# 亚洲诚信C2PA证书电子认证业务规则

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

### 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

亚洲诚信CA C2PA的CA证书依据算法，层次结构如下：

TrustAsia C2PA RSA Root CA（根证书）

—TrustAsia C2PA Claim Signing RSA CA 2026（C2PA生成器签名中级证书）

—TrustAsia C2PA TSA RSA CA 2026（C2PA时间戳中级证书）

TrustAsia C2PA ECC Root CA（根证书）

—TrustAsia C2PA Claim Signing ECC CA 2026（C2PA生成器签名中级证书）

—TrustAsia C2PA TSA ECC CA 2026（C2PA时间戳中级证书）

### 1.1.3 证书策略（CP）与电子认证业务规则（CPS）

本《亚洲诚信C2PA证书电子认证业务规则》(简称CPS)在符合当地法律法规的前提下进行编写。

本CPS阐明了亚洲诚信CA如何开展C2PA电子认证业务，包括申请、批准、签发、管理和撤销的业务方式和过程，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。订户的生成器产品实例使用证书对C2PA声明进行加密签名，为资产赋予C2PA内容凭证。根据本策略颁发的证书保证级别，依赖方可将其作为对包含内容凭证的资产进行信任评估的一部分。

本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. C2PA自本CPS发布前最新的证书策略

亚洲诚信CA会定期查看其更新情况，并持续修订CPS。如果本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C2PA证书电子认证业务规则。

## 1.2.1 证书策略标识

本节记录了C2PA证书中使用到了策略标识符、扩展标识符、扩展密钥标识符等。

| 对象标识符（OID） | 标识代表对象 |
| --- | --- |
| 1.3.6.1.4.1.62558.1.1 | C2PA证书策略 |
| 1.3.6.1.4.1.62558.3 | C2PA保证级别扩展 |
| 1.3.6.1.4.1.62558.3.10 | 保证级别1 |
| 1.3.6.1.4.1.62558.3.20 | 保证级别2 |
| 1.3.6.1.4.1.62558.4 | C2PA一致性产品列表记录ID扩展 |
| 1.3.6.1.4.1.62558.2.1 | C2PA签名密钥用法 |

## 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负责颁发、签署和撤销将公钥绑定到订户身份的数字证书。生成器产品可以使用由亚洲诚信CA颁发的数字证书来签署C2PA清单。

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 www.trustasia.com。

## 1.3.2 注册机构

由亚洲诚信CA授权，负责收集、核实并提交申请人和/或订户信息以录入公钥证书的实体。RA必须遵守本CPS。

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

已成为C2PA信任列表中CA的客户，并有资格为其合规生成器产品实例接收证书的申请人。

### 1.3.4 依赖方

根据签名者的身份和证书中编码的保证级别，评估 C2PA 资产中由签名者所做断言可信度的实体。

### 1.3.5 其他参与者

参与C2PA生态系统的人类或非人类（硬件或软件）实体。例如：相机（采集设备）、图像编辑软件、云服务或使用此类工具的人员。

## 1.4 证书应用

### 1.4.1 适合的证书应用

证书仅限由作为证书主体的生成器产品实例使用，用于在证书指示的保证级别下对 C2PA 声明进行数字签名。时间戳证书应用于时间戳服务，OCSP签名响应证书应用于OCSP响应。

### 1.4.2 限制的证书应用

不允许在C2PA内容凭证规范或合规计划之外使用本策略下颁发的证书。

### 1.4.3 正式证书和测试证书

亚洲诚信 CA 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 CA 正式认证系统签发，必须按照 CP&CPS 中的规定做严格的身份鉴别。

测试证书由亚洲诚信 CA 测试认证系统签发，证书不可信，一般用来测试证书申请流程、系统适用性及技术可行性，不能用于任何正式用途。由于使用数字证书来处理或保护信息的应用场景很广泛，差异也较大，依赖方在确定是否根据此 CP&CPS 签发证书时，必须评估自己的应用场景是否适用以及相关的风险。此 CP&CPS 涵盖了几种不同类型的订户证书，具有不同的保护级别，下表描述了每种证书的适用场景。

## 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CPS的最高权威机构。

### 1.5.4 CPS批准程序

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

## 1.6 定义和缩写

### 1.6.1 术语定义

| 术语 | 定义 |
| --- | --- |
| 管理当局 | 由C2PA理事机构授权，代表其运营合规计划的机构。它负责承认并认证同意参与该计划的关键合规角色。C2PA 技术工作组合规工作组 (Conformance Task Force) 以此身份运作。 |
| 申请人 | 已创建生成器产品 (Generator Product) 或验证器产品 (Validator Product)，并希望根据 C2PA 合规计划的治理框架被视为“合规产品”并添加到 C2PA 合规产品列表 (CPL) 的实体。 |
| 申请人代表 | 经申请人正式授权的自然人雇员或代理人。 |

| 术语 | 定义 |
| --- | --- |
| 断言 | 一种数据结构，用于表示签署人作出的（或“创建”）或在声明生成时收集的关于资产的声明。此数据是C2PA清单的一部分。 |
| 资产 | 一个包含数字内容、资产元数据以及可选C2PA清单的文件或数据流。 |
| 保证级别 | 向依赖方指示对其使用给定 C2PA 声明签名证书签署的断言和声明反映生成器产品实例预期行为的信心程度。保证级别越高，依赖方可以拥有的信心程度越高。 |
| 鉴证 | 为安全存储在硬件中的一组测量值提供数字签名，然后由请求方验证该签名及测量值组的过程。 |
| C2PA证书策略 | 一份规定了电子认证服务机构 (CA) 向实现 C2PA 合规产品（用于创建带有数字内容和 C2PA 清单的资产）的订户颁发数字证书时“必须”满足的要求，以及订户在使用证书时“必须”满足的要求的文件。 |
| C2PA声明 | 一种经过数字签名且具备防篡改可检测性的数据结构，它引用了一组关于某项资产的声明，以及表征内容绑定所需的信息。如果任何声明被编辑处理，则会包含相应的声明说明。此数据是C2PA清单的组成部分。 |
| C2PA声明签名证书 | 由C2PA信任列表中的CA颁发给合规实现者的合规生成器产品实例的X.509证书，证书主体名称为该生成器产品。 |
| C2PA合规计划 | 一个基于风险的治理计划，旨在让申请人证明其符合要求，并通过满足程序要求获得 C2PA 认可。该计划包括评估申请人产品的 C2PA 相关功能、评估安全属性以分配最高保证级别、评估 CA 的流程和技术能力，以及签署加入计划的法律协议。 |
| C2PA合规产品列表 | 根据 C2PA 合规计划规定被视为合规的所有合规产品的权威记录。 |
| C2PA 内容凭证 | 这是C2PA清单的首选非技术术语。因此，C2PA清单存储代表了资产的内容凭据。<br><br>内容凭据也指代整体的C2PA技术，因此本质上被视为复数名词。如果说C2PA清单是内容凭据，那么多个C2PA清单或更广泛、通用的概念就是内容凭据。 |
| C2PA 内容凭证规范 | 为数字资产内容溯源和真实性提供全球认可的标准，旨在通过创建丰富的生态系统使个人和组织能够采用数字溯源技术，同时满足安全要求。 |
| C2PA 治理框架 | 一套治理文件，定义了C2PA信任生态系统，包括角色、要求和流程。 |
| C2PA 清单 | 基于一个或多个声明（包括内容绑定）、一项声明和一个声明签名的组合所形成的关于资产来源信息集合。C2PA清单是C2PA清单存储的一部分。 |
| C2PA 信任列表 | 在合规计划背景下，由 C2PA 管理的 X.509 证书信任锚列表（根 CA 或从属 CA），这些 CA 根据本 C2PA 证书策略向合规生成器产品颁发证书。 |
| C2PA TSA 信任列表 | 由 C2PA 管理的信任锚列表，这些 CA 向时间戳机构 (TSA) 颁发时间戳签名证书。 |
| 电子认证服务机构 | 一个受信任的实体，负责颁发、签署和撤销将公钥绑定到订户身份的数字证书。生成器产品使用由 CA 颁发的数字证书来签署 C2PA 清单。 |

| 术语 | 定义 |
| --- | --- |
| 合规准则 | C2PA 要求受控方证明其符合合规计划的一组规范性要求，包括来自规范本身、生成器产品安全要求文档和 C2PA 证书策略的要求。 |
| 合规实现者 | 已成为 C2PA 合规计划成员，且在 CPL 列表中拥有至少一个状态良好的产品的申请人。 |
| 合规产品 | 被计划认定为合规并添加至 CPL 且状态为“conformant”的生成器或验证器产品。合规生成器产品会被分配一个最高保证级别。 |
| 动态证据 | CA 在生成器产品实例自动化注册证书期间评估的属性，通常以可验证的硬件支持工件形式转发（如密钥或平台鉴证报告）。 |
| 生成器产品 | 由申请人创建的软件、硬件和平台配置集合，作为一个系统共同工作，以产生带有 C2PA 清单的数字资产。该产品作为签名者，对生成的资产是否符合规范性要求负责。 |
| 生成器产品安全要求 | 为实现特定最高保障等级，生成器产品需满足的安全相关实施要求。 |
| 受管辖方 | 指在C2PA合规性计划中希望承担认可角色的组织。该计划要求其签署法律协议，并在产品列入C2PA信任列表或合规产品列表前接受审查。C2PA生态系统中的受管辖方包括选择申请并遵守C2PA合规性计划要求的认证机构与申请方。 |
| 管理机构 | 负责维护生态系统可信性的组织。其授权行政管理部门管理生态系统，并授权认证实体传递信任。C2PA指导委员会驱动的合规性计划即由其作为管理机构。 |
| 理事机构 | 负责生态系统信任的组织，授权管理当局管理生态系统。C2PA 是其合规计划的理事方，由指导委员会驱动。 |
| 托管环境 | 承载生成器产品或验证器产品机制与功能子集的服务器端环境。 |
| 实现类别 - 后端 | 一种评估目标的实现架构，其中资产、断言、声明及声明签名在一个或多个托管环境中生成，包括本地部署或商业云服务提供商托管的实例。 |
| 实现类别 - 分布式 | 一种评估目标的实现架构，由边缘子系统与后端子系统构成，其中资产、断言、声明及声明签名的生成过程分布在这两类子系统之间。 |
| 实现类别 - 边缘 | 一种评估目标的实现架构，其中资产、断言、声明及声明签名在网络边缘端点上生成。 |
| 最高保证级别 | 由 C2PA 合规计划根据对申请人生成器产品的安全功能、属性等进行评估后，自行决定的数字指定。 |
| 注册机构 | 受 CA 授权，负责收集、核实并提交申请人和/或订户信息以录入公钥证书的实体。RA 在 CA 的授权下运作，并遵守CA的CPS。 |
| 可靠的通信方式 | 一种通过申请人代表（Applicant’s Representative）以外的来源进行验证的通信方式，例如邮寄/快递地址、电话号码或电子邮件地址。 |
| 清单消费者 | 依赖内容凭证确保数字对象溯源和真实性的消费者数量众多且种类各异。为了消费 C2PA 支持的内容凭证，清单消费者必须使用 C2PA 批准的服务提供商。 |
| 依赖方 | 根据签名者的身份和证书中编码的保证级别，评估 C2PA 资产中由签名者所做断言可信度的实体。 |

| 术语 | 定义 |
| --- | --- |
| 安全事件 | 实际或可能危害信息系统及系统处理、存储或传输信息的机密性、完整性或可用性的事件，或构成违反（或即将违反）安全策略、安全程序及可接受使用策略的行为。 |
| 签名者 | 在合规计划背景下，CPL 列表中的合规生成器产品实例始终是签名者。 |
| 静态证据 | 生成器产品安全要求文档中记录的生成器产品评估目标属性，由行政管理部门在评估申请方生成器产品时进行审查，用以确定最高保障等级。 |
| 订户 | 成为 C2PA 信任列表中某 CA 的客户，并有资格为其合规生成器产品实例接收证书的申请人。 |
| 评估对象 | 由合规计划评估其功能正确性和实现安全性的系统，包括生成器产品或验证器产品及其依赖的子系统。 |
| 时间戳机构 | 提供电子认证和信任服务的服务器，通过创建哈希值来验证文件创建或修改的日期和时间，充当证明文件自签署以来未发生变化的独立证人。 |
| 可信执行环境 | 见NIST定义。 |
| 验证器 | 指执行验证过程中所述操作的清单消费者。 |
| 验证器产品 | 由申请人创建的软件、硬件和平台配置集合，作为一个系统共同工作以验证带有 C2PA 清单的数字资产。验证器产品可以单体式地集成验证器功能，也可以依赖本地（如设备上）或远程（如云服务托管）的独立验证器服务。由于验证器产品始终是列在 C2PA 合规产品列表（CPL）上的实体，因此无论其是直接集成还是依赖独立服务，都对按照规范性要求生成正确的验证结果负责。 |

### 1.6.2 约定

本文中的关键词“必须”、“不得”、“要求”、“应”、“不应”、“应该”、“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：CPS、订户协议、依赖方协议、根证书、中级CA证书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、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。

另外，亚洲诚信CA建立并维护一个不对外的安全的信息库，其中包含运营在本C2PA根CA下签发的所有证书记录。已颁发证书的记录在过期后至少保存1年。信息库中的记录包括：证书序列号、主体名称、有效期、X.509v3扩展及其值，以及撤销状态。信息库受到严格的访问控制和定期审计，以确保其完整性和机密性。

### 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会不定期跟进C2PA证书策略的变化，并及时调整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每天发布一次；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.501标准。

### 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。在C2PA信任模型下，DN项中的名称具有特定的代表性意义，可以与使用证书的最终实体的身份或特有的属性相关。

证书的主体必须是由订户创建，并且是用于签署C2PA声明的特定生成器产品。其在证书DN字段中的标识要求如下：

1. DN字段的值必须与C2PA合规产品列表中列出的该生成器产品的相应记录完全匹配。
2. DN项的所有字段值都需使用纯ASCII文本编写。

### 3.1.3 订户的匿名或伪名

亚洲诚信CA不会颁发匿名或伪名证书。

亚洲诚信CA颁发的证书不会唯一标识出其所颁发给的生成器产品的具体实例。例如，已颁发的证书不包含获得该证书的特定设备的唯一序列号。

### 3.1.4 不同名称形式的规则

亚洲诚信CA签发的C2PA声明签名证书符合X.509 V3标准，分配给证书持有者唯一的甄别名采用X.501标准命名方式。

### 3.1.5 名称的唯一性

颁发的证书必须确保名称的唯一性。亚洲诚信CA在其域内强制执行名称唯一性。当向同一实体颁发多个证书时，不视为违反名称唯一性。例如，亚洲诚信CA 可以向同一型号的多个设备或同一应用程序的多个实例颁发具有相同主体 DN 的证书。

### 3.1.6 商标的标识、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

在证书中指定的一方生成自己的密钥的所有情况下，该方将会被要求证明拥有私钥，该私钥对应于证书请求中的公钥。亚洲诚信CA通过使用CSR中的公钥验证订户在PKCS#10证书签名请求（CSR）上的数字签名来证

明订户拥有私钥。

### 3.2.2 组织身份鉴别

如果证书请求包含组织身份，亚洲诚信CA将验证提交用于签署C2PA合规声明的证书请求的实体是否控制与证书中引用的名称关联的应用程序，或者是否已获得应用程序所有者的授权代表其行事。

亚洲诚信CA会核实申请组织的经验状态未被标记为“已停止”、“非活跃”、“无效”、“非当前”或同等含义的状态，并将通过以下一项或多项来验证申请组织的身份和地址信息：

1. 申请组织合法设立、存在或获得认可的司法管辖区的政府机构。
2. 定期更新并被视为“可靠数据源”的第三方数据库，例如LEI全球法人识别编码数据来源。
3. 政府机构签发的有效注册文件，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。
4. 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。
5. 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CA认可的验证方式来确认组织的地址信息。
6. 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。

除上述身份地址和信息验证外，亚洲诚信CA还会通过定期更新并被视为可靠数据源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，以确认申请人代表所提供的信息的真实性。

对于证书的续期请求，亚洲诚信CA将在自上次身份验证后不超过398天内，使用章节3.2“初始身份确认”对订户身份进行重新验证。

### 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章节的验证方式与申请人代表核实申请人的申请意愿。

### 3.2.4 未验证的订户

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

亚洲诚信CA将核实申请人代表有权代表申请人为其生成器产品提交C2PA声明签名证书的申请，可以代表申请人签署订户协议并使申请人遵守协议的条款和条件。

亚洲诚信CA可以直接与申请人代表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CA认为合适的其他部门。

### 3.2.6 互操作准则

不适用。

### 3.2.7 合规性证明

亚洲诚信CA会核实申请人请求证书的生成产品是否已存在于C2PA合规产品清单中，并且其当前状态已经明确标记为“conformant”。

亚洲诚信CA会根据C2PA合规产品列表中该生成产品对应条目的最高保证级别字段值，获取该生成产品有资格获得的证书最高保证级别。

亚洲诚信CA不会向申请人颁发保证级别高于最高保证级别字段值的证书。

## 3.3 密钥更新请求标识与鉴别

亚洲诚信CA不支持重发密钥操作。

### 3.3.1 常规密钥更新的识别与鉴别

不支持此场景。

### 3.3.2 撤销后密钥更新的标识与鉴别

不支持此场景。

## 3.4 撤销请求的标识与鉴别

在亚洲诚信CA的证书业务中，证书撤销请求可以由订户、C2PA管理机构、亚洲诚信CA或经司法机构授权的司法人员发起。当撤销请求由订户发起时，亚洲诚信CA将验证撤销请求的真实性，并在72小时内撤销相关证书。

## 3.5 证书颁发与证书更新的身份验证与鉴别

对于续期请求，亚洲诚信CA将在自上次身份验证后不超过398天内，使用章节3.2“初始身份验证”对订户身份进行重新验证。

# 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

申请人通过亚洲诚信CA指定的方法提交正式申请以成为订户，从而启动证书请求流程。申请人需提供以下信息和文档。这包括：

1.申请证书的生成器产品信息，包括其在 C2PA 合规产品列表中的记录编号。

2.申请人为其生成器产品请求的证书保证级别，该级别不得超过该产品在 C2PA 合规产品列表中记录的最高保证级别。

3.若申请人的生成器产品在 CPL 记录中指示的保证级别有要求，则需提供能够使用该产品记录中列出的鉴证方法之一产生可验证工件的证据。

### 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验证团队将审查订户所提交的信息和文件是否完整准确，并且会按本CPS第3.2章节的要求，对订户的身份进行识别与鉴别。

当订户的生成器产品在C2PA合规产品列表中标注的保证级别含有特定要求，亚洲诚信CA将确认申请人具备获取以及向亚洲诚信CA提交平台证明报告(Platform Attestation Reports)的能力。

### 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. 订户证书的使用途径不符合其所在地的法律法规；
6. 亚洲诚信CA认为批准该申请将会对亚洲诚信CA带来争议、法律纠纷或者损失。
7. 提交申请的公钥长度、算法或其他存在不安全因素。

对于拒绝的证书申请，亚洲诚信CA将会邮件通知订户证书申请失败。

### 4.2.3 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 CA访问凭证

申请流程成功完成后，CA为新批准的订户关联新的或现有的安全访问凭证（例如用户名和密码、客户端证书或持有者令牌），用于在证书注册请求时对订户进行身份验证。

## 4.3 证书签发

证书签发遵守本CPS第3.2章规定进行订户身份的识别和鉴定。

若订户产品在 CPL 中指示的最高保证级别有要求，亚洲诚信CA请求并验证该保证级别所需的动态证据，此验证满足：

1.动态证据可以包括密钥证明报告、应用证明报告、平台证明报告或其他由硬件信任根支持的可验证工件。

2.在验证密钥和平台证明报告时，亚洲诚信CA遵循C2PA证书策略附录A中定义的“验证动态证据的要求”。

在成功验证上述动态证据后，亚洲诚信CA向订户的特定设备或应用程序实例颁发符合本CPS第7章规范的C2PA声明签名证书。

### 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。

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

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证书签发系统将证书发送给订户。

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。

#### 4.3.1.1 根CA证书签发的手动授权

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。

### 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

订户在接受证书时表示订户接受C2PA证书策略中必要条款的用户协议，也表示遵守本CPS。

### 4.4.1 构成接受证书的行为

根据本CPS颁发的证书仅限由作为证书主体的 C2PA 合规产品使用，这些产品必须由指定的订户实现，并列在 C2PA 合规产品列表中，用于在证书指示的保证级别下对 C2PA 声明进行数字签名。严禁将其用于任何其他用途。

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。
5. 用户通过生成器产品实例成功安装和使用证书。

### 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。

### 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

见本CPS第6.1.7节。

### 4.5.1 订户私钥和证书的使用

密钥使用场景应根据X509证书中的密钥用法扩展决定。与根据本CPS颁发证书的公钥相关联的私钥，应由生成器产品实例唯一控制，不得导出或与其它设备、应用实例或第三方共享，除非生成器产品安全要求允许。本CPS下颁发的证书仅限由作为主体的生成器产品使用，用于在指示的保证级别下签署C2PA 声明，严禁他用。

### 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

不支持此场景。

### 4.6.2 请求证书更新的实体

不支持此场景。

### 4.6.3 证书更新请求的处理

若需更新证书，应重新遵循本CPS第3章验证后重新申请。

### 4.6.4 签发新证书时对订户的通告

不支持此场景。

### 4.6.5 构成接受更新证书的行为

不支持此场景。

### 4.6.6 CA对更新证书的发布

不支持此场景。

### 4.6.7 CA对其他实体的通告

不支持此场景。

## 4.7 证书密钥更新

### 4.7.1 证书密钥更新的情形

不支持此场景。

### 4.7.2 请求证书密钥更新的实体

不支持此场景。

### 4.7.3 证书密钥更新请求的处理

若需密钥更新，应重新遵循本CPS第3章验证后重新申请。

### 4.7.4 签发新证书时对订户的通告

不支持此场景。

### 4.7.5 构成接受密钥更新证书的行为

不支持此场景。

### 4.7.6 CA对密钥更新证书的发布

不支持此场景。

### 4.7.7 CA对其他实体的通告

不支持此场景。

# 4.8 证书变更

## 4.8.1 证书变更的情形

不支持此场景。

## 4.8.2 请求证书变更的实体

不支持此场景。

## 4.8.3 证书变更请求的处理

若需证书变更，应重新遵循本CPS第3章验证后重新申请。

## 4.8.4 签发新证书时对订户的通告

不支持此场景。

## 4.8.5 构成接受变更证书的行为

不支持此场景。

## 4.8.6 CA对变更证书的发布

不支持此场景。

## 4.8.7 CA对其他实体的通告

不支持此场景。

# 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

1. 若出现以下情况的一种或多种，亚洲诚信CA必须在72小时内撤销证书，并使用相应的CRLReason:

a. 订户提出要求；
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、CPS中的一项或多项重大义务；
d. 怀疑或确认生成器产品遭到损害，或鉴证失败；
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C2PA证书策略、或亚洲诚信CA的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. 除本4.9.1.1节中描述的情况外，其他根据亚洲诚信CA的CPS要求进行撤销订户证书；

i. 亚洲诚信CA获悉通过某种经论证的方法可以证明订户私钥存在泄露情况或有明确的证据表明订户生成私钥的方法存在缺陷；

j. 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；

k. 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；

m. 生成器产品在 CPL 中的状态变更为以“已撤销 (revoked)”开头的任何状态；

n. C2PA 理事机构提出要求。

#### 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72小时之内撤销中级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、C2PA管理机构、亚洲诚信CA或经司法机构授权的司法人员。

### 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CA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CPS第 4.9.1.1章节中会导致订户证书被强制撤销的情形时，亚洲

诚信CA将通过内部流程申请撤销证书；

2. 在亚洲诚信CA的根证书或中级 CA证书相对应的私钥出现安全风险时，经国家电子认证服务主管部门批准后可直接进行订户证书撤销；
3. 当依赖方、司法机构、应用软件提供商、防病毒机构等第三方提请证书问题报告时，亚洲诚信CA应组织调查并根据调查结果来决定是否撤销证书；
4. 在证书被撤销后，亚洲诚信CA将通过适当的方式，包括邮件、电话等，通知最终订户证书已被撤销及被撤销的理由；若未能联络到订户，在必要情况下，亚洲诚信CA可以通过网站进行公告被撤销的证书；
5. 亚洲诚信CA提供7*24小时的证书问题报告及处理服务，相关方可通过本CPS第1.5.2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72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报告。

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，亚洲诚信CA会生成并发布：

1. 完整的CRL，或

2. CRL分区、聚合时可以恢复完整的CRL。

签发订户证书的CA：

1. 至少每4天更新一次并发布新的CRL
2. 在证书撤销后的24小时内更新并发布新的CRL

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：

1. 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
2. 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

亚洲诚信CA提供OCSP响应，以指示本CPS第2.2.1中涉及的生成器声明签名证书的撤销状态。

### 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 密钥损害的特别要求

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

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”。

### 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。

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C2PA证书链的CRL。

亚洲诚信CA全天候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

在订阅终止或相关活动停止时，订户应当销毁私钥。

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

亚洲诚信CA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

本节详细说明了亚洲诚信CA 运营和维护 PKI 系统完整性所需的物理、程序和人员控制、发布和证书管理。本节的重点在于逻辑和过程控制，反映了证书将使用的环境性质。

## 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）

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。

### 5.1.2 物理访问

#### 5.1.2.1 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。

#### 5.1.2.2 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。

#### 5.1.2.3 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。

### 5.1.3 电力与空调

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

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

### 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物理销毁。

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5.1.6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，遵循可信角色分离的原则。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. 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。

### 5.2.5 操作程序文档化

亚洲诚信CA维护详细的操作文档，以确保PKI系统的诚信、安全与合规。这些文档包括但不限于以下五个核心领域：

1. 证书的生命周期管理程序，包括证书的签发、续期和撤销流程。
2. 设备或应用内的密钥生成与管理规范。
3. 针对特定保证等级的认证验证程序。
4. 事件响应与灾难恢复计划。

5. 安全政策、指南和访问控制措施。

### 5.2.6 变更管理

亚洲诚信CA建立了正式的变更管理流程，以严格控制、记录并审核对C2PA认证业务基础设施、软件以及操作程序的所有变更。

#### 5.2.6.1 正式变更流程与记录

亚洲诚信CA实施公司内部的系统变更管理制度。凡涉及C2PA生产系统、安全架构、核心软件或业务流程的调整，必须提交变更申请，详细说明变更内容，受影响范围。所有变更活动均在审计范围内。

#### 5.2.6.2 测试与审批机制

在变更部署到生产环境之前，在独立的开发或测试环境中进行严格的验证，确保其不影响系统的稳定性以及对C2PA规范的合规性。变更必须经过受信任角色的审批，得到授权后方可实施。

#### 5.2.6.3 回滚与恢复计划

为应对变更实施过程中可能出现的不可预见问题，亚洲诚信CA针对变更制定回滚计划。若变更未能达到预期效果或引发系统异常，亚洲诚信CA将立即启动回滚程序，将基础设施、软件或操作环境恢复至安全稳定的状态。

## 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. 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. C2PA业务相关数据保护；
7. 岗位职责统一要求；
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，5年内必须至少接受亚洲诚信CA组织的培训一次。对于认证系统运营相关的人员，每5年至少进行一次相关技能和知识培训。此外，亚洲诚信CA将根据机构系统升级、策略调整等要求，不定期的要求人员进行继续培训。

### 5.3.5 工作岗位轮换周期和频率

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

### 5.3.7 独立合约人的要求

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. 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。

### 5.3.9 访问控制

亚洲诚信对C2PA认证系统、相关数据及基础设施实施严格的访问控制管理，以确保系统的保密性、完整性和可用性。

1. 最小权限原则：所有针对CA系统、数据库以及敏感数据的访问权限均基于“知所必须”原则进行授予。系统权限的分配严格遵循“最小权限”原则，确保受信任角色的人员仅拥有履行其岗位职责所必需的操作权限。
2. 身份鉴别与强口令策略：在访问CA系统或执行受信任角色任务前，必须通过身份验证。亚洲诚信CA实施严格的强口令策略，口令必须满足一定的长度和复杂度要求。
3. 多因素认证：亚洲诚信CA在关键访问路径上强制部署多因素认证机制，对于能够直接进行证书签发的账户，以及通过堡垒机进行的系统远程运维访问，必须使用多因素认证。
4. 定期评估访问权限。

## 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. 引入新证书档案和淘汰现有证书档案的记录。

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. 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；
c. 证书的签发；
d. CRL条目的生成；
e. 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

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

对系统安全日志，每年进行一次跟踪处理，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及其时间戳机构保留以下日志至少一年：

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. 在时间戳证书私钥被撤销或更新后的时间戳机构数据记录。
4. 当有事件发生后的任何安全事件记录。

**注意**：虽然这些要求设定了最短的保留期限，但亚洲诚信CA及其时间戳机构可选择更大的时间期限值，以利于调查需要回溯和检查的可能发生的安全事件或其他类型的事件。

### 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，并且每周备份；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1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1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。

亚洲诚信CA的时间戳机构（TSA）将记录以下信息，并将这些记录提供给具备资格的审计师，作为时间戳管理机构遵守这些要求的证明。

1. 对时间戳服务器的实际或远程访问，包括访问的时间和访问服务器的个人身份。
2. 时间戳服务器配置的历史。
3. 任何试图删除或修改时间戳日志的行为。
4. 安全事件，包括：

a. 成功和不成功的时间戳授权访问尝试。

b. 执行的时间戳管理局服务器行动。

c. 安全配置文件的变化。

d. 系统崩溃和其他异常情况；以及

e. 防火墙和路由器活动。

5. 撤销一个时间戳证书。
6. 对时间戳服务器的时间的重大改变，以及
7. 系统启动和关闭。

### 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，在内部存储服务器中完成收集备份工作。

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

### 5.6.1 密钥更替流程

亚洲诚信CA的ICA证书有效期最长不超过5年，任何由其签发的订户证书，其失效时间不超过ICA证书的失效时间。

ICA 证书对应的密钥对，当其ICA证书过期前2年时，亚洲诚信CA将启动密钥更替流程，替换即将过期的ICA密钥对。密钥更替按如下方式进行：

1. 在ICA证书过期前2年时，产生新的密钥对，签发新的ICA证书。
2. 在产生新的密钥对之后，对于批准的订户的证书请求，将逐步采用新的ICA密钥签发证书。
3. 在原ICA证书过期前1年时，停止用其私钥签发新的ICA证书。

### 5.6.2 用户通知

亚洲诚信CA针对任何计划内的密钥更替事件，将遵循以下规定对订户进行通告：

1. 提前通知义务：对于所有计划中的 CA 密钥更替，亚洲诚信CA会提前通知订户。该通知旨在确保订户有足够的时间对其生成产品或系统环境进行必要的配置更新，以维持 C2PA 信任链的完整性与连续性。
2. 通知时限：亚洲诚信CA在密钥更替正式实施前的合理时间内发出通知。通知的时限设定将充分考虑订户更新系统、进行兼容性测试以及部署新信任锚点所需的周期，确保将对订户业务的影响降至最低。

## 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。

#### 5.7.2.1 备份存储

亚洲诚信CA对关键业务数据、配置文件、归档记录及审计日志数据进行备份，并运送到异地安全场所保存。备份介质的存放设施符合本 CPS 第 5.1.6 节规定的物理访问控制标准，需至少 2 名可信人员在场方可访问。为确保备份数据在极端情况下依然具备有效性，亚洲诚信CA根据策略要求定期对备份数据进行可恢复性测试，验证备份介质的完整性及数据还原流程的准确性，以确保在需要时能迅速恢复业务运营。

2. **恢复计划**

亚洲诚信CA制定并维护一套详尽的、有正式文件记录的业务连续性计划和灾难恢复计划。该计划明确了在发生自然灾害、安全事件、计算机资源毁坏或大规模系统故障后恢复运行的详细程序。

## 5.7.3 私钥泄漏处理程序

1. 当证书订户发现证书私钥泄漏时，订户必须立即停止使用其私钥，并立即访问亚洲诚信CA证书服务站点撤销其证书，或立即通过电话邮件等方式通知亚洲诚信CA撤销其证书，并按照相关流程重新申请新的证书。亚洲诚信CA将按本CPS第4.9节发布证书撤销信息。
2. 当亚洲诚信CA订户的证书私钥受到泄漏时，亚洲诚信CA将立即撤销证书，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CA将按本CPS第4.9节发布证书撤销信息。

3. 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，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订户；
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。

密钥生成仪式脚本包含：

a. 角色和参与者职责定义；
b. 密钥生成仪式的授权或批准；
c. 仪式所需的加密硬件和激活材料；
d. 密钥生成仪式期间执行的具体步骤；
e. 仪式地点的物理安全要求；
f. 仪式后安全存储加密硬件和激活材料；
g. 参与者和见证人签字，表明仪式按照脚本执行；及
h. 密钥生成仪式中的异常或偏差。

#### 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

订户密钥对由订户自身生成，亚洲诚信CA不替订户生成证书密钥对。

订户生成密钥对的要求在 C2PA 合规计划的实施安全要求文档中定义，并可能根据实现的保证级别而有所不同。

亚洲诚信CA 仅为符合 C2PA 内容凭证规范和本 CPS 证书规范部分适用要求的声明签名密钥签发证书。

无论保证级别如何，订户只能将根据本 CPS 签发证书的密钥，用于签署由作为证书主体的设备或应用程序生成的 C2PA 声明。

### 6.1.2 私钥传送给订户

亚洲诚信CA不为用户生成和交付私钥。

### 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C2PA官网获取根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 或<br>SHA384 |
| RSA密钥长度 | 4096 | 4096 | 2048或3072或4096 |
| ECC 曲线 | P-384 | P-384 | P-256或P-384或P-521 |
| EdDSA 曲线 | - | - | Ed25519 |

### 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CPS 6.1.5中的要求。

亚洲诚信CA在签发证书前，会进行公钥参数检测，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；
3. OCSP响应签名证书；
4. 基础设施用途证书（管理角色证书、CA 内部运行设备证书）。

中级 CA 密钥一般用于签发以下证书和 CRL：

1. 订户证书；
2. 时间戳签名证书；
3. OCSP 响应签名证书。

订户的密钥根据签发的中级CA证书的密钥用法扩展项可以用于C2PA声明签名或时间戳服务身份证明或OCSP签名。

# 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。

用于保证级别2的密码模块符合或高于以下标准：

- FIPS140-2 Level 2，或
- CC EAL 4+ 或更高。

用于时间戳证书的密码模块符合或高于以下标准：

- FIPS140-2 Level 3，或
- CC EAL 4或更高。

## 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

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由多人控制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）。亚洲诚信CA制定了CA密钥备份恢复计划，并每年对该计划审查和恢复演练。

### 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

#### 6.2.7.1 CA密钥的私钥存储

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。

#### 6.2.7.2 时间戳服务的私钥存储

亚洲诚信CA用于时间戳服务的私钥存储符合本CPS第6.2.7.1节要求。

### 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

亚洲诚信CA证书的最长有效期为：

| 类型 | 私钥使用期限 | 证书期限 |
| --- | --- | --- |
| C2PA根CA | 无规定 | 25年 |
| C2PA声明签名中级CA | 无规定 | 5年 |
| C2PA时间戳CA | 无规定 | 15年 |
| 保证级别1级证书 | 无规定 | 不超过366天 |
| 保证级别2级证书 | 无规定 | 不超过90天 |
| 时间戳证书 | 无规定 | 不超过4110天 |

## 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。

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

### 6.4.3 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

订户的生成器产品应当遵守特定平台的安全指南和最佳实践，以防止未经授权的访问、恶意软件和其他网络威胁。

应当采用安全编码实践、代码签名和定期安全更新等安全措施。

对生成器产品内敏感数据或功能的访问应当受到限制，并由适当的身份验证和授权机制保护。

### 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

从签发到撤销的整个证书生命周期内，亚洲诚信CA实施安全控制以确保证书及其相关数据的机密性、完整性和可用性。

证书签发和撤销流程受到保护，防止未经授权的操作和篡改。

证书状态信息可通过 OCSP 或 CRL 等机制随时可供依赖方获取和访问。

## 6.7 网络的安全控制

亚洲诚信CA对网络安全采取以下控制：

1.生成器产品实例在证书操作期间与CA或RA交互时，采用了安全的通信协议和实践；

2.保护网络流量，防止窃听、篡改和未经授权的访问；

3.可信人员远程访问CA系统时需身份验证；

4.可信人员或CA系统与远程计算机建立连接时进行身份验证。

5.采用最小开放授权原则，未开放的端口访问限制。

6.采用防火墙来保护CA的内部网络免受来自其它区域的未经授权的访问。

7.采用最小开放授权原则，只向授权用户开放可用的网络服务，如SSH、https等。

8.记录所有网络的安全配置。

9.实施路由控制，确保计算机连接和信息流符合访问控制策略。

10.定期维护物理安全环境中的本地网络组件，并定期审核其配置以符合配置要求。

11.通过公共网络或不受信任的网络交换敏感数据时，对敏感数据进行加密。

# 6.8 时间戳

亚洲诚信CA的C2PA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。

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UTC(k)实验室同步，并将其时钟的精确度保持在一秒或更少。亚洲诚信CA会检测时间戳应用服务，若超过精度范围，时间戳应用服务将暂停签署时间戳。

时间戳应用服务使用专门保留的私钥进行签名，一个时间戳应用服务一次只有一个有效的签名密钥。

TSA的密钥生成符合本CPS第6.1.1节要求，TSA的密钥存储符合本CPS第6.2.7节要求。

# 7. 证书、证书撤销列表和在线证书状态协议

## 7.1 证书

亚洲诚信CA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。见本CPS第11章。

### 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中subjectPublicKeyInfo，不使用其它编码。

**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。

**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。

**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 |

**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。

### 7.1.4.1 名称编码

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

不适用。

## 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

同本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 | | | |
| | 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7天，中级证书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

## 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与渗透测试，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. 每年对物理控制、密钥管理、操作控制、鉴别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。
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。

## 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

审计工作涉及以下内容：

1. 证书生命周期管理程序：审查证书的签发、更新及撤销流程。重点核实亚洲诚信在操作过程中是否严格通过“合规产品列表”验证生成产品的合规状态，以及是否满足严禁旧密钥重用的政策要求。
2. 认证验证：评估 CA 在处理自动化证书注册请求时，对生成产品实例提供的动态证据的校验准确性。审计应确认 CA 是否正确解析了由硬件信任根支持的背书报告，并根据相应的保证等级核实了平台安全属性。
3. 密钥管理实践：审计范围涵盖亚洲诚信 CA 基础设施内的密钥生命周期管理，以及对订户生成产品内密

钥生成环境和保护措施的监督与验证实践。

4. 逻辑与程序性安全控制：验证 CA 认证系统的逻辑访问控制是否遵循“知所必须”与“最小权限”原则。同时，审计应覆盖职责分离的实施情况，确保认证验证、证书签发等关键职能由不同受信任角色履行。
5. 人员安全与培训：核查涉及背书验证和证书管理岗位人员的背景调查及资质。重点评估针对 C2PA 业务特有的技术流程所开展的岗前培训、定期再培训及其考核记录的完整性。
6. 事件响应与灾难恢复程序：验证业务连续性计划及灾难恢复计划的有效性。审计应重点关注：在私钥泄露或安全事故后的通报机制、关键数据的异地备份完整性以及业务连续性计划的演练记录。

第三方审计师事务所按照WebTrust CA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。

针对 C2PA 业务的审计报告管理遵循以下规范，以确保评估过程的透明性与纠正措施的有效性：

1. 不合规项的明确标识：审计报告应由独立审计机构出具，并在报告中清晰、准确地标识出任何不符合项安全缺陷或建议改进的领域，以便相关方评估亚洲诚信 PKI 系统的运营风险及合规程度。
2. 纠正措施与持续改进：针对内部审计或第三方审计中发现的问题与不足，亚洲诚信将采取以下措施：
    a. 由审计评估小组负责监督相关责任部门，针对发现的缺陷制定并执行纠正措施。
    b. 在规定期限内完成整改后，亚洲诚信应按照第三方审计机构的要求，接受再次审计或验证评估，以确认缺陷已得到有效修复。

亚洲诚信承诺将审计整改结果及处理情况留档，并作为后续合规评估的重要参考。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。应 C2PA 指导委员会及其他获授权方的正式请求，亚洲诚信应向其提供完整的合规审计报告及相关的解释性说明文件。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根据本CPS的规定，针对 C2PA 业务的安全性保障，在自评估体系中特别纳入以下安全事件审查机制：

1. 安全事件审查：
    a. 深度追溯：若发生安全事件，亚洲诚信必须进行彻底审查，以准确确定事件的根本原因、波及影响范围以及所取得的经验教训。
    b. 预防机制：审查过程必须产生具有可操作性的整改建议，旨在通过技术或流程改进，有效防止未来再次发生类似的机密性、完整性或可用性受损事件。
2. 信息共享与合规透明： 相关的安全事件审查报告必须与 C2PA 指导委员会以及 C2PA 技术工作组合规任务组共享，以确保生态系统治理方能及时掌握潜在风险并协同应对。

# 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。订户应承担其在本CPS下获得电子认证服务所产生的全部费用。

### 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。

### 9.1.6 费用调整

亚洲诚信CA保留根据市场环境、技术成本或治理要求修改其费用结构（包括证书签发、更新及相关技术服务费率）的权利。在实施任何费用调整之前，亚洲诚信将按照本 CPS 第 9.12.2 节的规定，通知受影响的订户。此类提前通知旨在确保费用管理的透明度与可预测性，以便订户能够有充足的时间进行预算规划或系统配置调整。

## 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。

### 9.2.4 订户财务责任

订户承担证书全生命周期内产生的全部费用，包括但不限于证书的签发、更新、撤销以及相关的技术服务费。订户应按照与亚洲诚信CA签署的《订户协议》或官方公示的价格标准及时足额支付款项。若订户未能按时履行缴费义务，亚洲诚信有权依据本规程撤销其证书并终止服务。

## 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。

除法律、行政法规及政府主管部门强制性要求，或因 WebTrust 等独立合规审计需要外，亚洲诚信承诺未经订户明确书面许可，不得将订户协议、审计记录及其他非公开业务信息泄露给任何第三方。亚洲诚信将依据法律及行政程序，在必要时向执法或行政机关披露相关信息。

### 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、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保证不会把订户个人信息提供给无关的第三方(包括公司或个人)。

## 9.4.5.1 目的限制

个人信息的收集与利用严格限于身份鉴别、证书签发及管理等本CPS明确规定的业务目的。未经订户许可，亚洲诚信CA保证不将除证书内置资料外的个人信息提供给第三方，法律法规或政府强制性要求除外。

## 9.4.5.2 主体权利

订户享有访问、更正或依法申请删除其在亚洲诚信CA留存的个人信息的权利。亚洲诚信CA在确保符合国家法律法规及电子认证业务监管约束的前提下，尊重并保障订户对其隐私数据的控制权。

## 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。

## 9.5.1 订户所有权

订户对其使用根据本CPS签发的证书进行签名的“声明生成实现”所涉及的所有知识产权，拥有完整的合法所有权和控制权。

## 9.5.2 认证机构所有权

亚洲诚信不对订户的上述技术实现或其涉及的知识产权主张任何所有权或权利要求。

# 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CA在提供电子认证服务活动过程中对订户的承诺如下：

1. 名称使用权担保：亚洲诚信CA保证已实施并严格遵循本CPS描述的程序，验证申请人对证书内产品名称及相关标识符拥有合法的权利或控制权。
2. 签发授权担保：亚洲诚信CA保证已通过正式程序验证证书主体已授权签发，并确认申请人代表具有合法请求权，且相关验证流程已在本文档中准确披露。
3. 信息准确性担保：亚洲诚信CA担保已执行完整程序验证证书内所有信息的准确性，并在签发过程中严格遵守本CPS披露的核实逻辑。
4. 协议合规性：亚洲诚信CA确保与订户已签署合法有效的《订户协议》，或其代表已明确认可使用条款。
5. 状态服务：亚洲诚信CA维护 7×24 小时公开访问的信息库，实时提供证书的有效或撤销状态。
6. 及时撤销：亚洲诚信CA承诺，在发生本CPS规定的撤销情形时，将按照既定时限履行撤销义务。

根 CA 责任： 亚洲诚信根 CA (Root CA) 对应其下级签发 CA 的合规性、履行行为及担保义务承担全部赔偿与连带责任，视同根 CA 亲自签发该证书。

## 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 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CPS中的所有条款和条件，并知悉和接受相应的订户协议。
2. 在证书的有效期内进行数字签名。
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. 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。
5. 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。
6. 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。
7. 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。
8. 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。
9. 采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件。

### 9.6.4 依赖方的陈述与担保

1. 遵守本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CPS的所有规定。

## 9.7 担保免责

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

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，由此造成的客户损失。
5. 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CA违反了本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：

- 在任何情况下，每张证书赔偿额，不得超过该证书市场购买价格的10倍。
- 每张证书基于每个订户或每个依赖方的赔偿额不低于2000美金。

如出现下述情形，亚洲诚信CA承担有限赔偿责任：

1. 亚洲诚信CA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；
2. 在订户提交信息或资料准确、属实的情况下，亚洲诚信CA签发的证书出现了错误信息，导致订户遭受损失的；
3. 在亚洲诚信CA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；
4. 由于亚洲诚信CA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；
5. 亚洲诚信CA未能及时撤销证书，导致订户遭受损失的。

另外，亚洲诚信CA赔偿限制如下：

1. 亚洲诚信CA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. 对于由订户或依赖方的原因造成的损失，亚洲诚信CA不承担责任，由订户或依赖方自行承担。
3. 亚洲诚信CA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。亚洲诚信CA对外公布准确且最新的联系方式，以便有效沟通。

## 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编写小组不定期修订本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，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CPS经过亚洲诚信CA 安全策略委员会批准后正式对外发布。在本CPS修订后继续使用亚洲诚信CA办法的证书，即构成订户对修订后条款和条件的接受。

### 9.12.2 通知机制和期限

修订后的CPS经批准后将立即在亚洲诚信CA官网发布。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

C2PA证书策略以及其产生的任何协议应受美国特拉华州法律管辖，并据其进行解释。对于相关C2PA业务协议引起的任何争议、诉讼或法律程序，各方一致同意由美国特拉华州的州法院或联邦法院行使排他性司法管辖权。

# 9.15 与适用法律的符合性

本 CPS 受适用的国家、州、地方和外国法律、法规、条例、条例、法令和命令的约束，包括但不限于对出口或进口软件、硬件或技术信息的限制。

亚洲诚信 CA 根据本 CPS 下运营的均应遵守适用法律。

# 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

### 9.16.1.1 CA与C2PA管理机构

亚洲诚信CA与 C2PA 管理机构之间的权利义务关系受双方签署的《电子认证服务机构协议》及本CPS的约束。

### 9.16.1.2 CA与订户

亚洲诚信CA与订户之间的法律关系受双方签署的《订户协议》及本规程相关条款的约束。

## 9.16.2 转让

亚洲诚信CA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CA事先书面同意的情况下，不能通过任何方式进行转让。

## 9.16.3 分割性

如果确定本 CPS 的一个部分不正确或无效，则本 CPS 的其他部分应保持有效，直到本 CPS 更新。

如果本 CPS 的条款或规定被法院或其他具有权力的法庭认定为不可执行，则 CPS的其余部分仍然有效。

## 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CA将不对此类事件负责。

## 9.17 其他条款

亚洲诚信CA对本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<br>验证CSR公钥长度<br>验证CSR公钥是否为弱密钥 |
| 组织验证 | 核实申请人名称是否合法合规<br>核实申请人是否合法存续经营<br>核实申请人的所在地的国家省份城市及地址<br>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<br>遵循CPS 3.2.2 |
| 个人身份验证 | 通过联系申请人代表核实申请人的申请意愿。 |
| 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；<br>与律师核对所签署的律师函的真实性、准确性。 |
| 合规项验证 | 保证1级和2级基础的合规项：<br>• 验证自动化申请证书能力<br>• 验证CPL的recordID（UUID）<br>• 验证DN与CPL记录中的信息匹配<br>• 验证CPL中记录的最高保证级别<br>• 生成器产品存在于CPL且状态显示为“合规”<br>保证级别2级动态证据验证项：<br>• 生成私钥的加密硬件模块证明<br>• 生成器产品平台证明报告<br>• 最高保证级别的验证方法 |

# 11 附录B–证书内容模板

## 11.1 根证书

注:证书分成RSA和ECC两个系列，模板将体现有区分之处

| 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 |
| TBSCertificate签名 | | | TrustAsia C2PA RSA Root CA:sha384withRSA<br>TrustAsia C2PA ECC Root CA:sha384withECDSA |
| 签发者 | | | 和主题逐字节匹配 |
| 有效期:notBefore | | | 距签发时间相差不超过24小时 |
| 有效期:notAfter | | | 25年 |
| 主题 | 通用名称（CN） | | TrustAsia C2PA RSA Root CA或<br>TrustAsia C2PA ECC Root CA |
| | 组织（O） | | TrustAsia Technologies, Inc. |
| | 国家（C） | | CN |
| 公钥信息 | | | RSA 4096<br>ECDSA 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 | 与subjectKeyIdentifier匹配 |
| 扩展: basicConstraints | | 关键 | Subject Type=CA<br>Path Length Constraint=2 |
| 扩展：keyUsage | | 关键 | keyCertSign，cRLSign |

## 11.2 中级证书

### 11.2.1 C2PA声明签名中级证书

| 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 |
| TBSCertificate签名 | | | TrustAsia C2PA Claim Signing RSA CA 2026:<br>sha384withRSA<br>TrustAsia C2PA Claim Signing ECC CA 2026:<br>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 | | | 不超过1827天 |
| 主题 | 通用名称（CN） | | TrustAsia C2PA Claim Signing RSA CA 2026 或TrustAsia C2PA Claim Signing ECC CA 2026 |
| | 组织（O） | | TrustAsia Technologies, Inc. |
| | 国家（C） | | CN |
| 公钥信息 | | | RSA 4096 或 ECDSA 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 | Policy Identifier=1.3.6.1.4.1.62558.1.1 |
| 扩展: basicConstraints | | 关键 | Subject Type=CA<br>Path Length Constraint=0 |
| 扩展：keyUsage | | 关键 | keyCertSign，cRLSign |
| 扩展: extKeyUsage | | 非关键 | c2pa-kp-claimSigning(1.3.6.1.4.1.62558.2.1)<br>id-kp-emailProtection(1.3.6.1.5.5.7.3.4)<br>id-kp-documentSigning(1.3.6.1.5.5.7.3.36) |
| 扩展: authorityInfoAccess | | 非关键 | ICA AccessMethod=1.3.6.1.5.5.7.48.2<br>URL=http://ica.c2pa.trustasia.com/<Issuername>.crt<br>OCSP AccessMethod=1.3.6.1.5.5.7.48.1<br>URL=http://ocsp.c2pa.trustasia.com/<Issuername> |

| 证书字段 | 关键扩展项 | 内容 |
| --- | --- | --- |
| 扩展: cRLDistributionPoints | 非关键 | CRL HTTP<br>URL=http://crl.c2pa.trustasia.com/<Issuername>.crl |

### 11.2.2 C2PA时间戳签名中级证书

| 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 |
| TBSCertificate签名 | | | TrustAsia C2PA TSA RSA CA 2026:<br>sha384withRSA<br>TrustAsia C2PA TSA ECC CA 2026:<br>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 | | | 15年 |
| 主题 | 通用名称（CN） | | TrustAsia C2PA TSA RSA CA 2026 或<br>TrustAsia C2PA TSA ECC CA 2026 |
| | 组织（O） | | TrustAsia Technologies, Inc. |
| | 国家（C） | | CN |
| 公钥信息 | | | RSA 4096 或 ECDSA 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 | Policy Identifier=1.3.6.1.4.1.62558.1.1 |
| 扩展: basicConstraints | | 关键 | Subject Type=CA<br>Path Length Constraint=0 |
| 扩展：keyUsage | | 关键 | keyCertSign，cRLSign |
| 扩展: extKeyUsage | | 非关键 | id-kp-timeSigning(1.3.6.1.5.5.7.3.8) |

| 证书字段 | 关键扩展项 | 内容 |
| --- | --- | --- |
| 扩展: authorityInfoAccess | 非关键 | ICA AccessMethod=1.3.6.1.5.5.7.48.2<br>URL=http://ica.c2pa.trustasia.com/<Issuername>.crt<br>OCSP AccessMethod=1.3.6.1.5.5.7.48.1<br>URL=http://ocsp.c2pa.trustasia.com/<Issuername> |
| 扩展: cRLDistributionPoints | 非关键 | CRL HTTP<br>URL=http://crl.c2pa.trustasia.com/<Issuername>.crl |

# 11.3 订户（终端实体）证书

## 11.3.1 C2PA保证1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 |
| TBSCertificate签名 | | | sha256withRSA 或 sha384withRSA 或<br>sha384withECDSA 或 Ed25519 |
| 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 | | | 不超过366天 |
| 主题 | 通用名称（CN） | | 与C2PA合规产品DN内容一致，其中CN、O、C必须、OU根据CPL中OU的存在 |
| | 组织（O） | | |
| | 部门（OU） | | |
| | 国家（C） | | |
| 公钥信息 | | | RSA2048 \| 3072 \| 4096 或 ECC P-256 \| P-384 \| P-521 或 Ed25519 |
| 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 | Policy Identifier=1.3.6.1.4.1.62558.1.1 |

| 证书字段 | 关键扩展项 | 内容 |
| --- | --- | --- |
| 扩展: basicConstraints | 关键 | Subject Type=End Entity<br>Path Length Constraint=None |
| 扩展：keyUsage | 关键 | digitalSignature,nonRepudiation |
| 扩展: extKeyUsage | 非关键 | c2pa-kp-claimSigning(1.3.6.1.4.1.62558.2.1)<br>id-kp-emailProtection(1.3.6.1.5.5.7.3.4)<br>id-kp-documentSigning(1.3.6.1.5.5.7.3.36) |
| 扩展: authorityInfoAccess | 非关键 | ICA AccessMethod=1.3.6.1.5.5.7.48.2<br>URL=http://ica.c2pa.trustasia.com/<Issuername>.crt<br>OCSP AccessMethod=1.3.6.1.5.5.7.48.1<br>URL=http://ocsp.c2pa.trustasia.com/<Issuername> |
| 扩展: cRLDistributionPoints | 非关键 | CRL HTTP<br>URL=http://crl.c2pa.trustasia.com/<Issuername>.crl |
| 扩展：C2PA Assurance Level(1.3.6.1.4.1.62558.3) | 非关键 | 1.3.6.1.4.1.62558.3.10 |
| 扩展：C2PA CPL Record ID(1.3.6.1.4.1.62558.4) | 非关键 | 36字符的CPL中生成器产品的UUID |

### 11.3.2 C2PA保证2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 |
| TBSCertificate签名 | | sha256withRSA 或 sha384withRSA 或<br>sha384withECDSA 或 Ed25519 |
| 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 | | 不超过90天 |

| 证书字段 | | 关键扩展项 | 内容 |
| --- | --- | --- | --- |
| 主题 | 通用名称（CN） | | 与C2PA合规产品DN内容一致，其中CN、O、C必须、OU可选 |
| | 组织（O） | | |
| | 部门（OU） | | |
| | 国家（C） | | |
| 公钥信息 | | | RSA2048 \| 3072 \| 4096 或 ECC P-256 \| P-384 \| P-521 或 Ed25519 |
| 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 | Policy Identifier=1.3.6.1.4.1.62558.1.1 |
| 扩展: basicConstraints | | 关键 | Subject Type=End Entity<br>Path Length Constraint=None |
| 扩展：keyUsage | | 关键 | digitalSignature,nonRepudiation |
| 扩展: extKeyUsage | | 非关键 | c2pa-kp-claimSigning(1.3.6.1.4.1.62558.2.1)<br>id-kp-emailProtection(1.3.6.1.5.5.7.3.4)<br>id-kp-documentSigning(1.3.6.1.5.5.7.3.36) |
| 扩展: authorityInfoAccess | | 非关键 | ICA AccessMethod=1.3.6.1.5.5.7.48.2<br>URL=http://ica.c2pa.trustasia.com/<Issuername>.crt<br>OCSP AccessMethod=1.3.6.1.5.5.7.48.1<br>URL=http://ocsp.c2pa.trustasia.com/<Issuername> |
| 扩展: cRLDistributionPoints | | 非关键 | CRL HTTP<br>URL=http://crl.c2pa.trustasia.com/<Issuername>.crl |
| 扩展：C2PA Assurance Level(1.3.6.1.4.1.62558.3) | | 非关键 | 1.3.6.1.4.1.62558.3.20 |
| 扩展：C2PA CPL Record ID(1.3.6.1.4.1.62558.4) | | 非关键 | 36字符的CPL中生成器产品的UUID |

### 11.3.3 OCSP签名证书

| 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 |
| TBSCertificate签名 | | | 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 | | | 不超过签名CA的notAfter |
| 主题 | 通用名称（CN） | | <CA Common Name> - OCSP Responder |
| | 组织（O） | | TrustAsia Technologies, Inc. |
| | 国家(C) | | CN |
| 公钥信息 | | | RSA 2048 \| 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: basicConstraints | | 关键 | Subject Type=End Entity<br>Path Length Constraint=None |
| 扩展：keyUsage | | 关键 | digitalSignature |
| 扩展: extKeyUsage | | 非关键 | OCSP 签名 (1.3.6.1.5.5.7.3.9) |
| 扩展: id-pkix-ocsp-nocheck(1.3.6.1.5.5.7.48.1.5) | | 非关键 | 0x0500 |

### 11.3.4 时间戳证书

| 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 |
| TBSCertificate签名 | | sha256withRSA 或 sha384withRSA 或<br>sha384withECDSA 或 Ed25519 |
| 签发者 | | 与签发CA的Subject逐字节匹配 |

| 证书字段 | | 关键扩展项 | 内容 |
| --- | --- | --- | --- |
| 有效期:notBefore | | | 距签发时间相差不超过24小时 |
| 有效期:notAfter | | | 不超过4110天 |
| 主题 | 通用名称（CN） | | TrustAsia C2PA Time-Stamp Signing RSA \| ECC <年份> |
| | 组织（O） | | TrustAsia Technologies, Inc. |
| | 国家（C） | | CN |
| 公钥信息 | | | RSA2048 \| 3072 \| 4096 或 ECC P-256 \| P-384 \| P-521 或 Ed25519 |
| 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 | Policy Identifier=1.3.6.1.4.1.62558.1.1 |
| 扩展: basicConstraints | | 关键 | Subject Type=End Entity<br>Path Length Constraint=None |
| 扩展：keyUsage | | 关键 | digitalSignature,nonRepudiation |
| 扩展: extKeyUsage | | 关键 | id-kp-timeSigning(1.3.6.1.5.5.7.3.8) |
| 扩展: authorityInfoAccess | | 非关键 | ICA AccessMethod=1.3.6.1.5.5.7.48.2<br>URL=http://ica.c2pa.trustasia.com/<Issuername>.crt<br>OCSP AccessMethod=1.3.6.1.5.5.7.48.1<br>URL=http://ocsp.c2pa.trustasia.com/<Issuername> |
| 扩展: cRLDistributionPoints | | 非关键 | CRL HTTP<br>URL=http://crl.c2pa.trustasia.com/<Issuername>.crl |