亚洲诚信 CA 证书业务声明

（CPS）V1.2

亚数信息科技（上海）有限公司

历史版本

版本号	更新内容	时间	编辑	审批	备注
V1.1	发布初版	2020/8/25	CPS 编写组	安全策略委员会	
V1.2	• 更新2.2.2，说明CRL的序列号为递增。 • 更新2.4及2.5的编号。 • 更新5.1.1，CA机房的建设实施标准。 • 更新6.2.10，说明CA不得损坏CA私钥的限制。 • 更新 9.14，更新适用的当地法律法规。	2020.10.23	CPS 编写组	安全策略委员会	

目录

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，简称 TrustAsia）成立于 2013 年 4 月，具备 ISO27001 信息安全管理体系认证，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。

亚洲诚信是 TrustAsia 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。

我们将以国际标准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 服务体系/层次架构

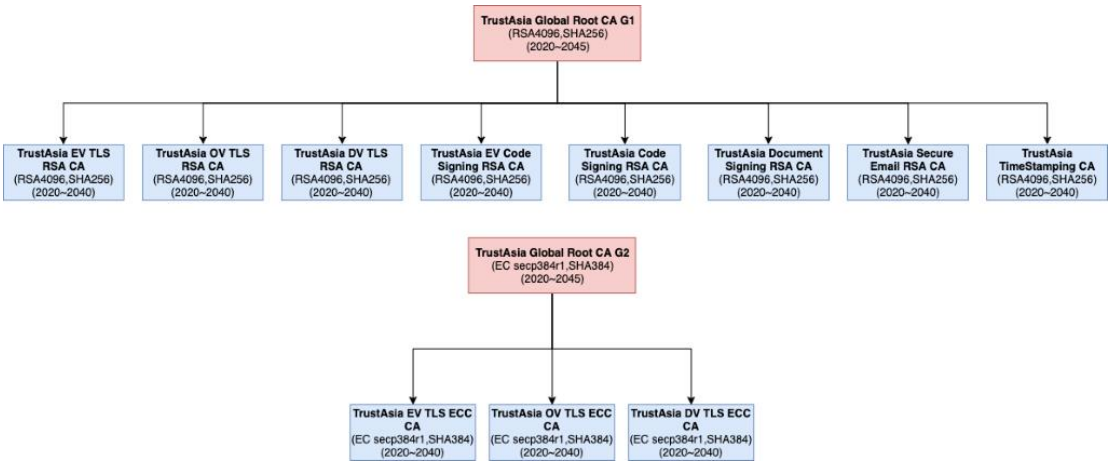
TrustAsia 根据公钥算法不同，下设 RSA 和 ECC 两套 证书链。

TrustAsia Global Root CA G1 为 RSA4096withSHA256 算法的根证书，有效期 25 年。根据实际业务类型下设不同的 RSA 中级证书：

- TrustAsia EV TLS RSA CA ，签发 RSA 增强型 TLS 服务器证书。
- TrustAsia OV TLS RSA CA，签发 RSA 企业型 TLS 服务器证书。
- TrustAsia DV TLS RSA CA，签发 RSA 域名型 TLS 服务器证书。
- TrustAsia EV Code Signing RSA CA ，签发 RSA 增强型代码签名证书。
- TrustAsia Code Signing RSA CA，签发 RSA 代码签名证书。
- TrustAsia Document Signing RSA CA，签发 RSA 文档签名证书。
- TrustAsia Secure Email RSA CA，签发 RSA 安全邮件证书。
- TrustAsia TimeStamping CA，签发 RSA 时间戳证书

TrustAsia Global Root CA G2 为 ECDSA(P-384)withSHA384 算法的根证书，有效期 25 年根据实际业务类型下设不同的 ECDSA 中级证书：

- TrustAsia EV TLS ECC CA ，签发 ECC 增强型 TLS 服务器证书。
- TrustAsia OV TLS ECC CA，签发 ECC 企业型 TLS 服务器证书。
- TrustAsia DV TLS ECC CA，签发 ECC 域名型 TLS 服务器证书。



TrustAsia 证书体系结构

1.1.3 电子认证业务规则（CPS）与证书策略的关系（CP）

本《电子认证业务规则》(简称 CPS) 的总体结构符合工业和信息化部所发布 的《电子认证业务规则规范(试行)》，并严格遵循《中华人民共和国电子签名法》、《电子认证服务管理办法》和《电子认证服务密码管理办法》等法律法规的规定，工业与信息产业部及密码管理局的要求，以及 RFC3647 的框架进行编写。

本 CPS 阐明了亚洲诚信如何开展电子认证业务，包括申请、批准、签发、管理、撤销和更新证书的业务方式和过程，以及相应的服务、法律和技术上的措施和保障，以供电子认证活动参与方了解并遵循。

本 CPS 所阐述的内容遵循亚洲诚信证书策略（简称 CP）、CA/Browser Forum（简称 CA/B Forum）发布的最新版本 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates（简称 BR）、Guidelines for the Issuance and Management of Extended Validation Certificates（简称 EV Guidelines）、《Network and Certificate System Security

Requirements》（简称 NCSSR）进行签发和管理公共可信任 SSL 数字证书，定期查看其更新情况，并将持续根据其发布的版本进行修订 CPS，如果本 CPS 与 CA/B Forum 发布的相关标准规范中的条款有不一致的地方，则以 CA/B Forum 正式发布的规范为准。

1.2 文档名称与标识

对象	OID
域名型 SSL/TLS 证书策略标识	2.23.140.1.2.1 1.3.6.1.4.1.44494.2.1.3
企业型 SSL/TLS 证书策略标识	2.23.140.1.2.2 1.3.6.1.4.1.44494.2.1.2
增强型 SSL/TLS 证书策略标识	2.23.140.1.1 1.3.6.1.4.1.44494.2.1.1
企业型代码签名证书策略标识	1.3.6.1.4.1.44494.2.2.1
增强型代码签名证书策略标识	1.3.6.1.4.1.44494.2.2.2
Adobe 文档签名证书策略标识	1.3.6.1.4.1.44494.2.3.1
Class 1 安全邮件证书策略标识	1.3.6.1.4.1.44494.2.4.1
Class 2 安全邮件证书策略标识	1.3.6.1.4.1.44494.2.4.2
时间戳证书策略标识	1.3.6.1.4.1.44494.2.5.1

1.3 电子认证活动参与者

1.3.1 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。

亚洲诚信作为多个 CA 的运营商，亚洲诚信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。有关亚洲诚信产品和服务的一般信息，请访问 www.trustasia.com。

1.3.2 注册机构

注册机构(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，批准订户的证书更新请求。

亚洲诚信除了承担 CA 的角色外，将自行担任 RA，不再另行设立 RA。

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、或设备。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。

订户并不总是证书中标识的一方，例如证书签发给组织的员工时。证书主题是证书中指定的一方。如本文所使用的，订户可以指证书的主题以及与亚洲诚信签订证书签发合同的实体。在验证身份和签发证书前，订户是申请人。在电子签名应用中，电子签名人、证书持有人即订户。

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

其他参与者是指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 证书应用

1.4.1 正式证书和测试证书

亚洲诚信认证系统 可以提供正式证书和测试证书。

正式证书由亚洲诚信正式认证系统签发，必须按照 CPS 中的规定做严格的身份鉴别。

测试证书由亚洲诚信测试认证系统签发，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 颁发证书签发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，具有不同的保护级别，下表描述了每种证书的适用场景。

证书类型	适用场景
增强型 SSL/TLS 服务端证书	对域名和企业信息做更严格的审核，适用于涉及交易及敏感信息或数据泄露后果严重的场景
企业型 SSL/TLS 服务端证书	对域名和企业信息做真实性审核，适用于涉及隐私信息及重要数据或存在欺诈风险的场景
域名型 SSL/TLS 服务端证书	只对域名做审核，用于实现 HTTPS 数据加密传输，适用于不涉及交易或隐私信息的低风险站点
增强型代码签名证书	以硬件为载体，用户标识软件或代码的发布者，支持 Windows10 内核驱动签名，具有更高的验证级别。
企业型代码签名证书	用户标识软件或代码的发布者，保护软件的完整性
文档签名证书	用于 Adobe 文档签名，可以显示签名这个信息，并验证文档的完整性
安全邮件证书	用于电子邮件的签名和加密，保护电子邮件的安全。

1.4.2 适合的证书应用

根据此 CPS 颁发的证书可以用于所有的身份认证、加密、访问控制和数字签名，由证书中的密钥用法和扩展密钥用法字段指定。

1.4.3 限制的证书应用

亚洲诚信所签发的 SSL 证书在功能上是受到限制的，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。

亚洲诚信所签发的证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用，也禁止在任何违法犯罪活动或法律禁止的相关业务下使用，否则由此造成的法律后果由订户自行承担。 特别声明，证书不设计用于、不打算用于、也不授权用于危险环境中的控制设备，或用于要求防失败的场合，如核设备的操作、航天飞机的导航或通讯系统、空中交通控制系统或武器控制系统中，因为它的任何故障都可能导致死亡、人员伤害或严重的环境破坏。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的管理机构是亚洲诚信安全策略委员会，该委员会负责制定、批准、发布、实施、更新、废止本 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、客户服务和人才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。

1.5.2 联系人

1.5.2.1 CPS 联系人

亚洲诚信将对 CPS 实施严格的版本控制，并指定专门的部门负责相关事宜。任何有关 CPS 的问题、建议、疑问等，可以通过以下方式进行联系。

联系部门：策略部门

联系信箱：cps@trustasia.com

联系地址：中华人民共和国上海市徐汇区桂平路 391 号 B 座 32 楼（200233）

电话号码：0086-021-58895880

传真号码：0086-021-51861130

官方网站：https://www.trustasia.com

1.5.2.2 证书撤销联系人

证书问题报告及证书撤销请求须通过以下方式之一提交，且证书撤销请求必须以书面形式提交:

- 邮件：revoke@trustasia.com
- 致电：400-880-8600（国内）or 86-21-58895880（国际）

1.5.3 决定 CPS 符合策略的机构

亚洲诚信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 CP 的最高权威机构。

1.5.4 CPS批准程序

本 CPS 由亚洲诚信安全策略委会组织 CPS 编写组编制，该小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，正式在亚洲诚信官方网站上发布。

本 CPS 根据国家的政策法规、技术要求、业务发展情况以及 CA/B Forum 发布的 BR 和 EV Guideline 的最新要求每年修订，由 CPS 编写组根据相关的情况拟定 CPS 修订内容，审查修订内容与 CP 的一致性后，提交安全策略委员会审核，经该委员会批准后，递增版本号、更新发布时间、生效时间及修订记录，并正式在亚洲诚信官网上发布。

1.6 定义和缩写

1.6.1 术语定义一览表

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。
注册机构(RA)	负责处理证书申请者和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 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	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	依赖于策略的信息，可能与 CP 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。
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	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。
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。
WebTrust	CPA 加拿大针对认证服务机构的 WebTrust 项目的当前版本。
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。

1.6.2 缩略语及其含义一览表

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	证书撤消列表
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

2信息发布与信息管理

2.1 信息库

亚洲诚信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：CP、CPS、订户协议、依

赖方协议、根证书、中级 CA 证书和以及其它由 亚洲诚信 在必要时发布的信息。

2.2 认证信息的发布

2.2.1 信息库发布

亚洲诚信信息库将及时在官方网站 https://www.trustasia.com 发布，或根据需要采取其他可能的形式进行信息发布。发布内容包括证书、CPS 修订和其它资料等，这些内容必须保持与 CPS 和有关法律法规一致。

2.2.2 CRL发布

亚洲诚信通过 HTTP 发布证书撤销列表 （CRL），订户或依赖方可以通过亚洲诚信签发的证书中 CRL 分发点地址获取 CRL。亚洲诚信发布的每个 CRL 包含一个递增的序列号。

2.2.3 OCSP发布

亚洲诚信提供在线证书状态查询服务（OCSP），订户或依赖方可实时查询证书的状态信息。

2.3 发布的时间和频率

2.3.1 CP和CPS发布时间和频率

亚洲诚信的 CP 和 CPS 可通过信息库 7d*24h 获得。至少每年发布一次 CP 和 CPS。

亚洲诚信会定期跟进 CA/B Forum BR 标准的变化，并及时调整 CP/CPS 来符合 BR 标准的变化。

2.3.2 CRL 发布时间和频率

亚洲诚信对于订户证书的 CRL 至少 7 天发布一次；对于子 CA 证书的 CRL 至少 12 个月发布一次，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。

2.3.3 OCSP 发布时间和频率

亚洲诚信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。

对于订户证书的 OCSP 响应数据至少 4 天更新一次，且最长有效期不超过 10 天。

对于中级 CA 证书的 OCSP 响应数据至少 12 个月更新一次，若 CA 证书被吊销则会在 24 小时内更新。

在紧急的情况下，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，这种发布应该是即时的、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。

2.5 高风险信息库

亚洲诚信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(包括 EV 证书)，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，亚洲诚信将申请机构与高风险机构名单进行比对，自动在申请阶段将其标记为“高风险申请者”，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) 参考国际反钓鱼工作组(APWG)及中国反钓鱼联盟(APAC)公布的钓鱼目标名单;

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

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

亚洲诚信签发的数字证书符合 X.509 标准，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。亚洲诚信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。对于 SSL/TLS 服务器证书，所有的域名或 IP 地址都添加到主题别名中，而通用名为主域名或 IP 地址，必须是一个出现在主题别名中的域名或 IP 地址。

在 TLS/SSL 证书的 subjectAltName 扩展名或 subject：commonName 字段中，不能包含保留私有 IP 地址或内部名称。在证书的 dNSName 条目中，不能带有下划线（_）字符。

在 DV 及 EV TLS/SSL 证书的 subjectAltName 扩展名中不能包含 IP 地址。

亚洲诚信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
省(S)	证书签发者所在省份，或者不用
地区(L)	证书签发者所在城市，或者不用
机构(O)	TrustAsia Technologies, Inc.
机构部门(OU)	亚洲诚信可能依据用户类型、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)	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
电子邮件(E)	订户的电子邮件地址，或不用
通用名(CN)	域名(SSL/TLS 证书)，或机构名(机构类型证书)，或个人姓名(个人类型证书)，或其他可识别的名称

3.1.2 对名称意义化的要求

亚洲诚信使用 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。

订户证书所包含的名称具有一定的代表性意义，其中包含的主体识别名称，应当能够明确确定证书持有机构以及所要标识的网络主机服务器、或互联网域名，并且可以被依赖方识别。主体甄别名称应当符合法律法规等相关规定的要求。

3.1.3 订户的匿名或伪名

本 CPS 所述证书的订户在进行证书申请时不能使用匿名或者伪名。

3.1.4 不同名称形式的规则

亚洲诚信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定义。

3.1.5 名称的唯一性

在亚洲诚信信任域内，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，亚洲诚信可以用其唯一的主体甄别名为其签发多张证书。当证书申请中出现不同订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

证书中每一个主题名称的唯一性规定如下：

SSL/TLS 服务器证书	域名的唯一性由互联网名称与数字地址分配机构(ICANN)控制。
客户端证书	要求唯一的电子邮件地址或组织名称与唯一的序列号相组合或关联。
代码签名证书（包含文档签名证书）	要求唯一的组织名称和地址或唯一的组织名称与唯一的序列号相组合或关联。
时间戳证书	要求唯一的散列和时间或唯一的序列号分配给时间戳。

3.1.6 商标的识别、鉴别和角色

亚洲诚信签发的证书的主体甄别名中不包含商标名。

3.2 初始身份确认

3.2.1 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，其证明方法可以是提交经过数字签名的 PKCS#10 格式证书签名请求(CSR)或其他与此相当的密钥标识方法，或亚洲诚信批准的其他方法。

3.2.2 申请者身份的鉴别

亚洲诚信需要对证书申请者的身份进行程序性的鉴别，包括但不限于以下几种方式：

1. 验证订户提供的身份证明材料；
2. 通过与订户所在辖区能证明其合法成立、存续或承认的政府机构确认；
3. 通过定期更新且被认为可信的第三方数据库确认；
4. 通过亚洲诚信或者亚洲诚信委托的第三方调查；

5. 通过证明函件来确认（例：律师信、会计师信等）；
6. 通过订户提供的物业账单、银行对账单、信用卡账单、政府签发的税单等亚洲诚信认可的验证方式来验证。

亚洲诚信首先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。亚洲诚信会按照本 CPS 之规定，对材料进行鉴别。亚洲诚信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的身份鉴别要求，那么就被视作放弃对证书的申请。

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

3.2.2.1 所在国的验证

若证书主题项包含国家字段，亚洲诚信将通过 3.2.2 中申请者提供的机构证明信息进行所在国家的确认。

3.2.2.2 机构商业名称的验证

若证书主题中包含 DBA 或商业名称，亚洲诚信可以至少使用以下一项方法去验证申请者有权使用 DBA 或商业名称：

1. 申请者所在辖区的政府机构提供的可证明其合法成立、存在或认可的文档，或与该政府机构沟通；
2. 可靠的数据来源；
3. 与负责管理此类 DBA 名称或商业名称的政府机构沟通；
4. 附带支持证明文件的证明函件；
5. 物业账单、银行对账单、信用卡对账单、政府签发的税单或其他亚洲诚信认为可靠的验证方式。

3.2.2.3 组织机构身份的鉴别

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。

对于包含组织身份信息的所有证书，亚洲诚信应验证组织的名称和注册或经营地址，亚洲诚信可根据组织所申请的证书类别的不同，执行不同的身份鉴别方式，一般而言，证书类别越高，安全级别越高，鉴别方式越严格，鉴别内容越全面。亚洲诚信可以选择以下一项或多项来验证组织的身份和地址信息：

1. 通过政府机构签发的有效文件（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）或通过签发有效文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。
2. 通过可信的第三方数据库获取组织的地址及联系方式，以电话、电子邮件、邮政信函等方式与组织进行联络，以确认申请者所提供的信息的真实性。
3. 通过有执业资格的律师、会计师等出具的证明函件来验证信息。
4. 通过物业账单、银行对账单、政府签发的税单或其他亚洲诚信认可的验证方式来确认组织的地址信息。
5. 委托第三方对组织进行调查，或要求申请者提供额外的信息及证明材料。

此外，必要时，亚洲诚信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。对于被识别为“高风险”的证书请求，亚洲诚信可直接予以拒绝。

3.2.3 个人身份的鉴别

如果申请者的身份是自然人，亚洲诚信将会审核其姓名、地址以及证书申请的真实性等相关必要信息。对于个人身份证书，亚洲诚信会根据个人所申请的证书类别的不同，执行不同的身份鉴别方式，一般而言，证书类别越高，安全等级越高，鉴别方式越严格，鉴别内容越全面。
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。

亚洲诚信通过以下一种或多种方式来鉴别和验证：

1. 采用发送相关校验码电子邮件或通过电话、手机短信等其他可靠的方式来鉴别和验证申请者证书请求的真实性。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；
2. 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；
3. 通过物业费账单、银行卡对账单或信用卡账单等核实申请者的地址或直接依赖政府签发的身份证明文件来确认地址。
4. 当申请信息包含组织信息时，可要求申请者提交任职证明文件、或查询第三方数据库、或发送确认电子邮件等方式来确认该组织是否存在，以及申请者是否是该组织成员。

此外，必要时，亚洲诚信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。对于被识别为“高风险”的证书请求，亚洲诚信可直接予以拒绝。

3.2.4 域名的确认和鉴别

用户在申请 SSL 证书时，亚洲诚信需要验证申请者对所申请证书中域名的控制权。对域名所有权的验证遵循 CA/B Forum BR 3.2.2.4 章节中原则：

1. 域名所在根域必须为 IANA 公布的合法根域。
2. 域名格式必须遵循 FQDN 标准，或 有且仅有一个 *. 位于 FQDN 最左侧的 通配符域名。
3. 域名控制权可以使用以下任意一种方式进行验证：

   a. 域名管理邮箱

      亚洲诚信将通过发送验证邮件到一下任意邮箱进行域名控制权验证：

      - 待验证域名的 whois 联系人邮箱 ，或一下默认管理员邮箱
      - Administrator@*待验证域名*
      - Admin@*待验证域名*
      - Postmaster@*待验证域名*
      - Hostmaster@*待验证名*
      - Webmaster@*待验证域名*

      订户接收到验证邮件后，进入域名验证链接,点击批准后即可完成域名所有权验证。

   b. DNS 验证码

      订户通过为待验证域名解析指定的带随机值的 TXT 或 CNAME 记录，亚洲诚信能够查询到指定记录 即可完成域名所有权验证。

   c. HTTP/HTTPS 验证码

      订户通过在待验证域名站点指定目录 /.well-known/pki-validation/ 下 放置指定的验证文件和随机验证值。

      亚洲诚信通过 HTTP/HTTPS 协议的默认端口能够成功访问到指定的验证内容 即可完成域名所有权验证。

4. 不支持最右端为.onion 的域名的验证，且不提供该证书的签发。
5. EV CS 证书不包含域名，不对域名进行审核验证。

3.2.5 IP 地址的确认和鉴别

亚洲诚信接受订户使用 公有 IP 申请 SSL 证书，公有 IP 不签发 域名和增强型证书。对 IP 使用权验证遵循 CA/B Forum BR 3.2.2.5 章节中的原则：

亚洲诚信通过以下任一方式进行 IP 使用权验证：

1. IP 注册主体信息与证书申请者主体信息一致。
2. IP 注册主体 为 证书申请者主体开具 IP 使用授权证明。
3. HTTP/HTTPS 验证码

   订户通过在待验证 IP 站点指定目录 /.well-known/pki-validation/ 下 放置指定的验证文件和随机验证值。

   亚洲诚信通过 HTTP/HTTPS 协议的默认端口能够成功访问到指定的验证内容 即可完成域名所有权验证。

3.2.6 认证机构授权记录

亚洲诚信遵循 CA/B Forum BR 3.2.2.8 规定，在证书签发前，对 SSL 证书申请中的所有 主题名称和备用名称中的域名进行 DNS CAA 记录检查。

CAA 查询若出现以下任一情况，亚洲诚信将拒绝为其签发证书：

1. CAA 响应数据中有 CAA 记录 ，但 issue, issuewild 不包含 trustasia.com
2. CAA 响应数据有 DNSSEC 签名，但签名验证失败。

3.2.7 电子邮件的审核

当邮件地址被作为证书主题内容申请证书时，亚洲诚信会对该邮件地址的有效性进行确认，并审核申请者对邮件地址的使用权，只有通过审核后才可在证书中签入 Email 项。具体的审核步骤如下：

1. 申请者完成生成证书申请请求文件后，系统检测到邮件地址则自动向该邮件地址发送随机值，随机值由系统产生，并且唯一；

2．申请者收到邮件并通过带随机值的链接进行批准操作；

3．亚洲诚信 CA 系统收到用户批准后，比对批准中的随机值与发送的随机值，若结果一致，则电子邮件审核通过。

在收件人及邮件整体内容不作任何改变的前提下，带有原随机值的邮件可被重复发送。邮件中随机值自生成当天开始，有效期不应超过 30 天。

3.2.8 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。

3.2.9 没有验证的订户信息

通常，除了该类型证书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。

3.2.10 授权确认

当机构订户授权申请代表人办理证书业务时，亚洲诚信会使用章节 3.2.3 中所列的来源去获取可靠的通讯方式，以此验证申请代表人申请证书的真实性。亚洲诚信可以直接与申请代表人确定证书申请的真实性，也可以与申请者组织内拥有权威的部门进行确认，例如申请者主要业务办公室，公司办公室，人力资源办公室，信息技术办公室或者亚洲诚信认为合适的其他部门。

亚洲诚信也可以允许申请代表人提供授权信、雇佣证明或任何同等方式来验证其属于上述机构以及其代表行为被该机构授权。

此外，亚洲诚信允许申请者指定独立个人来申请证书。若申请者以书面形式指定了可以进行证书申请的独立个人，则亚洲诚信不接受任何超出该授权的证书请求。在收到申请者已核实的书面请求时，亚洲诚信应向申请者提供其已授权人员的清单。

3.2.11 互操作准则

对于其他的电子认证服务机构，可以与亚洲诚信进行互操作，但是该电子认证服务机构的 CPS 必须符合亚洲诚信 CP 要求，并且与亚洲诚信签署相应的协议。

如果国家法律法规对此有规定，亚洲诚信将严格予以执行。

截至目前，亚洲诚信未签发任何交叉证书。

3.3 密钥更新请求的标识与鉴别

在证书到期之前，订户可以请求更新密钥。在收到更新密钥的请求后，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。

3.3.1 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请求，订户可以选择生成一个新的密钥对来替换正在使用的密钥对或即将到期的密钥对。

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，订户申请更新证书密钥的操作。

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） 订户需要获取多种算法的证书（RSA、ECC）；

4） 订户需要增加域名（仅限于多域名 SSL/TLS 服务器证书）；

5） 其他经亚洲诚信认可的原因。

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。若订户已验证的证书注册信息在 CA/B Forum BR 规定验证有效期内，亚洲诚信将基于其原有的信息对其重新签发证书。若已验证的证书注册信息距离初次验证已超过 CA/B Forum BR 规定验证有效期，则需对订户身份进行重新验证，验证流程及要求与初次申请相同。补发证书的有效期与原证书有效期一致。

2. 证书换发

换发是指在证书将要过期的 30 日（含）内，订户申请更新密钥的操作。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。若订户已验证的证书注册信息在 CA/B Forum BR 规定验证有效期内，亚洲诚信将基于其原有的信息对其重新签发证书。若已验证的证书注册信息距离初次验证已超过 CA/B Forum BR 规定验证有效期，则需对订户身份进行重新验证，验证流程及要求与初次申请相同。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。

3.3.2 撤销后密钥更新的标识与鉴别

亚洲诚信不提供证书被撤销后的密钥更新。

3.4 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 CPS 4.9.1.1 所述理由需要撤销订户的证书时，有权发起撤销订户证书。

订户通过一定的方式，如邮件、传真、电话等，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。

3.5 授权服务机构的标识与鉴别

亚洲诚信自行担任证书 RA，不再另行设立 RA。

4 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

申请者或被授权代表申请者申请证书的个人可以提交证书申请。申请者对其或被授权代表人向亚洲诚信提供的任何数据负责。

EV 证书申请必须由授权证书申请者提交并经证书批准人批准。证书申请必须附有合同签名人签署的（书面或电子）订户协议。

4.1.2 注册过程和责任

1. 注册过程包括：
   - 提交证书申请；
   - 生成密钥对；
   - 向亚洲诚信提供密钥对的公钥；
   - 同意适用的订户协议；
   - 支付任何适用的费用。
2. 责任：
   - 申请者应事先了解订户协议、CP 及本 CPS 等文件约定的事项，特别是其中关于证书适用范围、权利、义务和担保的相关内容。
   - 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。
   - 注册机构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。

4.2 证书申请处理

4.2.1 执行身份识别与鉴别

当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 CPS 第 3.2 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 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亚洲诚信 WEB 界面或者 API 直接提供的所有信息一起安全存储。

亚洲诚信会根据以往因被怀疑或鉴别为网络钓鱼或具有其他诈骗用途而被拒绝证书请求或撤销的证书，建立和维护 SSL 证书高风险数据库列表，在接受证书申请时将会查询该列表信息。对于列表中出现的订户，亚洲诚信有权拒绝证书请请求或执行额外的验证。

亚洲诚信会对待签发证书主题别名扩展项中的每一个 DNSName 做 CAA 记录检查，并按照 3.2.2.7 中的检查方法和结果判定是否批准该证书申请。

如果部分或所有的身份验证资料内容使用的语言不是亚洲诚信官方语言，那么亚洲诚信将会使用经过适当培训、具备足够的经验和判断能力的人员完成最终的交叉审核和尽职调查。

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接受、拒绝申请或要求申请者补充递交相关材料。

在鉴证 OV 与 EV 型证书中的信息时，若亚洲诚信根据本 CPS 第 3.2 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。

4.2.2 证书申请批准和拒绝

4.2.2.1 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 CPS 第 3.2 章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。

4.2.2.2 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) 该申请不符合本 CPS 第 3.2 章节关于订户身份识别和鉴别的规定；
2) 订户不能根据要求提供所需的身份证明材料；
3) 订户反对或者不能接受订户协议的有关内容和要求；
4) 订户没有或者不能够按照规定支付相应的费用；
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，亚洲诚信将会邮件通知订户证书申请失败。

4.2.2.3 处理证书申请的时间

在正常情况下，亚洲诚信会在合理时间范围内验证订户的信息并签发证书。除非与相关订户另有协议或其他协议中另有说明，否则并不规定完成证书申请的处理时间。

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。

4.3 证书签发

4.3.1 证书签发中 CA 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。

亚洲诚信不直接从其根证书颁发最终实体证书。 在两个或多个证书透明度数据库中记录要在 Chrome 中受信任的 SSL / TLS 服务器证书。

在证书颁发期间发生的数据库和 CA 进程受到保护，以防止未经授权的修改。

对于有效的证书签发请求，CA 证书签发系统发送给订阅服务器。

4.3.2 对订户证书签发的通告

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，亚洲诚信会在申请过程中，通过电子邮件将证书发送到订阅者指定的电子邮件地址。

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

亚洲诚信把证书交付给订户视为证书的发布。亚洲诚信视用户证书使用场景，同时会根据谷歌、苹果的要求，选择将证书发布在多个 CT 日志服务器中。

亚洲诚信遵照本 CPS 中 2.4 和 2.5 章节中关于信息库机制的规定，向订户颁发证书。该信息库只有 CA 被授权的角色人员才能监控并管理该高风险数据库或备用颁发机制，同时，被授予权限的角色人员应维护并管理

其完整性。若保密法等相关法律法规有要求，亚洲诚信将遵照相关要求，在获得订户同意后，再让其证书处于可检索状态。

4.4.3 CA 对其他实体的通告

亚洲诚信将不对其他实体进行通告。其他实体可以通过从目录服务器中查询到已经签发的数字证书。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户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。

订户应按协议规定、法律法规、CPS 的范围内使用密钥对。

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吊销；
4) 证书的用途适用于对应的签名；
5) 使用证书上的公钥验证签名。
6) 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 证书更新

4.6.1 证书更新的情形

对于亚洲诚信签发的订户证书，证书到期前 30 日（含）起可以进行证书更新。订户选择保留原有密钥对重新签发证书,则订户需要保证其密钥对的安全性没有受到威胁。在证书到期前 30 日（含）起，亚洲诚信会通过邮件通知的方式通知订户更新证书。

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，且原证书的验证时效未超过本 CPS 第 4.2.1 章节规定的期限，则亚洲诚信可以参照原证书核实的数据及证明文件来验证更新证书的信息。

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本 CPS 第 4.2.1 章节规定的期限，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。

4.6.2 请求证书更新的实体

请求证书更新的实体为已经申请过亚洲诚信证书的订户或其他授权代表人，且其证书剩余有效期少于 30 日（含）。

4.6.3 证书更新请求的处理

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 CPS 第 3.3.1 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。

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 构成接受更新证书的行为

同本 CPS 第 4.4.1 章节。

4.6.6 电子认证服务机构对更新证书的发布

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

当订户的证书出现下列情形时，订户可选择证书密钥更新服务：

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) 订户需要获取多种算法的证书（RSA、ECC）；
4) 订户需要增加域名（仅限于多域名 SSL/TLS 服务器证书）；
5) 订户证书即将到期且认为更新证书时需要更新密钥。
6) 其他可能导致密钥更新的情形。

4.7.2 请求证书密钥更新的实体

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

4.7.3 证书密钥更新请求的处理

亚洲诚信对证书密钥更新请求的处理通过证书更新请求处理流程完成，参见本 CPS 第 4.6.3 章节的描述。

4.7.4 颁发新证书时对订户的通知

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，证书扩展信息的备用名称发生变更但不更新密钥，而重新签发新的证书。

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，亚洲诚信会对证书信息进行重新验证，若原证书的申请资料可用且未过期（企业型、增强型证书申请资料及验证有效期为 398 天，域名型证书每一次都要验证），则可以参考原资料进行审核验证，若上述资料不可用或已超期，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，审核通过后，亚洲诚信将重新签发新的证书。

4.8.4 签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 证书撤销和挂起

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，或不再符合 Baseline Requirements 第 6.1.5 节及第 6.1.6 节的相关要求；
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、CP/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吊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) 亚洲诚信获悉某通配符证书被用于鉴别具有欺骗误导性的子域名；
9) 亚洲诚信获悉证书中所含信息出现重大变化；
10) 亚洲诚信获悉证书的签发未能符合 Baseline Requirements 要求，或亚洲诚信的 CP 或 CPS；
11) 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；
12) 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；

13) 亚洲诚信依据 Baseline Requirements 签发证书的权力失效，或被撤销或被终止，除非其继续维护 CRL/OCSP 信息库；

14) 亚洲诚信的 CP 或 CPS 要求撤销订户证书；

15) 亚洲诚信被告知出现了可使订户私钥泄露的经验验证的方法，此类方法可根据公钥轻易地计算私钥值（例如 Debian 弱密钥，见：http://wiki.debian.org/SSLkeys），或者有明确的证据证明订户用来生成私钥的方法是有缺陷的；

16) 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；

17) 亚洲诚信已经履行催缴义务后，订户仍未缴纳服务费。

18) 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（例如，CA/浏览器论坛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并由 CA 取代）。

19) CA 获得证据或被告知订户在其签名的软件对象中具有可疑代码。

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，亚洲诚信应在 7 天之内吊销中级 CA 证书：

1) 中级证书颁发机构正式书面申请吊销；

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，或不再符合 Baseline Requirements 第 6.1.5 节及第 6.1.6 节的相关要求；

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 Baseline Requirements 要求，或中级 CA 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) 亚洲诚信依据 Baseline Requirements 签发证书的权力失效，或被吊销或被终止，除非其继续维护 CRL/OCSP 信息库；

9) 本 CP 或相应的 CPS 要求撤销中级 CA 证书。

10) 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（例如，CA /浏览器论坛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、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，防病毒机构或其他的第三方可以提交证书问题报告，告知亚洲诚信有合理理由吊销证书。

涉及恶意软件的事件，亚洲诚信将按照以下方式处理：

•在获悉事件后的 1 个工作日内，与软件发行商联系，并在 72 小时内请求答复。

•在了解到事件的 72 小时内，确定受影响的依赖方的数量。

•如果收到发行商的答复，则 CA 和发布者确定撤销的“合理日期”

•如果未从发行商处收到任何答复，则 CA 会通知发布者，CA 将在 7 天内吊销证书，除非它有书面证据证明这将对公众产生重大影响。

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；
2. 亚洲诚信按本 CPS 第 3.4 章节的规定进行证书撤销请求的鉴别；
3. 亚洲诚信完成撤销工作后应及时将其发布到证书撤销列表；

4. 证书被撤销后，亚洲诚信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，亚洲诚信可以通过网站进行公告被撤销的证书；
5. 亚洲诚信提供 7*24 小时的证书撤销申请服务，订户可通过本 CPS 第 1.5.2 章节中所提供的联系方式申请证书撤销。

4.9.3.2 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 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，亚洲诚信将通过内部流程申请撤销证书；
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，亚洲诚信应组织调查并根据调查结果来决定是否撤销证书；
4. 在证书被撤销后，亚洲诚信将通过适当的方式，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，亚洲诚信可以通过网站进行公告被撤销的证书；
5. 亚洲诚信提供 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 1.5.2 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。

4.9.7 CRL 发布频率

对于订户证书的 CRL 发布周期为 7 天至少发布一次，且有效期不超过 10 天。

对于中级证书的 CRL 发布周期 6 个月至少发布一次，且有效期不超过 12 个月，若对中级证书有吊销行为 CRL 应在 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 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

亚洲诚信为订户证书 提供证书状态在线查询服务，并符合 RFC6960 标准，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

亚洲诚信提供的 OCSP 服务支持 POST 和 GET 两种请求方式。

对于订户证书的 OCSP 响应数据至少 4 天更新一次，且最长有效期不超过 10 天。

对于中级 CA 证书的 OCSP 响应数据至少 12 个月更新一次，若 CA 证书被吊销则会在 24 小时内更新。

亚洲诚信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

若订阅者证书使用场景中的访问流量较高，亚洲诚信可以根据 RFC4366 中的规定，要求订阅者使用 OCSP 装订的方式来访问 OCSP 服务。

4.9.12 密钥损害的特别要求

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

4.9.13 证书挂起的情形

亚洲诚信不支持证书挂起。

4.9.14 请求证书挂起的实体

不适用。

4.9.15 挂起请求的流程

不适用。

4.9.16 挂起的期限限制

不适用。

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，亚洲诚信在该证书到期前，不删除其在 CRL 及 OCSP 中的撤销记录。

4.10.2 服务可用性

证书状态服务全天候提供。亚洲诚信运行并维护其 CRL 和 OCSP 功能，其资源足以在正常工作条件下提供 10 秒或更短的响应时间。

在正常网络条件下，通过模拟电话线可以在不超过 3 秒的时间内下载 EV CS SSL 证书链的 CRL。

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 终止服务

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；
- 证书到期前被吊销。

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

亚洲诚信详细记录吊销证书的操作过程，并定期将订购终止后的证书及相应订户数据进行归档。

4.12 密钥生成、备份与恢复

亚洲诚信不托管任何数字证书订户的私钥，因此也不提供密钥恢复服务。

4.12.1 签名密钥生成、备份与恢复的策略与行为

不适用。

4.12.2 加密密钥的生成、备份与恢复的策略与行为

不适用。

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

亚洲诚信的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）

5.1.1.1 公共区

亚洲诚信场地的入口、配电在该区域，采用访问控制措施，需要使用门禁卡和指纹鉴别才可进入。

5.1.1.2 管理服务区

服务区是 亚洲诚信 操作人员、管理人员的工作区，需要 2 名可信人员同时使用门禁卡和密码鉴别才可以进入，人员进出服务区有日志记录。

5.1.1.3 核心区

核心区是 CA 运营管理区域，此区域必须使用门禁卡和密码鉴别才可以进入。

同时，证书认证系统、加密设备等相关密码物品也存放在该区域，其中 CA 服务器、数据库系统、以及加密设备等相关密码物品位于核心区内的屏蔽机房内。 屏蔽机房必须两名可信人员同时使用门禁卡和密码鉴别才可以进入，确保在屏蔽区内单个人员无法完成敏感操作。

在屏蔽区内有单独的缓冲区，防止在开启屏蔽门时，电磁波泄露发生。

5.1.2 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:

- 采用门禁卡和密码鉴别的控制方式控制每道门的进入；
- 进出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 3 个月，以备查询。

5.1.3 安防监控

视频监控无死角（施行 24 小时监控，视频资料保留 3 个月以上，对于重大事件的视频单独存档 ）；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。

5.1.4 电力与空调

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。

5.1.5 水患防治

亚洲诚信机房高于地面 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。

5.1.6 火灾防护

亚洲诚信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。

5.1.7 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，采取了介质使用登记进行记录介质情况，并防止介质受到意外损坏。

5.1.8 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，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理销毁。

在处理作废内容时，至少 2 名可信人员在场。

5.1.9 异地备份

亚洲诚信对关键数据、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 5.1.7 介质存储的描述。

5.2 程序控制

5.2.1 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:

a. 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;

b. 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;

c. 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;

d. 安全管理人员：负责场地安全、日常安全管理工作;

e. 安全审计人员：负责对业务操作行为进行审计;

f. 人力资源管理人员：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。

可信角色由管理层任命。每年维护和审查被任命为受信任角色的人员名单。

5.2.2 每项任务需要的角色

亚洲诚信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，亚洲诚信还对以下敏感操作实施多个可信角色共同完成，例如:

a. 屏蔽区场地访问：设置为 2 个可信人员进出模式;

b. 鉴别、审核和签发证书：需要 2 个可信人员共同完成;

c. 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;

d. 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 ;

e. CA 系统后台操作：需要 2 个可信人员共同完成;

f. 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：

1. 对于可信人员的物理访问，通过门禁卡和密码识别进行鉴别，并确定相应的权限。
2. 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。
3. 对于系统维护人员，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。

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 亚洲诚信的可信角色由不同的人担任。亚洲诚信进行职责分离的角色，包括但不限于下列角色:

	密钥与密码设备管理员	鉴证和客服员	系统维护员	安全管理员	安全审计员	人力资源管理员
密钥与密码设备管理员	——	NO	NO	NO	YES	NO
鉴证和客服员	NO	——	NO	NO	NO	NO
系统维护员	NO	NO	——	NO	NO	NO
安全管理员	NO	NO	NO	——	NO	NO
安全审计员	YES	NO	NO	NO	——	NO
人力资源管理员	NO	NO	NO	NO	NO	——

5.3 人员控制

5.3.1 资格、经历和无过失要求

亚洲诚信对承担可信角色的工作人员的资格要求如下:

a. 具备良好的社会和工作背景。

b. 遵守国家法律、法规，无违法犯罪记录。

c. 遵守 亚洲诚信 有关安全管理的规范、规定和制度。

d. 具有认真负责的工作态度和良好的从业经历。

e. 具备良好的团队合作精神。

f. 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。.

5.3.2 背景审查程序

亚洲诚信或与有关的政府部门和调查机构合作，完成对可信员工的背景调查。

所有的可信员工和申请调入的可信员工都必须书面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，社会关系和社会安全方面的调查。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。这些培训包括：

- 基本公钥基础设施（PKI）知识；
- CP 和 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；
- 岗位职责统一要求；
- CA /浏览器论坛指南；
- 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组织的培训一次。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

亚洲诚信在职人员的工作岗位轮换周期和顺序将依据本机构的安全管理策略而制定。

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系统操作认证业务等情况时，亚洲诚信一经确认，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

该名人员调理工作岗位、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

亚洲诚信目前未聘用外部独立合约人从事认证相关的工作。

5.3.8 提供给员工的文档

亚洲诚信提供给人员的文档通常包括但不限于以下几类：

- CP 和 CPS 及相关标准与规范；
- 员工手册；
- 岗位职责说明书、工作流程和规范；
- 内部操作文件，包括业务连续性管理和灾难恢复方案；
- 安全管理制度等。

5.4 审计日志程序

5.4.1 记录事件的类型

亚洲诚信支持其 CA 和应用程序的所有基本事件审核功能以记录下列事件。如果亚洲诚信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:

- 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，申请资料的验证、申请及验证资料的保存等；
- 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。

日志记录一般需包含：

- 记录的日期和时间；
- 记录的序列号；
- 做日志记录的实体的身份；
- 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。

5.4.3 审计日志的保存期限

亚洲诚信 CA 应该妥善保存所有电子认证服务的审计日志，在证书失效后至少保存 10 年。

5.4.4 审计日志的保护

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。

5.4.5 审计日志备份程序

亚洲诚信的系统日志实时同步到日志服务器，并且每周备份到异地；手工电子记录备份到 SVN，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

亚洲诚信的审计日志收集系统涉及：

1. 证书管理系统;
2. 证书签发系统;
3. 证书目录系统;
4. 远程通信系统;
5. 证书受理系统;
6. 访问控制系统;
7. 网站、数据库安全管理系统;
8. 其他需要审计的系统。

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 对异常事件的通告

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。

5.4.8 脆弱性评估

亚洲诚信根据审计发现的安全事件，将每年对系统、物理场地、运营管理等方面进行安全脆弱性评估，并根据评估报告采取措施，以降低运营风险。

5.5 记录归档

5.5.1 归档记录的类型

亚洲诚信对以下几类事件进行归档记录，包括但不限于：

1. 证书系统建设和升级文档；
2. 证书和证书撤销列表；
3. 证书申请信息，证书服务批准和拒绝信息；
4. 审计记录；
5. CP 和 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。

5.5.2 归档记录的保存期限

对于不同的归档记录，其保留期限是不同的。对于系统操作事件和系统安全事件记录，其归档应保留到完成安全脆弱性评估或一致性审计。

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. 订户证书数据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 CA 证书和密钥生命周期之外，额外保留 10 年。

5.5.3 归档文件的保护

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。

5.5.4 归档文件的备份程序

对于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；对于手工生成的电子记录，归档以 SVN 服务器进行备份。

对于纸质资料，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

亚洲诚信的所有日志都有时间记录，均由操作人员手工记录或系统自动添加。

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，且每周异地备份。

对于手工生成的电子记录，由 SVN 服务器（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。

5.6 电子认证服务机构根证书有效期限

亚洲诚信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。

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，替换已经过期的 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。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

为了及时响应和处理事故和损害发生的情况，亚洲诚信建立了一系列应急处理预案和事故处理方案，例如:

- 系统故障处理规范
- 网络故障处理规范
- 硬件故障处理规范
- 系统备份与恢复方案
- 密钥应急方案

5.7.2 计算资源、软件和/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，亚洲诚信将按照灾难恢复计划实施恢复。

5.7.3 私钥损害处理程序

1. 当证书订户发现证书私钥损害时，订户必须立即停止使用其私钥，并立即访问亚洲诚信证书服务站点吊销其证书，或立即通过电话邮件等方式通知亚洲诚信吊销其证书，并按照相关流程重新申请新的证书。亚洲诚信将按本 CPS 第 4.9 节发布证书吊销信息。
2. 当亚洲诚信证书订户的证书私钥受到损害时，亚洲诚信将立即吊销证书，通知证书订户;订户必须立即停止使用其私钥，并按照相关流程重新申请新的证书。亚洲诚信将按本 CPS 第 4.9 节发布证书吊销信息。
3. 当亚洲诚信的根 CA 或中级 CA 出现私钥损害时，亚洲诚信将按照密钥应急方案进行紧急处理，并及时通过各种途径通知依赖方。

5.7.4 灾难后的业务连续性能力

一旦物理场地出现了重大灾难，亚洲诚信将根据业务连续性计划在 48 小时内恢复部分服务。

5.8 CA或RA的终止

当亚洲诚信需要停止其业务时，将会严格按照《中华人民共和国电子签名法》及相关法规中对认证机构中止业务的规定要求进行有关工作。

在亚洲诚信终止前，必须:

- 委托业务承接单位;
- 起草亚洲诚信终止声明;
- 通知与亚洲诚信停止相关的实体;
- 处理存档文件记录;
- 停止认证中心的服务;
- 存档和关闭主目录服务器;
- 处理和存储敏感文档;

6 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

6.1.1.1 CA 密钥对的生成

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。密钥的生成、管理、存储、备份和恢复应遵循 FIPS140-2 标准的相关规定。由于国家对于密码产品有严格的管理要求，而 FIPS140-2 标准并非是国家密码主管部门认可和支持的标准，因此 FIPS140-2 标准仅参照执行，是在通过国家密码主管部门鉴定、认证，并在国家密码管理政策许可前提下选择性适用，具体参照设备制造商提供的资料。

CA 密钥对的生成过程，由亚洲诚信专门的密钥管理员和若干名可信人员、以及独立第三方审计人员见证下，在亚洲诚信屏蔽机房按照密钥生成规程完成。密钥对生成过程和操作均需全程录像记录并保存。

6.1.1.2 订户密钥对的生成

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。

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。

亚洲诚信不替订户生成密钥对。

6.1.2 私钥传送给订户

不适用。

6.1.3 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。

6.1.4 电子认证服务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根 CA 证书和中级 CA 证书。

6.1.5 密钥的长度

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	SHA256, SHA384, SHA512	SHA256, SHA384, SHA512	SHA256, SHA384, SHA512
RSA 密钥长度	4096	3072,4096	2048,3072,4096
ECC 曲线	P-384，P-521	P-384，P-521	P-256，P-384, P-521

6.1.6 公钥参数的生成和质量检查

公钥参数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，并遵从这些设备的生成规范和标准。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。

6.1.7 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：

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

除非 WebTrust BR 中有规定，Root CA 私钥不用于签署 CS、 EV CS、EV SSL 证书或创建 CS、EV 签名。

中级 CA 密钥一般用于签发以下证书和 CRL：

- 订户证书；
- 特定用途的 PKI 体系功能证书(如 OCSP 证书)；
- 订户 CRL。订户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。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

亚洲诚信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《GM/T 0028-2014 密码模块安全技术要求》，该标准与 FIPS 140-2 标准等同，具体参照设备制造商提供的资料。

6.2.2 私钥多人控制（m 选 n）

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，将私钥的管理权限分散到若干位密钥管理员中，至少在半数以上的密钥管理员在场并许可的情况下，插入管理员 IC 卡并输入 PIN 码，才能对私钥进行操作。

6.2.3 私钥托管

亚洲诚信的根私钥和 CA 私钥不允许托管，也不向订户提供私钥托管服务。

6.2.4 私钥备份

亚洲诚信对根私钥和 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）。

6.2.5 私钥归档

亚洲诚信对私钥不进行归档。

6.2.6 私钥导入、导出密码模块

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

6.2.7 私钥在密码模块的存储

亚洲诚信私钥以加密的形式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。

6.2.8 激活私钥的方法

亚洲诚信 CA 私钥存放在硬件密码模块中，激活需要按本 CPS 第 6.2.2 节，在至少半数以上的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 卡并输入 PIN 码才能完成。

6.2.9 解除私钥激活状态的方法

对于亚洲诚信私钥，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，在至少半数以上的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并输入 PIN 码进行。

6.2.10 销毁私钥的方法

在亚洲诚信 CA 私钥生命周期结束后，亚洲诚信将 CA 私钥继续保存在一个备份硬件密码模块中，其他的 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。

在 CA 私钥的商业目的或其应用已失去价值或法律责任到期之前，CA 不得毁坏其私钥。

归档的 CA 私钥在其归档期限结束后，或当 CA 私钥备份或副本不再用于有效的商业目的时，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。

6.2.11 密码模块的评估

亚洲诚信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。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

亚洲诚信公钥归档参考第 5.5 章节。

6.3.2 证书操作期和密钥对使用期限

6.3.3 密钥对使用周期

亚洲诚信证书的最长有效期为：

类型	私钥使用	证书期限
公开信任的根 CA	无规定	25 年
公开信任的子 CA	无规定	20 年
DV SSL/TLS	无规定	398 天
OV SSL/TLS	无规定	398 天
EV SSL/TLS	无规定	398 天
文档签名	无规定	39 个月
代码签名	无规定	39 个月
EV 代码签名	无规定	39 个月
安全邮件证书	无规定	39 个月

6.4 激活数据

6.4.1 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

6.4.2 激活数据的保护

对于 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。

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 码保护私钥匙，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。

6.4.3 激活数据的其他方面

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，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、订户用于申请证书的口令，申请成功后失效。

2、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 个月后应要进行修改。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

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。

对每位拥有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。

6.5.2 计算机安全评估

亚洲诚信的 CA 系统及其运营环境通过了第三方的安全评估及渗透测试，获得了相应测试报告。

6.6 生命周期技术控制

6.6.1 系统开发控制

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。

同时，亚洲诚信的软件开发操作规范参考 ISO15408 的标准，执行相关的规划和开发控制。

6.6.2 安全管理控制

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安全管理。

认证系统的信息安全管理，严格遵循国家密码管理局的有关运行管理规范进行操作。

认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行安全使用，任何修改和升级会记录在案。

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。

6.6.3 生命期的安全控制

亚洲诚信通过内部变更控制流程来控制证书认证系统的研发和上线工作，确保该系统安全可靠。

6.7 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 进行网络的攻击防御，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。

6.8 时间戳

亚洲诚信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。这些时间标识不需要采用基于密码的数字时间戳技术。

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

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

亚洲诚信签发的证书符合 ITU-T X.509v3 和 RFC 5280:Internet X.509 公钥基础设施证书和 CRL 结构。

亚洲诚信通过 CSPRNG 生成长度为至少 64 位的非序列性的证书序列号。

7.1.1 版本号

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

- 密钥用法： 数字签名，不可抵赖，密钥加密，数据加密，密钥协议，证书签名，CRL 签名，仅加密，仅解密。

	服务器证书	代码签名证书	安全邮件证书	时间戳证书	CA 证书	文档签名证书
0 Digital Signature	√	√	√	√	√	√
1 Non Repudiation	×	×	×	×	×	√
2 Key Enciphermen t	√（ ECC 算法无此 KU）	×	√	×	×	×
3 Data Enciphermen t	×	×	×	×	×	×
4 Key Agreement	×	×	×	×	×	×
5 Key Cert Sign	×	×	×	×	√	×
6 CRL Sign	×	×	×	×	√	×

7 Encipher Only	×	×	×	×	×	×
8 Decipher Only	×	×	×	×	×	×

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。

- 扩展密钥用法

	时间戳证书	代码签名证书	服务器证书	安全邮件证书	文档签名证书
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	×	×	√	√	×
代码签名 1.3.6.1.5.5.7.3.3	×	√	×	×	×
安全电子邮件 1.3.6.1.5.5.7.3.4	×	×	×	√	×
时间戳 1.3.6.1.5.5.7.3.8	√	×	×	×	×
PDF 签名	×	×	×	×	√

1.2.840.113583. 1.1.5					
MS Document Signing 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

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 CPS 附录中关于证书自定义扩展项说明。

7.1.3 算法对象标识符

亚洲诚信证书使用以下算法之一进行签名：

SHA-256 with RSA	1.2.840.113549.1.1.11
SHA-384 with RSA	1.2.840.113549.1.1.12
SHA-256 with ECDSA	1.2.840.10045.4.3.2
SHA-384 with ECDSA	1.2.840.10045.4.3.3

亚洲诚信和订户可以使用以下方式生成密钥对：

RSA	1.2.840.113549.1.1.1
ECDSA	1.2.840.10045.2.1

7.1.4 名称形式

亚洲诚信签发的证书名称形式的格式和内容符合 RFC5280 的要求，且符合 CA/B Forum Baseline Requirements 中 7.1.4 章节的要求。

7.1.5 名称限制

无规定。

7.1.6 证书策略对象标识符

证书策略对象标识符同本 CPS 第 1.2 节。

7.1.7 策略限制扩展项的用法

无规定。

7.1.8 策略限定符的语法和语义

无规定。

7.1.9 关键证书策略扩展项的处理规则

无规定。

7.2 证书撤销列表

亚洲诚信定期签发 CRL，供订户和依赖方查询使用。

7.2.1 版本号

亚洲诚信的证书吊销列表符合 X.509 v2 的版本及格式要求。

7.2.2 CRL 和 CRL 条目扩展项

与 ITU X.509 和 RFC3280 规定一致。

- CRL 的版本号：用来指定 CRL 的版本信息，亚洲诚信采用的是和证书 X.509 V3 对应的 CRL X.509 V2 版本。
- 签名算法：亚洲诚信 采用 SHA256RSA 和 SHA384ECDSA 签名算法。
- 颁发者：指定签发机构的 DN 名，由国家、省、市、机构、单位部门和通用名等组成。
- 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。
- 颁发机构密钥标识符(Issuer Unique Identifier)：本项标识用来验证在 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。

7.3 在线证书状态协议

亚洲诚信认证系统提供 OCSP 服务，签发的 OCSP 响应符合 RFC6960 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。

7.3.1 版本号

RFC6960 定义的 OCSP V1 版本。

7.3.2 OCSP 扩展项

与 RFC6960 一致。

8 认证机构审计和其他评估

8.1 评估的频率和情形

亚洲诚信执行如下审计和评估：

1) 每年进行一次安全脆弱性评估，对系统、物理场地、运营管理等方面评估，并根据评估报告采取措施，以降低运营风险。
2) 每年进行一次运营工作质量评估，以保证运营服务的可靠性、安全性和可控性。
3) 每季度执行一次鉴证内审，抽取至少 3%的证书样本。
4) 每年根据 CA/B Forum 上 BR 的要求，进行一次 BR 自评估工作。
5) 每年对物理控制、密钥管理、操作控制、鉴证执行等情况执行一次审计，以确定实际发生情况是否与预定的标准、要求一致，并根据审查结果采取行动。
6) 每年进行一次运营风险评估工作，识别内部与外部的威胁，评估威胁事件发生的可能性及造成的损害，并根据风险评估结果，制定并实施处置计划。

7） 除了内部审计和评估外，亚洲诚信还聘请独立的审计师事务所，按照 WebTrust 对 CA 的审计规范，每年进行一次外部审计和评估。

8.2 评估者的资质

内部审计和评估，由亚洲诚信内部审计评估小组执行此项工作。

外部审计，由具备以下的资质机构负责：

- 必须是经许可的、有执业资格的评估机构，在业界享有良好的声誉；
- 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作；
- 具备检查系统运行性能的专业技术和工具；
- 具备 WebTrust 审计的资质。

8.3 评估者与被评估者之间的关系

内部审计人员与本机构的系统管理员、业务管理员、业务操作员的工作岗位不能重叠。

外部评估者和亚洲诚信之间是相互独立的关系，双方无任何足以影响评估客观性的利害关系。

8.4 评估内容

内部审计工作涉及以下内容：

1）运营工作流程和制度是否得到严格遵守;

2）是否严格按 CP、CPS、业务规范和安全要求开展认证业务;

3）各种日志、记录是否完整，是否存在问题;

4）是否存在其他可能存在的安全风险。

第三方审计师事务所按照 WebTrust CA 规范的要求，对亚洲诚信进行独立审计。

8.5 对问题与不足采取的措施

对于本机构内部审计结果中的问题，由审计评估小组负责监督相关责任部门的改进情况。

第三方审计师事务所评估完成后，亚洲诚信按照其工作报告进行整改，并接受再次审计和评估。

8.6 评估结果的传达与发布

亚洲诚信的内部审计结果向本机构各责任部门进行正式通报，对可能造成的订户安全隐患，亚洲诚信将及时向订户通报。

第三方审计师事务所评估完成后，向亚洲诚信提供审计报告，亚洲诚信完成整改工作和再评估后，将在官网公布最终审计结果。

8.7 其他评估

无规定。

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明的价格和亚洲诚信公布的价格不一致，以协议中的价格准。

9.1.2 证书查询费用

在证书有效期内，亚洲诚信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，将由亚洲诚信与用户协商收取。

9.1.3 证书撤销或状态信息的查询费用

亚洲诚信对吊销列表(CRL)的获取不应收取费用。

9.1.4 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。

9.1.5 退款策略

如果由于亚洲诚信的原因，造成订户合同无法履行、订户证书无法使用，亚洲诚信会将相关费用返还给订户。如非亚洲诚信原因，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

亚洲诚信向证书订户提供证书使用保障。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（具体情形参见本 CPS 第 9.9 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

亚洲诚信如违反了本 CPS 中规定的职责，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)。经亚洲诚信确认后，可对该实体进行赔偿。赔偿限制如下:

- 亚洲诚信所有的赔偿义务不得超出本节 9.2.1 中规定的保险范围，赔偿金额不得高于赔偿金额上限，赔偿金额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。
- 亚洲诚信只有在证书有效期限内承担损失赔偿责任。

9.3 业务信息保密

9.3.1 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。
- 其他由亚洲诚信及其 RA 保存的个人和公司信息应视为保密，除法律要求，不可公布。

9.3.2 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、CPS 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。

9.3.3 保护保密信息的责任

亚洲诚信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 个人隐私保密

9.4.1 隐私保密原则

亚洲诚信尊重证书订户个人资料的隐私权，保证完全遵照国家对个人资料隐私保护的相关规定及法律。同时，亚洲诚信将确保全体职员严格遵从安全和保密标准对个人隐私给予保密。

9.4.2 作为隐私处理的信息

亚洲诚信将有关证书或 CRL 内容中未公开提供的个人的所有个人信息视为私人信息。 亚洲诚信使用适当的保护措施和合理的谨慎程度来保护私人信息。

9.4.3 不被视为隐私的信息

订户持有的证书信息，以及证书状态信息不被视为隐私信息。

9.4.4 保护隐私的责任

亚洲诚信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。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)。

9.4.6 依法律或行政程序的信息披露

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。

9.4.7 其他信息披露情形

如果证书订户要求亚洲诚信提供某类特定客户支援服务，如资料邮寄，亚洲诚信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。

对其他信息的披露受制于法律、订户协议。

9.5 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(以下简称 DN)以及该域中颁发给终端实体的证书，均为亚洲诚信的财产。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

亚洲诚信在提供电子认证服务活动过程中对订户的承诺如下:

- 遵守《中华人民共和国电子签名法》等法律法规，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，对其注册机构电子认证业务是否符合本 CPS 约定进行审计。
- 签发给订户的证书符合本 CPS 的所有实质性要求。
- 不会签发具有误导依赖方相关 CA 验证的证书信息的证书。

- 将向证书订户通报任何已知的，将在本质上影响订户的证书的有效性和可靠性事件。
- 将根据 CPS 的要求及时吊销证书。
- 根据 CPS 的要求验证申请人的身份。
- 若亚洲诚信与订户无关联，则亚洲诚信与订户是合法有效且可执行的订户协议双方，该订户协议符合 CA/浏览器论坛发布的 BRs 等要求；若亚洲诚信与订户为同一实体或有关联，则申请人代表已认可使用条款。
- 针对所有未过期的证书的当前状态信息(有效或已吊销)建立及维护 24*7 公开的信息库。

证书公开发布后，亚洲诚信保证除未经验证的订户信息外，证书中的其他订户信息都是准确的。

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。

9.6.2 注册机构的陈述与担保

亚洲诚信的注册机构在参与电子认证服务过程中的承诺如下:

- 提供给证书订户的注册过程完全符合亚洲诚信的 CPS 的所有实质性要求。
- 在亚洲诚信生成证书时，不会因为其注册机构的失误而导致证书中的信息与证书申请者的信息不一致。
- 亚洲诚信将按 CPS 的规定，及时提交撤销、更新等服务申请。

9.6.3 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 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。
- 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。
- 对于代码签名证书的订户，若发现以下情况，应立即向亚洲诚信申请撤销证书:1) 证书中的信息为或将成为错误或不准确的信息; 2)证书中与公钥有关的私钥被误用或被损坏; 3)有证据表明，该代码签名证书被用于签署恶意代码。

9.6.4 依赖方的陈述与担保

- 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。

9.6.5 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 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 CPS 第 9.6.3 之承诺时，或依赖方违反本 CPS 第 9.6.4 之承诺时，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。

9.8 有限责任

证书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 CPS 第 9.9 节规定的有限赔偿责任。

9.9 赔偿

9.9.1 赔偿范围

如亚洲诚信违反了本 CPS9.6.1 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本 CPS 9.2.1，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。

9.9.2 订户的赔偿责任

如因下述情形而导致亚洲诚信或依赖方遭受损失，订户应当承担赔偿责任:

1. 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致亚洲诚信或第三方遭受损害;

2. 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知亚洲诚信，以及不当交付他人使用导致亚洲诚或第三方遭受损害；
3. 订户使用证书的行为，有违反本 CPS 及相关操作规范，或者将证书用于非本 CPS 规定的业务范围；
4. 证书订户或者其它有权提出撤销证书的实体提出撤销请求后，到亚洲诚信将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果亚洲诚信按照本 CPS 的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任；
5. 提供的资料或信息不真实、不完整或不准确；
6. 证书中的信息发生变更但未停止使用证书并及时通知亚洲诚信和依赖方；
7. 没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄露等；
8. 在得知私钥丢失或存在危险时，未停止使用证书并及时通知亚洲诚信和依赖方；
9. 证书到期但仍在使用证书；
10. 订户的证书信息侵犯了第三方的知识产权；
11. 在规定的范围外使用证书，如从事违法犯罪活动。

9.9.3 依赖方的赔偿责任

如因下述情形而导致 亚洲诚信 或订户遭受损失，依赖方应当承担赔偿责任：

1. 没有履行 亚洲诚信 与依赖方的协议和本 CPS 中规定的义务；
2. 未能依照本 CPS 规范进行合理审核，导致亚洲诚信或第三方遭受损害；
3. 在不合理的情形下信赖证书，如依赖方明知证书存在超范围、超期限使用的情形或证书已经或有可能被人窃取的情形，但仍然信赖证书；
4. 依赖方没有对证书的信任链进行验证；
5. 依赖方没有通过查询 CRL 或 OCSP 确认证书是否被撤销。

9.10 有效期限与终止

9.10.1 有效期限

本 CPS 和 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。

9.10.2 终止

当亚洲诚信终止业务时，本 CPS 终止。

9.10.3 效力的终止与保留

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后，不影响文件中其他条款的法律效力。

9.11 对参与者的个别通告与沟通

亚洲诚信在必要的情况下，如在主动吊销订户证书、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。

9.12 修订

9.12.1 修订程序

经亚洲诚信安全策略委员会授权，CPS 编写小组每年至少审查一次本 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 CP 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，由 CPS 编写小组提出修订意见，经 亚洲诚信安全策略委员会 批准后，由 CPS 编写小组负责完成修订，修订后的 CPS 经过亚洲诚信 安全策略委员会批准后正式对外发布。

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官网发布。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OID的情形

亚洲诚信全权负责确定 CPS 的修订是否需要更改 OID。

9.12.4 必须修改业务规则的情形

亚洲诚信必须对本 CPS 进行修改的情形包括：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

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 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。

9.14 管辖法律

亚洲诚信 的 CPS 受中华人民共和国法律法规的管辖。

9.15 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 CPS 的执行、解释和程序有效性均适用中华人民共和国各项法律法规和国家信息安全主管部门要求。任何与亚洲诚信就本 CPS 所涉及的任何争议，均适应中华人民共和国法律。

9.16 一般条款

9.16.1 完整协议

本 CPS 完整的文档结构包括：标题、目录、主体内容 3 部分。关于对目录和主体内容修改后的替代内容，将完全代替所有先前部分、并被放置在亚洲诚信的网站中以供查阅和浏览。

9.16.2 转让

亚洲诚信声明，根据本 CPS 中详述的认证实体各方的权利和义务，各方当事人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。

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

亚洲诚信声明，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

如果因战争、瘟疫、火灾、地震和天灾等不可抗力造成了违反、延误或无法履行本 CPS 规定的担保责任，那么亚洲诚信将不对此类事件负责。

9.17 其他条款

亚洲诚信对本 CPS 具有最终解释权。