亚洲诚信标志证书策略和电子认证业务规则（CP&CPS）V1.0.0

亚数信息科技（上海）有限公司

2026-05-09

目录

1 概括性描述

1.1 概述

本文档是亚数信息科技（上海）有限公司（TrustAsia Technologies, Inc,中文简称“亚洲诚信”，英语简称“TrustAsia”）针对标志证书（Mark Certificates）服务制定的《证书策略和电子认证业务规则》（简称CP&CPS）。本文档采用RFC 3647格式，概述了由亚洲诚信CA认证的X.509数字证书相关的原则与实践。

亚洲诚信CA关于标志证书（Mark Certificates）的颁发与管理的各项实践，均遵照《Minimum Security Requirements for Issuance of Mark Certificates》（简称“MCR”）的最新版本执行。这些要求可通过https://bimigroup.org/supporting-documents/ 获取。所有订阅者、标志声明实体、使用方和依赖方均受《MCR》中附录D的“MC Terms”的约束。

1.1.1 公司介绍

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

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

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

我们将以国际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

本文的描述了亚洲诚信CA执行的一套集成技术、协议以及身份和商标验证标准，此标准是为签发受消费者信任的标志证书。本CP&CPS包含以下四种类型的标志证书：

普通标志证书 (Common Mark Certificates):

a. 先前使用的标志证书 (Prior Use Mark Certificates)

b. 修改的注册商标证书 (Modified Registered Trademark Certificates)

认证标志证书 (Verified Mark Certificates):

a. 注册标志证书 (Registered Mark Certificates)

b. 政府标志证书 (Government Mark Certificates)

亚洲诚信CA根据使用场景和算法不同，具体可见信息库 https://repository.trustasia.com。

1.1.3 证书策略（CP）与电子认证业务规则（CPS）

本CP&CPS按照中华人民共和国工业和信息化部发布的《电子认证服务管理办法》和《电子认证业务规则规范(试行)》进行编写。

本CP&CPS阐明了亚洲诚信CA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CP&CPS所阐述的内容遵循以下政策、指引和要求：

1. 互联网工程任务组（IETF）发布的 RFC3647 标准
2. BIMI Group发布的Mark Certificate Guidelines最新版（自本CP&CPS发布前）

亚洲诚信CA会定期查看其更新情况，并持续修订CP&CPS。如果本CP&CPS与上述相关标准规范中的条款有不一致的地方，则以上述正式发布的规范为准。

1.2 文档名称与标识

本文档为亚洲诚信标志证书服务证书策略和电子认证业务规则。

1.2.1 对象标识

亚洲诚信CA遵循 MCR 要求颁发标志证书，在证书策略扩展项（Certificate Policies Extension）中包含MC policy OID，具体见本CP&CPS第7.1.6节。

以下为本CP&CPS使用的一些对象标识符：

对象标识符（OID）	标识代表对象	类型
1.3.6.1.4.1.44494.2.7	亚洲诚信CA标志证书策略标识	证书策略
1.3.6.1.4.1.53087.1.1	保留的标志证书策略标识	证书策略
1.3.6.1.5.5.7.3.31	BIMI扩展密钥用途	增强型密钥用法
1.3.6.1.5.5.7.3.9	OCSP响应签名用途	增强型密钥用法
1.3.6.1.4.1.53087.1.13	标志类型	Subject字段
1.3.6.1.4.1.53087.1.3	商标注册地	Subject字段
1.3.6.1.4.1.53087.1.2	商标局名称	Subject字段
1.3.6.1.4.1.53087.1.4	商标标识符	Subject字段
1.3.6.1.4.1.53087.1.5	法令实体识别码(LEI)	Subject字段
1.3.6.1.4.1.53087.1.6	文字商标	Subject字段
1.3.6.1.4.1.53087.3.2	法令国家代码	Subject字段

对象标识符（OID）	标识代表对象	类型
1.3.6.1.4.1.53087.3.3	法令省份/州名	Subject字段
1.3.6.1.4.1.53087.3.4	法令所在地名	Subject字段
1.3.6.1.4.1.53087.3.5	法令引用	Subject字段
1.3.6.1.4.1.53087.3.6	法令URL	Subject字段
1.3.6.1.4.1.53087.5.1	先前使用标志来源URL	Subject字段
1.3.6.1.4.1.311.60.2.1.1	辖区城市/所在地	Subject字段
1.3.6.1.4.1.311.60.2.1.2	辖区省/州	Subject字段
1.3.6.1.4.1.311.60.2.1.3	辖区国家	Subject字段
1.3.6.1.5.5.7.1.12	徽标扩展	证书扩展
1.3.6.1.4.1.11129.2.4.2	SCT记录	证书扩展

1.2.2 修订历史

发布日期	更新内容	发布版本
2026-05-09	发布初版	V1.0.0

1.3 PKI 参与者

1.3.1 电子认证服务机构

亚洲诚信CA同时作为电子认证服务机构（CA）和标志验证机构（MVA）运营。

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，亚洲诚信CA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CA产品和服务的信息，请访问http://www.trustasia.com[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CA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CA获得证书的所有最终用户，也可称为标志声明实体。

1.3.4 依赖方

依赖方是指依赖于亚洲诚信CA签发的标志证书，或依赖于标志证书所包含的信息或标志，或依赖于消费实体向其展示的信息或标志的任何自然人或法人。

1.3.5 其他参与者

其他参与者是指为亚洲诚信CA的电子认证活动提供相关服务的其他实体，包括参与工作的加拿大专业会计师协会 (CPA Canada) WebTrust工作组。

1.4 证书应用

1.4.1 适合的证书应用

根据此CP&CPS签发的证书旨在实现高效安全的电子通信，同时解决用户对证书信任度的担忧，帮助用户在依赖证书时做出知情决定。

1.4.2 限制的证书应用

亚洲诚信CA所签发的数字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CP&CPS限定的应用范围，将不受本CP&CPS保护。

亚洲诚信CA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，禁止用于中间人（MITM）攻击，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。

1.5 策略管理

1.5.1 策略文档管理机构

本CP&CPS的管理机构是亚洲诚信CA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CP&CPS。亚洲诚信CA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CA将对CP&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)或 86-21-58895880(国际)

1.5.3 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CP&CPS的最高权威机构。

1.5.4 CPS批准程序

本CP&CPS由亚洲诚信CA安全策略委员会组织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CA官方网站上发布。

本CP&CPS根据国家的政策法规、技术要求、业务发展情况以及BIMI Group的标志证书MCR要求修订，由CPS编写组根据相关情况拟定CP&CPS修订内容，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CA官网上发布。

1.6 定义和缩写

1.6.1 术语定义

术语	定义
执业会计师	指在申请人成立或注册辖区内，或申请人设有办公室或实体设施的任何辖区内，持有注册会计师、特许会计师或同等执照的人员；前提是该辖区的会计标准机构维持国际会计师联合会（IFAC）的全权会员资格
关联方	指控制另一实体、受其控制或与其受共同控制的公司、合伙企业、合营企业或其他实体；或是在政府实体直接控制下运行的机构、部门、政治分部或任何实体
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，也称标志验证机构（MVA），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。
CAA	认证机构授权，允许域名持有人指定授权为其签发证书的CA
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。

术语	定义
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，本文档主要指标志证书。
交叉证书	用于在两个根 CA 之间建立信任关系的证书。
CSPRNG	用于加密系统的随机数生成器。
证书问题报告	关于证书误签发、滥用或其他欺诈、泄露、不当行为的投诉。
证书配置文件	定义证书内容和扩展要求的文件或文件集。
证书撤销列表	由签发CA定期更新、带有时间戳并经过数字签名的已吊销证书列表。
证书批准人	指受雇于申请人或拥有代表申请人明确授权的自然人，负责行使证书请求人的职能并批准其他请求人提交的请求。
证书数据	指CA拥有、控制或可访问的证书请求及相关数据。
证书管理流程	指与密钥、软件和硬件使用相关的流程、实践和程序，CA 通过这些流程验证数据、签发证书、维护存储库及吊销证书。
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	指基于对电子签名认证证书或电子签名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。

术语	定义
申请人	已申请但尚未被授予“标志证书”的个人、实体或组织；或指目前已持有“标志证书”（一份或多份）且正在申请续期该“标志证书”，或申请额外“标志证书”的个人、实体或组织。
申请人代表	指本身即为申请人，或者是受雇于申请人、或拥有代表申请人明确授权的自然人或人类发起人：(i) 代表申请人签署并提交或批准证书请求，和/或 (ii) 代表申请人签署并提交订阅人协议，和/或 (iii) 在申请人为 CA 的关联方或 CA 本身时，代表申请人确认使用条款。
确认人	申请人组织内负责确认特定事实的职位。
标志主张实体（“MAE”）	标志证书的申请人/订阅方。可与申请人和（或）订阅方为同一实体。
冲突商标所有者	断言标志证书中的标志表现形式侵犯其注册商标权的注册商标所有者或许可人。
法院侵权裁定	来自具有管辖权的法院或商标局法庭的最终命令，声明标志证书中的标志表现形式不当侵犯了冲突商标所有者的注册商标。
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。
消费实体	根据MC条款在其产品和服务中整合并使用标志表现形式及相关数据的实体，包括邮箱提供商。
委托第三方	获 CA 授权通过履行一项或多项 CA 要求来协助证书管理流程的自然人或法律实体。
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。
商标表示形式	指组合标志、图形标志或文字标志的数字化表示形式（如数字或计算机文件），包含可被解析以重建（渲染）该商标视觉表现形式从而使其可见的结构化二进制或文本数据。该商标表示形式将用作第7.1.2.3节下的徽标类型扩展。
应用软件供应商	依赖方应用软件的供应商，该软件能够显示或使用“标记证书”，并集成了“根证书”
网页存档来源	可靠且能显示网页截图以及截图制作日期的在线公开来源。
证明信	指由会计师、律师、政府官员或其他习惯上受信任的可靠第三方撰写的，证明主体信息准确的信函
审计周期	在一段时期的审计中，指审计师在业务中涵盖的从运行第一天（开始）到最后一天（结束）的期间
审计报告	由合资格从业者出具的报告，说明该实体的流程和控制是否符合本要求的强制性规定

术语	定义
合格从业者	满足本CPS第8.2节要求的自然人或法律实体。
合格政府信息源	由政府实体维护的、法律要求报告数据且虚假报告受法律惩罚的公开数据库。
合格独立信息源	定期更新且通用的、旨在提供准确信息的公开数据库，被公认为可靠的信息源。
授权域名	用于获得给定 FQDN 证书签发授权的域名
授权端口	指以下端口之一：80 (http)、443 (https)、25 (smtp)、22 (ssh)
基础域名	申请的 FQDN 中，位于注册机构控制的后缀或公共后缀左侧的第一个域名节点及其后缀（例如 "example.com"）
商业实体	指除私营组织、政府实体或非商业实体之外的任何实体。例如普通合伙企业、非法人协会、个体工商户等
普通标志	申请人或订阅方主张其依据普通法（或大陆法系国家的同等法律）享有使用权的标志或徽标。普通标志可能是也可能不是注册商标。
图形标志	由图形设计、风格化徽标或图像组成，不包含文字和/或字母的标志。为更明确起见，“图形标志”包括仅由设计元素构成的标志。
文字标志	仅由文本构成的标志，该文本的表达不考虑字体、样式、大小或颜色。
设计标志	由图形设计、艺术化徽标或图像组成，不含文字和/或字母的标志。
组合标志	由图形设计、风格化徽标或图像，连同具有特定风格化外观的文字和/或字母组成的标志。为更明确起见，“组合标志”包括由文字元素和设计元素共同构成的标志。
普通标志证书	包含《MCR》中规定的主体信息和扩展项，且已由标志验证机构按照《MCR》进行验证并签发的证书。此外，该证书包含的标志表示形式未被验证为“注册商标”或“政府商标”的标志证书。
认证标志证书	包含《MCR》中规定的主体信息和扩展项，且已按照《MCR》进行验证并签发的证书。此外，该证书包含的标志表示形式已被验证为“注册商标”或“政府商标”。
政府标志	通过正式法令、法规、条约或政府行为授予政府组织（或授予私营组织及其他组织）或由其主张的商标或同等标识，其外观或描述如该法令、法规、条约或政府行为中所示，并由商标验证机构按照第 3.2.17.2 节规定的程序进行确认。由政府实体向商标局注册为商标的标志不被视为“政府商标”。
标志审核机构	签发标志证书的机构，也称为CA。
标志证书（MC）	包含本要求指定的属性和扩展，并由标志审核机构验证签发的证书
MC授权机构	除证书批准人以外的来源，用于核实证书批准人已获得申请人的明确授权。
MC证书请求	申请人向 CA 发出的、由证书批准人签署的签发证书请求。
MCR	本标志证书要求。
MC条款	适用于标志证书及其中数据的展示和使用的条款，见本CPS第12章

术语	定义
WebTrust	CPA 加拿大针对认证服务机构的 WebTrust项目的当前版本。
域名授权文件	由域名注册商或注册人提供的证明申请人有权请求特定域名空间证书的文件。
域名联系人	在WHOIS记录、DNS SOA 记录或直接从域名注册商处获得的域名注册人、技术联系人或管理联系人。
内部名称（Internal Name）	证书的通用名称或主题备用名称字段中的一串字符（不是 IP 地址），由于它没有以在 IANA 的根区域数据库中注册的顶级域名结尾，因此在证书颁发时无法在公共 DNS 中验证其全局唯一性。
顶级域名（Top-Level Domain）	根据 RFC 8499， 顶级域是比根域名低一级的区域，如“com”或“cn”。
SVG指南	AuthIndicators 工作组发布的关于 SVG Tiny PS 规范及验证工具的文档。
商标局	世界知识产权组织（WIPO）认可的负责商标注册的知识产权办公室。

1.6.2 缩略语及含义

BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	公信证书的签发和管理基准要求
CA	Certification/Certificate Authority	电子认证服务机构
CAA	Certification Authority Authorization	认证机构授权
ccTLD	Country Code Top-Level Domain	国家顶级域名
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
CRL	Certificate Revocation List	证书撤销列表
CSR	Certificate Signing Request	证书请求文件
DBA	Doing Business As	商业名称
DN	Distinguished Name	甄别名
DNS	Domain Name System	域名系统
EV	Extended Validation	扩展验证/增强验证
EVG	Guidelines for the Issuance and Management of Extended Validation Certificates	扩展验证证书签发与管理指南
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

BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	公信证书的签发和管理基准要求
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
MAE	Mark Asserting Entity	标志主张实体
MVA	Mark Verifying Authority	标志验证机构
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
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
S/MIME	Secure/Multipurpose Internet Mail Extensions	安全/多用途邮件扩展
TLS	Transport Layer Security	传输层安全
TTL	Time to Live	IP包的生存时间
X.509	The ITU-T standard for Certificates and their corresponding authentication	ITU-T证书标准及其相应的认证

1.6.3 参考资料

- 互联网工程任务组（IETF）发布的 RFC3647 标准
- BIMI Group发布的Mark Certificate Guidelines最新版（自本CP&CPS发布前）
- Apple Root Certificate Program

1.6.4 约定

本文中的关键词“必须”、“不得”、“要求”、“应”、“不应”、“应该”、“不宜”、“推荐”、“可以”和“可选”根据RFC 2119进行解释。

本文档所提日期的省略时间为北京时间 00:00:00（UTC+8）。

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：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CA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CA信息库将及时在官方网站(https://www.trustasia.com/cps)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CA证书、CP&CPS修订和其它资料等，这些内容必须保持与CP&CPS和有关法律法规一致。

2.2.2 CRL发布

亚洲诚信CA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CA签发的证书中CRL分发点地址获取CRL。亚洲诚信CA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证书的状态信息。

2.3 发布的时间和频率

2.3.1 CPS发布时间和频率

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

亚洲诚信CA会定期跟进BIMIGroup MCR变化，并及时调整CP&CPS来符合标准。

2.3.2 CRL发布时间和频率

亚洲诚信CA对于订户证书的CRL至少每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。

2.4 信息库的访问控制

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。

所有版本的CP&CPS，包括历史的版本，均会在信息库中公开。

3 身份标识和鉴别

3.1 命名

3.1.1 名称类型

亚洲诚信CA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。其命名做法符合RFC 5280和MCR。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。

MC证书主体属性不会仅包含元数据，如“.”、“-”和“ ”（即空格）字符，和任何其他表明值缺失、不完整或不适用的迹象。使用者备用名称扩展至少包含一个条目，每个条目包含一个完全限定域名，不得使用内部名称，dNSName的条目符合RFC5280规定的首选名称语法，不包含下划线字符。

3.1.2 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。

3.1.3 订户的匿名或伪名

亚洲诚信CA不为MC证书颁发匿名或伪名证书。

3.1.4 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。

3.1.5 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。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。

3.1.6 商标的识别、鉴别和角色

证书申请者不得在证书申请中使用可能侵犯他人知识产权的名称。亚洲诚信CA签发证书时并不验证订户对商标的使用权，也不负责解决商标相关纠纷。亚洲诚信CA可以拒绝或撤销具有商标争议的相关证书。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

由于标志证书中包含的公钥不会被使用，所以亚洲诚信CA不要求申请人证明其拥有相关的私钥。订户可以自行生成私钥，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)。

3.2.2 组织和域名鉴别

3.2.2.1 组织机构的身份鉴别

亚洲诚信CA只向符合以下规定的私营企业、政府实体、商业实体和非商业实体的申请人颁发标志证书。

在颁发标志证书之前，亚洲诚信CA会确保所有包含在证书中的主体组织信息均符合相关要求，并选择以下一项或多项来验证组织的身份和地址信息，并使用可靠的通信方式获得申请组织的申请意愿：

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QGIS或合格独立信息源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，以确认申请组织所提供的信息的真实性以及申请人的授权。
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。

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。

3.2.2.1.1 私营组织主体身份鉴别

申请组织必须符合以下所有标准或已获得以下指定信息，可被认定为私营组织：

1. 私营组织的法律存在必须是由其注册管辖区或登记管辖区内的注册机构或登记机关通过备案或采取相应行动创建或认可的（例如，通过颁发公司注册证书、分配注册号等），或者是由政府机构创建或认可的（例如根据章程、条约、公约或等效的认可文件）；
2. 私营组织的具体注册号码是由其注册管辖区或登记管辖区内的注册机构或登记机关分配的。如果注册机构或登记机关未分配注册号码，亚洲诚信CA则使用私营组织的注册成立日期；
3. 私营组织必须向公司注册机构或登记机关指定注册代理人、注册办事处（根据其注册管辖区或登记管辖区的法律要求）或同等机构；
4. 私营组织不得在公司注册机构或登记机关的记录中被标记为“不活跃”、“无效”、“非当前”或具有同等含义的标签；
5. 私营组织提供的实际地址必须是申请组织或其母公司/子公司开展业务运营的地址，并且是申请组织的营业场所地址。如果申请组织的营业地点不在公司注册地或成立所在国，申请组织也可以提供经验证的专业意见函，证名申请组织的营业地点地址，并确认业务在该地点开展；
6. 为了验证申请组织从事业务的能力，亚洲诚信CA选择以下任意一项验证申请组织或其关联公司、母公司或子公司的经营存在：
   a.申请组织、关联公司、母公司或子公司的成立日期，不得少于证书申请前三年，或者已列入当前的合格独立信息源（QIIS）或合格政府税务信息源（QTIS）中；或

b.通过直接从受监管金融机构接收申请组织、关联公司、母公司或子公司经过认证的证明文件，验证申请组织、关联公司；母公司或子公司在该机构拥有活跃的当前活期存款账户；或

c.通过经验证的专业意见函验证申请组织在受监管的金融机构拥有活跃的当前活期存款账户；

7. 私营组织的注册、登记、章程或执照管辖区和其营业地点不得位于亚洲诚信CA运营管辖区法律禁止开展业务或颁发证书的任何国家/地区，以及不得被列入亚洲诚信CA运营管辖区政府拒绝名单或禁止名单中。

3.2.2.1.2 政府实体主体身份鉴别

申请组织必须符合以下所有标准或已获得以下指定信息，可被认定为政府实体：

1. 政府实体的法律存在必须是由其运营所在的政治分支机构确定；
2. 亚洲诚信CA将尝试获取政府实体的成立、注册或设立日期，或创建该政府实体的立法法案的标识符。对于没有注册号码或无法轻易核实成立日期的政府实体，亚洲诚信CA将以“政府实体”一词代替；
3. 该政府实体不得位于亚洲诚信CA运营管辖区法律禁止开展业务或颁发证书的任何国家/地区，以及不得被列入亚洲诚信CA运营管辖区政府拒绝名单或禁止名单中。

3.2.2.1.3 商业实体主体身份鉴别

任何不属于私营组织、政府实体以及非商业实体的实体，则被列入商业实体。包括但不限于：普通合伙企业、非法人协会、个人独资企业等。申请组织必须符合以下所有标准或已获得以下指定信息：

1. 商业实体必须是依法认可的实体，其设立需向所属管辖区的注册机构提交表格，并由该注册机构颁发或批准章程、证书或执照，且其存在和通过该注册机构进行核实；
2. 商业实体提供的实际地址必须是申请组织开展业务运营的地址，并且是申请组织的营业场所地址；
3. 商业实体的唯一注册号码是由其注册管辖区的注册机构分配的。如果注册机构未分配注册号码，亚洲诚信CA则使用其注册成立日期；
4. 为了验证申请组织从事业务的能力，亚洲诚信CA选择以下任意一项验证申请组织或其关联公司、母公司或子公司的经营存在：

a.商业实体的成立日期，不得少于证书申请前三年，或者已列入当前的合格独立信息源（QIIS）或合格政府税务信息源（QTIS）中；或

b.通过直接从受监管金融机构接收申请组织经过认证的证明文件，验证申请组织在该机构拥有活跃的当前活期存款账户；或

c.通过经验证的专业意见函验证申请组织在受监管的金融机构拥有活跃的当前活期存款账户；

5. 亚洲诚信CA必须和至少一名与该商业实体相关联的“主要个人”进行“面对面验证”。“主要个人”可以是该实体所有者、合伙人、管理成员、董事或高级职员，或由申请组织出具授权书证明其为“主要个人”身份的个人。亚洲诚信CA会安排“主要个人”进行“面对面审核”。面对面审核（或等同于面对面审核）的方式包括但不限于视频电话、视频录像、当面审核等。在面对面审核过程中，“主要个人”需要出具政府签发的身份证明文件，并提供至少两份辅助文件证据来证明其身份，其中一份必须来自金融机构，“主要个人”需要按审核人员的要求出示身份证明文件的原件，并当场签署关于个人信息陈述的申请表以完成审核。“主要个人”还需证明其在订户协议中所做陈述属实。亚洲诚信CA会审核客户提供的文件确保信息一致，以及与申请表中的信息相符，并能识别“主要个人”的身份；
6. 该商业实体以及与其相关的已确定的“主要个人”不得位于亚洲诚信CA运营管辖区法律禁止开展业务或颁发证书的任何国家/地区，该商业实体以及与其相关的已确定的“主要个人”均不得被列入亚洲诚信CA运营管辖区政府拒绝名单或禁止名单中。

3.2.2.1.4 非商业实体主体身份鉴别

申请组织必须符合以下所有标准或已获得以下指定信息，可被认定为非商业实体：

1. 非商业实体是一个国际组织实体，其成立依据多个国家政府（或代表多个国家政府）签署的章程、条约、公约或等效文书；

2. 对于无法轻易创建立法文件标识符或无法轻易验证成立日期的非商业实体，亚洲诚信CA将使用“国际组织实体”一词代替；
3. 为了验证申请组织从事业务的能力，亚洲诚信CA选择以下任意一项验证申请组织或其关联公司、母公司或子公司的经营存在：

a.申请组织、关联公司、母公司或子公司的成立日期，不得少于证书申请前三年，或者已列入当前的合格独立信息源（QIIS）或合格政府税务信息源（QTIS）中；或

b.通过直接从受监管金融机构接收申请组织、关联公司、母公司或子公司经过认证的证明文件，验证申请组织、关联公司；母公司或子公司在该机构拥有活跃的当前活期存款账户；或

c.通过经验证的专业意见函验证申请组织在受监管的金融机构拥有活跃的当前活期存款账户；

4. 非商业实体的总部所在国家不得位于亚洲诚信CA运营管辖区法律禁止开展业务或颁发证书的任何国家/地区，以及不得被列入亚洲诚信CA运营管辖区政府拒绝名单或禁止名单中。

另外，符合非商业实体资格的实体的下属组织或机构，也可申请非商业实体标志证书。

3.2.2.2 面对面验证程序

亚洲诚信CA要求申请组织的合同签署人或证书审批人必须执行面对面验证程序。亚洲诚信CA将参照MCR所述中，视频会议的验证要求为其安排“面对面审核”。

亚洲诚信CA将与指定人员发起实时录制的视频会议，指定人员在视频会议中需要陈述其基本信息，包括姓名、地址、组织名称、电话号码、身份证类型（护照、居民身份证、驾驶执照等）以及身份证号码。

指定人员还需按要求在视频会议中出示身份证件。视频会议结束后，亚洲诚信CA会根据审核结果批准或拒绝身份验证请求，并将录像安全归档。

3.2.2.3 机构商业名称的验证

申请人组织可以请求在证书中包含假定名称，但申请组织必须已经向其注册成立或注册地管辖范围内的相关政府机构登记了其对假定名称的使用，且其假名备案仍然有效。

亚洲诚信CA将通过以下任意一项途径来核实假定名称的真实性：

1. 通过QGIS或直接通过邮件、电话、网址联系相关政府机构核实；
2. 当QIIS已经向相应的政府机构验证了假定名称，亚洲诚信CA可以通过使用QIIS验证；
3. 通过经验证的专业意见函，意见函中需表明申请组织开展业务时所使用的假定名称、注册该假定名称的政府机构，并且该备案仍然有效。

3.2.2.4 所在国的验证

若证书主题项包含国家字段，亚洲诚信CA将通过3.2.2.1章节中申请者提供的机构证明信息进行所在国家的确认。

3.2.2.5 域名的确认和鉴别

用户在申请标志证书时，亚洲诚信CA需要验证申请者对所申请证书中域名的控制权，此验证过程由亚洲诚信CA执行，不会委托给第三方。

亚洲诚信CA会维护每个域名的验证记录，包括使用了哪种验证方法以及对应的MC版本号。

3.2.2.5.1 验证申请人为域联系人

亚洲诚信CA不支持此方法。

3.2.2.5.2 向域联系人发送电子邮件、传真、短信或邮政信件

亚洲诚信CA不支持此方法。

3.2.2.5.3 域联系人电话联系

亚洲诚信CA不支持此方法。

3.2.2.5.4 构造电子邮件到域联系人

按照MCR第3.2.14.4节中的定义，构造电子邮件至域联系人。

通过以下方式使用构建的电子邮件地址直接与域联系人通信，确认申请人对请求的 FQDN 的控制：

1. 将电子邮件发送到一个或多个通过使用“admin”、“administrator”、“webmaster”、“hostmaster”或“postmaster”作为邮件地址部分，后跟符号 (“@”)，再后跟待验证的域名，
2. 在电子邮件中包含一个随机值，以及
3. 让申请人向亚洲诚信CA的服务器提交（通过单击或其他方式）随机值以确认接收和授权。

亚洲诚信CA可以重新发起电子邮件，包括重新使用随机值，邮件内容和收件人将保持不变。

唯一的随机值由亚洲诚信CA生成，并在生成之日起有效期不超过30 天。

3.2.2.5.5 域名授权文件

亚洲诚信CA不支持此方法。

3.2.2.5.6 商定的网站变更

亚洲诚信CA不支持此方法。

3.2.2.5.7 DNS 变更

按照MCR第3.2.14.7节中的定义，订户通过为待验证域名解析指定的带随机值或请求令牌的TXT或CNAME记录，亚洲诚信CA能够查询到指定记录即可完成域名所有权验证。

唯一的随机值由亚洲诚信CA 生成，并在生成之日起有效期不超过30 天。若域名通过此方式完成控制权验证，亚洲诚信CA可以为此域名以及以此域名结尾的下级域名签发证书。

3.2.2.5.8 IP地址

亚洲诚信CA不支持此方法。

3.2.2.5.9 测试证书

亚洲诚信CA不支持此方法。

3.2.2.5.10 使用TLS随机数

亚洲诚信CA不支持此方法。

3.2.2.5.11 任何其他方法

亚洲诚信CA不支持此方法。

3.2.2.5.12 验证申请人为域名联系人

亚洲诚信CA不支持此方法。

3.2.2.5.13 向 DNS CAA 联系人发送电子邮件

亚洲诚信CA不支持此方法。

3.2.2.5.14 向 DNS TXT 联系人发送电子邮件

按照MCR第3.2.14.14节中的定义，亚洲诚信CA将发送验证邮件到通过DNS查询到的“_validation-contactemail.待验证域名”TXT 解析的域名联系人邮箱。验证邮件中会包含一个唯一的随机值，订户收到验证邮件后，访问带随机值的验证链接，点击批准后即可完成域名所有权验证。

唯一的随机值由亚洲诚信CA 生成，并在生成之日起有效期不超过30天。若域名通过此方式完成控制权验证，亚洲诚信CA可以为此域名以及以此域名结尾的下级域名签发证书。

3.2.2.5.15 电话验证域名联系人

亚洲诚信CA不支持此方法。

3.2.2.5.16 向DNS TXT 中电话联系人进行电话联系

亚洲诚信CA不支持此方法。

3.2.2.5.17 向DNS CAA 中电话联系人进行电话联系

亚洲诚信CA不支持此方法。

3.2.2.5.18 商定的网站变更v2

按照MCR第3.2.14.18节中的定义，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值或请求令牌。亚洲诚信CA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。

唯一的随机值由亚洲诚信CA生成，并在生成之日起有效期不超过30天。若域名通过此方式完成控制权验证，亚洲诚信CA仅可为此域名签发证书。亚洲诚信CA支持http协议层发起的状态码为301、302的重定向请求验证，重定向后的地址必须和验证域名一致，可以采用http或者https方式，且端口必须是默认授权访问的。

3.2.2.5.19 使用ACME方式的网站变更

按照MC要求第3.2.14.19节中的定义，通过使用RFC 8555第8.3节中定义的ACME HTTP质询方法验证FQDN的域控制，确认申请人对FQDN的控制。

令牌唯一随机值（RFC 8555第8.3节中所定义）由亚洲诚信CA生成，自生成之日起30天内有效。

亚洲诚信CA支持http方式发起的状态码为301、302的重定向请求验证，重定向后的地址必须和验证域名一致，可以采用http或者https方式，且端口必须是默认授权访问的。此方法不用于验证通配符域名。

3.2.2.5.20 使用TLS的ALPN扩展

亚洲诚信CA不支持此方法。

3.2.2.6 标志证书的CAA记录

见本CPS第4.2.4节。

3.2.2.7 普通标志证书中标志验证

普通标志证书分为先前使用标志证书和修改的注册商标证书。

3.2.2.7.1 验证先前使用标志证书

1. 这种类型的标志证书适用于非注册商标的普通标志。

申请人应向亚洲诚信CA提供其希望包含在标志证书中的 SVG 格式标志表现形式。亚洲诚信CA将核实以下内容：

a. 当前网址上展示的商标必须与申请证书时提供的标志图样相符合。并且申请人对网址域名拥有的控制权必须通过MCR要求第3.2.14节规定的至少一种方式进行验证；
b. 与该标志表现形式匹配的标志，在标志验证日期之前的至少12个月，就已显示在上述经验证由申请人控制的同一域名上。历史显示记录必须通过“网页存档资源（Archive Webpage Sources）”进行验证。亚洲诚信CA必须在验证过程中可以获取标志表现形式的网址并将其写入相应证书字段。

亚洲诚信CA还将保留申请人提供的标志表现形式的截图或其他记录，以及在上述验证过程中发现的所有标志图像。

2. 亚洲诚信CA执行的Mark Representation验证将使用以下存档网页来源之一：
    - https://archieve.org

此核准名单可能会不时修改。

3. 颜色限制：基于先前使用证明的标志证书，其标志表现形式需遵循相关司法管辖区适用于普通标志的相同颜色规则，需与先前使用时的颜色保持一致。亚洲诚信CA将审查先前使用情况，以确定标志所有人所主张的任何特定验证。

3.2.2.7.2 验证修改的注册商标证书

亚洲诚信CA将根据以下验证要求，对申请人拟修改的注册商标进行验证。申请人需提供其希望包含在标志证书中的SVG格式的标志表现形式。

1. 商标表现形式的确认

亚洲诚信CA可以接受以下几种对注册商标在标志表现形式中的修改方式：

a. 组合商标：对于组合商标，任何文字标志要素的位置可以相对于设计标志要素进行重新排列。
b. 图形商标和组合商标：对于图形商标和组合商标，可以移除部分外观设计要素，移除部分不得超过外观

设计要素的49%，剩余部分不得更改。对于组合商标，文字标志的要素可以按照a)条所述，但相对于剩余的设计标志要素需要进行调整。

c. 文字商标和组合商标：对于文字商标以及文字标志要素由单个单词组成的组合商标，该单词可以被分成多个部分，这些部分可以堆叠排列，也可以不堆叠排列。

d. 文字商标和组合商标：对于文字商标以及文字标志要素由多个单词组成的组合商标，该单词可以被分成多个部分，这些部分可以堆叠排列，也可以不堆叠排列，或者可以将多个单词合并为一个单词。

e. 修改后的注册商标可以采用任何字体或颜色，并可以搭配彩色背景或图案背景。

亚洲诚信CA会验证修改后的标志表现形式，以确定该修改是否对原始标志（与注册商标相比）的显而易见含义造成了重大改变。如果造成重大改变，亚洲诚信CA将通知申请人，其所提交的修改不能被接受，必须进一步修改。申请人可以选择继续申请提交修改后的标志证书。

作为接受对注册商标的标志表现形式进行修改的条件，亚洲诚信CA可以要求申请人就因该修改而可能由任何一方引起的任何索赔进行辩护、赔偿并使亚洲诚信CA免受损害。

2. 商标国家或地区验证

亚洲诚信CA必须验证注册商标的商标局所在国家或地区，并以WIPO ST.3标准里的两字母国家以及政府间/区域机构代码的形式填写。

3. 商标局名称验证

当商标所述的国家或地区拥有超过一个可以注册商标的国家或地区级知识产权机构时，为了消除歧义，亚洲诚信CA会明确具体机构。当该国家或地区只有一个官方商标注册机构时，亚洲诚信CA可不做明确。

亚洲诚信CA会通过插入WIPO国家和地区知识产权机构名录中“办公室”栏中列出的商标局名称标识商标局以及亚洲诚信CA认可的可靠数据来源。

4. 商标号验证

申请人必须向亚洲诚信CA提供商标号，亚洲诚信CA会验证商标局分配的用于识别注册商标或注册商标申请的商标号与申请人提供的是否一致。并且，亚洲诚信CA还会通过获取相关商标局的官方数据库或WIPO全球品牌数据库核实该商标号对应的商标是否处于“良好状态”。

3.2.2.8 已验证的标志证书中商标验证

亚洲诚信CA为已在商标局注册并符合注册商标资格的商标颁发已验证的标志证书。已验证的标志证书类型分为注册商标证书和政府标志证书。亚洲诚信CA将通过以下方式中的其中一项验证已验证的标志证书中的商标。

3.2.2.8.1 验证注册标志证书

1. 商标局的商标验证

亚洲诚信CA将验证订阅者提供的：

a. 注册商标的商标注册号以及授予该商标注册的商标局名称；

b. 申请人希望包含在验证的标志证书中的SVG格式的标志表现形式。

注册商标必须有效，且必须通过查阅相关商标局的官方数据库进行验证，才可以准许包含在VMC证书中。

作为替代方案，亚洲诚信CA可以通过WIPO全球品牌数据库（https://www.wipo.int/reference/en/branddb/）验证注册商标。

2. 注册商标所有权或许可验证

亚洲诚信CA将确认，在相关商标局官方数据库或WIPO全球品牌数据库中识别的注册商标所有者与通过本CPS第3.2.2.1章中核实的主体组织是同一组织，或是该组织的母公司、子公司或关联公司。

如果注册商标的所有者不是该组织，则主体组织必须已通过与注册商标登记所有者（或所有者的母公司、子公司或关联公司）签署的双方同意的许可协议，获得了该注册商标的使用权。

如果注册商标的所有者不是申请人，除非亚洲诚信CA获得注册商标登记所有者出具的授权书，否则将不为该注册商标颁发证书。

3. 商标表现形式的确认

亚洲诚信CA将核实申请人提交的商标是否与已注册商标完全一致。此项验证会通过将商标与相关商标局的官方数据库或WIPO全球品牌数据库进行对比的方式予以记录。

4. 颜色限制

组合标志和外观设计标志的验证商标证书只能显示相关商标局明确允许注册商标使用的颜色范围。亚洲诚信CA将审查该注册商标，以确定注册商标所有人所主张的任何特定颜色。

5. 商标国家或地区验证

参考本CPS 3.2.2.7.2（2）。

6. 商标局名称验证

参考本CPS 3.2.2.7.2（3）。

7. 商标号验证

参考本CPS 3.2.2.7.2（4）。

3.2.2.8.2 验证政府标志证书

亚洲诚信CA为政府实体或非商业实体（国际组织）授予或声称拥有的标志，或由政府实体或非商业实体（国际组织）通过官方法令、条例、条约或政府行为授予给某个私营组织或其他组织的标志。该标志应与相关法令、条例、条约或政府行为中所呈现或描述的一致，并须经商标验证机构确认。

1. 法令、法规、条约或行为的验证

亚洲诚信CA必须通过核实官方法令、条例、条约或政府行为中的公开记录，来确认该政府标志已授予或已被声称由政府实体或非商业实体（国际组织）所拥有。

政府标志也可以通过官方法令、条例、条约或政府行为，由政府实体或非商业实体授予给私营组织或其他类型的组织。

亚洲诚信CA将保存相关法令、条例、条约或政府行为的副本，包括所有官方参考信息（例如法规或条例编号及其管辖范围），以及法令或条例中所包含或引用的该标志的副本。亚洲诚信CA还将保留申请人提供的标志表现形式的截图或其他记录，以及从相关法令、条例、条约或政府行为中获得的用于支持政府标志验证的所

有信息。授予或声明该政府标志的官方法令、条例、条约或政府行为的具体引用会包含在证书里。亚洲诚信CA可以使用缩写，并且会尽可能符合相关司法管辖区关于此类官方法令、条例、条约或政府行为通常引用方式的适用法律指南（例如，《蓝皮书：统一引证体系》或其他类似的标准引证体系）。

2. 政府标志所有权或许可验证

亚洲诚信CA需确认（1）中确定的政府标志所有者与通过本CPS第3.2.2.1章中核实的主体组织是同一组织，并且已通过相关法令、法规、条约或政府行为，或通过双方认可的许可协议，获得了该政府标志的使用权。

当政府标志的所有者不是申请人时，申请人只有在亚洲诚信CA获得政府标志登记所有人的书面授权书后方可使用该政府标志。

在确定申请人是否为对应标志表现形式的政府标志的所有者或被许可人时，亚洲诚信CA将根据（1）中要求保存的记录中，保留其决策及理由。

3. 商标表现形式的确认

亚洲诚信CA会确认申请人提交的标志表现形式与根据（1）中确认的政府标志相匹配并保留相关决策及理由。

4. 颜色限制

验证标志证书中包含的组合标志和设计标志的标志表现形式，仅限使用经亚洲诚信CA验证的法令、法规、条约或政府行为所允许该政府标志使用的颜色。

亚洲诚信CA将审查提交的政府标志，以确定主体组织对于订阅者所提交的标志表现形式中的颜色拥有何种权利。

亚洲诚信CA会根据(1)的要求，判定订阅者提交的标志表现形式中的颜色是否符合经亚洲诚信CA 验证的法规、条例、条约或政府行为所允许的颜色。

5. 设立政府标志的政府实体所属的主管法律管辖区

亚洲诚信CA必须验证设立政府标志的政府实体所属的主管法律管辖区，具体验证项为法令所在国家、法令所在州/省、法令所在地。

验证内容为：除非与通过法令、条例、条约或政府行为设立政府标志的政府实体或非商业实体（国际组织）的级别相关，否则证书不得包含以下字段。

比如，在国家层面运营的政府实体或非商业实体（国际组织）的管辖范围必须包含“法令所在国家”字段，但不得包含“法令所在州/省”和“法令所在地”字段。

适用的政府实体或非商业实体（国际组织）在州或省级别的管辖范围必须包含“法令所在国家”和“法令所在州/省”字段，但不得包含“法令所在地”字段。

适用的政府实体或非商业实体（国际组织）在地方级的管辖范围必须包含“法令所在国家”和“法令所在州/省”字段以及“法令所在地”字段。

亚洲诚信CA会使用两字母ISO国家/地区代码指定“法令所在国家”字段。

“法令所在州/省”和“法令所在地”字段将使用适用管辖区的全称指定。

3.2.3 个人身份的鉴别

亚洲诚信CA的证书颁发对象必须是申请人，即组织实体。但在亚洲诚信CA的证书颁发过程中将会验证申请人代表的个人身份，申请人代表必须是自然人，可以是申请组织的授权员工或授权代理人。亚洲诚信CA会使用3.2.2.1章节的验证方式与申请人代表核实申请人的申请意愿。

申请人代表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CA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。

对于申请标志证书的商业实体类型组织，亚洲诚信CA将会按照3.2.2.1.3中的要求，对“主要个人”进行“面对面验证”。

3.2.4 未验证的订户信息

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，验证来自于可信第三方数据源，未经验证的信息不得写入证书。

3.2.5 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CA对申请人的授权验证包括：

1. 申请组织相关角色人员的验证：

亚洲诚信CA将验证证书经办人、证书审批人以及合同签署人的姓名、职务及授权；并且审查这些角色人员是否被列入拒绝人员名单中。若被列入名单中，亚洲诚信CA有权拒绝签发证书或要求更换相关联系人。亚洲诚信CA将会通过第3.2.2.1节中的验证方式选择有效通讯方式跟证书经办人或证书审批人联系，获得足够肯定的答复，以此验证申请代表人申请证书的真实性。

证书经办人：标志证书申请的提交者以及订单审核的联系人。证书经办人是一个自然人，可以是申请组织的雇员或具有明确授权代表申请组织提交证书申请的授权代理人。

证书审批人：标志证书请求批准的审批人。证书审批人是一个自然人，可以是申请组织的雇员或具有明确授权代表申请组织批准证书申请的授权代理人。

合同签署人：标志证书订户协议的签署人，合同签署人是一个自然人，可以是申请组织的雇员或具有明确授权代表申请组织签署订户协议的授权代理人。

申请组织可以授权一个人担任其中的两个或多个角色，申请组织也可以授权一个以上的人担任这些角色中的任何一个。

2. 订户协议的签名验证

亚洲诚信CA要求合同签署人或被正式授权的个人必须签署订户协议并同意使用条款。对于订户协议的签名，亚洲诚信CA将要求订户在下单页面完成。

3. 证书请求的签名验证

亚洲诚信CA要求证书审批人必须签署证书请求，亚洲诚信CA会通过电子邮件的方式发送在线批准链接，证书审批人完成在线批准。

3.2.6 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CA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CA CP&CPS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。

亚洲诚信CA会披露签发的所有交叉证书。

3.3 密钥更新请求的标识与鉴别

订户自行生成的密钥，亚洲诚信CA会依赖之前提供或获得的信息进行密钥更新请求的鉴别。

3.3.1 常规密钥更新的标识与鉴别

亚洲诚信CA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。

3.3.2 撤销后密钥更新的标识与鉴别

亚洲诚信CA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CA的证书业务中，证书撤销请求可以来自订户、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，商标冲突方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。另外，当亚洲诚信CA有本CP&CPS第4.9.1.1节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CA提交请求，亚洲诚信CA通过与证书保障级别相应的方式来确认要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。

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CA提供的任何数据负责。亚洲诚信CA维护一个包含所有先前因怀疑网络钓鱼或其他欺诈用途而被吊销的证书及被拒绝的证书请求的内部数据库，亚洲诚信CA利用此数据库识别后续的可疑请求。

VMC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CA提供密钥对的公钥（经签名的CSR）；
    - 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、本CP&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CA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CA接收到订户的证书申请后，亚洲诚信CA验证团队会按本CP&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CA会维护系统和流程，以便根据CP&CPS充分验证申请人的身份。通过电话、传真或电子邮件进行沟通的内容将与申请者通过亚洲诚信CA WEB界面或者API直接提供的所有信息一起安全存储。

申请人信息必须包含至少一个完全限定域名，该域名将包含在证书的使用者备用名称扩展中。

在普通标志证书中的信息时，若亚洲诚信CA根据本CP&CPS第3.2章节指定来源获得的数据证明文件不超过398天且该信息未发生变化，则亚洲诚信CA可使用该数据或证明文件；对于已验证的标志证书，亚洲诚信CA根据本CP&CPS第3.2章节指定来源获得的数据证明文件不超过1858天且该信息未发生变化，则亚洲诚信CA可使用该数据或证明文件。

对于上述398天验证数据重用存在例外情况，亚洲诚信CA维护一个由订户授权的最新授权代表系统，在此系

统中的授权代表只要和亚洲诚信CA在证书有效期内有直接联系，则无需对订户重复验证。

4.2.2 证书申请批准和拒绝

亚洲诚信CA不签发包含内部名称和保留IP地址的证书。

4.2.2.1 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，通过签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CP&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CA有权拒绝证书申请：

1. 该申请不符合本CP&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。
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CA将会邮件通知订户证书申请失败。

4.2.3 处理证书申请的时间

在正常情况下，亚洲诚信CA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CA的管理要求。证书申请请求会持续有效直至被拒绝。

4.2.4 CAA记录

对于标志证书，在证书签发前，对证书申请中的所有备用名称中的域名进行DNS CAA记录检查。

亚洲诚信CA根据MCR中的规定处理CAA记录中"issuevmc"，"iodef"属性标签。

亚洲诚信CA在处理CAA记录中的属性标签时，不会对"iodef"属性标签的内容进行操作。亚洲诚信CA识别关键标签，但遇到关键标签中设置了无法识别的属性时，将拒绝为其签发证书。

CAA记录中若存在"issuevmc"标签，且其值不包含"trustasia.com"，亚洲诚信CA将拒绝为其签发相应证书。

CAA查询若出现以下失败情况，亚洲诚信CA仍可为其签发证书：

1. CAA查询失败不是由亚洲诚信CA的基础设施引起的，和
2. 亚洲诚信CA至少重试过一次查询，和
3. 域名所在域不存在指向ICANN根域的DNSSEC验证链。

亚洲诚信CA将在查询CAA记录的有效期（有效期以CAA记录的生存时间或8小时中的较大值为准）内，向订户签发证书；同时也将详细记录CAA记录阻止的潜在签发。

4.3 证书签发

4.3.1 证书签发中CA的行为

对于订户证书，亚洲诚信CA在签发之前确认证书请求的来源。在颁发标志证书之前，会将该证书的预证书记录到一个或多个受认可的证书透明度日志中。

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。

根CA的证书签发过程由亚洲诚信CA授权的个体（CA系统操作员、系统管理员或PKI管理员）手动发出明确的指令，以便根CA执行证书签名操作。

亚洲诚信CA不直接从其根证书签发最终实体证书。

在证书签发期间发生的数据库存储和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户。

亚洲诚信CA为所有能够直接签发证书的账户部署了多因素认证。

4.3.2 对订户证书签发的通告

亚洲诚信CA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CA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签发的证书。

订户被认为接受已签发的证书的行为包括但不仅限于：

1. 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。
2. 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。
3. 证书获取通知发送给订户后，订户通过该通知下载证书。

4. 订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容。

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。亚洲诚信CA视订户证书使用场景，同时会根据BIMI Group MCR的要求，选择将证书发布在一个或多个受认可的CT日志服务器中。

4.4.3 CA对其他实体的通告

亚洲诚信CA将不对其他实体进行通告。

4.5 密钥对的使用

4.5.1 订户私钥和证书的使用

标志证书订户私钥无需保护，可在使用后丢弃，因为公钥仅用于标志表现形式的标识，不用于加密通信。

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. 验证证书的有效期，确保证书在有效期内使用；
3. 确认该签名对应的证书是依赖方信任的证书；
4. 通过查询CRL或OCSP确认该签名对应的证书是否被撤销；
5. 证书的用途适用于对应的签名；
6. 使用证书上的公钥验证签名。
7. 考虑本CP&CPS或其它地方规定的其它信息

以上条件不满足的话，依赖方有责任拒绝签名信息。

4.6 证书更新

4.6.1 证书更新的情形

对于亚洲诚信CA签发的订户证书，证书到期前可以进行证书更新。订户选择保留原有密钥对重新签发证书。在证书到期前，亚洲诚信CA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CP&CPS第4.2.1章节规定的期限，则亚洲诚信CA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CP&CPS第4.2.1章节规定的期限，则亚洲诚信CA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CA证书的订户或其他授权代表人。

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：

a. 订户的原证书存在并且由亚洲诚信CA所签发；

b. 证书更新请求在许可期限内；

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CP&CPS第3.3.1章节之规定进行处理；亚洲诚信CA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CA才可以批准签发证书。

4.6.4 签发新证书时对订户的通告

同CP&CPS第4.3.2章节。

4.6.5 构成接受更新证书的行为

同CP&CPS第4.4.1章节。

4.6.6 CA对更新证书的发布

同CP&CPS第 4.4.2章节。

4.6.7 CA对其他实体的通告

同CP&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）丢失或泄漏或订户认为原有证书和密钥不安全；
2. 订户证书，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. 订户证书即将到期且认为更新证书时需要更新密钥。
5. 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CA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CA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CP&CPS第4.6.3章节的描述。

4.7.4 签发新证书时对订户的通告

同CP&CPS第4.3.2章节。

4.7.5 构成接受密钥更新证书的行为

同CP&CPS第 4.4.1章节。

4.7.6 CA对密钥更新证书的发布

同CP&CPS第 4.4.2章节。

4.7.7 CA对其他实体的通告

同CP&CPS第 4.4.3章节。

4.8 证书变更

4.8.1 证书变更的情形

当证书非主体信息发生变更时，可以发起证书变更。

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

如果符合以下条件，依据先前已验证的证书请求颁发替换证书，所引用的证书并非因欺诈或其他非法行为而被吊销。

1.补发证书的有效期与被替换的MC的有效期相同，并且

2.证书的主题信息与被替换的 MC 中的主题相同。

4.8.4 签发新证书时对订户的通告

同CP&CPS第4.3.2章节。

4.8.5 构成接受变更证书的行为

同CP&CPS第 4.4.1章节。

4.8.6 CA对变更证书的发布

同CP&CPS第 4.4.2章节。

4.8.7 CA对其他实体的通告

同CP&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

亚洲诚信CA在订户协议中列出以上撤销原因，并提供有关何时选择每个选项的解释。亚洲诚信CA 向订户提供的撤销工具可以让订户自行指定原因，当订户不选择时，默认值为“unspecified（0）”，此时CRL中没有提供“reasonCode”扩展。

1. 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，并使用相应的CRLReason：

a. 订户以书面形式请求撤销证书；

b. 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；

c. 亚洲诚信CA获得证据，证书中所包含的域名的控制权验证已不再可靠。

2. 若出现以下情况的一种或多种，亚洲诚信CA宜在24小时内撤销证书，且必须在5天内撤销证书，并使用相应的CRLReason:

a. 亚洲诚信CA获悉证书不再符合BR第6.1.5节及第6.1.6节的相关要求；

b. 亚洲诚信CA获得了证书遭到误用的证据；

c. 亚洲诚信CA获悉订户违反了订户协议、CP&CPS中的一项或多项重大义务；

d. 亚洲诚信CA获悉任何表明 FQDN或电子邮件地址的使用不再被法律许可（例如，某法院或仲裁员已经撤销了域名注册人使用域名的权力，域名注册人与申请人的相关许可及服务协议被终止，或域名注册人未成功续期域名，或证书正式的电子邮件地址不再被订户合法使用）；

e. 亚洲诚信CA获悉证书中所含信息出现重大变化；

f. 亚洲诚信CA获悉证书的签发未能符合亚洲诚信CA的CP&CPS；

g. 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；

h. 亚洲诚信CA依据 BIMI Group MCR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；

i. 除本4.9.1.1节中描述的情况外，其他根据亚洲诚信CA的CP&CPS要求进行撤销订户证书；

j. 亚洲诚信CA收到侵权法院命令，确认该法院命令的真实性，并向订户发出3个工作日的通知；

k. CP&CPS中职责的履行被延迟或受不可抗力的阻碍；自然灾害；计算机或通信失败；法律、规章或其它

法律的改变；政府行为；或其它超过个人控制的原因并且对他人信息构成威胁的；

l. 亚洲诚信CA已经履行催缴义务后，订户仍未缴纳服务费；

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. 中级证书签发机构正式书面申请撤销；
2. 中级证书签发机构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，或不再符合BR第6.1.5节及第6.1.6节的相关要求；
4. 亚洲诚信CA获得了证书遭到误用的证据；
5. 亚洲诚信CA获悉中级证书的签发未能符合BR要求，或中级CA未能符合CP&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. 亚洲诚信CA依据BR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；
9. 本CP&CPS要求撤销中级CA证书。

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，商标冲突方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. 订户向亚洲诚信CA提交撤销证书申请及相关身份证明材料，申请材料中需说明撤销原因；
2. 亚洲诚信CA按本CP&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CA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；
5. 亚洲诚信CA提供7*24小时的证书撤销申请服务，订户可通过本CP&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CA有充分的理由确信出现本CP&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、商标冲突方或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；

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CP&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CA不支持撤销请求宽限期。

4.9.5 CA处理撤销请求的时限

亚洲诚信CA在收到撤销请求后的24小时内，将调查与撤销请求相关的事实和情况，并向订阅者和提交撤销请求的实体提供初步调查报告。对于法院侵权裁定，亚洲诚信CA将在商业合理的期限内核实事实并采取行动。

在审查事实和情况后，CA 将协助订户以及上报该证书初步报告或其他撤销相关的实体，以确定是否撤销证书或采取其他合理处置方式。如果确定撤销，CA将从收到撤销请求或与撤销相关的通知到发布撤销的时间不会超过第4.9.1.1中规定的时间范围。

撤销的时间，CA 将考虑以下标准：

1. 问题的性质（范围、背景、严重性、严重程度、伤害风险）；
2. 撤销的后果（对订户和依赖方的直接和附带影响）；
3. 收到的关于特定证书或订户的撤销请求数量；
4. 提出投诉的实体（例如，执法人员对网站从事非法活动的投诉比消费者声称他们没有收到他们订购的商品的投诉更重要）；和
5. 相关立法。

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

CRL可以通过公开的HTTP URL来访问。在签发第一张证书后的24小时内，CA会生产并发布：

- 完整的CRL，或
- CRL分区、聚合时可以恢复完整的CRL。

签发订户证书的CA：

1. 至少7天更新并发布新的CRL，CRL最大有效期不超过10天；
2. 在证书撤销后的24小时内更新并发布新的CRL。

签发CA证书的CA：

1. 至少每12个月更新并发布新的CRL；
2. 在证书撤销后的24小时内更新并发布新的CRL。

CA会一直发布CRL，直到以下情况：

- 所有包含相同主题公钥的CA证书均已过期或者被撤销；或者
- 相应的CA私钥被销毁。

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 在线撤销/状态查询的可用性

OCSP响应的有效时间间隔是 thisUpdate和 nextUpdate字段之间的时间差，包括边界。在计算时间差时，3,600 秒等于一小时，86,400 秒等于一天，忽略闰秒。

对于以下证书序列号的情况，证书标记为“assigned”：

1. 具有该序列号的证书或预签名证书由签发CA签发，或者
2. 具有该序列号的证书或预签名证书由与签发CA关联的预证书签名证书签发。

对于序列号未被标记为“assigned”的证书，则标记为“unassigned”。

以下内容适用于包含带有id-ad-ocsp访问方法的授权信息访问扩展的证书和预证书。

亚洲诚信CA提供的OCSP请求服务支持GET和POST两种方法，亚洲诚信CA按照RFC 8954的规定处理Nonce扩展（1.3.6.1.5.5.7.48.1.2）。

对于订户或预签名证书的状态：

- 在证书或预签名证书首次发布或以其他方式提供后不超过15分钟内，提供正确的OCSP响应；
- 如果OCSP响应的有效时间间隔小于十六小时，亚洲诚信CA在nextUpdate前的有效期一半之前更新通过在线证书状态协议提供的信息；

如果OCSP响应的有效时间间隔大于或等于十六小时，亚洲诚信CA在nextUpdate前至少八小时并且在thisUpdate后不超过四天内更新通过在线证书状态协议提供的信息，订户证书OCSP响应的有效时间间隔大于或等于八小时并且小于或等于十天。

对于下级CA证书的状态：

亚洲诚信CA至少每十二个月更新一次通过在线证书状态协议提供的信息；并且在吊销下级CA证书后的24小时内更新信息。

以下内容适用于OCSP响应者需要做出响应的证书状态。

亚洲诚信CA提供的 OCSP响应符合RFC 6960和/或RFC 5019，OCSP响应满足以下任一条件：

1. 由正在检查其撤销状态的签发证书的CA签名，或者

2. 由OCSP响应器签名，该响应器的证书由签发正在检查其撤销状态的证书的 CA签名。

如果OCSP响应器收到“unassigned”序列号的证书状态请求，则响应器不以“good”状态作出响应。

4.9.10 在线撤销检查要求

与RFC6960一致。

4.9.11 其它形式的撤销公告

不适用。

4.9.12 密钥泄漏的特别要求

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CP&CPS要求撤销密钥受损的证书，并重发证书。

任何依赖方发现私钥泄露，可通过邮箱（revoke@trustasia.com）向亚洲诚信CA报告，邮件中需要提供私钥泄露的证据：

1. 私钥本身；
2. 用泄露私钥签名的CSR，CSR 通用名称为“Proof of Private Key Compromise for TrustAsia”；
3. 通过RFC 8555第7.6节中定义的ACME协议的证书撤销方法证明私钥泄露。

4.9.13 证书挂起的情形

亚洲诚信CA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CA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（7*24）提供。亚洲诚信CA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。

亚洲诚信CA全天候（7*24）响应优先级较高的证书问题。在适当情况下，亚洲诚信CA将此类疑问转交给执法机构，并且撤销此类疑问有关的主题证书。

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

以下情况将被视为用户终止使用亚洲诚信CA提供的证书服务：

1. 证书到期后未按时续缴服务费；
2. 证书到期后没有进行证书更新或密钥更新；
3. 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。

4.12 密钥生成、备份与恢复

不适用。

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

亚洲诚信CA 开发、实施和维护完整的安全计划旨在：

1. 保护证书数据和证书管理流程的机密性、完整性和可用性；
2. 防止对证书数据和证书管理流程的机密性、完整性和可用性的预期威胁或危害；
3. 防止未经授权或非法访问、使用、披露、更改或破坏任何证书数据或证书管理流程；
4. 防止任何证书数据或证书管理流程意外丢失、毁坏或损坏；和
5. 遵守法律适用于 CA 的所有其他安全要求。

亚洲诚信CA的证书管理流程包括：

1. 物理安全和环境控制；
2. 系统完整性控制，包括配置管理、可信代码的完整性维护和恶意软件检测/预防；
3. 网络安全和防火墙管理，包括端口限制和IP地址过滤；
4. 用户管理、独立的受信任角色分配、教育、意识和培训；和
5. 逻辑访问控制、活动日志记录和不活动超时，以提供个人责任制。

亚洲诚信CA 的安全计划包括年度风险评估，其中：

1. 识别可预见的内部和外部威胁，这些威胁可能导致未经授权访问、披露、滥用、更改或破坏任何证书数据或证书管理流程；
2. 评估这些威胁的可能性和潜在损害，同时考虑证书数据和证书管理流程的敏感性；和
3. 评估CA为应对此类威胁而制定的政策、程序、信息系统、技术和其他安排的充分性。

根据风险评估，亚洲诚信CA制定、实施和维护安全计划，该计划由安全程序、措施和产品组成，旨在实现上述目标，并管理和控制风险评估期间确定的风险，与证书数据和证书管理过程的敏感性。安全计划包括与证书数据和证书管理过程的敏感性相适应的管理、组织、技术和物理保障措施。安全计划还考虑当时可用的技术和实施具体措施的成本，并应实施合理的安全级别，以适应安全漏洞和受保护数据的性质可能造成的危害。

5.1 物理控制

5.1.1 场地位置与建筑

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

5.1.1.2 管理服务区

服务区是亚洲诚信CA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指纹鉴别才可以进入，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指纹鉴别才可以进入。

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指纹鉴别才可以进入，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数据中心安装了具有以下功能的门禁系统：

1. 采用门禁卡和指纹鉴别的控制方式控制每道门的进入；
2. 进出每一道门都有日志记录；
3. 管理服务区和核心区的门都设有强开报警和超时报警；
4. 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，监控无盲区，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，重大事件视频单独存档，以备查询。设置非法入侵检测报警、环境控制检测报警，声光报警，同时通知运维人员。

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出现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。

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。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，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。

5.1.7 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，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理销毁。

在处理作废内容时，至少2名可信人员在场。

5.1.8 异地备份

亚洲诚信CA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：

1. 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；
2. 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；
3. 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；
4. 安全管理人员：负责场地安全、日常安全管理工作；
5. 安全审计人员：负责对业务操作行为进行审计；
6. 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CA在具体业务规范中对关键任务进行严格控制。对以下敏感操作实施多个可信角色共同完成，例如：

1. 屏蔽区场地访问：设置为2个可信人员进出模式；
2. 鉴别、审核和签发证书：需要2个可信人员共同完成；

3. 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；
4. CA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 ；
5. CA系统后台操作：需要2个可信人员共同完成；
6. 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，通过门禁卡和指纹识别进行鉴别，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CA的可信角色由不同的人担任。对于MC证书，亚洲诚信CA确保没有任何一个人可以单独验证和授权签发此类证书，且此类控制是可审计的。

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：

1. 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。
2. 通过电话、网络等形式对其提供的材料的真实性进行鉴定。
3. 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。
4. 完成调查后，将结果上报主管相关工作的领导进行批准。
5. 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，将员工参加培训的情况形成记录并存档。这些培训包括：

1. 基本公钥基础设施（PKI）知识；
2. CP&CPS及相关标准和程序；
3. 身份认证和验证政策和程序；
4. 安全管理策略和机制；
5. 灾难恢复和业务连续性程序；
6. 岗位职责统一要求；
7. CA/Browser论坛的BR、EVG等指南；
8. 国家关于电子认证服务的法律、法规及标准、程序；
9. 其他需要进行的培训等

履行信息验证职责的审核人员，必须在上岗前接受上述全部培训，以确保其能令人满意地履行职责。审核人员须通过亚洲诚信CA定期安排的相关知识考核，以确保其具备履行职责所需技能。

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，不定期接受亚洲诚信CA组织的培训一次。对于认证系统运营相关的人员，相关技能和知识培训应达到任职要求一致的水平。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频率

亚洲诚信CA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CA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CA提供给人员的文档通常包括但不限于以下几类：

1. CP&CPS及相关标准与规范；
2. 员工手册；
3. 岗位职责说明书、工作流程和规范；
4. 内部操作文件，包括业务连续性管理和灾难恢复方案；
5. 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CA将记录处理证书申请和签发证书所采取行动的细节，包括产生的所有信息和收到的与证书申请相关的文件、时间和日期、以及参与人员。

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：

1. CA 证书及密钥生命周期管理事件，包括：

a. 密钥的生成、备份、存储、恢复、归档和销毁；
b. 证书请求、续期和更新密钥请求，以及撤销；
c. 证书申请的批准和拒绝，包括成功或失败的证书操作；
d. 加密设备生命周期管理事件，包括：设备接收、安装、卸载、激活、使用、维修等；
e. CRL条目的生成；
f. 签署OCSP响应；
g. 引入新证书配置和淘汰现有证书配置的记录。

2. 订户的生命周期管理事件：

a. 证书请求、更新、更新密钥请求和撤销；
b. BIMI Group要求及本CP&CPS中规定的所有验证活动；
c. 证书请求的接受和拒绝，包括接受订户协议，申请资料的验证、申请及验证资料的保存等；
d. 证书的签发；

e. CRL条目的生成；
f. 签署OCSP响应；

3. 安全事件：

a. 成功和不成功的PKI系统访问尝试；
b. 执行的PKI和安全系统行动；
c. 安全配置文件的更改；
d. 证书系统上软件的安装、更新和删除；
e. 系统崩溃、硬件故障和其他异常情况；
f. 防火墙和路由器活动；以及
g. 进入和离开CA设施的情况，包括授权人员与非授权人员及安全存储设施的进出访问。

4. 系统操作事件，包括：

a. 系统启动和关闭，
b. 系统权限的创建、删除，设置或修改密码；
c. 对于 CA 系统网络的非授 权访问及访问企图；
d. 对于系统文件的非授权的访问及访问企图；
e. 安全、敏感文件或记录的读、写或删除；

5. 可信人员管理记录，包括：

a. 网络权限的帐号申请记录；
b. 系统权限的申请、变更、创建申请记录；
c. 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。

5.4.1.1 路由器和防火墙的活动日志

亚洲诚信CA路由器以及防火墙日志至少包括：

1. 路由器和防火墙的成功和不成功登录尝试；
2. 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；
3. 记录对防火墙规则所做的所有更改，包括添加、修改和删除；
4. 记录所有系统事件和错误，包括硬件故障、软件崩溃和系统重新启动。

5.4.2 处理日志的周期

不定期处理系统的自动日志和操作人员的手工记录。

不定期处理系统安全日志，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保留以下日志至少两年：

1. 在以下情况发生后的CA证书和密钥生命周期管理事件记录。

a. CA私钥销毁；或

b. 证书中X.509v3 基本约束扩展项的CA字段设定为“是”，且与该CA私钥享有共同公钥的最终CA证书被撤销或到期。

2. 在订户证书撤销或过期后的订户证书生命周期管理事件记录。
3.
4. 当有事件发生后的任何安全事件记录。

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。

5.4.5 审计日志备份程序

亚洲诚信CA的系统日志实时同步到日志服务器，并且不定期备份到异地；手工纸质记录定期归档保存到专门的文件柜内。

5.4.6 审计收集系统

关于电子审计信息，亚洲诚信CA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每年执行一次风险评估：

1. 识别可能导致未经授权访问的可预见的内部和外部威胁，任何证书数据或证书管理的披露、滥用、更改或销毁流程；
2. 评估这些威胁的可能性和潜在损害，同时考虑到证书数据和证书管理过程的敏感性；和
3. 评估政策、程序、信息系统、技术和其他方面的充分性，亚洲诚信CA 为应对此类威胁而制定的安排。根据风险评估，制定、实施和维护安全计划，包括旨在实现上述目标并管理的安全程序、措施和产品控制风险评估中识别出的风险。安全计划包括行政、适用于证书数据敏感性的组织、技术和物理保护措施，以及证书管理流程。安全计划还考虑了当时可用的技术和实施具体措施的成本，并实施适当的合理安全级别安全漏洞可能导致的损害以及要保护的数据的性质。

5.5 记录归档

5.5.1 归档记录的类型

亚洲诚信CA除了归档第5.4.1章相关内容外，还对以下几类事件进行归档记录，包括但不限于：

1. 与其证书系统、证书管理系统、根CA系统和授权第三方系统的安全有关的文件；以及
2. 与证书申请和证书的验证、签发和撤销有关的文件。

5.5.2 归档记录的保存期限

存档的审计日志（如第5.5.1章中所述）将从其记录创建时间戳起至少保留2年，或者根据第5.4.3章要求保留的时间，两者以时间更长的为准。

亚洲诚信CA至少保留2年的记录包括：

1. 第5.5.1章中规定的与证书系统、证书管理系统和根CA系统的安全相关的所有存档文件；和
2. 在发生以下情况后，与证书申请和证书（如第5.5.1章中规定）的验证、签发和撤销相关的所有存档文件：

a. 此类记录和文件最后依赖于证书请求和证书的验证、签发或撤销；或
b. 依赖于此类记录和文件的订户证书的到期。

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，在内部存储服务器中完成收集备份工作。

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CA在创建归档记录时，会自动用系统时间（非加密方法）对其进行时间标记。亚洲诚信CA的时间源服务器时间与通过国家测量研究所认可的世界协调时间（universal coordinated time，简称UTC)时间源同步。

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，且不定期异地备份。

对于手工生成的电子记录，由内部存储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。

5.6 电子认证服务机构密钥更替

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。

CA 证书对应的密钥对，当其使用有效期超过本CP&CPS规定的最大生命期时，亚洲诚信CA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

亚洲诚信CA制定并记录业务连续性计划和灾难恢复计划，以便在发生灾难、安全事件或者业务受损时通知到软件供应商、订户以及依赖方。亚洲诚信CA不公开披露业务连续性计划，但受审计人员审计；并且每年测试、审查和更新这些程序。业务连续性计划包括：

1. 启动该计划的条件。
2. 应急程序。
3. 后退程序。
4. 恢复程序。
5. 该计划的维护时间表。
6. 意识和教育要求。
7. 个人的责任。
8. 恢复时间目标（RTO）。
9. 应急计划的定期测试。
10. CA在关键业务流程中断或失效后，及时维护或恢复CA业务运营的计划。
11. 要求将关键的密码材料（即安全的密码设备和激活材料）储存在另一个地点。
12. 什么是可接受的系统中断和恢复时间。
13. 重要业务信息和软件的备份副本的频率如何。
14. 恢复设施与CA主站点的距离；以及
15. 在灾难发生后以及在原址或远程站点恢复安全环境之前的一段时间内，尽可能保护其设施的程序。

5.7.2 计算机资源、软件和/或数据的损坏

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

5.7.3 私钥泄漏处理程序

当亚洲诚信CA的根CA或中级CA出现私钥泄漏时，亚洲诚信CA将按照密钥应急方案进行紧急处理，撤销所有该CA签发的证书。

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CA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CA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CA终止前，必须：

1. 委托业务承接单位；
2. 起草亚洲诚信CA终止声明；
3. 至少提前90天通知与亚洲诚信CA停止运营涉及的相关实体；
4. 处理存档文件记录；

5. 停止认证中心的服务；
6. 存档相关系统日志；
7. 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，使用符合 FIPS140-2 Level 3的密码设备中生成。密钥的生成、管理、存储、备份和恢复遵循 FIPS140-2 标准的相关规定。

CA 密钥对的生成过程，由亚洲诚信CA多名密钥管理员和若干名可信人员、以及具有资质的独立第三方审计人员见证下，按照亚洲诚信CA事先准备的密钥生成脚本在亚洲诚信CA屏蔽机房中完成。CA密钥对生成过程和操作均需全程录像记录。并由具有资质的独立第三方审计人员出具报告表明亚洲诚信CA在CA密钥对生成过程中的流程和控制能够保证CA密钥对的完整性和机密性。

6.1.1.2 RA密钥对的生成

不适用。

6.1.1.3 订户密钥对的生成

不适用。

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CA。

6.1.4 CA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官网下载根CA证书和中级CA证书。

6.1.5 密钥长度

为保证密钥的安全强度，亚洲诚信CA在签发证书前，使用lint工具进行密钥长度检测，以确保亚洲诚信CA不同类型的证书密钥遵循以下标准：

证书类型	根证书	中级证书	订户证书
摘要算法	SHA384	SHA384	SHA256 | SHA384
RSA密钥长度	4096	4096	2048 | 3072 | 4096
ECC 曲线	P-384	P-384	P-256 | P-384

6.1.6 公钥参数的生成和质量检查

亚洲诚信CA和订户均需遵循本CP&CPS 6.1.1中的规定生成公钥，公钥参数由合规的设备/平台生成以保证公钥参数的质量。公钥需满足本CP&CPS 6.1.5中的要求。

亚洲诚信CA在签发证书前，进行公钥参数检测，以确保公钥参数满足以下：

- 对于RSA公钥：

1. 公共指数为大于或等于3的奇数
2. 公共指数范围应在2^16+1 ~ 2^256-1之间
3. 模数为奇数
4. 模数位数至少2048位且是8的整数倍
5. 模数不是质数的幂
6. 模数没有小于752的因数。
    - 对于ECDSA公钥：

所有密钥的有效性都通过完整的ECC公钥验证程序或ECC部分公钥验证程序来确认。

6.1.7 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，其用法与RFC 5280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，且这些证书唯一EKU为id-kp-BIMIInternet；
3. OCSP响应签名证书。

中级 CA 密钥一般用于签发以下证书和 CRL：

1. 订户证书，且唯一EKU为id-kp-BIMIInternet；
2. OCSP 响应签名证书；

6.2 私钥保护和密码模块工程控制

亚洲诚信CA实施物理和逻辑保护措施以防止未经授权的证书签发。在上述指定的已验证系统或设备之外的私钥备份，亚洲诚信CA将密钥片段加密存储在不同实体的物理设备中，以防止私钥泄漏。加密私钥片段所使用的算法以及密钥长度根据现有技术，该算法和密钥长度能够在加密密钥或密钥部分的剩余生命周期内抵御密码分析攻击。

6.2.1 密码模块的标准和控制

亚洲诚信CA用于CA密钥对和时间戳密钥对的加密模块均符合FIPS 140-2 Level 3标准。

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5位密钥管理员中，至少在3人及以上的密钥管理员在场并许可的情况下，插入管理员IC卡或USBKey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CA不会托管私钥。

6.2.4 私钥备份

见本CPS第5.2.2节，另外亚洲诚信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权限IC卡或USBKey并保存到公司的保险柜（或银行保管箱等安全等级不低于本地备份的场所）。

6.2.5 私钥归档

亚洲诚信CA不对订户证书的私钥进行归档，所有CA证书私钥也不由第三方进行归档。

6.2.6 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。所有这些有效防止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CA私钥以加密的形式存放在符合FIPS 140-2级别3标准的硬件密码模块中，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，激活需按本CP&CPS第6.2.2节，在至少半数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卡或USBKey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CA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卡或USBKey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

参考本CP&CPS 6.2.1。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

亚洲诚信CA公钥归档参考第5.5章节。

6.3.2 证书有效期和密钥对使用期限

标志证书的最终订户证书最大有效期不超过398天。如果是注册商标或文字商标的被许可方而非商标注册人，则证书的过期日不晚于订户持有该注册商标或文字商标的最终到期日。

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

6.4.2 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。

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将销毁，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。

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ISO 27001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。

对所有能够直接导致证书发放的账户实施多因素认证。

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CA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CA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。

6.6.2 安全管理控制

亚洲诚信CA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CA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 生命周期的安全控制

亚洲诚信CA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CA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。

亚洲诚信CA的网络安全控制符合 CA/Browser 论坛NCSSR。

6.8 时间戳

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

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

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

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

标志证书符合本节规定的配置要求，亚洲诚信CA在满足第2.2节、第6.1.5节、第6.1.6节的规定的技术要求基础上，根据本章节以下规范签发证书。

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 证书内容以及扩展

亚洲诚信CA在按照RFC5280规定要求基础上，以下配置覆盖所有签发的证书。

- 7.1.2.1 根证书配置
- 7.1.2.2 中级CA证书配置
- 7.1.2.3 订户证书配置

7.1.2.1 根CA证书配置

见第11.1节。

7.1.2.2 中级CA证书配置

见第11.2节。

7.1.2.3 订户证书配置

见第11.3节。

7.1.3 算法对象标识符

7.1.3.1 主题公钥信息

以下要求适用于证书或者预证书中subjectPublicKeyInfo，不使用其它编码。

7.1.3.1.1 RSA

亚洲诚信CA使用 rsaEncryption（OID：1.2.840.113549.1.1.1）算法标识符指示 RSA 密钥，并且显示NULL，编码时，RSA的密钥算法标识符16进制编码为300d06092a864886f70d0101010500。

7.1.3.1.2 ECDSA

亚洲诚信CA 使用 id-ecPublicKey（OID：1.2.840.10045.2.1）算法标识符指示 ECDSA 密钥。

参数使用曲线名称编码：

- 对于P-256密钥，曲线是 secp256r1（OID：1.2.840.10045.3.1.7）。

- 对于P-384密钥，曲线是 secp384r1（OID：1.3.132.0.34）。

编码时，ECDSA的密钥标识为以下16进制编码：

- P-256密钥301306072a8648ce3d020106082a8648ce3d030107
- P-384密钥301006072a8648ce3d020106052b81040022

7.1.3.2 签名算法标识符

亚洲诚信CA私钥来签名的对象以及派生出来的内容签名均符合上下文中所使用的算法。

特别是以下所有对象和字段：

1. 证书或预证书的signatureAlgorithm字段。
2. 待签名证书的signature字段。
3. 证书列表的signatureAlgorithm字段。
4. 待签名证书的signature的字段
5. OCSP响应的signatureAlgorithm字段。

7.1.3.2.1 RSA

亚洲诚信CA使用两种RSA签名算法和编码，如下：

签名算法	OID	16进制编码
SHA-256 with RSA	1.2.840.113549.1.1.11	300d06092a864886f70d01010b0500
SHA-384 with RSA	1.2.840.113549.1.1.12	300d06092a864886f70d01010c0500

7.1.3.2.2 ECDSA

亚洲诚信CA使用两种ECDSA签名算法和编码，如下：

签名算法	OID	16进制编码
SHA-256 with ECDSA	1.2.840.10045.4.3.2	300a06082a8648ce3d040302
SHA-384 with ECDSA	1.2.840.10045.4.3.3	300a06082a8648ce3d040303

7.1.4 名称形式

本节介绍了适用于 CA 签发的所有证书的编码规则。第7.1.2节中可能会规定进一步的限制，但这些限制不会取代这些要求。

亚洲诚信CA对于每个有效的认证路径（由RFC 5280 第6节定义）：

- 对于证书路径中的每个证书，证书的签发者甄别名字段的编码内容与签发 CA 证书的主题甄别名字段的编码形式逐字节相同。
- 对于认证路径中的每个CA证书，证书的主题甄别名字段的编码内容在其主题可区分名称可以根据RFC 5280 第7.1节进行比较的所有证书中逐字节相同，并且包括过期和撤销的证书。

在编码名称时：

- 每个名称（Name）包含一个RDNSequence。
- 每个相对甄别名（RelativeDistinguishedName）恰好包含一个AttributeTypeAndValue。
- 每个名称在所有相对甄别名中不包含多个给定的AttributeTypeAndValue实例。

7.1.5 名称限制

不使用此扩展。

7.1.6 证书策略对象标识符

7.1.6.1 保留证书策略标识符

见本CP&CPS第1.2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

不适用。

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按照以下配置来生成并发布CRL。

CRL覆盖该CA所有的签发的证书。如果使用CRL分区，则这些分区的聚合等于完整的CRL。CA不间接签发CRL。

属性	是否存在	描述
tbsCertList		

属性		是否存在	描述
	version	存在	v2版本
	signature	存在	
	issuer	存在	与签发CA主题逐字逐句匹配
	thisUpdate	存在	CRL的签发日期
	nextUpdate	存在	订户证书不超过10天，中级证书不超过12个月
	revokedCertificate	不使用	
	extensions	存在	见下表
signature		存在	

7.2.1 版本号

亚洲诚信CA的证书撤销列表符合X.509 v2的版本及格式要求。

7.2.2 CRL和CRL条目扩展项

CRL扩展：

扩展	是否存在	是否关键	描述
authorityKeyIdentifier	是	非	与签发CA的SubjectKeyIdentifier逐字逐句匹配
CRLNumber	是	非	为非负且不超过2^159次方的递增的整数
IssuingDistributionPoint	*	-	见本CP&CPS 7.2.2.1

撤销证书组件：

组件	是否存在	描述
serialNumber	是	与撤销证书的序列号逐字逐句匹配
revocationDate	是	通常为撤销日期，如果亚洲诚信CA有充足的证据表明该证书私钥泄漏日期早于撤销日期，那么此日期将回溯到该泄漏日期。
crlEntryExtensions	可能	见下面crlEntryExtensions组件表

crlEntryExtensions组件：

CRL条目扩展	是否存在	描述
reasonCode	可能	当原因代码为0时，不存在；且此原因代码为订户协议中指定的默认提供的选项。当原因代码为其它时，存在且不为关键。

7.2.2.1 CRL分发点

亚洲诚信CA使用完整的CRL时候，不使用此扩展。当使用CRL分片时，启用此扩展。

7.3 在线证书状态协议

如果OCSP响应是针对根CA或下级CA证书（包括交叉认证的下级CA证书）的，并且该证书已被吊销，那么在CertStatus的RevokedInfo中，revocationReason字段必须存在。

所指示的CRLReason包含第7.2.2节中规定的CRL允许的值。

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。OCSP响应的singleExtensions不包含reasonCode (OID 2.5.29.21) CRL条目扩展。

8 认证机构审计和其他评估

亚洲诚信CA在任何时候都：

1. 遵守BIMI Group MCR最新版的指南要求；
2. 遵守本章节中规定的WebTrust审计要求；
3. 获得工信部授权CA运营许可证。

8.1 评估的频率和情形

亚洲诚信CA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. 每季度执行一次内部审计，抽取1份或至少3%中的较大者的证书样本。
4. 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。
5. 除了内部审计和评估外，亚洲诚信CA还聘请独立的审计师事务所，按照 WebTrust对CA以及标志证书的审计规范，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CA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：

1. 独立的审计主体；
2. 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；
3. 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；
4. 具备检查系统运行性能的专业技术和工具；
5. 具备WebTrust审计的资质。
6. 持有保额至少为一百万美元的专业责任/错误与遗漏保险。

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CA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 for CA 及 MC规范的要求，对亚洲诚信CA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CA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CA在审计期结束后的三个月内公开审计报告。如果延迟超过三个月，亚洲诚信CA提供由合格审计员签署的解释性信函。

审计报告满足本CPS第8.6节其余部分规定的要求，包含以下明确标记的信息：

1. 被审计组织的名称；
2. 执行审核的组织的名称和地址；
3. 审核范围内的所有根和从属 CA 证书（包括交叉证书）的 SHA-256 指纹；
4. 审计标准，带有版本号，用于审计每个证书（和相关密钥）；
5. 审计期间引用的 CA 政策文件列表，以及版本号；
6. 审计评估的是一段时间还是一个时间点；
7. 审计期的开始日期和结束日期，对于涵盖一段时间的审计期；
8. 对于一些时间点的日期；
9. 报告发布的日期，在结束日期或时间点日期之后。

亚洲诚信CA确保由合格审计员提供公开可用于审计的权威英语版本的审计报告。报告以PDF格式提供，并且可通过文本搜索所有所需信息。审计报告中的每个SHA-256指纹均是大写字母，并且不包含冒号、空格或换行符。

8.7 自评估

亚洲诚信CA将根据国际、国内相关标准和CP&CPS的规定，通过至少每年一次的内部风险评估和至少每季度一次的自我监督抽查，不断进行自我审核，严格控制服务质量。自我审计评估从上一个审查期结束到当前审计期初始阶段的电子认证活动是否符合相关规定。抽查的样本量不应少于1份或者该期间签发证书总数的3%中的较大者。

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CA签署的协议中指明的价格和亚洲诚信CA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

亚洲诚信CA对撤销列表(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购买了商业一般责任保险，保单限额至少为200万美元，专业责任/错误与遗漏保险的保单限额至少为500万美元。

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如违反了本CP&CPS中规定的职责，证书订户可以申请亚洲诚信CA承担赔偿责任(法定或约定免责除外)。经亚洲诚信CA确认后，可对该实体进行赔偿。赔偿限制如下：

1. 亚洲诚信CA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CA根据情况重新制定，亚洲诚信CA会将重新制定后的情况立刻通知相关当事人。
2. 亚洲诚信CA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CA提供的电子认证服务中，以下信息视为保密信息：

1. 亚洲诚信CA订户申请证书时提交或签订的协议等，未在证书内公开的内容。
2. 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。
3. 其他由亚洲诚信CA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CA将以下信息视为不保密信息：

1. 由亚洲诚信CA发行的证书和CRL中的信息。
2. 由亚洲诚信CA支持、CP&CPS识别的证书策略中的信息。
3. 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。
4. 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CP&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CA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CA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隐私。亚洲诚信CA使用适当的保护措施和合理的谨慎程度来保护隐私。

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CA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CA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。

对其他信息的披露受制于法律、订户协议。

9.5 知识产权

1. 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。
2. 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。
3. 亚洲诚信CA有权决定采用何种软件系统。
4. 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。
5. 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。
6. 对外运营管理策略和规范为亚洲诚信CA财产。
7. 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)以及该域中签发给终端实体的证书，均为亚洲诚信CA的财产。
8. 本CP&CPS采用“知识共享署名-禁止演绎（CC-BY-ND）4.0国际许可协议”进行许可。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

通过签发证书，亚洲诚信CA向以下证书受益人作出本证书所列的保证：

1. 订户，即证书订户协议或使用条款的当事方；
2. 所有与根证书颁发机构签订合同，将根证书包含在其分发的软件中的应用软件供应商；以及
3. 所有合理依赖有效证书的依赖方。

亚洲诚信CA向证书受益人声明并保证，在证书有效期内，证书颁发机构在签发和管理证书时，已遵守MCR及本CPS。

亚洲诚信CA遵守CPS程序颁发证书，保证条款具体包括但不限于以下内容：

1. 域名使用权， 保证在签发时已执行并遵守验证流程，确认申请人拥有或控制证书中列出的域名。
2. 证书授权，保证已核实主体授权签发该证书，且申请人代表有权代表主体提交请求；
3. 信息的准确性，保证已执行相关程序，验证并确认证书中所含的所有信息在签发时均准确无误；
4. 申请人身份，保证已按照 MCR和CPS 第 3.2 节的规定验证了申请人的身份；
5. 用户协议，保证已与订阅人签署了合法有效且符合要求的订阅人协议或使用条款；
6. 证书状态服务，保证维持一个 24x7 全天候可公开访问的存储库，提供证书的当前状态（有效或已吊销）；
7. 证书撤销，保证在出现CPS的任何吊销情形时，将履行吊销义务。

9.6.2 注册机构的陈述与担保

亚洲诚信CA的注册机构在参与电子认证服务过程中的承诺如下：

1. 提供给证书订户的注册过程完全符合亚洲诚信CA的CP&CPS的所有实质性要求。
2. 在亚洲诚信CA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。
3. 亚洲诚信CA将按 CP&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

亚洲诚信实施一套流程，以确保每份用户协议或使用条款对申请人均具有法律约束力。无论采用哪种方式，协议都必须适用于根据证书申请将要颁发的证书。

在签发证书之前，申请人与亚洲诚信CA签订的订户协议。使用电子协议或“点击式”协议，每个证书申请可以使用单独的协议，也可以使用一份协议来涵盖多个未来的证书申请及其产生的证书。

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：

1. 一经接受证书，即表示订户知悉和接受本CP&CPS中的所有条款和条件，并知悉和接受相应的订户协议。
2. 承认并接受，如果申请人违反用户协议或使用条款，或者 CA 发现证书被用于实施网络钓鱼攻击、欺诈或传播恶意软件等犯罪活动，CA 有权立即撤销证书。
3. 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。
4. 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。
5. 一经接受证书，订户就应当承当如下责任：有义务并保证审核并核实证书内容的准确性。
6. 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。
7. 证书在本 CP&CPS 中规定使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的。

8. 如果证书中的任何信息不正确或不准确，则有义务和保证立即请求撤销证书并停止使用该证书。
9. 对于 MC证书，订户有责任和义务保证只在证书中列出的使用者主题备用名对应的域名中实施证书，并且仅在遵守所有适用法律和完全按照订户协议或使用条款的情况下使用证书。

9.6.4 依赖方的陈述与担保

1. 遵守本CP&CPS的所有规定。
2. 确认证书在规定的范围和期限使用证书。
3. 在信赖证书前，对证书的信任链进行验证。
4. 在信赖证书前，通过查询CRL或OCSP确认证书是否被撤销。
5. 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。
6. 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 其他参与者的陈述与担保

从事电子认证活动的其他参与者须承诺遵守本CP&CPS的所有规定。

9.7 担保免责

除本CP&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：

1. 不保证证书订户、信赖方、其他参与者的陈述内容。
2. 不对电子认证活动中使用的任何软件做出保证。
3. 不对证书在超出规定目的以外的应用承担任何责任。
4. 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。
5. 订户违反本CP&CPS第9.6.3之承诺时，或依赖方违反本CP&CPS第9.6.4之承诺时，得以免除亚洲诚信CA之责任。
6. 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。
7. 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 有限责任

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将承担对订户或依赖方依法认可和可证明的索赔的责任限制在每位订户或依赖方每份商标证书的金额不低于两千美元。

9.9 赔偿

9.9.1 赔偿范围

如亚洲诚信CA违反了本CP&CPS 9.6.1中的陈述，证书订户可以申请亚洲诚信CA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，每张 VMC证书基于每个订户或每个依赖方的赔偿额不低于2000美金。

9.9.2 订户的赔偿责任

如因下述情形而导致亚洲诚信CA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CA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CA，以及不当交付他人使用导致亚洲诚信CA或第三方遭受损害；
3. 订户使用证书的行为，有违反本CP&CPS及相关操作规范，或者将证书用于非本CP&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CA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CA按照本CP&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CA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CA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CA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CA与依赖方的协议和本CP&CPS中规定的义务；
2. 未能依照本CP&CPS规范进行合理审核，导致亚洲诚信CA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CP&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

当亚洲诚信CA终止业务时，本CP&CPS终止。

9.10.3 效力的终止与保留

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

当由于某种原因，如内容修改、与适用法律相冲突，CP&CPS、订户协议、依赖方协议和其他协议中的某些条款失效后，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CA安全策略委员会授权，CPS编写小组每年至少审查一次本CP&CPS，确保其符合国家法律法规和主管部门的要求及相关国际标准，并符合认证业务开展的实际需要。

本CP&CPS的修改和更新，由CPS编写小组提出修订意见，经亚洲诚信CA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CP&CPS经过亚洲诚信CA 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CP&CPS经批准后将立即在亚洲诚信CA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OID的情形

亚洲诚信CA全权负责确定CP&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CA必须对本CP&CPS进行修改的情形包括：CP&CPS中相关内容与管辖法律的不一致、国家监管部门对本机构认证业务有明确的更改或调整要求等。

9.13 争议处理

亚洲诚信CA、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CA就本CP&CPS所涉及的任何争议提起诉讼的，各方同意提交亚洲诚信CA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CA的CP&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CP&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CA就本CP&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CP&CPS完整的文档结构包括：标题、目录、主体内容三部分。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CA的网站中以供查阅和浏览

9.16.2 转让

亚洲诚信CA声明，根据本CP&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

当本CP&CPS要求与中国大陆任何司法管辖区的法律、法规或政府命令（以下简称“法律”）发生冲突，亚洲诚信CA在必要的最小范围内对任何与之冲突的要求进行修改，以使其在管辖范围内合法有效。这仅适用于受该法律约束的操作或证书签发。在这种情况下，亚洲诚信CA立即（并在根据修改后的要求签发证书之前）在本CP&CPS第9.16.3节中详细引用具体的法律，以及具体实施的这些要求的相关修改。

此外，亚洲诚信CA（并在根据修改后的要求签发证书之前），通过向BIMI Group工作组发送信息并收到确认回执的方式，通知其 CPS 中新增加的相关内容，以便BIMI Group工作组据此考虑对MCR可能的修订。

亚洲诚信CA根据MCR所做的任何修改，在以下任一情况发生时予以终止：

1.相关法律不再适用；

2.MCR经过修订，使得 CA 能够同时遵守两者。

如遇上述情况，必须在 90 天内完成以下三项工作（如前文所述）：

1.做出相应的实践变更；

2.修改 CA 的 CPS；

3.通知BIMI Group工作组。

9.16.4 强制执行

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

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CP&CPS规定的担保责任，那么亚洲诚信CA将不对此类事件负责。

9.17 其他条款

亚洲诚信CA对本CP&CPS具有最终解释权。

10 附录A–验证要求

10.1 验证项目及要求

亚洲诚信CA对订户证书鉴别要求如下：

鉴别条目	鉴别要求
CSR 验证	验证CSR签名数据 验证CSR公钥长度 验证CSR公钥是否为弱密钥
域名验证	依据CPS 3.2.2.5 验证域名控制权
CAA 验证	依据CPS 4.2.4 验证CAA
组织验证	核实申请人名称是否合法合规 核实申请人是否合法存续经营 核实申请人的所在地的国家省份城市及地址 核实电话号码、传真号码、电子邮件地址或邮政投递地址作为申请人已核实的沟通方式 组织注册司法管辖验证（注册地所在国家、州/省，注册地点、注册号） 证书审批人及合同签署人的姓名、职务及授权验证 1. 证书审批人：验证其姓名和职务，以及验证其证书申请审批权限 2. 合同签署人：验证其姓名和职务，以及验证其代表申请人订立订户协议（或其他相关的合同性责任）的权限 订户协议和证书请求的签名验证 申请组织业务能力验证 申请组织商业类别鉴别及验证 1. 私有组织：合法存续、组织名称、注册号、注册机构 2. 政府实体：合法存续、组织名称、注册号 3. 商业实体：合法存续、组织名称、注册号、主要个人 4. 非商业实体：合法存续、组织名称、注册号 商业实体的“主要个人”面对面验证： 合同签署人或证书审批人面对面验证 遵循CPS 3.2.2组织验证相关章节

鉴别条目	鉴别要求
先前使用标志验证	验证标志类型、先前使用期限、标志来源、颜色限制、标志表现形式 遵循CPS 3.2.2.7.1章节
修改注册商标验证	验证标志类型、商标注册国家或地区、商标局名称、商标号、颜色限制、标志表现形式 遵循CPS 3.2.2.7.2章节
注册商标验证	验证标志类型、商标注册国家或地区、法规引用、商标局名称、商标号、颜色限制、商标表现形式 遵循CPS 3.2.2.8.1
政府标志验证	核实标志类型、法令/法规/条约或政府行为的具体引用和具体网址来源、政府标志所有权或许可、商标表现形式、颜色限制、设立该政府标志的政府实体所述的主管法律管辖区（法令所在国家、法令所在州/省、法令所在地） 遵循CPS 3.2.2.8.2
个人身份验证	依据CPS 3.2.3 验证个人身份
证书经办人验证	验证证书申请经办人的姓名和职务，以及验证其为申请人的代理； 通过联系证书申请经办人来确认申请人的相关信息以及所需申请的证书类型。
高风险验证	查询内部数据库保存所有之前撤销的证书和拒绝的证书申请，以识别后续可疑的证书申请。 使用以下所示的验证方法识别“高风险申请人”并采取额外的合理必要的防范措施以确保此类申请人得到适当验证： 通过查询相关常被用于钓鱼欺诈或其他方式的欺骗行为的机构名称列表以识别高风险申请，并且自动标记与列表匹配的证书申请，以便在签发之前对其进一步调查。 采用由本机构的高风险标准认定的信息，以标记可疑证书申请。依据文件化程序对任何标记为可疑或高风险的证书申请进行额外的验证。 确定实体是否被识别为从高风险关注区域申请标志证书。 若申请人、证书经办人、证书审批人、合同签署人或申请方注册辖区或业务所在地出现以下情况，不签发标志证书： • 在任何政府拒绝清单、禁止人员清单或CA运作辖区内的国家中，其他禁止与该机构或个人进行业务往来的清单中；或 • 对于注册辖区，注册机关或者业务所在地所在的国家，CA辖区的法律禁止与其进行业务往来。
律师身份验证	核对律师相关信息，检查律师执业证书或查询其执业证书注册备案情况，与其所在律所确认执业情况； 与律师核对所签署的律师函的真实性、准确性。 若使用律师信则需要执行此项验证。

11 附录B–证书内容模板

11.1 根证书

证书字段		关键扩展项	内容
版本			v3
序列号			包含至少64位的CSPRNG
签发者			和主题逐字节匹配
TBSCertificate签名			TrustAsia Verified Mark RSA Root CA:sha384withRSA TrustAsia Verified Mark ECC Root CA:sha384withECDSA
有效期:notBefore			生成仪式当天
有效期:notAfter			25年
主题	通用名称（CN）		TrustAsia Verified Mark RSA	ECC Root CA
	组织（O）		TrustAsia Technologies, Inc.
	国家（C）		CN
公钥信息			RSA4096 (OID: 1.2.840.113549.1.1.1) or secp384r1 (OID: 1.3.132.0.34)
签名算法			与TBSCertificate签名匹配
扩展: subjectKeyIdentifier		非关键	根据RFC 5280，subjectPublicKey的160位SHA-1哈希值
扩展：basicConstraints		关键	Subject Type=CA Path Length Constraint=None
扩展: keyUsage		关键	keyCertSign, cRLSign

11.2 中级证书

证书字段	关键扩展项	内容
版本		v3
序列号		包含至少64位的CSPRNG
签发者		与签发CA的Subject信息逐字节匹配
TBSCertificate签名		TrustAsia Verified Mark RSA CA 2026：sha384withRSA TrustAsia Verified Mark ECC CA 2026：sha384withECDSA

证书字段		关键扩展项	内容
有效期:notBefore			生成仪式当天
有效期:notAfter			20年
主题	通用名称(CN)		TrustAsia Verified Mark RSA CA 2026 或 TrustAsia Verified Mark ECC CA 2026
	组织（O）		TrustAsia Technologies, Inc.
	国家（C）		CN
公钥算法			RSA4096 (OID: 1.2.840.113549.1.1.1) or secp384r1 (OID: 1.3.132.0.34)
签名算法			与TBSCertificate签名匹配
扩展: subjectKeyIdentifier		非关键	根据RFC 5280，subjectPublicKey的160位SHA-1哈希值
扩展: authorityKeyIdentifier		非关键	匹配签名证书的 subjectKeyIdentifier
扩展: certificatePolicies		非关键	Policy Identifier=Any Policy（2.5.29.32.0）
扩展: basicConstraints		关键	Subject Type=CA Path Length Constraint=0
扩展: keyUsage		关键	keyCertSign，cRLSign
扩展: extKeyUsage		非关键	id-kp-BIMIInternet
扩展: authorityInfoAccess		非关键	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.vmc.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.vmc.trustasia.com/<Issuername>
扩展: cRLDistributionPoints		非关键	CRL HTTP URL= http://crl.vmc.trustasia.com/<Issuername>.crl

11.3 订户（终端实体）证书

证书字段	关键扩展项	内容
版本		v3
序列号		包含至少64位的CSPRNG

证书字段	关键扩展项	内容
TBSCertificate签名		sha256withRSA 或 sha384withRSA 或 sha384withECDSA
签发者		与签发CA的Subject逐字节匹配
有效期:notBefore		距签发时间相差不超过24小时
有效期:notAfter		见第6.3.2节
主题		见本节主题内容表
公钥信息		RSA2048 | 3072 | 4096 或 ECDSA P-256 | P-384
签名算法		和TBSCertificate匹配
扩展: subjectKeyIdentifier	非关键	根据RFC 5280，subjectPublicKey的160位SHA-1哈希值
扩展: authorityKeyIdentifier	非关键	匹配签名证书的 subjectKeyIdentifier
扩展: certificatePolicies	非关键	[1] Policy Identifier=1.3.6.1.4.1.44494.2.7 policyQualifier=https://www.trustasia.com/cps [2] Policy Identifier=1.3.6.1.4.1.53087.1.1
扩展: basicConstraints	关键	Subject Type=End Entity
扩展: subjectAltName	非关键	只能是dNSName类型，不能为通配符类型、不得使用内部域名或者保留IP
扩展: extKeyUsage	非关键	id-kp-BIMIInternet
扩展：Signed Certificate Timestamp List	非关键	与预证书LogEntryType匹配
扩展: authorityInfoAccess	非关键	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.vmc.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.vmc.trustasia.com/<Issuername>
扩展: cRLDistributionPoints	非关键	CRL HTTP URL=http://crl.vmc.trustasia.com/<Issuername>.crl
扩展：logotype extension (1.3.6.1.5.5.7.1.12)	非关键	经验证的遵循RFC6170的SVG商标

主题内容：

		普通标志证书(CMC)		认证标志证书(VMC)	
通用名称(CN)		经验证的组织名称或文字商标			
组织（O）		经验证的组织，可以是DBA（经营别名）			
街道(Street)		经验证的组织所在街道			
城市(L)		经验证的组织所在城市，若ST存在，可选			
省份(ST)		经验证的组织所在省份，若L存在，可选			
国家（C）		经验证的组织所在国家			
部门(OU)		可选			
商业类别 (businessCategory)		以下4种之一： 私营企业(Private Organization)丨政府机构(Government Entity)丨商业实体(Business Entity)丨非商业实体(Non-Commercial Entity)			
注册司法管辖区(JOI)	注册地所在城市(jurisdictionLocalityName)	注册地辖区所在城市，必须包含省份和国家			
	注册地所在省份/州(jurisdictionStateOrProvinceName)	注册地辖区所在省份/州，必须包含国家			
	注册地所在国家(jurisdictionCountryName)	注册地辖区所在国家			
序列号(serialNumber)		见第3.2.2的描述			
法律实体标识(LEI)		可选			
组织标识(OI)		可选			
标志类型(MarkType)		先前使用标志证书(Prior Use Mark)	修改后的注册商标证书(Modified Registered Mark)	注册标志证书(Registered Mark)	政府标志证书(Government Mark)

			普通标志证书(CMC)		认证标志证书(VMC)	
	先前使用标志来源URL(priorUseMarkSourceURL)		经验证的商标URL			
	商标注册地(trademarkCountryOrRegionName)			注册商标局所在国家或地区	注册商标局所在国家或地区	
	商标局名称(trademarkOfficeName)			适用的商标局唯一时可选	适用的商标局唯一时可选	
	商标标识符(trademarkIdentifier)			商标标识	商标标识	
	法令政府信息(SGI)	法令所在地名(statuteLocalityName)				法令所在地，必须包含省份/州
		法令省份/州名(statuteStateOrProvinceName)				法令所在省/州，必须包含国家
		法令国家代码(statuteCountryName)				法令所在国家
	法令引用(statuteCitation)					标志所引用的法规、条例、条约
	法令URL(statuteURL)					标志URL，可选

12 标志证书使用条款

商标证书使用条款（“MC 条款”）

所有**商标声明实体（MAE）**作为获得商标证书的条件，均须同意本 MC 条款。**消费实体（Consuming Entities）**、**依赖方（Relying Parties）**及任何其他人对任何商标证书（及其中的任何商标表现形式、其他数据或信息）的任何及所有使用、展示或依赖，均以接受本 MC 条款为前提。商标证书中的 **OID 1.3.6.1.4.1.53087.1.1** 通过引用并入了本 MC 条款。如果任何人不同意本 MC 条款，则不得获取、使用、发布或依赖任何商标证书或商证书中的任何标志表现形式或任何其他数据或信息。

1. 定义

首字母大写的词语其含义见《标志证书要求》第 1.6 节。

2. 有限的复制与展示权利

在符合 MC 要求和本 MC 条款的条款、条件及限制的前提下，MAE 特此授予：

1. **授予签发 CA**：一项有限的、非排他的、全球范围内的许可，用于签发包含 MC 标志的标志证书，并按 MC 要求将该证书记录在有限数量的**证书透明度（CT）日志**中。
2. **授予消费实体**：一项有限的、非排他的、全球范围内的许可，用于配合内部徽标识别系统使用 MC 标志，并在与 MAE 撰写或提供的通信、信件或服务有直接视觉关联的情况下，托管、存储、复制、展示、处理及（根据第 3.1 条允许的）修改 MC 标志；且此类通信等必须来自或通过标志证书“主体别名（SAN）”字段中包含的相同域名。
3. **授予证书透明度日志运营商**（若不同于签发 CA）：一项有限的、非排他的、全球范围内的许可，用于保留标志证书的副本并进行复制，以支持这些已签发证书的长期公共记录，并允许公众审计标志证书的核实情况。

未向任何其他方或出于任何其他用途授予任何其他许可。

3. 许可限制与条件

任何通过已签发并发布的标志证书将 MC 标志纳入或打算纳入其产品和服务的消费实体，均同意其获得的相关许可受以下限制并以其为条件：

1. **质量控制与同等待遇**： 消费实体在展示时**不得扭曲**从发布的标志证书中获取的任何标志表现形式，不得更改其颜色或背景，不得修改其透明度，或除了调整其大小、比例或以与其他标志表现形式一致的方式进行裁剪外，不得以任何方式对其进行更改。如果消费实体展示从发布的标志证书中获取的文字标志，必须以中立的方式进行，且与在同一视觉环境中显示的所有其他标志证书的文字标志保持一致。消费实体可以仅展示标志而不展示文字标志，但**不得在不展示标志的情况下单独展示文字标志**。
2. **不暗示合伙或关系**： 除非消费实体与 MAE 之间另有明确协议，否则 MC 标志或标志证书的任何其他内容均不得以任何合理暗示消费实体与 MAE 之间存在除本 MC 条款创建的纯粹许可方与被许可方关系之外的任何关系的方式使用或展示。
3. **CRL 或 OCSP 查询**： 消费实体必须检查由 CA 维护的**证书吊销列表（CRL）不得低于每 7 天一次**，以确定标志证书是否已被吊销。
4. **合法使用**： 消费实体只能根据适用法律使用标志证书中的标志表现形式。
5. **充足的所有权或许可**： **MAE 保证**通过标志证书发布的 MC 标志代表了 MAE 拥有或已获得充分许可的**注册标志**（及文字标志，如有），从而能够授予本 MC 条款中的有限许可；且如果 MAE 不再拥

有或不再拥有相关注册标志（或文字标志）的充分许可，MAE 将**立即吊销**该标志证书。对于因 MAE 申请标志证书的内容而引起的针对任何消费实体、依赖方或 CA 的任何知识产权或其他索赔，MAE 将进行辩护并承担责任。

6. **无展示义务**： MAE 承认消费实体没有义务在其发布的与 MAE 拥有或控制的域名相关的中展示 MC 标志，即使通信或消息已被确认来自 MAE 且可以从相应的标志证书中获得并安全展示合适的 MC 标志。消费实体可以根据本 MC 条款选择展示或不展示 MC 标志。
7. **终止**： 一旦标志证书吊销或过期，MAE 将立即停止发布或使用该标志证书，且上述第 2.2 条授予消费实体的许可**应当终止**。如果消费实体违反本 MC 条款的任何规定，第 2.2 条授予该消费实体的许可也将**自动且立即终止**。许可终止后，消费实体必须立即停止对 MC 标志的任何及所有使用。
8. **MC 要求与 MC 条款的更新**： MC 要求和 MC 条款可能会不时更新。各方均同意，标志证书签发时有效的 MC 要求和 MC 条款版本应一直适用至该标志证书过期或吊销之日。任何获取、使用、发布或依赖标志证书的实体，均有责任不时查看并熟悉 MC 要求和 MC 条款的任何更新版本。