提供证书存储介质及相关服务，亚洲诚信将在与订户或者其他实体签署的协议中指明该项价格。

其他亚洲诚信将要或者可能提供的服务的费用，亚洲诚信将会及时告知用户。

8.1.3 退款策略

除非亚洲诚信违背了本 CP&CPS 所规定的责任，证书持有者可以要求退款。否则，亚洲诚信对证书持有者收取的费用均不退还。

证书持有者应当提供符合亚洲诚信要求的完整、真实、准确的个人信息，否则亚洲诚信对此造成的损失和后果不承担任何责任。

8.2 财务责任

8.2.1 责任担保范围

亚洲诚信根据业务发展情况决定其投保策略。如果由于亚洲诚信的原因造成用户在使用证书过程中遭受损失，亚洲诚信将向证书订户提供赔偿。

8.2.2 其他资产

机构证书持有者需具有足够的财务实力来维持其正常经营并保证相应义务的履行，他们必须合理地承担对证书持有者及对依赖方的责任。

此要求对亚洲诚信同样适用。

8.3 业务信息保密

8.3.1 保密信息范围

在亚洲诚信提供的电子认证服务中，以下信息视为保密信息：

- 亚洲诚信订户的数字签名及解密密钥。
- 审计记录包括：本地日志、服务器日志、归档日志的信息，这些信息被亚洲诚信视为保密信息，只有安全审计员和业务管理员可以查看。除法律要求，不可在公司外部发布。
- 其他由亚洲诚信保存的个人和公司信息应视为保密，除法律要求，不可公布。

-
- 订户私钥属于机密信息，订户应当根据本 CP&CPS 的规定妥善保管，如因订户自己泄漏私钥造成的损失，订户应自行承担。

8.3.2 不属于保密的信息

亚洲诚信将以下信息视为不保密信息：

- 由亚洲诚信发行的证书和 CRL 中的信息。
- 由亚洲诚信支持、CP&CP 识别的证书策略中的信息。
- 亚洲诚信许可的只有亚洲诚信订户方可使用的、在亚洲诚信网站公开发布的信息。
- 其它亚洲诚信信息的保密性取决于特殊的数据项和申请。

8.3.3 保护保密信息

亚洲诚信有妥善保管与保护上述第 8.3.1 中规定的保密信息

8.4 个人隐私保密

8.4.1 保护隐私的责任

亚洲诚信有妥善保管与保护第 8.4.2 中规定的证书申请者个人隐私的责任与义务。

8.4.2 使用隐私信息的告知与同意

亚洲诚信在认证业务范围内使用所获得的任何订户信息，无论是否涉及到隐私，亚洲诚信都没有告知订户的义务，也无需得到订户的同意。除非根据法律或政府的强制性规定，在未得到证书订户的许可之前，亚洲诚信保证不会把证书订户的除写入数字证书的个人资料外的个人信息提供给无关的第三方(包括公司或个人)。

8.4.3 依法律或行政程序的隐私信息的使用

依据法律、行政法规、规章、决定、命令等，由于司法执行或法律授权的行政执行需要，亚洲诚信有可能需要将有关信息在订户知晓或不知晓的情况下提供有关执法机关、行政执行机关。

8.4.4 不被视为隐私的信息

隐私信息不包括证书，CRL 或证书中已经公开的信息。

8.5 知识产权

- 亚洲诚信享有并保留对证书以及亚洲诚信提供的所有软件的全部知识产权。
- 亚洲诚信对数字证书系统软件具有所有权、名称权、利益分享权。
- 亚洲诚信有权决定采用何种软件系统。
- 亚洲诚信网站上公布的一切信息均为亚洲诚信财产，未经亚洲诚信书面允许，他人不能转载用于商业行为。
- 亚洲诚信发行的证书和 CRL 均为受亚洲诚信支配的财产。
- 对外运营管理策略和规范为亚洲诚信财产。
- 用来表示目录中亚洲诚信域中的实体的甄别名(DN)以及该域中颁发给终端实体的证书，均为亚洲诚信的财产。

8.6 陈述与担保

8.6.1 认证机构的陈述与担保

亚洲诚信采用经过国家有关管理机关审批的信息安全基础设施开展电子认证服务业务。

亚洲诚信的运作遵守《中华人民共和国电子签名法》等法律规定，接受行业主管部门的指导，对签发的数字证书承担相应法律责任。

根据《电子政务电子认证服务管理办法》要求，亚洲诚信将不定期对其注册机构电子政务电子认证业务是否符合本 CP&CPS 约定进行审计，并随着业务的调整对 CP&CPS 进行修订。

亚洲诚信不负责评估证书是否在适当的范围内使用，订户和依赖方依照订户协议和依赖方协议确保证书用于允许使用的目的。

8.6.2 注册机构的陈述与担保

作为亚洲诚信的注册机构应遵照本 CP&CPS，承担电子政务电子认证业务中注册机构的应尽的责任和义务。

8.6.3 订户的陈述与担保

订户一旦接受亚洲诚信签发的证书，就被视为向亚洲诚信及信赖证书的有关当事人作出以下承诺：

- 一经接受证书，即表示订户知悉和接受本 CP&CPS 中的所有条款和条件，并知悉和接受相应的订户协议。
- 在证书的有效期内进行数字签名。
- 订户在申请证书时向亚洲诚信提供的信息都是真实、完整和准确的，愿意承担任何提供虚假、伪造等信息的法律责任。如果存在代理人，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，通知亚洲诚信或其授权的证书服务机构。
- 与订户证书所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并进行签名时，证书是有效证书(证书没有过期、撤销)，证书的私钥为订户本身访问和使用。
- 除非经订户和发证机构间书面协议明确规定，订户保证不从事发证机构(或类似机构)所从事的业务。
- 一经接受证书，订户就应当承担如下责任：始终保持对其私钥的控制，使用可信的系统，采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用。
- 不得拒绝任何来自亚洲诚信公示过的声明、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和删减等。
- 证书在本 CP&CPS 中规定使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的。
- 采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件。
- 对于 SSL/TLS 证书，订户有责任和义务保证只在证书中列出的主题别名对应的服务器中部署证书。

8.6.4 依赖方的陈述与担保

依赖方声明和承诺：

-
- 遵守本 CP&CPS 的所有规定。
 - 确认证书在规定的范围和期限使用证书。
 - 在信赖证书前，对证书的信任链进行验证。
 - 在信赖证书前，通过查询 CRL 或 OCSP 确认证书是否被撤销。
 - 一旦由于疏忽或者其他原因违背了合理检查的条款，依赖方愿意就此而给亚洲诚信带来的损失进行补偿，并且承担因此造成的自身或他人的损失。
 - 不得拒绝任何来自亚洲诚信公示过的声明、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和删减等。

8.6.5 其他参与者的陈述与担保

从事电子认证活动的其他参与者须承诺遵守本 CP&CPS 的所有规定。

8.7 担保免责

除上述第 8.6.1 中的明确承诺外，亚洲诚信不承担其他任何形式的保证和义务：

- 不保证证书订户、信赖方、其他参与者的陈述内容。
- 不对电子认证活动中使用的任何软件做出保证。
- 不对证书在超出规定目的以外的应用承担任何责任。
- 对由于不可抗力，如战争、自然灾害等造成的服务中断，并由此造成的客户损失承担责任。
- 订户违反本 CP&CPS 承诺时，或依赖方违反承诺时，得以免除亚洲诚信之责任。
- 因亚洲诚信的设备或网络故障等技术故障而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。本项所规定之“技术故障”引起原因包括但不限于：关联单位如电力、电信、通讯部门而致、黑客攻击、亚洲诚信的设备或网络故障。
- 亚洲诚信已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

8.8 偿付责任限制

订户因亚洲诚信提供的电子认证服务从事民事活动遭受损失，亚洲诚信将承担不超过本 CP&CPS 第 8.9 节中规定的有限赔偿责任。

8.9 赔偿责任

如亚洲诚信违反了本 CP&CPS 8.6.1 中的陈述，证书订户可以申请亚洲诚信承担赔偿责任(法定或约定免责除外)。对于直接损失所负法律责任的上限为：在任何情况下每张服务器证书赔偿额不得超过证书市场购买价格的 10 倍。

如出现下述情形，亚洲诚信承担有限赔偿责任：

- 亚洲诚信将证书错误的签发给订户以外的第三方，导致订户遭受损失的；
- 在订户提交信息或资料准确、属实的情况下，亚洲诚信签发的证书出现了错误信息，导致订户遭受损失的；
- 在亚洲诚信明知订户提交信息或资料存在虚假谎报的情况，但仍然向订户签发证书，导致真实实体遭受损失的；

-
- 由于亚洲诚信的原因导致证书私钥被破译、窃取、泄露，导致订户遭受损失的；
 - 亚洲诚信未能及时撤销证书，导致订户遭受损失的。

另外，亚洲诚信赔偿限制如下：

- 亚洲诚信所有的赔偿义务不得高于赔偿上限，这种赔偿上限可以由亚洲诚信根据情况重新制定，亚洲诚信会将重新制定后的情况立刻通知相关当事人。
- 对于由订户或依赖方的原因造成的损失，亚洲诚信不承担责任，由订户或依赖方自行承担。
- 亚洲诚信只有在证书有效期限内承担损失赔偿责任。

8. 10有效期限与终止

8. 10. 1 有效期限

本 CP&CPS 的任何修订在发布到亚洲诚信的在线信息库时正式生效，并且在更换为新版本之前以及亚洲诚信终止业务时一直有效。

8. 10. 2 终止

亚洲诚信终止电子认证服务时，本 CP&CPS 终止。

8. 10. 3 效力的终止与保留

本 CP&CPS 终止后，其效力将同时终止，但对终止之日前发生的法律事实，本 CP&CPS 中对各方责任的规定及责任免除仍然适用，包括但不限于 CP&CPS 中涉及审计、保密信息、隐私保护、知识产权等内容，以及涉及赔偿的有限责任条款，在本 CP&CPS 终止后继续有效。

当由于某种原因，如内容修改、与适用法律相冲突，CP&CPS、订户协议、依赖方协议和其他协议中的某些条款失效，不影响文件中其他条款法律效力。

8. 11对参与者的个别通告与沟通

亚洲诚信在必要的情况下，如在主动撤销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为时，会通过邮件等方式，个别通知订户、依赖方。

8. 12修订

8. 12. 1 修订程序

经亚洲诚信安全策略委员会授权，“CPS 编写组”每年至少审查一次本 CP&CPS，确保其符合国家法律法规和主管部门的要求及相关国际标准，并符合认证业务开展的实际需要。

本 CP&CPS 的修改和更新的具体程序同第 1. 4. 3 节。

8.12.2 通知机制和期限

修订后的 CP&CPS 经批准后将立即在亚洲诚信官网发布，如在修订发布后 7 个工作日内订户没有书面提出异议，将被视为同意该修改。

对于需要通过电子邮件、信件、媒体等方式通知的修改，亚洲诚信将在合理的时间范围内通知有关各方，合理的时间应保证有关方受到的影响最小。

8.12.3 必须修改业务规则的情形

当本 CP&CPS 描述的规则、流程和相关技术已经不能满足电子政务电子认证业务要求，CP&CPS 中相关内容与管辖法律的不一致，国家监管部门对本机构认证业务有明确的更改或调整要求等。

8.13 争议处理

亚洲诚信、证书订户、依赖方等最终实体在电子认证活动中产生争议的，首先应根据协议友好协商解决，协商未果的，可通过法律途径解决。

任何与亚洲诚信就本 CP&CPS 所涉及的任何争议提起诉讼的，各方同意提交亚洲诚信工商注册所在地人民法院管辖处理。

8.14 管辖法律

本 CP&CPS 受《中华人民共和国电子签名法》、《中华人民共和国网络安全法》、《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》等相关法律法规管辖。

8.15 与适用法律的符合性

无论亚洲诚信的证书订户、依赖方等实体在何地居住以及在何处使用亚洲诚信的证书，本 CP&CPS 的执行、解释和程序有效性均适用中华人民共和国的法律。任何与亚洲诚信就本 CP&CPS 所涉及的任何争议，均适应中华人民共和国法律。

8.16 一般条款

8.16.1 完整协议条款

CP&CPS、订户协议、依赖方协议及其他补充协议构成电子政务电子认证服务各方的完整协议。

8.16.2 转让条款

根据本 CP&CPS 中详述的认证实体各方的权利和义务，在未经过亚洲诚信事先书面同意的情况下，不能通过任何方式进行转让。

8.16.3 分割性条款

如果本 CP&CPS 的任何条款被主管法院或法庭认定为无效或不可执行，则 CP&CPS 的其余部分仍然有效且可执行。

本 CP&CPS 中规定责任限制，免责声明或免除损害的每项规定均可分割，并且独立于任何其他规定。

8.16.4 强制执行条款

若证书订户、依赖方等实体未执行本 CP&CPS 中某项规定，不被认为该实体将来不执行该项或其他规定。

8.16.5 不可抗力条款

亚洲诚信不对因战争、瘟疫、火灾、地震、其他天灾、互联网或其他基础设施瘫痪等不可抗力事件所造成本 CP&CPS 规定担保责任的违反、延误或无法履行负责。

8.17 其他条款

亚洲诚信对本 CP&CPS 有最终解释权。