亚洲诚信CA电子认证业务规则

V1.6.2

亚数信息科技（上海）有限公司

2026-08-27

目录

1. 概括性描述 . . . 1
1.1 承诺 . . . 1
1.2 基本信息 . . . 1
1.2.1 公司介绍 . . . 1
1.2.2 服务体系/层次结构 . . . 1
1.3 文档名称与标识 . . . 2
1.3.1 证书策略标识 . . . 2
1.3.2 修订历史 . . . 3
1.4 电子认证活动参与者 . . . 5
1.4.1 电子认证服务机构 . . . 5
1.4.2 注册机构 . . . 5
1.4.3 订户 . . . 5
1.4.4 依赖方 . . . 5
1.4.5 其他参与者 . . . 6
1.5 证书应用 . . . 6
1.5.1 适合的证书应用 . . . 6
1.5.2 限制的证书应用 . . . 7
1.6 策略管理 . . . 7
1.6.1 策略文档管理机构 . . . 7
1.6.2 策略文档批准程序 . . . 7
1.6.3 联系人 . . . 7
1.6.4 决定 CPS 符合策略的机构 . . . 8
1.7 定义和缩写 . . . 8
1.7.1 缩写及其含义一览表 . . . 8
1.7.2 定义一览表 . . . 9
2. 信息发布与信息管理 . . . 11
2.1 信息库 . . . 11
2.2 认证信息的发布 . . . 11
2.3 发布的时间或频率 . . . 11
2.4 信息库访问控制 . . . 12
2.5 高风险信息库 . . . 12
3. 身份标识与查验 . . . 13
3.1 身份查验通用要求 . . . 13
3.1.1 订户告知 . . . 13
3.2 初始身份确认 . . . 13
3.2.1 证明拥有私钥的方法 . . . 14
3.2.2 组织机构身份的查验 . . . 14
3.2.3 个人身份的查验 . . . 15
3.2.4 数据源的准确性 . . . 16

3.3 订户意愿记录 16
3.3.1 机构高等级电子签名认证证书的意愿记录 16
3.3.2 机构基础级电子签名认证证书的意愿记录 17
3.3.3 个人高等级电子签名认证证书的意愿记录 17
3.3.4 个人基础级电子签名认证证书的意愿记录 17
3.3.5 机构高等级文档签名证书的意愿记录 17
3.3.6 个人高等级文档签名证书的意愿记录 17
3.4 订户协议 17
3.5 未验证的订户信息 17
3.6 互操作要求 18
3.7 命名 18
3.7.1 名称类型 18
3.7.2 对名称意义化的要求 18
3.7.3 订户的匿名或伪名 18
3.7.4 理解不同名称形式的规则 18
3.7.5 名称的唯一性 18
3.7.6 商标的识别、鉴别和角色 18
4. 证书生存周期操作要求 19
4.1 通用要求 19
4.2 证书申请 19
4.2.1 证书申请实体 19
4.2.2 注册过程与责任 19
4.2.3 证书申请处理 20
4.3 证书签发 20
4.3.1 证书签发中注册机构和电子认证服务机构的行为 21
4.3.2 电子认证服务机构和注册机构对订户的通告 21
4.4 证书接受 21
4.4.1 构成接受证书的行为 21
4.4.2 CA 对证书的发布 21
4.4.3 CA 对其他实体的通告 21
4.5 密钥对和证书的使用 21
4.5.1 订户私钥和证书的使用 21
4.5.2 依赖方公钥和证书的使用 22
4.6 证书续期 22
4.6.1 证书续期的情形 22
4.6.2 请求证书续期的实体 23
4.6.3 证书续期请求的处理 23
4.6.4 颁发新证书时对订户的通告 23
4.6.5 构成接受续期证书的行为 23
4.6.6 电子认证服务机构对续期证书的发布 23
4.6.7 电子认证服务机构对其他实体的通告 23

4.7 证书密钥更新 23
4.7.1 证书密钥更新的情形 23
4.7.2 请求证书密钥更新的实体 24
4.7.3 证书密钥更新请求的处理 24
4.7.4 颁发新证书时对订户的通告 24
4.7.5 构成接受密钥更新证书的行为 24
4.7.6 电子认证服务机构对密钥更新证书的发布 24
4.7.7 电子认证服务机构对其他实体的通告 24
4.8 证书变更 24
4.8.1 证书变更的情形 24
4.8.2 请求证书变更的实体 24
4.8.3 证书变更请求的处理 24
4.8.4 颁发新证书时对订户的通告 25
4.8.5 构成接受变更证书的行为 25
4.8.6 电子认证服务机构对变更证书的发布 25
4.8.7 电子认证服务机构对其他实体的通告 25
4.9 证书撤销或冻结 25
4.9.1 证书撤销的情形 25
4.9.2 请求证书撤销的实体 26
4.9.3 撤销请求的流程 26
4.9.4 撤销请求宽限期 26
4.9.5 电子认证服务机构处理撤销请求的时限 27
4.9.6 依赖方检查证书撤销的要求 27
4.9.7 CRL 发布频率 27
4.9.8 CRL 发布的最大滞后时间 27
4.9.9 在线状态查询的可用性 27
4.9.10 在线状态查询要求 27
4.9.11 撤销信息的其他发布形式 27
4.9.12 密钥损害的特别要求 27
4.9.13 证书冻结的情形 27
4.9.14 请求证书冻结的实体 28
4.9.15 冻结请求的流程 28
4.9.16 冻结的期限限制 29
4.10 证书状态服务 29
4.10.1 操作特征 29
4.10.2 服务可用性 29
4.10.3 可选特征 29
4.11 停止使用认证服务 29
4.12 密钥托管与恢复 30
5. 认证机构设施、管理和操作控制 31
5.1 物理控制 31

5.1.1 场地位置与建筑 31
5.1.2 物理访问 31
5.1.3 电力与空调 31
5.1.4 水患防治 32
5.1.5 火灾防护 32
5.1.6 介质存储 32
5.1.7 废物处理 32
5.1.8 异地备份 32
5.2 操作过程控制 32
5.2.1 可信角色 32
5.2.2 每项任务需要的人数 33
5.2.3 每个角色的识别与鉴别 33
5.2.4 需要职责分割的角色 33
5.3 人员控制 34
5.3.1 资格、经历和无过失要求 34
5.3.2 背景审查程序 34
5.3.3 培训要求 34
5.3.4 再培训周期和要求 35
5.3.5 工作岗位轮换周期和顺序 35
5.3.6 未授权行为的处罚 35
5.3.7 独立合约人的要求 35
5.3.8 提供给员工的文档 35
5.4 审计日志程序 35
5.4.1 记录事件的类型 35
5.4.2 处理日志的周期 37
5.4.3 审计日志的保存期限 37
5.4.4 审计日志的保护 37
5.4.5 审计日志备份程序 37
5.4.6 审计收集系统 37
5.4.7 对导致事件实体的通告 37
5.4.8 脆弱性评估 37
5.5 记录归档 37
5.5.1 归档记录的类型 37
5.5.2 归档记录的保存期限 38
5.5.3 归档文件的保护 38
5.5.4 归档文件的备份程序 38
5.5.5 记录时间戳要求 38
5.5.6 归档收集系统 38
5.5.7 获得和检验归档信息的程序 39
5.6 电子认证服务机构根证书密钥更替 39
5.7 损害和灾难恢复 39

5.8 电子认证服务机构终止 40
5.9 重大事项报告 40
6. 认证系统技术安全控制 42
6.1 技术安全管理制度要求 42
6.2 密钥对的生成和安装 42
6.2.1 CA密钥对的生成和安装 42
6.2.2 订户密钥对的生成和交付 42
6.2.3 公钥传送给证书签发机构 42
6.2.4 电子认证服务机构公钥传送给依赖方 42
6.2.5 密钥的长度 43
6.2.6 公钥参数的生成和质量检查 43
6.2.7 密钥使用目的 43
6.3 私钥保护和密码模块工程控制 43
6.3.1 CA私钥保护和密码模块的工程控制 43
6.3.2 订户私钥保护和密码模块工程控制 44
6.3.3 私钥托管 44
6.3.4 私钥备份 44
6.3.5 私钥归档 44
6.3.6 私钥导入、导出密码模块 45
6.3.7 私钥在密码模块的存储 45
6.3.8 激活私钥的方法 45
6.3.9 解除私钥激活状态的方法 45
6.3.10 销毁私钥的方法 45
6.3.11 密码模块的评估 45
6.4 密钥对管理的其他方面 45
6.4.1 公钥归档 45
6.4.2 证书操作期和密钥对使用期限 45
6.5 激活数据 46
6.5.1 激活数据的产生和安装 46
6.5.2 激活数据的保护 46
6.5.3 激活数据的其他方面 46
6.6 计算机安全控制 47
6.7 生存周期安全控制 47
6.8 网络安全控制 47
6.9 时间戳 47
7. 证书、证书撤销列表和在线证书状态协议 49
7.1 证书 49
7.1.1 版本号 49
7.1.2 证书扩展项 49
7.1.3 算法对象标识符 50
7.1.4 主体名称 50

7.1.5 名称限制 51
7.1.6 证书策略对象标识符 51
7.1.7 策略限制扩展项的用法 51
7.1.8 策略限定符的语法和语义 51
7.1.9 关键证书策略扩展项的处理规则 52
7.2 证书撤销列表 52
7.2.1 版本号 52
7.2.2 CRL 和 CRL 条目扩展项 52
7.3 在线证书状态协议 52
8. 认证机构审计和其他评估 53
8.1 审计评估制度 53
8.2 认证业务审计 53
8.3 全面符合性评估 53
9. 法律责任和其他业务条款 54
9.1 费用 54
9.1.1 证书签发和更新费用 54
9.1.2 证书查询费用 54
9.1.3 证书撤销或状态信息的查询费用 54
9.1.4 其他服务费用 54
9.1.5 退款策略 54
9.2 财务责任 54
9.2.1 保险范围 55
9.2.2 其他资产 55
9.2.3 对最终实体的保险或担保 55
9.3 业务信息保密 55
9.3.1 保密信息范围 55
9.3.2 不属于保密的信息 55
9.3.3 保护保密信息的责任 55
9.4 个人隐私保护 55
9.4.1 隐私保护方案 55
9.4.2 作为隐私处理的信息 56
9.4.3 不被视为隐私的信息 56
9.4.4 保护隐私的责任 56
9.4.5 使用隐私信息的告知与同意 56
9.4.6 依法律或行政程序的信息披露 56
9.4.7 其他信息披露情形 56
9.5 知识产权 56
9.6 陈述和担保 56
9.6.1 电子认证服务机构的陈述和担保 56
9.6.2 注册机构的陈述和担保 57
9.6.3 订户的陈述和担保 57

9.6.4 依赖方的陈述和担保 57
9.6.5 其他参与者的陈述和担保 58
9.7 担保免责 58
9.8 偿付责任规则 58
9.9 赔偿 58
9.10 有效期限和终止 59
9.10.1 有效期限 59
9.10.2 终止 59
9.10.3 效力的终止和保留 59
9.11 对参与者的个别通告与沟通 59
9.12 修订和发布 59
9.12.1 修订程序 59
9.12.2 通知机制和期限 59
9.12.3 必须修改业务规则的情形 60
9.13 争议处理与举证 60
9.13.1 争议解决机制 60
9.13.2 举证制度与能力体系 60
9.14 管辖法律 60
9.15 与适用法律的符合性 60
9.16 一般条款 60
9.16.1 完整协议 60
9.16.2 转让 60
9.16.3 分割性 61
9.16.4 强制执行 61
9.16.5 不可抗力 61
9.17 其他条款 61

1. 概括性描述

1.1 承诺

亚洲诚信CA承诺：

- 开展经营和服务活动时，遵守法律、行政法规，树立以人民为中心的服务理念，承担社会责任；
- 与客户建立业务关系前，开展应用业务调研，建立应用接入业务风险评估及内部定责机制，严禁为存在违法违规风险的业务提供电子认证服务；
- 使用经过国家密码管理局审查的电子认证服务系统开展电子认证服务；
- 接受政府和社会监督，对主管部门检测发现的问题及时整改，建立问题纠治长效机制，持续符合整改要求。

1.2 基本信息

1.2.1 公司介绍

亚数信息科技（上海）有限公司，又称亚洲诚信CA，英文名称为“TrustAsia Technologies, Inc.”（简称“亚数CA”、“TrustAsia CA”），成立于2013年4月，法定代表人翟新元，具备ISO27001信息安全管理体系认证、ISO9001质量管理体系认证、ISO22301业务连续性管理体系认证，是国内杰出的网络信息安全数字证书及安全监测解决方案提供商。我们以合规标准化的运营管理和服务水平，提供专业的国内外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。

亚洲诚信CA已取得由中华人民共和国工业和信息化部2021年11月17日批准颁发的《电子认证服务许可证》（ECP31010421056），有效期自2021年11月17日至2026年11月16日。

《亚洲诚信CA电子认证业务规则》（以下简称“亚洲诚信CA CPS”、“CPS”）是亚数信息科技（上海）有限公司按照《中华人民共和国电子签名法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《商用密码管理条例》《电子认证服务管理办法》《电子认证服务密码管理办法》等法律法规的规定，国家工业和信息化部及密码管理局的要求，以及RFC3647 的框架进行编写，规范亚洲诚信CA的电子认证业务的服务、管理，保障认证体系的可靠，维护电子认证的权威性，有效地防范安全风险。明确规定亚洲诚信CA在审核、签发、发布、存档和撤销数字证书等证书生存周期管理以及相关的业务应遵循的各项操作规范。定期查看其更新情况，持续根据其发布的版本进行修订。报国家工业和信息化部备案，并在公司官网上进行公示。

亚洲诚信CA CPS作为实际应用和操作的文件依据，适用于所有亚洲诚信CA认证体系内的成员。作为公告，向社会公布本机构关于证书服务的基本立场和观点。亚洲诚信CA认证体系内的实体以及数字证书持有者，必须完整地理解和执行本CPS所规定的条款，承担相应的责任和义务。

1.2.2 服务体系/层次结构

亚洲诚信CA 运营的CA证书层次结构如下：

CA类型	甄别名	公钥算法类型	序列号	有效期	服务年限
Root CA	C=CN,O=TrustAsia Technologies, Inc.,OU=GMCA,CN=TrustAsia SM2 Root CA	SM2	49AD97D1D672FB45DA0E1369BC47F4C7	2020-12-23至2040-12-23	不超过20年
Sub CA	C=CN,O=TrustAsia Technologies, Inc.,OU=GMCA,CN=TrustAsia SM2 Identity CA	SM2	E44F30AF8E	2020-12-23至2030-12-21	不超过10年
Sub CA	C=CN,O=TrustAsia Technologies, Inc.,CN=TrustAsia SM2 Identity CA 2026	SM2	629EAC49004630D540A28F735DA40942B770AC77	2026-01-21至2036-01-21	不超过10年

- TrustAsia SM2 Identity CA，签发用于个人及机构的电子签名认证证书。
- TrustAsia SM2 Identity CA 2026，签发用于个人及机构的电子签名认证证书。

CA类型	甄别名	公钥算法类型	序列号	有效期	服务年限
Root CA	C=CN,O=TrustAsia Technologies, Inc.,CN=TrustAsia RSA Root CA	RSA4096	41EBDAD5061424A6A49B165A0E118B62337A04D6	2026-03-16至2046-03-16	不超过20年
SubCA	C=CN,O=TrustAsia Technologies, Inc.,CN=TrustAsia RSA Identity CA 2026	RSA2048	43EBA183DD2CB44CC9FF960B112F7370F093BB6A	2026-03-16至2036-03-16	不超过10年

- TrustAsia RSA Identity CA 2026，签发用于个人及机构的电子签名认证证书。

CA类型	甄别名	公钥算法类型	序列号	有效期	服务年限
Root CA	C=CN,O=TrustAsia Technologies, Inc.,CN=TrustAsia Document Signing RSA Root CA	RSA4096	10181B4EA901E561FCEF143B16E2D1294FF7DDC4	2026-05-11至2051-05-11	不超过25年
Root CA	C=CN,O=TrustAsia Technologies, Inc.,CN=TrustAsia Document Signing ECC Root CA	ECC P-384	6C123ECBADE1878CB965158C87E48DCB6FCFBEF4	2026-05-11至2051-05-11	不超过25年

- 签发用于文档签名证书。

1.3 文档名称与标识

1.3.1 证书策略标识

此文档的名称为《亚洲诚信CA电子认证业务规则》，简称为“亚洲诚信CA CPS”，并在亚洲诚信CA网站发布，网址：www.trustasia.com/cps-cn。

本文档适用文档签名证书以及电子签名认证证书，它们的策略OID 为:

证书类型	策略OID
个人高等级文档签名证书	1.3.6.1.4.1.44494.2.3.2 2.16.156.339.2.1.1.2 1.2.156.10197.6.4.1.2.1
机构高等级文档签名证书	1.3.6.1.4.1.44494.2.3.3 2.16.156.339.2.1.2.2 1.2.156.10197.6.4.1.2.2
个人基础级电子签名认证证书	2.16.156.339.2.1.1.1 1.2.156.10197.6.4.1.2.1
个人基础级加密证书	1.2.156.115224.2.4.1.1
个人高等级电子签名认证证书	2.16.156.339.2.1.1.2 1.2.156.10197.6.4.1.2.1
个人高等级加密证书	1.2.156.115224.2.4.1.2
机构基础级电子签名认证证书	2.16.156.339.2.1.2.1 1.2.156.10197.6.4.1.2.2
机构基础级加密证书	1.2.156.115224.2.4.2.1
机构高等级电子签名认证证书	2.16.156.339.2.1.2.2 1.2.156.10197.6.4.1.2.2
机构高等级加密证书	1.2.156.115224.2.4.2.2

1.3.2 修订历史

版本号	更新内容	生效日期
V1.1	发布初版	2020-10-10
V1.2	• 更新5.1.2，从“门禁卡和密码鉴别”变更为“门禁卡和人体特征鉴别”; • 更新8.1将“每年进行第三方审计”变更为“每年进行等级保护三级测评”; • 更新全文,将“第三方审计”变更为“审计人员”。	2021-2-4

版本号	更新内容	生效日期
V1.3	• 更新1.1.2，删除SM2 Device证书层次结构; • 更新1.2，CPS发布链接，并删除设备证书OID; • 更新4.2.3，明确证书申请的处理时间; • 更新4.3.2，明确证书申请后对订户的交付及通知方式; • 更新4.9.16，明确冻结处理时限; • 更新5.3.2，修订背景审查程序; • 更新5.4.8，修订脆弱性评估的内容; • 更新6.4.3，明确生成和传递激活数据的安全可靠方式; • 更新全文，删除设备证书相关内容。	2021-07-19
V1.4	• 更新1.1.1，公司介绍变更; • 更新3.2.2.1，个人证件类型支持军官证; • 更新4.9.15，明确了证书冻结的处理时限; • 删除编写及备注列，简化目录。	2022-07-01
V1.4.1	• 将“修订历史”移至第 1.2.2 节 • 更新第5章节，调整5.2.3角色的鉴别、更新5.4.3关于审计日志的内容、调整5.5.2关于归档时限 • 更新9.12.1调整CPS的发布周期为至少每365天 • 更新全文，保持专用术语的统一	2023-6-26
V1.4.2	• 更新全文，调整证书策略OID、证书分类及密钥用途 • 更新对注册机构的要求及其可操作的内容 • 更新中级CA的CRL更新频率为至少12个月	2023-10-24
V1.4.3	• 修正了密钥用法 • 补充了部分扩展描述	2024-10-14
V1.4.4	• 取消了使用whois协议进行域名验证的方法	2025-10-22
V1.5.0	• 调整了PKI结构，增加RSA的Root证书以及新的ICA • 根据团标T/CQAE 11034-2025进行修改 • 根据团标T/SHCCIA 001-2026 进行修改	2026-04-02
V1.6.0	• 根据团标T/CQAE 11034-2025的修订进行修改	2026-06-26

版本号	更新内容	生效日期
V1.6.1	• 更新全文，移除服务器身份认证证书相关内容，并删除3.8域名的确认和鉴别章节 • 更新1.6.1，明确安全策略委员会的组成及其CPS维护职责 • 更新4.2.4，明确证书申请的处理及签发时限 • 更新4.6.1、4.7.1，调整证书续期及密钥更新的身份查验要求 • 更新5.6，增加根密钥泄露或存在安全隐患时的密钥更替流程	2026-07-17
V1.6.2	• 更新1.5.1，完善电子签名证书描述与分类 • 更新3.3.1，明确采用录音录像等记录意愿 • 更新4.5.1，明确订户私钥和证书的使用要求 • 更新5.1.8，完善异地保存要求 • 更新5.7，完善RTO与RPO描述 • 更新6.2.1，明确录音录像保存 • 更新8.1-8.3，明确审计周期、内容以及抽样要求	2026-08-27

1.4 电子认证活动参与者

1.4.1 电子认证服务机构

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CA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CA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。

1.4.2 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CA自己承担RA的职责，不授权外部机构作为RA。

1.4.3 订户

订户是指从亚洲诚信CA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CA签订合约以获得证书，并承担作为证书订户的责任。

1.4.4 依赖方

依赖方是基于对亚洲诚信CA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。

1.4.5 其他参与者

为亚洲诚信CA的电子认证活动提供相关服务的其他实体。

1.5 证书应用

1.5.1 适合的证书应用

亚洲诚信CA 可以提供正式证书和测试证书。

正式证书由亚洲诚信CA正式认证系统签发，必须按照CPS签发。测试证书由亚洲诚信CA测试认证系统签发，证书不可信，一般用来测试证书申请流程、系统适用性及技术可行性，不能用于任何正式用途。由于使用数字证书来处理或保护信息的应用场景很广泛，差异也较大，依赖方在确定是否根据此CPS颁发证书时必须评估自己的应用场景是否适用以及相关的风险。此CPS涵盖了几种不同类型的用户证书，分为电子签名认证证书（用于电子政务电子签名参考电子政务电子认证服务业务规则规范）以及文档签名证书，下表描述了每种证书的适用场景。

1. 电子签名认证证书（机构证书）

按照证书主体对象的类型和风险等级，分为机构高等级电子签名认证证书和机构基础级电子签名认证证书。其中机构高等级电子签名认证证书适用于高风险业务、符合《电子签名法》的机构电子签名认证证书；机构基础级电子签名认证证书适用于低风险业务、符合《电子签名法》的机构电子签名认证证书。

2. 电子签名认证证书（个人证书）

按照证书主体对象的类型和风险等级，分为个人高等级电子签名认证证书和个人基础级电子签名认证证书。其中个人高等级电子签名认证证书适用于高风险业务、符合《电子签名法》的个人电子签名认证证书；个人基础级电子签名认证证书适用于低风险业务、符合《电子签名法》的个人电子签名认证证书。

3. 加密证书

加密证书用于数据加密、解密或密钥保护，与对应的电子签名认证证书配套使用。按照电子签名认证证书的等级，分为个人高等级加密证书、个人基础级加密证书、机构高等级加密证书和机构基础级加密证书四种类型。加密证书不适用于生成电子签名，不属于电子签名认证证书。

4. 个人高等级文档签名证书

主要颁发给自然人，用于验证签署者身份、确保电子文档未被篡改，并赋予签名法律效力，使电子签名与手写签名具有同等可信度和不可抵赖性。

5. 机构高等级文档签名证书

主要颁发给法人或其他组织，用于验证签署机构身份、确保电子文档（如电子合同、公文等）自签署后未被篡改，并赋予签名法律效力，使电子签名与实体盖章具有同等法律效力和不可抵赖性。

文档签名证书是高等级电子签名认证证书在电子文档签署场景下的专用证书类型。文档签名证书中包含对应的主管部门高等级电子签名认证证书策略 OID 和亚洲诚信CA文档签名证书策略 OID，并包含文档签名专用扩展密钥用途（通用文档签名、Adobe PDF签名和Microsoft文档签名）。

此外，亚洲诚信CA还会签发服务器证书、代码签名证书，邮件安全签名证书等，它们不适用于电子签名认证证书。

1.5.2 限制的证书应用

亚洲诚信CA所签发的证书在功能上通过证书的各项扩展进行了限制，只能应用于证书所代表的主体身份适合的用途。对于证书的应用超出本CPS限定的应用范围，将不受本 CPS 保护。

亚洲诚信CA颁发的证书禁止用于以下应用场景，包括但不限于：

a) 涉及人身关系，如婚姻、收养、继承等；

b) 涉及停止公共事业服务的，如停止供水、供热、供气等；

c) 法律、行政法规规定的其他不适用电子签名的应用场景或类型；

d) 国家法律法规禁止的活动。

涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。

1.6 策略管理

1.6.1 策略文档管理机构

亚洲诚信CA 设立了安全策略委员会，由公司管理层、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，并在公司内部公示成员名单。 安全策略委员会是亚洲诚信CA所有策略的最高管理机构，所有重大决议的相关文件和会议记录均被妥善保存。 安全策略委员会负责CPS以及配套制度的维护，包括但不限于以下职责： a) 确定维护CPS策略及其它关联文档的职能分工，建立合理有效的修订和批准流程； b) 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批； c) 每年至少进行一次CPS的全面评审，根据实际需要及时修订策略文档； d) 每年组织运营风险评估并形成报告。

本策略文档的对外咨询服务等日常工作由策略部门负责。

1.6.2 策略文档批准程序

本 CPS 由亚洲诚信CA安全策略委员会组织 CPS 编写组编制，每年至少进行一次CPS的全面评审，根据实际需要及时修订本文档。每年组织运营风险评估并形成报告。 CPS 编写组完成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CA官方网站上发布。

所有正式发布的 CPS 版本将根据《电子认证服务管理办法》中规定，从对外发布之日起的三十日之内向工业和信息化部备案。亚洲诚信CA从cps-cn@trustasia.com接受内部审核和外部反馈，编写组根据收到的信息进行内容评估，若评估采纳，则再次按照此程序执行。

1.6.3 联系人

1.6.3.1 CPS 联系人

如对本 CPS 有任何疑问，请与亚洲诚信CA 策略部联系：

电话：021-58895880（转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）

1.6.3.2 证书撤销、冻结联系人

证书问题报告及证书撤销、证书冻结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)

以及其它亚洲诚信CA可接受的方式。

1.6.4 决定 CPS 符合策略的机构

亚洲诚信CA安全策略委员会是策略制定的主要机构，也是审核批准本CPS、决定本CPS是否符合亚洲诚信CA 策略的最高权威机构。

1.7 定义和缩写

1.7.1 缩写及其含义一览表

缩写	英文全称	中文含义
CA	Certification/Certificate Authority	电子认证服务机构
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
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
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

缩写	英文全称	中文含义
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)
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

1.7.2 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。
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 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 CPS 标识符共同出现在 X.509 证书中。该信息可能包含可用 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。
电子签名认证证书	由依据《中华人民共和国电子签名法》设立的电子认证服务机构签发的，可证实电子签名人与电子签名制作数据有联系的数字证书。
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。

术语	定义
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CA信息库之前必须由依赖方阅读和接受的协议。
对象标识符	用于无歧义地标识对象的全局唯一值。
证书链	证书链是一个用于证书验证的证书序列。
身份查验	证实某个实体就是所声称身份的过程。
激活数据	用于使密码模块进入可操作状态的数据。可为口令、生物特征等。
时间戳	对时间和其他待签名数据进行签名得到的，用于表明数据时间属性的数据
证书续期	指在不改变订户信息的情况下，用一个新证书来代替旧证书的过程。
密钥更新	用新密钥替换旧密钥的过程。
密钥恢复	将归档或备份的密钥恢复到可用状态的过程。
证书认证系统	对数字证书的申请、签发、发布、更新、撤销、验证等数字证书全生存周期进行管理和服务的系统。
高等级电子签名认证证书	适用于涉及生命健康、财产权益等高风险场景的电子签名认证证书。
基础级电子签名认证证书	适用于除高等级证书规定场景外的其他电子签名场景的证书。

2. 信息发布与信息管理

2.1 信息库

亚洲诚信CA的信息库是一个对外公开的、面向订户及证书应用依赖方提供信息服务的信息库。该信息库包括但不仅限于以下内容：

a. 详细的业务办理指南，包括但不限于服务网点地址、营业时间、联系电话等；
b. 依赖方协议；
c. 订户协议或服务协议；
d. 查询本机构的电子认证业务规则、证书策略的指引；
e. 投诉处理政策及投诉方式，包括但不限于：投诉处理部门的地址、联系电话、电子邮件地址。

2.2 认证信息的发布

亚洲诚信CA通过其对外公开的官方信息库发布认证信息，并提供证书信息查询服务与证书状态信息查询服务。发布的认证信息包括但不限于：

a. 证书信息：在征得订户同意的前提下，亚洲诚信CA在官方信息库中提供证书查询入口，订户及依赖方可通过证书序列号、证书主题等信息查询并获取相应证书；未获订户授权的证书不在信息库中对外发布；
b. 证书状态信息（CRL）：订户或依赖方可通过CRL 发布站点获取证书撤销列表，查询证书是否已被撤销；
c. 证书状态信息（OCSP）：亚洲诚信CA提供在线证书状态查询服务（OCSP），订户或依赖方可实时查询单张证书的状态信息；
d. 本CPS、证书策略及相关业务规则等公开文件。

亚洲诚信CA也将会根据需要采取其他可能的形式进行信息发布。 亚洲诚信CA按照国家电子认证服务管理平台的要求进行了备案，并且会完成与国家电子认证服务管理平台的技术对接，实现根据证书唯一编码、订户身份信息等维度查询本机构已签发证书列表的功能。

2.3 发布的时间或频率

CPS 以及相关业务规则在完成1.6.2 所述的批准流程后的15个工作日内发布到亚洲诚信CA 网站上，并可确保7*24 小时可访问。

亚洲诚信CA对于订户证书的CRL至少24小时发布一次；对于中级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，如果有中级CA证书撤销的情况，则在24小时之内更新发布CA证书的CRL。

亚洲诚信CA签发的订户证书一经签发即可下载，订户可通过邮件或亚洲诚信CA提供的证书服务站点获得已签发的证书，并通过OCSP对证书状态进行查询。当证书被撤销或冻结时，亚洲诚信CA应立即更新OCSP。

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CA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。

2.4 信息库访问控制

亚洲诚信CA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CA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。

2.5 高风险信息库

亚洲诚信CA将维护内部数据记录，用于记录所有曾经因为网络钓鱼或可能被其他欺诈手段利用等原因，而被撤销或被拒绝申请的证书信息，这些证书的申请机构在今后的身份验证中标识为可能的高风险证书申请。

在进行身份验证时，亚洲诚信CA将申请机构与高风险机构名单进行比对，确保证书在签发前申请机构的身份得到充分验证。同时，亚洲诚信CA将拒绝处于高风险信息库中的证书申请。

“高风险组织机构”名单包括：

1)被政府列入黑名单或经营存在异常的组织;

2) 因为可能遭到网络钓鱼或其他身份欺诈攻击而撤销其数字证书的申请者组织机构。

3. 身份标识与查验

3.1 身份查验通用要求

亚洲诚信CA在受理证书申请时，将会对订户和/或受托人进行告知、身份确认、意愿记录和协议签署；

亚洲诚信CA开展电子认证身份查验业务时，不将身份查验业务委托给外部机构或个人（非属同一法人主体的机构视为外部机构）。

3.1.1 订户告知

3.1.1.1 告知内容

亚洲诚信CA在受理证书申请时，将对订户和/或受托人告知以下内容：

- 订户的权利和义务；
- 服务收费的项目和标准；
- 电子签名认证证书、电子签名的使用条件；
- 信息安全保障措施；
- 亚洲诚信CA和订户的责任划分；
- 订户签名私钥的存储方式及安全要求；
- 订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

3.1.1.2 告知方式

亚洲诚信CA将根据证书的可信等级，分类实施订户告知程序并完整保留告知记录：

a. 高等级证书：采用面对面、电话、视频确认或主管部门认可的其他方式告知；
b. 基础级证书：除可沿用高等级证书的告知方式外，还可以采用强制阅读、短信、电子邮件等电子方式进行告知。

3.2 初始身份确认

亚洲诚信CA将在颁发证书之前对证书申请者的身份信息和相关属性进行查验，验证其身份真实，核实意愿。

对于电子签名认证证书和文档签名证书，亚洲诚信CA将在颁发证书之前根据所申请证书类型采取合理措施确认证书订户的真实意愿。

上述过程都将通过书面文件或可追溯、不可篡改的电子记录方式予以留存，作为订户意愿表达之有效证据。

同时，亚洲诚信CA也会要求申请者对其递交的材料作真实性声明，并承担相应的法律责任。亚洲诚信CA会按照本CPS之规定，对材料进行鉴别。亚洲诚信CA也可能采取附加的或者额外的方式进行这种鉴别。

如果申请者拒绝亚洲诚信CA的身份鉴别要求，则被视作放弃对证书的申请。

亚洲诚信CA声明，亚洲诚信CA可以拒绝任何申请请求，并且没有对此说明原因的义务。

3.2.1 证明拥有私钥的方法

对于电子签名认证证书和文档签名证书，证书申请者按照本CPS第6.2.2章节规定生成私钥，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CA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。

3.2.2 组织机构身份的查验

3.2.2.1 机构电子签名认证证书

亚洲诚信CA受理机构证书订户的申请时，将查验机构证书订户提供的有效证件，有效证件包括但不限于：营业执照或非企业单位（法人）登记证书、统一社会信用代码证、政府主管部门的批文或登记证书，以及法律法规和国家有关文件规定的其他有效证件。同时，机构证书订户通过法定代表人或受托人办理证书申请时，亚洲诚信CA会查验法定代表人或受托人的个人身份信息。具体查验方式及内容如下：

法定代表人或受托人申请时，必须出示其有效身份证件或有效身份证件信息，查验方法见3.2.3章节，并且受托人还须提供机构加盖公章的有效书面授权证明。

亚洲诚信CA在进行身份查验时，会根据机构证书订户所申请的证书类型采取不同的审核标准对法定代表人或受托人进行实人查验。

3.2.2.1.1 机构高等级电子签名认证证书实人查验

亚洲诚信CA 将通过以下方式之一对订户开展实人查验：

a. 法定代表人实人查验方法见3.2.3.1章节；
b. 受托人实人查验方法见3.2.3.1章节，并通过机构对公账户随机金额打款验证或主管部门认可的其它方式。

亚洲诚信CA将完整记录并保存身份查验过程和结果，做到查验过程和结果可追溯，为每张证书建立独立的身份验证记录。

3.2.2.1.2 机构基础级电子签名认证证书实人查验

亚洲诚信CA 将通过以下方式之一对订户开展实人查验：

a. 法定代表人实人查验方法见3.2.3.2章节；
b. 受托人实人查验方法见3.2.3.2章节;
c. 由申请人持有的同等级或者更高等级的有效机构证书签名验证。

亚洲诚信CA将完整记录并保存身份查验过程和结果，为每张证书建立独立的身份验证记录。

3.2.2.2 机构高等级文档签名证书

亚洲诚信CA受理机构高等级文档签名证书订户的申请时，机构身份查验方式见3.2.2.1章节。亚洲诚信CA对订户开展实人查验的要求参考3.2.2.1.1章节。

3.2.3 个人身份的查验

亚洲诚信CA受理个人证书订户的申请时，个人订户应出示能表明其真实身份的有效身份证件或输入有效身份证件信息，以核实申请人身份的有效性。有效身份证件包括但不限于：中国居民身份证或临时身份证、港澳台居民居住证、港澳居民往来内地通行证、台湾居民来往大陆通行证、护照、外国人永久居留身份证、外国人身份证、外交部开具的外国人身份证明等，以及法律法规和国家有关文件规定的其他有效身份证件。

亚洲诚信CA在对个人订户进行身份查验时会通过证件机读工具、权威数据库或主管部门认可的其他方式核验个人订户身份证件的真实性和有效性。

当个人订户授权他人代为办理时，亚洲诚信CA还需要代理人同时出示代理人与被代理人的有效身份证件或输入有效身份证件信息，以及被代理人本人签署的有效书面授权证明（明确授权事项、权限范围及有效期）。亚洲诚信CA将仔细查验代理人与被代理人身份的有效性和真实性，同时仔细检查授权材料。

亚洲诚信CA在进行身份查验时，会根据所申请证书类型采取不同的审核标准对申请人进行实人查验。

3.2.3.1 个人高等级电子签名认证证书实人查验

亚洲诚信CA将通过以下方式之一对订户开展实人查验：

a. 面对面查验：申请人持有效证件原件现场办理证书申请。亚洲诚信CA在受理申请时，通过与申请人面对面的接触，核验其身份的有效性和真实性；
b. 远程人工面对面查验：亚洲诚信CA通过音视频方式与申请人进行实时沟通，并采用录音录像记录其真实身份和真实证书申请意愿。申请人需在线出示由政府签发的有效身份证件原件，并在亚洲诚信CA的见证下，签署确认申请亚洲诚信电子签名认证证书的申请文件；
c. 生物特征验证：通过活体人脸、指纹、声纹、掌纹等生物识别技术的应用；
d. 主管部门认可的其他方式。

亚洲诚信CA将完整记录并保存身份查验过程和结果，做到查验过程和结果可追溯，为每张证书建立独立的身份验证记录。

3.2.3.2 个人基础级电子签名认证证书实人查验

亚洲诚信CA将通过以下方式之一对订户开展实人查验：

a. 通过第3.2.3.1章节规定的方式查验；
b. 运营商三要素：核对姓名、证件号码、手机号在电信运营商的一致性，并通过对应手机号的随机短信验证码核验；
c. 银行卡四要素：核对姓名、证件号码、银行卡号、银行预留手机号在银行的一致性，并通过预留手机号的随机短信验证码短信核验；
d. 由申请人持有的有效电子签名认证证书签名验证；
e. 通过主管部门认可的其他方式：如居民身份网络可信凭证、公民网络电子身份标识、国家网络身份认证系统、内地银行或支付机构对外提供的个人账户和身份信息对应关系验证等。

亚洲诚信CA将完整记录并保存身份查验过程和结果，为每张证书建立独立的身份验证记录。

3.2.3.3 个人高等级文档签名证书实人查验

个人高等级文档签名证书的实人查验方式与个人高等级电子签名认证证书一致，见3.2.3.1章节。

此外，必要时，亚洲诚信CA还可以设定其它所需要的鉴别方式和资料。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。

对于亚洲诚信CA签发的订户证书，亚洲诚信CA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CA可直接予以拒绝。

3.2.4 数据源的准确性

在将任何数据来源作为可依赖数据来源使用之前，亚洲诚信CA会对该来源的可依赖性、准确性及更改或伪造的可抗性进行评估，并考虑以下因素：

1. 所提供信息的年限；
2. 信息来源更新的频率；
3. 数据供应商及数据搜集的目的；
4. 数据对公众的可用性及可访问性；
5. 伪造或更改数据的难度。

亚洲诚信CA使用的可信第三方公开数据源包括但不限于：

1. 国家企业信用信息公示系统：http://www.gsxt.gov.cn/index.html
2. 全国组织机构统一社会信用代码数据服务中心：https://www.cods.org.cn
3. 机关赋码和事业单位登记管理网：http://www.gjsy.gov.cn/
4. 中华人民共和国中央人民政府门户网站：http://www.gov.cn/index.htm
5. 企查查：https://www.qcc.com/

3.3 订户意愿记录

亚洲诚信CA对于订户意愿记录内容的确认，包括但不限于：

a. 订户身份信息；
b. 亚洲诚信CA的信息；
c. 签名私钥保存方及其保存义务；
d. 订户对电子签名的法律责任；
e. 订户对上述a) 至d) 项内容已充分知晓并同意的明确意愿表示。

亚洲诚信CA将根据订户所申请的证书类型采取不同的审核标准核验法定代表人或受托人的身份的真实性以及申请意愿，并且会完整记录并保留意愿确认的过程和结果，做到查验过程和结果可追溯。

3.3.1 机构高等级电子签名认证证书的意愿记录

1. 法定代表人申请时，亚洲诚信CA将按照3.3.3章节的方式确认机构法定代表人的意愿；

2. 受托人申请时，亚洲诚信CA将按照3.3.3章节的方式确认受托人的意愿。同时，受托人还需提供加盖机构公章的授权文件（明确授权事项、权限范围及有效期）。

亚洲诚信CA将采用录音录像或通过主管部门认可的其他方式记录订户意愿。

3.3.2 机构基础级电子签名认证证书的意愿记录

1. 法定代表人申请时，亚洲诚信CA将按照3.3.4 章节的方式确认机构法定代表人的意愿；
2. 受托人申请时，亚洲诚信CA将按照3.3.4 章节的方式确认受托人的意愿。同时，受托人还需提供加盖机构公章的授权文件（明确授权事项、权限范围及有效期）。

3.3.3 个人高等级电子签名认证证书的意愿记录

订户意愿的确认将采用下列方式之一：

a. 现场办理时，亚洲诚信CA将通过面对面确认或让申请人手抄提示语，并采用录音录像等方式记录订户意愿；
b. 远程办理时，亚洲诚信CA将通过音视频方式或主管部门认可的其他方式确认并记录订户意愿。

3.3.4 个人基础级电子签名认证证书的意愿记录

订户意愿的确认将采用下列方式之一：

a. 与高等级证书相同的方式，见 3.3.3章节；
b. 采用强制阅读、短信或邮件确认等电子方式确认并记录订户意愿。

3.3.5 机构高等级文档签名证书的意愿记录

订户意愿的确认同3.3.1章节方式一致。

3.3.6 个人高等级文档签名证书的意愿记录

订户意愿的确认同3.3.3章节方式一致。

3.4 订户协议

亚洲诚信CA在受理证书申请时，必须与订户或其受托人正式签署相关协议，以确立双方法律关系。

订户协议完整涵盖3.1.1.1章节中规定的内容。

3.5 未验证的订户信息

除了本CPS 3.2章节所必须要求的身份信息需要得到明确、可靠的验证以外，对于没有要求验证的订户信息，亚洲诚信CA不承诺相关信息的真实性，不承担相关的法律责任。

证书中的信息必须经过验证，未经验证的信息不得写入证书。

3.6 互操作要求

亚洲诚信CA可根据业务情况，与其他经过国家主管部门批准的CA签订互操作协议，但是该电子认证服务机构的 CPS 必须符合亚洲诚信CA策略的要求，并且与亚洲诚信CA签署相应的协议。

如果国家法律法规对此有规定，亚洲诚信CA将严格予以执行。

截至目前，亚洲诚信CA未签发任何交叉证书。

3.7 命名

3.7.1 名称类型

亚洲诚信CA签发的数字证书，分配给证书持有者唯一的甄别名(Distinguished Name)，采用X.500标准命名方式，符合GB/T 16264.8要求。根据证书类型的不同，签发的证书主体甄别名有所不同。关于DN的详细说明见本CPS的7.1.4章节。

3.7.2 对名称意义化的要求

亚洲诚信CA使用DN项 (Distinguished Name)来标识证书主体及证书签发者的实体，DN项中的名称具有一定的代表性意义，可以与使用证书的最终实体的身份或特有的属性相关。证书主题名称标识了本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

3.7.3 订户的匿名或伪名

订户在进行证书申请时不能使用匿名或者伪名。

3.7.4 理解不同名称形式的规则

亚洲诚信CA签发的数字证书符合X.509 V3标准，甄别名格式遵守X.500标准。甄别名的命名规则由亚洲诚信CA定义。

3.7.5 名称的唯一性

在亚洲诚信CA信任域内，不同订户的证书的主体甄别名不能相同，且必须是唯一的。但对于同一订户，亚洲诚信CA可以用其唯一的主体甄别名为其签发多张证书。

3.7.6 商标的识别、鉴别和角色

用户在申请数字证书时不得使用可能侵犯他人知识产权的信息。如订户提交的申请信息包含商标信息，则需要订户提交有关的商标注册文件，例如由政府机构出具的合法性证明文件。亚洲诚信CA颁发数字证书时，仅对商标的合法性证明文件进行形式审查，不审查证书订户是否处于纠纷中，且无需对任何订户关于知识产权的使用行为负法律责任。当发生有关争议或纠纷时，亚洲诚信CA有权在必要时驳回相关证书申请或撤销已签发证书。

4. 证书生存周期操作要求

4.1 通用要求

在证书整个生存周期操作中的各方责任，包括不限于：

- 亚洲诚信CA承担建立、运营和维护注册通道的责任；
- 亚洲诚信CA承担与订户签订电子认证服务协议的责任；
- 订户承担提供准确信息的责任；
- 亚洲诚信CA承担记录并保存相关信息的责任。

4.2 证书申请

4.2.1 证书申请实体

证书申请实体包括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CA提供的任何数据负责。

4.2.2 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CA的审核；
    - 同意适用的订户协议以及CPS；
    - 支付任何适用的费用。
2. 责任：
    - 亚洲诚信CA负有建立、运营和维护注册通道的责任。
    - 订户即申请证书的实体，应事先了解并书面接受本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CA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CA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CA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。
    - 订户应明确表示每一个证书申请的真实意愿。
    - 亚洲诚信CA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。
    - 亚洲诚信CA应妥善记录并保管证书相关信息。

4.2.3 证书申请处理

4.2.3.1 执行识别与鉴别功能

亚洲诚信CA接收到订户的证书申请后，亚洲诚信CA验证团队会按本CPS第3.2章节的要求，对订户的身份进行识别与鉴别，并根据既定审核准则对申请进行评估，决定批准或拒绝该证书申请。亚洲诚信CA会维护系统和流程，以便根据CPS充分验证申请人的身份。无论是通过电话、传真或电子邮件进行沟通的内容还是申请者通过亚洲诚信CA WEB界面或者通过其他方式提供的资料，所有信息都将一起安全存储。

4.2.3.2 证书申请批准和拒绝

4.2.3.2.1 证书申请的批准

亚洲诚信CA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CA可以批准证书申请：

1. 该申请完全满足CPS第3.2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。

4.2.3.2.2 证书申请的拒绝

如果发生下列情形，亚洲诚信CA有权拒绝证书申请：

1. 申请不满足 CPS 第3.2章节的规定；
2. 订户不能根据要求提供所需的身份证明材料；
3. 订户不接受或反对订户协议的内容和要求；
4. 订户未按照规定支付相关费用；
5. 订户证书的使用途径不符合其所在地的法律法规；
6. 亚洲诚信CA认为批准该申请将会对亚洲诚信CA带来争议、法律纠纷或者损失。
7. 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CA将会邮件通知订户证书申请失败。

4.2.3.3 处理证书申请的时间

在正常情况下，亚洲诚信CA会在收到证书请求后的2个工作日内处理证书申请，对申请材料进行验证和审核，当订户提交的申请材料完整或者补充材料完整时，亚洲诚信CA将在5个工作日内签发证书。如有特殊情况，亚洲诚信CA将会与订户协商申请处理的时间期限。

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CA的管理要求。证书申请请求会持续有效直至被拒绝。

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

亚洲诚信CA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。

4.3.2 电子认证服务机构和注册机构对订户的通告

亚洲诚信CA在证书签发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CA会在订户申请审核通过后，对订户的通告有以下几种方式：

- 面对面告知，亚洲诚信CA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；
- 电话通知；
- 电子邮件告知；
- 其它亚洲诚信CA认为安全可行的方式通知订户并交付证书。

4.4 证书接受

4.4.1 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仅限于：

- 订户自行访问专门的亚洲诚信CA证书服务网站，将证书下载至数字证书载体中，并下载完毕。
- 亚洲诚信CA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。
- 证书获取通知发送给订户后，订户通过该通知下载证书。
- 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。

4.4.2 CA 对证书的发布

亚洲诚信CA把证书交付给订户视为证书的发布。证书签发后，在征得订户同意的前提下，亚洲诚信CA将其发布至官方信息库，订户及依赖方可按本CPS第2.2章节所述方式，通过证书序列号、证书主题等信息查询并获取相应证书；未获订户授权的证书不在信息库中对外发布。

4.4.3 CA 对其他实体的通告

亚洲诚信CA不会对其他实体进行通告。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

密钥对和证书的使用：

1. 交付前的安全保护：在将密钥对交付订户保管之前，亚洲诚信CA 采取有效措施保障其安全性，包括但

不限于：

a. 保障签名私钥生成和传输过程的安全；

b. 审核订户密钥是否符合国家或行业相关安全标准要求，对不符合要求的（如 RSA 密钥长度小于 2048 位、使用 MD5、SHA-1 等不安全算法）拒绝颁发证书；

2. 私钥管理服务要求：亚洲诚信CA 提供订户签名私钥管理服务并承诺：

a. 未经订户书面授权，不得保存或委托他人保存其签名私钥；

b. 机构证书签名私钥的使用，设置法定代表人或受托人作为授权主体；

c. 仅在获得订户明确授权的情况下使用其签名私钥；

d. 签名私钥应以加密形式存储，且存储条件符合安全标准；

e. 所有涉及签名私钥的操作应有完整、可追溯的记录；

3. 安全事件反馈：亚洲诚信CA建立便捷的外部安全事件反馈渠道，及时受理和处理证书信息错误、私钥失控或证书被盗用等异常情况。

4.5.2 依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。

4.6 证书续期

4.6.1 证书续期的情形

证书续期是指在不改变订户主体身份信息、可沿用原密钥对的情况下，在原证书到期前为订户签发新证书，以延续证书有效期。以下情形适用证书续期：

1. 原证书到期前，订户主体身份信息未变，申请延续证书有效期。

续期身份查验：对电子签名认证证书，若自订户上次完成身份查验之日起至本次续期申请日未满三年，可使用有效的原证书进行电子签名验证的方式进行确认；否则，按照本CPS第3.2章节的规定重新进行身份查验。对文档签名证书，可参考原证书验证方式审核验证，验证数据的复用期限按本CPS第4.2.3.1章节执行；超过复用期限或原验证信息不可用的，按照证书初次申请的流程及要求重新验证。

原证书已过期再次申请的，按照证书初次申请的流程及要求办理。

4.6.2 请求证书续期的实体

请求证书续期的实体为已经申请过亚洲诚信CA证书且其证书未过期的订户或其授权代表人。

4.6.3 证书续期请求的处理

对于证书续期，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：
    a. 订户的原证书存在并且由亚洲诚信CA所签发；
    b. 证书续期请求在许可期限内；
    c. 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CA将按照本CPS第3.2章节的规定进行处理；亚洲诚信CA也可以根据订户证书续期的具体申请情况，选择按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CA才可以批准签发证书。

4.6.4 颁发新证书时对订户的通告

同本 CPS 第4.3.2章节。

4.6.5 构成接受续期证书的行为

同本 CPS 第4.4.1章节。

4.6.6 电子认证服务机构对续期证书的发布

同本 CPS 第4.4.2章节。

4.6.7 电子认证服务机构对其他实体的通告

同本 CPS 第4.4.3章节。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

证书密钥更新是指为订户生成新的密钥对，并为其新公钥签发新证书（订户主体身份信息可不变）。以下情形适用证书密钥更新：

1. 原证书密钥即将到期或已到期，需以新密钥对延续证书；
2. 订户私钥已泄露、疑似泄露或被认为不再安全，需更换密钥对；
3. 因算法、密钥长度等合规要求需要更换密钥对；
4. 其他经亚洲诚信CA认可、需更换密钥对的情形。

密钥更新身份查验：对电子签名认证证书，若自订户上次完成身份查验之日起至本次更新申请日未满三年，除订户私钥泄露情形外，可使用有效的原证书进行电子签名验证的方式进行确认；否则，按照本CPS第3.2章

节的规定重新进行身份查验。对文档签名证书，可参考原证书验证方式审核验证，验证数据的复用期限按本CPS第4.2.3.1章节执行；超过复用期限或原验证信息不可用的，按照证书初次申请的流程及要求重新验证。

4.7.2 请求证书密钥更新的实体

同本 CPS 第4.6.2章节。

4.7.3 证书密钥更新请求的处理

同本 CPS 第4.6.3章节。

4.7.4 颁发新证书时对订户的通告

同本 CPS 第4.3.2章节。

4.7.5 构成接受密钥更新证书的行为

同本 CPS 第4.4.1章节。

4.7.6 电子认证服务机构对密钥更新证书的发布

同本 CPS 第4.4.2章节。

4.7.7 电子认证服务机构对其他实体的通告

同本 CPS 第4.4.3章节。

4.8 证书变更

4.8.1 证书变更的情形

证书变更是指订户的证书在其有效期内，改变证书中除订户公钥之外的信息而签发新证书的情形， 包括但不限于：

a. 订户更名；

b. 证书扩展变更等。

亚洲诚信CA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。

4.8.2 请求证书变更的实体

请求证书变更的实体为已经申请过亚洲诚信CA证书且其证书未过期的订户或其授权代表人。

4.8.3 证书变更请求的处理

当订户提交证书信息变更申请后，对于文档签名证书，若原证书的验证可用且时效未过期，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CA会按照初次申请证书流程和要求进行审核验证。电子签名认证证书会按照本CPS第3.2章节的规定重新进行身份查验。审核通过后，亚洲诚信CA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。

4.8.4 颁发新证书时对订户的通告

同本 CPS 第4.3.2章节。

4.8.5 构成接受变更证书的行为

同本 CPS 第4.4.1章节。

4.8.6 电子认证服务机构对变更证书的发布

同本 CPS 第4.4.2章节。

4.8.7 电子认证服务机构对其他实体的通告

同本 CPS 第4.4.3章节。

4.9 证书撤销或冻结

4.9.1 证书撤销的情形

4.9.1.1 订户证书撤销的原因

若出现以下情况的一种或多种，亚洲诚信CA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CA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CA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CA获得了证书遭到误用的证据；
5. 亚洲诚信CA获悉订户违反了订户协议、CPS 中的一项或多项重大责任；
6. 亚洲诚信CA获悉证书中所含信息出现重大变化；
7. 亚洲诚信CA获悉证书的签发未能符合亚洲诚信CA的CPS；
8. 亚洲诚信CA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；
9. 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；
10. 亚洲诚信CA已经履行催缴义务后，订户仍未缴纳服务费。
11. 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）。

4.9.1.2 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CA应在7天之内撤销中级CA证书：

1. 中级CA正式书面申请撤销；
2. 中级CA发现并通知亚洲诚信CA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CA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CA获得了证书遭到误用的证据；
5. 亚洲诚信CA获悉中级CA证书的签发未能符合CPS；
6. 亚洲诚信CA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CA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。

4.9.2 请求证书撤销的实体

请求证书撤销的实体可为订户、订户的授权代理人、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有合理理由撤销证书。

4.9.3 撤销请求的流程

4.9.3.1 订户主动提出撤销申请

1. 订户可通过信息库中提供的渠道向亚洲诚信CA提交撤销证书申请及相关身份证明材料；
2. 亚洲诚信CA按本CPS第3.2章节的规定进行证书撤销请求的鉴别；
3. 亚洲诚信CA进行撤销请求鉴别后，一并确认订户所需撤销的证书是否为亚洲诚信CA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；
4. 亚洲诚信CA完成撤销工作后应及时将其发布到证书撤销列表；
5. 证书被撤销后，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撤销的证书；
6. 亚洲诚信CA提供7*24小时的证书撤销申请服务，订户主动申请证书撤销的，必须提交书面申请资料。

4.9.3.2 订户被强制撤销证书

1. 当亚洲诚信CA有充分的理由确信出现本 CPS第 4.9.1.1章节中会导致订户证书被强制撤销的情形时，亚洲诚信CA将通过内部流程申请撤销证书；
2. 在亚洲诚信CA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进行订户证书撤销；
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撤销证书，若决定撤销将告知其结果；
4. 在证书被撤销后，亚洲诚信CA将通过适当的方式，包括邮件、电话等，通知最终订户证书已被撤销及被撤销的理由；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撤销的证书；
5. 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CPS第1.6.3章节中所提供的联系方式进行问题报告。

4.9.4 撤销请求宽限期

亚洲诚信CA不支持撤销请求宽限期。

4.9.5 电子认证服务机构处理撤销请求的时限

亚洲诚信CA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。

4.9.6 依赖方检查证书撤销的要求

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CA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CA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。

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

4.9.8 CRL 发布的最大滞后时间

亚洲诚信CA 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。

4.9.9 在线状态查询的可用性

亚洲诚信CA 的 OCSP 查询服务符合 GB/T 19713—2025 及 RFC6960 标准，服务7*24 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。

4.9.10 在线状态查询要求

亚洲诚信CA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CA若收到未签发证书的 OCSP请求，不会响应“good”状态。

4.9.11 撤销信息的其他发布形式

若订户证书使用场景中的访问流量较高，亚洲诚信CA可以根据RFC6066 中的规定，要求订户使用 OCSP 装订的方式来访问 OCSP服务。

4.9.12 密钥损害的特别要求

若订户或亚洲诚信CA发现或怀疑私钥泄露，应立即采取措施根据CPS要求撤销密钥受损的证书，并重发证书。

4.9.13 证书冻结的情形

出现以下情形之一，亚洲诚信CA可将订户证书暂时冻结：

1）订户请求冻结证书；

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，申请冻结订户证书；

3）亚洲诚信CA发现订户的征信或经营状态出现重大问题；

4）亚洲诚信CA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CA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CA有理由相信订户未履行订户协议下的义务、陈述或保证；

7）本CPS要求或有相关法律法规要求冻结订户证书。

4.9.14 请求证书冻结的实体

请求证书冻结的实体可为订户、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有合理理由冻结证书。

4.9.15 冻结请求的流程

4.9.15.1 订户主动提出冻结申请

1. 订户可通过向亚洲诚信CA提交冻结证书申请表及相关身份证明材料；
2. 亚洲诚信CA按本CPS第3.2章节的规定进行证书冻结请求的鉴别；
3. 亚洲诚信CA进行冻结请求鉴别后，一并确认订户所需冻结的证书是否为亚洲诚信CA所发放，证书是否在有效期内，冻结理由是否属实，若均通过则对证书进行冻结；
4. 亚洲诚信CA完成冻结工作后应及时将其发布到CRL及OCSP上；
5. 证书被冻结后，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冻结的证书；
6. 亚洲诚信CA提供7*24小时的证书冻结申请服务，订户主动申请证书冻结的，必须提交书面申请资料。
7. 亚洲诚信CA在鉴别冻结请求有效后，于2个工作日内完成证书冻结。

4.9.15.2 订户被强制冻结证书

1. 当亚洲诚信CA有充分的理由确信出现本 CPS第 4.9.13章节中会导致订户证书被强制冻结的情形时，亚洲诚信CA将通过内部流程申请冻结证书；
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冻结证书，若决定冻结将告知其结果；
3. 在证书被冻结后，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冻结及被冻结的理由；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冻结的证书；
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CPS第1.6.3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个工作日完成证书冻结。

4.9.16 冻结的期限限制

订户证书一旦被冻结将处于冻结状态直至：

- 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；
- 当证书被动冻结时，订户可在收到冻结通知后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；
- 当证书被动冻结的原因消除后，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；
- 当被冻结的证书到期时，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。

4.10 证书状态服务

4.10.1 操作特征

证书状态信息可通过CRL和OCSP响应获得。

对于被撤销的证书，亚洲诚信CA在该证书到期前，不删除其在CRL及OCSP中的撤销记录。

冻结的证书将在CRL中发布，当被冻结的证书失效后，将不再出现在CRL中。证书冻结后，亚洲诚信CA将在周期性签发的CRL中，于最近的下次更新时间发布所冻结的证书，并立即更新OCSP查询数据库，确保实时发布所冻结的证书。

4.10.2 服务可用性

亚洲诚信CA提供7*24小时不间断证书状态查询服务与CRL下载服务，服务可用率不低于99%。

4.10.3 可选特征

OCSP响应程序可能不适用于所有证书类型。

4.11 停止使用认证服务

订购服务终止包含以下情况：

- 证书到期后未按时续缴服务费；
- 证书到期后没有进行证书更新或密钥更新；
- 证书到期前被撤销。

一旦用户在证书有效期内终止使用亚洲诚信CA的证书认证服务，亚洲诚信CA在批准其终止请求后，将实时把该订户的证书撤销，并按照 CRL 发布策略进行发布。

亚洲诚信CA详细记录撤销证书的操作过程，并定期将订购终止后的证书及相应订户数据进行归档，订户自行保管的私钥将无法再次被用于证书申请，委托在亚洲诚信CA的订户私钥将被销毁。

4.12 密钥托管与恢复

亚洲诚信CA不会将根证书私钥托管给任何第三方机构或个人，而是在自身控制的安全环境中保管。亚洲诚信CA对根私钥和 CA 私钥进行备份，按照加密设备制造商提供的操作规范生成备份密文文件和备份恢复激活材料并保存到屏蔽机房的保险柜（或银行保管箱等安全等级不低于本地备份的场所）。

5. 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

亚洲诚信CA电子认证服务整体机房，位于上海市浦东新区及松江区。每个机房按功能分为4个区域，分别是公共区、RA区、CA区、KM区。

整体机房严格遵照国家机房相关规范标准建设，采用全模块化结构设计，达到国家标准（如 GB 50174-2017 A级）。

亚洲诚信CA的机房和系统建设遵循下列标准实施：

1. 《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》（GM/T 0034-2014）
2. 《电子信息系统机房设计规范》（GB 50174-2017）
3. 《建筑内部装修设计防火规范》（GB 50222-2017）
4. 《低压配电设计规范》（GB 50054-2011）
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）

5.1.2 物理访问

外来人员进入亚洲诚信CA机房，需经过楼内保安登记审核及亚洲诚信CA门禁系统，且需要有亚洲诚信CA工作人员陪同进入。

亚洲诚信CA操作人员进入CA机房，需在2人可信人员同时在场，且经过双因素认证进入。

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：

- 采用门禁卡和人体特征鉴别的控制方式控制每道门的进入；
- 进入每一道门都有日志记录；
- 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。

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，对于重大事件的视频保留1年以上并单独存档。设置非法入侵检测报警、环控检测报警，设置声光报警器，触发报警同时通知运维人员；所有机房门禁系统采用两种以上认证方式。

5.1.3 电力与空调

亚洲诚信CA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供电中断时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负载可续航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、设备满负载情况配置，保证机房各个区域的温湿度能满足系统运行、人员活动和其他辅助设备的要求。

5.1.4 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。

5.1.5 火灾防护

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，并每月开展消防安全检测。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。

5.1.6 介质存储

亚洲诚信CA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。

5.1.7 废物处理

亚洲诚信CA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其初始化并进行特殊销毁。

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。

5.1.8 异地备份

亚洲诚信CA 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。

对关键数据及审计日志进行备份，并在距离 10 公里以上的异地数据中心进行实时同步备份；同时，定期进行离线备份，并将备份介质存放在其中一个数据中心。保存设施满足5.1.6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。

5.2 操作过程控制

5.2.1 可信角色

亚洲诚信CA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：

a. 系统管理员：负责对本机构电子认证服务系统进行系统策略配置、业务管理、系统用户管理、角色权限设置、业务授权等；

b. 技术运维员：负责对本机构物理环境、网络、服务器、平台软件、电子认证服务系统等基础设施进行日常监控、维护与保障；

c. 数据库管理员：负责对本机构的各类数据库进行日常运维、性能优化，并严格按制度执行数据备份、归档策略；

d. 系统审计员：负责对系统和网络进行审计，包括上述系统的日志记录管理与审计、审计报告的生成和审核，并对审计结果进行汇报等；

e. 密钥管理员：负责根密钥材料的安全保管，组织及参与CA密钥生成仪式，负责参与CA密钥对的创建与生存周期维护。其人员数量需符合密钥控制策略的具体要求；

f. 业务操作员：负责证书申请的受理、审核和证书制作，对证书订户的身份真实性、申请意愿及过程的真实性进行鉴证，核实证书主体与订户的一致性；

g. 客户档案管理员：负责客户证书申请及相关档案资料的归档和维护，保障客户信息资料的完整性与保密性；

h. 运营审计员：负责对客户鉴证、证书签发、客户服务等核心业务的业务流程进行独立审计， 依据CPS、CP及相关法律法规标准，评估运营的合规性、安全性与服务能力。

5.2.2 每项任务需要的人数

亚洲诚信CA在具体业务规范中对关键任务进行严格控制，个人不能同时承担多项重要角色。

另外，亚洲诚信CA还对以下敏感操作实施多个可信角色共同完成，例如：

- 屏蔽区场地访问：设置为2 个可信人员进出模式；
- 鉴别、审核和签发证书：需要 2 个可信人员共同完成；
- 保存根密钥激活数据的保险柜：设置为2 个可信人员开启模式；
- 密钥和密码设备的操作和存放：需要 5 个可信人员中的 3 个共同完成；
- CA系统后台操作：需要 2 个可信人员共同完成；
- 重要系统数据操作和维护：需要至少1人操作，1人监督记录。

5.2.3 每个角色的识别与鉴别

亚洲诚信CA在授予人员可信角色前会对其进行严格的身份验证和背景调查，并对其进行相关角色的培训及考核。然后才会对这些人员授予所需的访问权限，发放访问设备并允许其执行特定的操作。

5.2.4 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即亚洲诚信CA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：

a. 系统管理员、技术运维员、数据库管理员、系统审计员的角色不能相互兼任；

b. 业务操作员在人工受理审核过程中，对同一个证书业务，证书信息录入和审核环节由不同人员完成；

c. 业务操作员、客户档案管理员、运营审计员不能相互兼任；

d. 密钥管理员与系统管理员、技术运维员不能兼任；

e. 密钥管理员与本CPS第5.2.1中除策略管理机构成员以外的其他可信角色均不宜兼任。

5.3 人员控制

5.3.1 资格、经历和无过失要求

亚洲诚信CA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CA 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CA相关的培训和考核后方能上岗。

5.3.2 背景审查程序

亚洲诚信CA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，并签署劳动合同。

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。
- 在背景调查中，对发现以下情形的人员，可直接拒绝其成为可信人员的资格：
  - 存在捏造事实或资料的行为；
  - 借助不可靠人员的证明；
  - 使用非法的身份证明或者学历、任职资格证明；
  - 工作中有严重不诚实的行为。
- 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CA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。

5.3.3 培训要求

亚洲诚信CA根据可信角色的职位需求，给予相应的岗前培训，所有可信人员在正式上岗前完成不少于20小时的岗前培训并通过考核，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；
- 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。

5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年必须至少接受亚洲诚信CA组织的培训一次，培训时长不少于20小时。对于认证系统运营相关的人员，每年至少进行一次相关技能和知识培训。此外，亚洲诚信CA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。

5.3.5 工作岗位轮换周期和顺序

亚洲诚信CA 将依据本机构的安全管理策略而制定在职人员的工作岗位轮换周期和顺序。

5.3.6 未授权行为的处罚

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，亚洲诚信CA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，实施对该名人员调离工作岗位、通报批评、罚款、辞退以及提交司法机构处理等措施。

5.3.7 独立合约人的要求

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。

5.3.8 提供给员工的文档

亚洲诚信CA向其员工提供完成其工作所必须的文档。

5.4 审计日志程序

5.4.1 记录事件的类型

亚洲诚信CA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：

这些事件包括但不限于：

1. CA密钥生存周期内的管理事件，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；
2. 密码设备生存周期内的管理事件，包括：

- 设备接收、安装、卸载、激活、使用、维修等；

3. 证书申请事件，包括：
   - 订户接受订户协议，申请资料的验证、申请及验证资料的保存等；
4. 证书生存周期内的管理事件，包括：
   - 证书的申请、批准、更新、撤销等；
   - 成功或失败的证书操作；
5. 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；
   - 路由器和防火墙相关活动。
6. 路由器和防火墙活动的日志记录至少包括:
   - 路由器和防火墙的成功和失败的登录尝试；以及
   - 记录在路由器和防火墙上执行的所有管理操作，包括配置更改、固件更新和访问控制修改；以及
   - 记录对防火墙规则所做的所有更改，包括添加、修改和删除；以及
7. 记录所有系统事件和错误，包括硬件故障、软件崩溃和系统重启。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；
   - OCSP响应签名、CRL的签发与发布等
8. 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；
9. 可信人员管理记录，包括：
   - 网络权限的账号申请记录，
   - 系统权限的申请、变更、创建申请记录，
   - 人员情况变化。

日志记录一般需包含：

1. 记录的日期和时间；
2. 记录的序列号；
3. 做日志记录的实体的身份；
4. 记录内容的描述。

5.4.2 处理日志的周期

对于系统的自动日志和操作人员的手工记录，亚洲诚信CA每月进行一次检查和汇总。

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，包括但不仅限于证书认证系统、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季度审计一次。

5.4.3 审计日志的保存期限

亚洲诚信CA 所有审计日志在证书失效后至少保存5年。

5.4.4 审计日志的保护

亚洲诚信CA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CA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，亚洲诚信CA 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。

5.4.5 审计日志备份程序

亚洲诚信CA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。

5.4.6 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。

对于纸质审计信息，则有专门的文件柜来实现收集归档。

5.4.7 对导致事件实体的通告

当亚洲诚信CA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CA有权决定是否对事件相关实体进行通知。

5.4.8 脆弱性评估

亚洲诚信CA根据政策、管理的变化，每年不少于1次对系统进行安全脆弱性评估，并根据报告采取措施，以降低运营风险。

5.5 记录归档

5.5.1 归档记录的类型

亚洲诚信CA对以下几类事件进行归档记录，包括但不限于：

1. 证书申请材料和订户的意愿记录；
2. 所有审计日志；
3. 密码设备全生存周期管理记录；
4. 密码设备的日常操作与使用记录；
5. 根证书或密钥生存周期管理的全部记录；
6. 证书认证系统运行日志；
7. 已识别的安全事件及处理记录；
8. 证书认证系统关键操作日志；
9. 电子认证服务过程中其他操作记录。
10. 员工资料，包括但不限于背景调查、录用、培训等资料；
11. 各类外部、内部评估文档。

5.5.2 归档记录的保存期限

1. 对订户证书生存周期内的管理事件的归档，保留5年以上。
2. 对 CA 证书和密钥生存周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生存周期。
3. 订户证书的归档保留期限不少于证书失效后5年。
4. CA 证书和密钥的归档在 CA 证书和密钥生存周期之外，额外保留10年。

5.5.3 归档文件的保护

亚洲诚信CA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。

5.5.4 归档文件的备份程序

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。

5.5.5 记录时间戳要求

亚洲诚信CA 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。

5.5.6 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。

5.5.7 获得和检验归档信息的程序

亚洲诚信CA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。

5.6 电子认证服务机构根证书密钥更替

亚洲诚信CA的根证书有效期最长不超过25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。

当根密钥发生泄露或者存在安全隐患时，将立即启动密钥更替。

1. 调查并向上级机构和主管部门上报事件；
2. 在安全可靠环境中生成新密钥对；
3. 在信息库服务发布新的根CA公钥，并将其发布给订户和依赖方（如存在）；
4. 在完成密钥更替后，按照GB/T 25056-2018 中8.2.4.3规定的方式，销毁旧私钥及其备份，并保留相关操作记录。

CA 证书对应的密钥对，当其寿命超过本 CPS 规定的最大生存周期到期前2年时，亚洲诚信CA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 密钥的生存周期之前，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，并发布新的CA公钥证书。
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。

5.7 损害和灾难恢复

损害与灾难恢复的预案与流程，包括：

1. 业务连续性目标：
    a. 恢复时间目标 (RTO)：确保在灾难发生后 72 小时内恢复证书状态查询服务（包括 CRL 和 OCSP），并恢复证书签发认证业务。
    b. 恢复点目标 (RPO)：通过健全的数据备份与同步机制，确保灾难发生时丢失的数据时间跨度不超过24小时。
2. 恢复流程：
    a. 证书库的恢复过程：包括重建安全运行环境的流程，生成受影响并被撤销的证书列表，对订户密钥的处理方式，以及重新向实体提供公钥证书的要求和流程；
    b. 根密钥损害恢复过程：包括重建安全环境的流程，为订户重新签发公钥证书，向订户提供新的公钥证书的流程；
    c. 其他关键资产恢复过程：包括对 CA 物理设施、计算资源、网络环境、软件或数据，以及其他密钥数据的恢复方案。

3. 根私钥应急处理：建立根私钥泄露的应急流程，流程需明确应急响应时间要求、责任人员、处置步骤和上报机制，每年进行一次应急演练；
4. 事件报告：见本CPS 第5.9章；
5. 定期验证：定期验证备份的设备、数据可用性，包括备份恢复测试和功能验证，每年至少进行一次灾难恢复演练。

5.8 电子认证服务机构终止

当亚洲诚信CA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》等相关法律法规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进行相关工作，包括但不限于：

1. 起草并发布CA终止声明，至少提前九十日通知与证书订户、依赖方等相关实体，至少提前六十日向主管部门报告；
2. 具有资质的电子认证服务业务承接单位，并签署承接协议，明确约定承接机构的工作范围和责任；
3. 向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；
4. 停止证书状态服务并归档相关数据；
5. 停止其他电子认证相关服务并归档相关数据；
6. 停止密码设备并归档相关密钥数据；
7. 及时撤销或冻结业务管理员和业务操作员的操作权限；
8. 对所有存档文件记录进行整理和封存；
9. 对所有敏感文档和数据进行安全处理和封存；
10. 清除主机和密码硬件设备中的敏感数据；
11. 其他涉及CA运营的数据、密钥安全的操作；
12. 如果有与订户电子签名认证证书签发、管理相关的外部合作机构，在此文档中明确描述合作机构终止服务和通告相关的过程。

5.9 重大事项报告

亚洲诚信CA在处理重大事件时，在识别事件发生的3个工作日内向公司管理层报告，并决定是否向上级机构和主管部门报告。重大事件包括但不限于：

1. 证书认证系统迁移或改造：包括系统软件、网络、部署的重大改变。符合以下之一：
    a. 机房迁移，或机房内服务区、管理区或核心区划设范围改变；
    b. 变更电子签名认证证书签发逻辑；
    c. 新增远程证书注册子系统；
    d. 新增、更改或者删除用于签发电子签名认证证书的证书链；
    e. 其他对电子认证服务安全、用户资料安全有影响的改变。
2. 重大安全事故：包括电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等，导致系统无法正常运行或数据安全性受到严重威胁的情形。符合以下任意之一：

a. 证书签发及验证服务连续停机时间超过24h；

b. 发生根证书密钥等关键数据泄露；

c. 持续或较大范围未经授权的私钥访问记录或其他异常活动；

d. 系统日志持续或较大范围显示异常操作(如非授权时间或网络地址访问敏感功能)。

3. 订户信息泄露事件：包括订户身份信息、证书申请资料等敏感数据被泄露等。符合以下任意之一：

a. 个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；

b. 数据丢失导致无法恢复证书状态信息。

4. 合规性事件：包括不符合相关法律法规、标准或监督要求的情形。符合以下任意之一：

a. 涉及电子认证服务的司法判定；

b. 收到行政部门违规通知或处罚决定。

5. 人力资源类事件：包括一个月内核心管理层集体离职、大规模劳动纠纷、重大职场安全事件等。符合以下任意之一：

a. 涉及2名及以上管理层人员或10%以上可信人员的离职；

b. 劳动纠纷参与人数超过员工总数10%，且经法院或仲裁机构生效裁决确认由CA承担法律责任。

6. 认证系统技术安全控制

6.1 技术安全管理制度要求

亚洲诚信CA建立了技术安全管理制度，其中包括了密钥管理、系统开发、网络防护等领域，并且每年定期召开安全策略委员会会议进行相关制度评审。

6.2 密钥对的生成和安装

6.2.1 CA密钥对的生成和安装

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生成。加密机采用密钥分割或密钥共享机制进行备份。

在生成CA 密钥对时，亚洲诚信CA 按照加密机密钥管理办法，在获得安全策略委员会授权的情况下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CA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音录像记录并保存不少于操作完成后十年。

6.2.2 订户密钥对的生成和交付

订户密钥对的生成、交付及控制方式按证书类型确定：

（一）电子签名认证证书

签名密钥对的生成、交付及控制方式，符合以下要求之一：

1. 由订户持有的符合国家安全标准的密码模块产生和存储；
2. 由亚洲诚信CA产生、保存，并提供技术措施确保订户对签名私钥的独占控制权；
3. 其它主管部门认可的创新性保护方案。

（二）文档签名证书

由订户在符合相应标准的密码模块或介质中生成并存储私钥，公钥经CSR提交给亚洲诚信CA。

订户签名私钥的相关操作日志将被完整记录，包括时间、方式、操作人员等信息，保存期不少于证书失效后五年。

6.2.3 公钥传送给证书签发机构

对于由订户自行生成密钥对的证书，作为证书申请流程的一部分，订户在CSR中将公钥提交给亚洲诚信CA；对于由亚洲诚信CA或其密钥管理系统生成密钥对的情形，公钥在签发流程内部传递。

6.2.4 电子认证服务机构公钥传送给依赖方

亚洲诚信CA的公钥包含在亚洲诚信CA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CA官网下载。

6.2.5 密钥的长度

亚洲诚信CA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CA不同类型的证书密钥遵循以下标准：

证书类型	根证书	中级CA证书	订户证书
签名算法	SM3WithSM2或 SHA384WithRSA	SM3WithSM2或 SHA384WithRSA	SM3WithSM2或 SHA384WithRSA或SHA256WithRSA
公钥算法	SM2或 RSA4096	SM2或 RSA2048或 RSA4096或 ECC-P384	SM2或 RSA2048或RSA3072或RSA4096或 ECC-P256或ECC-P384

6.2.6 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。

6.2.7 密钥使用目的

亚洲诚信CA签发的X.509 v3 证书包含了密钥用法扩展项（见 7.1.2 章节描述），其用法与RFC5280 标准相符。对于亚洲诚信CA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，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。

6.3 私钥保护和密码模块工程控制

6.3.1 CA私钥保护和密码模块的工程控制

亚洲诚信CA所用的密码模块都是经国家密码管理局批准和许可的产品，符合《GB/T 37092-2018 信息安

全技术密码模块安全要求》，具体参照设备制造商提供的资料。

亚洲诚信CA私钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制，即采取五选三方式。CA 私钥存放在加密机中，加密机的管理密钥被分割保存在 5 份激活材料中，私钥激活材料的管理权限分散到 5 位密钥管理员中，至少在其中 3 人在场并许可的情况下，输入 PIN 码，才能对私钥进行操作。

6.3.2 订户私钥保护和密码模块工程控制

由订户持有的电子签名认证证书签名私钥，应遵守服务协议采取预防措施防止私钥及其激活数据丢失、泄露、更改或未经授权的使用；由亚洲诚信CA委托保管的签名私钥，适用以下：

1. 用于电子签名模式；
2. 定期评估安全控制措施；
3. 每次签名私钥调用获得订户的明确授权，并完整记录该授权；
4. 提供订户关于签名私钥及激活数据安全使用的指导与建议；
5. 电子签名模式和控制措施符合相关标准或主管部门认可的其它方式。

6.3.3 私钥托管

亚洲诚信CA对私钥托管遵循以下原则：

1. 亚洲诚信CA的根证书私钥及中级CA私钥不得托管给任何第三方机构或个人，由亚洲诚信CA在自身控制的安全环境中保管。
2. 对于电子签名认证证书和文档签名证书，经订户明确授权，亚洲诚信CA提供订户签名私钥托管服务，并遵守以下要求：
    a. 仅由亚洲诚信CA保存其签名私钥；
    b. 签名私钥以加密形式存储，存储条件符合相关安全标准；
    c. 仅在获得订户明确授权的情况下使用其签名私钥，且每次调用均完整记录该授权；
    d. 机构证书签名私钥的使用，以法定代表人或受托人作为授权主体；
    e. 所有涉及签名私钥的操作均有完整、可追溯的记录。

6.3.4 私钥备份

亚洲诚信CA对根私钥和CA私钥进行备份，可分为两种，一是按照加密设备制造商提供的操作规范生成备份密文文件和备份恢复权限IC卡并保存到屏蔽机房的保险柜（或银行保管箱等安全等级不低于本地备份的场所）；一是按照加密设备制造商提供的操作规范生成克隆设备和管理员操作员IC 卡并存放在屏蔽机房（或银行保管箱等安全等级不低于本地备份的场所）。

6.3.5 私钥归档

当亚洲诚信CA的CA密钥对到期后，这些密钥对将被归档保存至少 10年。归档的CA 密钥对保存在本CPS 6.2.1所述的硬件密码模块中，并且亚洲诚信CA 的密钥管理策略和流程都确保了归档后的CA密钥对不会再被用于生产系统中。当归档CA密钥对达到归档保存期限之后，亚洲诚信CA将按照本 CPS 6.3.10 所述的方法进行安全地销毁。

亚洲诚信CA基于PKI理论为订户产生的加密私钥的归档参照CA的密钥归档方法进行归档。

6.3.6 私钥导入、导出密码模块

亚洲诚信CA密钥对在硬件密码模块上生成，保存和使用。为了实现恢复，亚洲诚信CA按照加密设备制造商提供的操作规范，由多人控制对 CA 密钥进行备份。

另外，亚洲诚信CA还有严格的密钥管理流程对 CA 密钥对复制进行控制。有效防止了 CA 私钥的丢失、失窃、修改、非授权的泄露、非授权的使用等。

6.3.7 私钥在密码模块的存储

亚洲诚信CA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。

6.3.8 激活私钥的方法

同本 CPS第6.3.1章节。在至少3名密钥管理员在场并许可的情况下，使用加密设备的操作员权限实现。当需要使用CA私钥时（在线或离线），需要密钥管理员提供操作员IC卡才能完成。

6.3.9 解除私钥激活状态的方法

对于亚洲诚信CA私钥，当CA系统向密码模块发出退出登录，或密码管理软件向密码模块发出关闭指令，或存放私钥的硬件密码模块断电时，私钥进入非激活状态。

解除私钥的操作，在至少3名密钥管理员在场并许可的情况下，密钥管理员使用含有自己的管理员卡登录服务器密码机进行。

6.3.10 销毁私钥的方法

在亚洲诚信CA私钥生存周期结束后，亚洲诚信CA将CA私钥继续保存在一个备份硬件密码模块中，其他CA私钥备份被安全销毁。同时，所有用于激活私钥的PIN码、IC卡等也必须被销毁。

归档的CA私钥在其归档期限结束后，需在多名可信人员参与的情况下安全销毁。CA私钥的销毁将确保CA私钥从硬件密码模块中彻底删除，不留有任何残余信息。

6.3.11 密码模块的评估

亚洲诚信CA使用国家密码管理局批准和许可的密码产品，密码模块的评估由国家密码管理局负责。

6.4 密钥对管理的其他方面

6.4.1 公钥归档

参照本 CPS第5.5.2章节。

6.4.2 证书操作期和密钥对使用期限

证书类型	证书最大有效期	密钥最大有效期
根证书	25年	25年

证书类型	证书最大有效期	密钥最大有效期
中级CA证书	15年	15年
文档签名证书	39个月	无限制
电子签名认证证书	39个月	39个月

CA以及电子签名认证证书到期后，签名私钥不可用于电子签名。

6.5 激活数据

6.5.1 激活数据的产生和安装

亚洲诚信CA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3位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卡的登录口令等，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CA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。

6.5.2 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CA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。

6.5.3 激活数据的其他方面

订户的密钥对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存周期，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个月后应进行修改。

6.6 计算机安全控制

计算机安全建立并实施符合GB/T25056-2018中第8.2要求的计算机安全控制体系，包括但不限于：

1. 至少每半年检查一次系统升级补丁，记录系统升级审批及实施过程；
2. 对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划；
3. 对所有服务器和终端安装杀毒软件；
4. 病毒库更新间隔；
5. 病毒扫描时间间隔。

6.7 生存周期安全控制

亚洲诚信CA建立并实施符合GB/T 25056-2018中第10、11、12章要求的生存周期安全控制体系。

6.8 网络安全控制

亚洲诚信CA建立并实施符合GB/T 25056-2018中5.3.8要求的网络安全控制体系，包括但不限于：

- 网络结构满足GB/T 25056-2018附录A中规定形式的一种；
- 对所有Web服务配置防火墙、Web应用防火墙、入侵检测系统等网络安全防护措施；
- 建立并维护网络拓扑图，包含所有网路设备、连接关系和安全边界，定期更新，与机房实际情况保持一致；

网络访问控制：

- 建立针对证书签发子系统及数据库的访问白名单机制，仅授权证书注册子系统的必要功能模块及必要的管理设备进行访问；
- 建立针对证书注册子系统和数据库的访问白名单机制。

网络监控：

- 定期对系统日志进行分析；
- 分析内容包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

6.9 时间戳

亚洲诚信CA认证系统签发的数字证书、CRL包含日期信息，且这些日期信息经过数字签名。

认证系统日志、操作日志都有相应的时间标识。

认证系统所取的时间源是世界协调时间（ Coordinated Universal Time，简称UTC）。

亚洲诚信CA提供符合RFC3161的时间戳服务，主要用于代码签名或者文档签名。

7. 证书、证书撤销列表和在线证书状态协议

7.1 证书

亚洲诚信CA签发的证书格式符合 GB/T 20518 数字证书格式规范，包含如下证书域。

7.1.1 版本号

亚洲诚信CA 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。

7.1.2 证书扩展项

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

- 密钥用途（关键）

证书类型	0	1	2	3	4	5	6	7	8
个人证书	×	√	×	×	×	×	×	×	×
机构证书	×	√	×	×	×	×	×	×	×
文档签名证书	√	√	×	×	×	×	×	×	×
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CA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，见本CPS第1.3.1定义。

- 基本限制（关键）

根证书值为True，证书数目上限不设置；

中级CA证书值为True，证书数目上限为0；

订户证书值为False。

- 扩展密钥用途

	文档签名证书	个人电子签名认证证书（包括高等级和基础级）	机构电子签名认证证书（包括高等级和基础级）
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	×	√	√
文档签名 1.3.6.1.5.5.7.3.36	√	√	√
PDF签名 1.2.840.113583.1.1.5	√	×	×
微软文档签名 1.3.6.1.4.1.311.10.3.12	√	×	×

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

若存在，CRL分发点扩展项包含可以获取CRL 的URL，用于验证证书状态。

- 机构信息访问

若存在，包含上级签名证书访问以及OCSP地址信息。

7.1.3 算法对象标识符

亚洲诚信CA签发的证书符合RFC5280标准，采用SM2 Signing with SM3（1.2.156.10197.1.501）算法签名。SM2算法其OID为：1.2.840.10045.2.1，附加参数为：1.2.156.10197.1.301。对于RSA算法其OID为：1.2.840.113549.1.1.1，签名使用RSA Signing with SHA256（1.2.840.113549.1.1.11）或者 RSA Signing with SHA384（1.2.840.113549.1.1.12）。对于ECC算法其OID为：1.2.840.10045.2.1,其签名使用ECDSA Signing with SHA256（1.2.840.10045.4.3.2）或者ECDSA Signing with SHA384（1.2.840.10045.4.3.3）。

7.1.4 主体名称

亚洲诚信CA的证书含有签发机构和证书订户主体甄别名，对证书申请者的身份和其他属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名形式包含在证书主题内，是证书持有者的唯一甄别名。

亚洲诚信CA证书签发机构的主体甄别名命名规则如下：

属性	值
国家(C)	CN
机构(O)	TrustAsia Technologies, Inc.

属性	值
机构部门(OU)	亚洲诚信CA可能依据用户类型、应用领域、区域的不同采用不同的签发者为用户签发证书，所以亚洲诚信CA证书中可包含不同的签发者名称。
通用名(CN)	此属性为CA名

亚洲诚信CA证书订户的主体甄别名命名规则如下：

属性	值
国家(C)	订户所属的国家代码
省(S)	订户所在省份，或者不用
地区(L)	订户所在城市，或者不用
机构(O)	对于有确定机构的订户，是订户所在机构名称
机构部门(OU)	不用或者可以包含以下一个或多个内容: 订户所在机构的具体部门 其他描述身份或证书类型的文字
名字(givenName)	申请人的个人法定名字，或者不用
姓名(surname)	申请人的个人法定姓氏，或者不用
序列号（OID2.5.4.5）(SN)	订户或者机构敏感信息的唯一的可识别摘要信息，或者不用 个人证书主体序列号：身份证件代码和身份证件号码拼接的字符串的杂凑值 机构证书主体序列号：机构证件号码
通用名(CN)	机构名或个人姓名(电子签名证书)，或其他可识别的名称

7.1.5 名称限制

亚洲诚信CA签发的证书，其实体名称不允许为无意义的匿名或者伪名，必须是有明确含义的识别名称，使用英文名称时应能正确表达实体名称。

7.1.6 证书策略对象标识符

CA证书的证书策略扩展项中，certificatePolicies:policyIdentifier 设置为 anyPolicy。终端实体证书策略见本CPS第1.3.1节。

7.1.7 策略限制扩展项的用法

不适用。

7.1.8 策略限定符的语法和语义

允许policyQualifiers存在，为限定符id-qt-cps（OID：1.3.6.1.5.5.7.2.1），内容为亚洲诚信CA的证书策略、证书实践声明、依赖方协议的HTTP或HTTPS URL。

7.1.9 关键证书策略扩展项的处理规则

不适用。

7.2 证书撤销列表

亚洲诚信CA定期签发CRL，供订户和依赖方查询使用。

7.2.1 版本号

亚洲诚信CA的CRL符合GB/T 20518版本及格式要求。

7.2.2 CRL 和 CRL 条目扩展项

CRL数据定义如下：

- CRL的版本号：用来指定CRL的版本信息，亚洲诚信CA采用的是和证书 X.509 V3 对应的CRL X.509 V2 版本。
- 签名算法：亚洲诚信CA 采用 RSA Signing with（SHA-256或384）或者ECDSA Signing with（SHA-256或384）或者 SM2 Signing with SM3（1.2.156.10197.1.501）签名算法。
- 颁发者：指签发机构的DN名，由国家、机构、单位部门和通用名组成。
- 生效时间：指定一个日期/时间值，用以表明本 CRL 生成的时间。
- 更新时间：指定一个日期/时间值，用以表明下一次 CRL 将要生成的时间(本标准强制使用该域)。
- 撤销证书列表：指定已经撤销的证书列表。本列表中含有证书的序列号和证书被撤销的日期和时间。

7.3 在线证书状态协议

亚洲诚信CA认证系统提供OCSP服务，其符合 GB/T 19713—2025 标准，该标准定义了一种标准的请求和响应信息格式以确认证书状态。

在正常的网络状态下，亚洲诚信CA可确保有足够的资源使CRL和OCSP服务在合理的时间内向用户反馈查询结果。

8. 认证机构审计和其他评估

8.1 审计评估制度

亚洲诚信CA制定了审计评估制度，制度内容包括但不限于：

- 审计评估的类型，至少包括认证业务审计和全面符合性评估；
- 执行审计评估的频率，或是引发评估事件的条件；
- 参与执行审计评估人员的专业背景；若由外部机构执行审计，规定对外部机构的要求；
- 审计评估所涵盖的主题和评估的方法。

8.2 认证业务审计

亚洲诚信CA认证业务审计方式包括：

1. 认证业务至少每年进行一次内部审计；
2. 审计内容包括但不限于证书申请、续期、密钥变更、更新、撤销、冻结等业务中订户告知、身份查验、意愿记录、协议签署、资料保存的合规性；
3. 审计采用抽样审计方式，抽样率不低于该审计周期内所签发证书数量的 1%，且抽样数量至少为 1 份，两者以较大者为准；
4. 对于审计发现的问题，通知相关部门和人员及时整改，并跟踪整改落实情况。

8.3 全面符合性评估

亚洲诚信CA符合性评估方式，包括：

a. 评估周期不少于每年一次；
b. 评估内容包括但不限于：年度电子认证服务开展情况、电子认证服务许可条件符合性情况以及认证规则和证书策略符合性情况等；
c. 审计采用抽样方式的，抽样率不低于本CPS第8.2章 的要求；
d. 对于审计发现的问题，通知被审计部门及时整改，并跟踪整改落实情况；
e. 在每年主管部门要求的时间前将上一年度符合性评估报告报送主管部门。

9. 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

亚洲诚信CA开展了服务成本核算，制定价格策略，各项服务收费包括但不限于：

1. 证书颁发或更新费用；
2. 证书查询费用；
3. 撤销证书的费用；
4. 状态信息访问费用；
5. 电子签名的费用；
6. 签名验证的费用；
7. 签名验证报告的费用；
8. 其他服务的费用。

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。 收费或退款信息可通过线下营业处、官网线上或应用系统内等渠道获取。

9.1.2 证书查询费用

在证书有效期内，亚洲诚信CA不对证书查询收取专门的费用。如果用户提出特殊需求，可能需要支付额外的费用，将由亚洲诚信CA与用户协商收取。

9.1.3 证书撤销或状态信息的查询费用

暂不对此项服务收费，但保留对此项服务收费的权利。

9.1.4 其他服务费用

如果亚洲诚信CA向订户提供证书存储介质及相关服务，亚洲诚信CA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CA将要或者可能提供的服务的费用，亚洲诚信CA将会及时告知用户。

9.1.5 退款策略

如果由于亚洲诚信CA的原因，造成订户合同无法履行、订户证书无法使用，亚洲诚信CA会将相关费用返还给订户。如非亚洲诚信CA原因，订户需要退款，以订户协议为准。

9.2 财务责任

9.2.1 保险范围

亚洲诚信CA根据业务发展情况决定其投保策略。如果由于亚洲诚信CA的原因造成用户在使用证书过程中遭受损失，亚洲诚信CA将向证书订户提供赔偿，具体情形参见本 CPS 第 9.9 章节。

9.2.2 其他资产

无规定。

9.2.3 对最终实体的保险或担保

亚洲诚信CA 通过购买保险来做赔付保障，保险额度不低于上一年营业收入1.5%。

9.3 业务信息保密

9.3.1 保密信息范围

在亚洲诚信CA提供的电子认证服务中，以下信息视为保密信息:

- 亚洲诚信CA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CA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CA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 CPS 的规定妥善保管，如因订户自己泄露私钥造成的损失，订户应自行承担。

9.3.2 不属于保密的信息

亚洲诚信CA将以下信息视为不保密信息:

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

9.3.3 保护保密信息的责任

亚洲诚信CA有妥善保管与保护本 CPS 第 9.3.1 中规定的保密信息的责任与义务。

9.4 个人隐私保护

9.4.1 隐私保护方案

亚洲诚信CA参照GB/T 35273规定实施保护个人隐私信息。

9.4.2 作为隐私处理的信息

亚洲诚信CA将有关证书或CRL内容中未公开提供的所有个人信息视为私人信息。亚洲诚信CA将采取适当的步骤保护证书订户的个人隐私，并将采取可靠的安全手段保护已存储的个人隐私信息。

9.4.3 不被视为隐私的信息

私人信息不包括证书，CRL或证书中已经公开的信息。

9.4.4 保护隐私的责任

亚洲诚信CA有妥善保管与保护本节 9.4.2 中规定的证书申请者个人隐私的责任与义务。

9.4.5 使用隐私信息的告知与同意

亚洲诚信CA依照GB/T 35273-2020等标准处理用户信息。在认证业务范围内使用已获得的订户信息时，若使用目的未超出收集时告知并同意的范围，无需就每次具体使用行为另行告知或重复征得同意。超出上述范围使用时，将另行告知订户并征得其同意，法律法规另有规定的除外。

9.4.6 依法律或行政程序的信息披露

亚洲诚信CA保证不会将订户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），法律法规另有规定或订户另行同意的除外。

9.4.7 其他信息披露情形

如果证书订户要求亚洲诚信CA提供某类特定客户支援服务，如资料邮寄，亚洲诚信CA则需要把证书订户的姓名和邮寄地址等信息提供第三者，如邮寄公司。

9.5 知识产权

- 亚洲诚信CA享有并保留对证书以及亚洲诚信CA提供的所有软件的全部知识产权。
- 亚洲诚信CA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CA有权决定采用何种软件系统。
- 亚洲诚信CA网站上公布的一切信息均为亚洲诚信CA财产，未经亚洲诚信CA书面允许，他人不能转载用于商业行为。
- 亚洲诚信CA发行的证书和CRL均为受亚洲诚信CA支配的财产。
- 对外运营管理策略和规范为亚洲诚信CA财产。
- 用来表示目录中亚洲诚信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，均为亚洲诚信CA的财产。

9.6 陈述和担保

9.6.1 电子认证服务机构的陈述和担保

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

亚洲诚信CA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。

9.6.2 注册机构的陈述和担保

作为亚洲诚信CA的注册机构，应遵照亚洲诚信CA的CPS，承担电子认证业务中注册机构的应尽的责任和义务。

9.6.3 订户的陈述和担保

订户一旦接受亚洲诚信CA签发的证书，就被视为向亚洲诚信CA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CA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CA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，订户就应当承当如下责任：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CA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 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。

9.6.4 依赖方的陈述和担保

依赖方声明和承诺：

- 遵守本 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CA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CA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。

9.6.5 其他参与者的陈述和担保

从事电子认证活动的其他参与者须承诺遵守本 CPS 的所有规定。

9.7 担保免责

除本 CPS 第9.6.1 中的明确承诺外，亚洲诚信CA不承担其他任何形式的保证和义务：

- 不保证证书订户、依赖方、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。
- 不对由于不可抗力，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 CPS承诺时，或依赖方违反承诺时，得以免除亚洲诚信CA之责任。
- 因亚洲诚信CA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CA的设备或网络故障。
- 亚洲诚信CA已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.8 偿付责任规则

亚洲诚信CA制定了偿付责任机制，证书订户因亚洲诚信CA提供的电子认证服务从事民事活动遭受损失，亚洲诚信CA将承担不超过本 CPS 第 9.9 节规定的有限赔偿责任。

9.9 赔偿

亚洲诚信CA为因其提供的电子认证服务过错而遭受损失的订户或依赖方建立赔偿机制。赔偿的申请、审核、审批及支付流程规定如下：

1.赔偿申请

申请条件：当订户或依赖方认为因本 CA 的过错导致其遭受经济损失时，应在发现损失之日起30个工作日内向本 CA 提交书面赔偿申请。

提交材料：申请人需提供身份证明、受损证书信息、损失详情说明及相关证据材料（如交易记录、损失鉴定报告等）。

2.赔偿审核

审核流程：本CA（如客户服务部或合规部）在收到完整申请材料后，将对事件进行内部调查，核实事故原因是否属于 CA 责任范围，并评估损失金额。

审核时限：本 CA 将在收到申请后的10 个工作日内完成初步审核并向申请人反馈审核意见。

3.赔偿审批

审批流程：审核通过后的赔偿建议需报送（如安全策略委员会或高级管理层）进行最终审批。

审批时限：审批流程应在审核完成后5个工作日内完成，并由本CA出具书面赔偿处理决定。

4.赔偿支付

支付方式：审批通过且双方签署赔偿协议后，本CA将通过银行转账等方式支付赔偿金。

支付流程与时限：赔偿金将在协议签署后的15个工作日内完成支付流程。

9.10 有效期限和终止

9.10.1 有效期限

本CPS的任何修订在发布到亚洲诚信CA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CA终止业务时一直有效。

9.10.2 终止

亚洲诚信CA 终止电子认证服务时，本CPS 终止。

9.10.3 效力的终止和保留

本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 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 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，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。

9.11 对参与者的个别通告与沟通

亚洲诚信CA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、站内通知等方式，个别通知订户、依赖方。

9.12 修订和发布

9.12.1 修订程序

经亚洲诚信CA安全策略委员会授权，编写小组至少每年审查一次本 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，符合 CPS 的要求，并符合认证业务开展的实际需要。

本CPS的修改和更新的具体程序同本CPS 1.6.2。

9.12.2 通知机制和期限

修订后的 CPS 经批准后将立即在亚洲诚信CA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CA将在合理的时间内通知有关各方，合理的时间应保证有关方受到的影响最小。

9.12.3 必须修改业务规则的情形

当本 CPS 描述的规则、流程和相关技术已经不能满足电子认证业务要求，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。

9.13 争议处理与举证

9.13.1 争议解决机制

亚洲诚信CA负责受理与本CPS实施、电子认证服务质量以及证书使用过程中产生的相关争议。争议发生后，各方应首先通过友好协商解决。亚洲诚信CA承诺在收到书面投诉后5个工作日内启动协商程序，协商时限不超过30个工作日。若协商不成，可向行业主管部门或双方认可的第三方调解机构申请调解。若协商或调解均未能解决争议，任何一方可向亚洲诚信CA工商注册所在地人民法院提起诉讼，争议解决适用中华人民共和国法律。

9.13.2 举证制度与能力体系

亚洲诚信CA建立覆盖证书全生存周期的举证体系，确保在争议发生时能提供完整、真实、可靠的证据链。证书签发环节，亚洲诚信CA完整记录并保存订户的身份验证记录、纸质或电子申请材料审查记录、告知记录以及意愿确认记录（如录音录像、电子签名确认等）。签名环节，针对亚洲诚信CA提供的签名服务，系统将记录签名请求验证信息、签名操作日志及相关时间戳记录。验证签名环节：系统将记录验证请求记录、验证结果记录，以及对验证过程中产生的异常情况处理记录。

9.14 管辖法律

亚洲诚信CA 的 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》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《商用密码管理条例》《电子认证服务管理办法》《电子认证服务密码管理办法》等相关法律法规管辖。

9.15 与适用法律的符合性

无论亚洲诚信CA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CA的证书，本 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CA就本 CPS 产生的争议，均适用中华人民共和国法律。

9.16 一般条款

9.16.1 完整协议

CPS、订户协议、依赖方协议及其他补充协议构成电子认证服务各方的完整协议。本 CPS 自发布实施之日起，将替代本 CA 先前所有版本以及同时期的完整协议。

订户协议及依赖方协议中标明对应的CPS版本为当前最新版本。

9.16.2 转让

根据本 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CA事先书面同意的情况下，不能通过任何方式进行转让。

9.16.3 分割性

如果本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CPS的其余部分仍然有效且可执行。本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。

9.16.4 强制执行

若证书订户、依赖方等实体未执行本 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。

9.16.5 不可抗力

亚洲诚信CA不对因战争、瘟疫、火灾、地震和其他天灾等不可抗力的事件所造成本 CPS 规定担保责任的违反、延误或无法履行负责。

9.17 其他条款

亚洲诚信CA 对本 CPS 有最终解释权。