亚洲诚信全球可信服务证书策略和电子认证业务规则（CP&CPS）

V2.1.1

亚数信息科技（上海）有限公司

2025-12-22

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 签发的 CA 证书信息见信息库 https://repository.trustasia.com 。

1.1.3 证书策略（CP）与电子认证业务规则（CPS）

本《证书策略与电子认证业务规则》(简称 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. CA/Browser 论坛（ https://cabforum.org ）发布的以下最新版要求（自本 CP&CPS 发布前）：
    - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
    - Network and Certificate System Security Requirements
    - Guidelines for the Issuance and Management of Extended Validation Certificates
    - Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
    - Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

3. Mozilla Root Store Policy
4. Microsoft Trusted Root Program
5. AATL Technical Requirements
6. Apple Root Certificate Program
7. Chrome Root Program
8. 360 Browser Root Certificate Program
9. Oracle Root Certificate Program

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。若中国法律法规或政府机构认定 EVG 中的任何规定是非法的，亚洲诚信 CA 将通知 CA/Browser 论坛。

1.2 文档名称与标识

本文档为亚洲诚信全球可信服务证书策略和电子认证业务规则。

1.2.1 证书策略标识

CA/B Forum OID({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1)}):

对象标识符（OID）	标识代表对象
2.23.140.1.2.1	域名型 TLS 服务器证书策略标识
2.23.140.1.2.2	企业型 TLS 服务器证书策略标识
2.23.140.1.1	增强型 TLS 服务器证书策略标识
2.23.140.1.4.1	企业型代码签名证书策略标识
2.23.140.1.4.2	时间戳证书策略标识
2.23.140.1.3	增强型代码签名证书策略标识
2.23.140.1.5.1.3	基础型邮件安全证书策略标识
2.23.140.1.5.4.2	个人型邮件安全证书策略标识
2.23.140.1.5.2.3	企业型邮件安全证书策略标识
2.23.140.1.5.3.2	企业型邮件安全证书高级版策略标识

TrustAsia OID（{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 44494}）：

对象标识符（OID）	标识代表对象
1.3.6.1.4.1.44494.2.1.3	域名型 TLS 服务器证书策略标识
1.3.6.1.4.1.44494.2.1.2	企业性 TLS 服务器证书策略标识

对象标识符（OID）	标识代表对象
1.3.6.1.4.1.44494.2.1.1	增强型 TLS 服务器证书策略标识
1.3.6.1.4.1.44494.2.2.1	企业型代码签名证书策略标识
1.3.6.1.4.1.44494.2.2.2	增强型代码签名证书策略标识
1.3.6.1.4.1.44494.2.3.1	Adobe 文档签名证书策略标识
1.3.6.1.4.1.44494.2.4.3.3	基础型邮件安全证书策略标识
1.3.6.1.4.1.44494.2.4.6.2	个人型邮件安全证书策略标识
1.3.6.1.4.1.44494.2.4.4.3	企业型邮件安全证书策略标识
1.3.6.1.4.1.44494.2.4.5.2	企业型邮件安全证书高级版策略标识
1.3.6.1.4.1.44494.2.5.1	时间戳证书策略标识
1.3.6.1.4.1.44494.2.5.2	Adobe 文档签名时间戳证书策略标识

1.2.2 修订历史

发布日期	更新内容	发布版本
2020-08-25	发布初版	V1.1
2020-10-23	• 更新 2.2.2，说明 CRL 的序列号为递增。 • 更新 2.4 及 2.5 的编号。 • 更新 5.1.1，CA 机房的建设实施标准。 • 更新 6.2.10，说明 CA 不得损坏 CA 私钥的限制 • 更新 9.14，更新适用的当地法律法规。	V1.2
2021-05-18	• 全篇章节及格式调整，以对应 CA/Browser 目录 • 更新第 1 章，优化公司介绍、证书层次结构和文档标识 OID • 更新第 3 章，更新商标的识别、初始身份确认 • 更新 4.9 证书撤销 • 更新 5.7.3 私钥损害处理程序 • 更新 6.1.5，密钥长度 • 更新第 7 章，阐明证书扩展项及算法对象标识符 • 新增附录 A(10) 验证要求	V1.3

发布日期	更新内容	发布版本
2021-10-28	• 更新第 1 章，补充本 CP&CPS 遵循的要求，阐明禁止中间人攻击用途的证书申请 • 更新 2.2.3，更新 OCSP 发布频率 • 更新第 3 章，阐明组织机构和通配符域名的身份鉴别，CAA 中 idoef 属性的说明 • 更新第 4 章，补充身份识别与鉴别的执行、阐明所有直接签发证书的账户部署了多因素认证、补充证书撤销情形及撤销时间限制 • 更新第 5 章，阐明记录事件类型、审计日志、时间戳机构的要求等 • 更新第 6 章，阐明密钥对生成的要求、订户证书 RSA 密钥长度限制、公钥参数的生成及质量检查、密钥使用目的、密码模块标准、网络安全控制标准以及时间戳要求 • 更新 7.2.2 补充 reasonCode 扩展项 • 更新第 9 章，阐明 CGL 与 PI 保险、知识产权共享协议、EV 证书的赔偿范围 • 更新附录 A(10) 验证要求	V1.4
2022-05-24	• 更新第 1 章，优化公司介绍，阐明时间戳证书 OID 及文档签名时间戳证书 OID • 更新第 3 章，阐明国际化域名处理方法、邮件地址等验证方法 • 更新第 5 章，新增记录和归档文件的种类 • 更新第 6 章，增加代码签名证书的相关要求、补充密钥保护和验证方法、阐明邮件安全证书最长有效期及时间戳证书时效 • 更新 7.1.4 补充名称格式相关内容 • 简化修订历史，删除“编辑”和“评论”列	V1.5

发布日期	更新内容	发布版本
2022-12-15	• 更新全文，统一称谓、术语名词，并调整格式和语法以符合最新版 BRs 要求 • 更新第 1 章，新增邮件安全证书相关的 OID • 更新 2.3，调整 CPS 和订户证书 CRL 的发布频率 • 更新第 3 章，新增各类证书的主体甄别名、阐明对各类邮件安全证书相关的规定和鉴别要求、补充 ACME 协议下私钥拥有的证明方法、补充验证数据的相关要求 • 更新第 4 章，补充根证书签发前的授权操作和服务器证书签发前的检查操作，阐明 CRLReason 用法、撤销请求的处理、OCSP 请求中证书序列号要求、ACME 协议下密钥泄露证据 • 更新第 5 章，补充 CA 开发维护、证书管理、风险评估的控制目标、风险评估及业务连续性计划内容，调整归档记录的类型及保存期限、阐明并限定通知相关实体的时限 • 更新第 6 章，阐明证书签发前对密钥长度和公钥参数的检测要求、补充私钥保护的控制 • 更新第 7 章，调整订户证书的扩展项、阐明 RFC5280 中预证书、补充算法的使用要求 • 更新第 8 章，阐明审计遵守的要求及审计评估的传达 • 更新附录 A(10.2)，调整各类订户证书验证项 • 新增附录 B(11)，展示各证书内容模板	V1.6
2023-02-10	• 将“修订历史”移至第 1.2.2 节 • 更新附录 B (11)	V1.6.1
2023-08-30	• 根据 SC-062 更新了第 7 章（该调整于 2023-09-01 与 SMC-001 同步生效） • 更新文档签名证书 OU 字段的验证说明 • 更新 1.6 缩写的定义 • 更新 2.4 语言描述 • 更新 3.2 补充对商业实体中“主要个人”的验证要求，对 subject:organizationalUnitName 字段的描述，以及对申请文件进行“关于个人信息陈述的”限定 • 更新 9.16.3 内容 • 更新附录 B（11），使证书模板的顺序与 BR 一致，并新增 OCSP 签名证书模板	V1.7.0
2023-12-21	• 2024-03-15 遵循 SC-063 更新了 4.9 章相关内容 • 更新 7.2，补充 CRL 相关内容和要求 • 证书模版中添加 SCT 扩展	V1.7.1

发布日期	更新内容	发布版本
2024-04-25	• 根据 SMC05，更新 4.2.4，更新 CAA 相关信息 • 根据 SC69v3 更新 5.4.1.1，阐述对防火墙以及路由器的日志要求 • 根据 CSC-22，更新 6.2.7, 高风险变更 • 根据 CSC-24，更新对时间戳私钥的保护 • 调整全文，统一使用“签发”代替“颁发”数字证书 • 更新附录证书模板	V1.7.2
2024-07-23	• 加入专用 CA 系列 • 调整 CAA 部分的描述 • 根据 SC-75，增加证书签名流程中的 linting 控制描述 • 更新 5.2 程序控制中对人员职责分割的要求	V2.0.0
2024-10-22	• 根据 SC-67，调整 3.2.2.9 • 禁用第 3.2.2.4.2 的域名验证方法 • 根据 SC-76，调整第 4.9.9 节、第 4.9.10 节 • 优化第 7.3.2 节等关于 OCSP 的要求等相关描述	V2.0.1
2025-06-13	• 根据 MRSP v3.0 要求，将 CPS 标题对齐 RFC3647 标题结构 • 根据 SC-84 新增 3.2. 2.4.21 • 根据 SC-83 CPS 更新 • 根据 SC-81v3，调整审核信息复用时长及证书有效期 • 2025-09-15 起拒绝为 arpa 域名颁发证书	V2.0.2
2025-08-28	• 根据SC-79v2，增加交叉认证CA的章节 • 根据SC-085,增加关于DNSSec相关的内容 • 根据SC-89，添加批量撤销相关内容 • 根据NSR-008，在6.7节中添加漏洞时间管理	V2.0.3
2025-10-20	• 调整第1.1.2章节PKI显示，调整至信息库，去除G1和G2相关内容，并增加新的ICA。 • 根据新的产品结构，调整第6.1.5章节、第10.2章、第11章。	V2.1.0
2025-12-22	• 根据CSC-31调整代码签名的最大有效期。 • 根据SC-88v3添加第3.2.2.4.22章节。 • 根据SC-91 添加第3.2.2.5.3章节。 • 清理工作，包括第9.9章、第3.2.2.4章、第7.1.2.7.9章等。	V2.1.1

1.3 PKI 参与者

1.3.1 电子认证服务机构

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

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

亚洲诚信 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

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，可以是个人、机构、或设备。订户通常需要同亚洲诚信 CA 签订合约以获得证书，并承担作为证书订户的责任。

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

1.3.4 依赖方

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

1.3.5 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。

1.4 证书应用

1.4.1 适合的证书应用

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

1.4.2 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。

1.4.3 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。

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

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 CA/Browser 论坛发布的 BR 和 EVG 的最新要求每年修订，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
安全策略委员会	认证服务体系内的最高策略管理监督机构和 CPS 一致性决定机构
电子认证服务机构（CA）	证书认证机构，是签发证书的实体，负责建立，签发，撤销及管理证书的某个机构。该术语适用于根 CAs 及中级 CAs。
注册机构 (RA)	负责处理证书申请者和证书订户的服务请求，并将之提交给认证服务机构，为最终证书申请者建立注册过程的实体，负责对证书申请者进行身份标识和鉴别，发起或传递证书撤销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。
证书策略 (CP)	一套命名的规则集，用以指明证书对一个特定团体或者具有相同安全需求的应用类型的适用性。例如，一个特定的 CP 可以指明某类证书适用于鉴别从事企业到企业交易活动的参与方，针对给定价格范围内的产品和服务。

术语	定义
认证业务规则(CPS)	电子认证服务机构在签发、管理、撤销或更新证书、密钥过程中所采纳的业务实践的通告。
认证路径	一个有序的证书序列 (包含路径中起始对象的公钥)，通过处理该序列可获得末端对象的公钥。
策略限定符	依赖于策略的信息，可能与 CP 标识符共同出现在 X.509 证书中。该信息可能包含可用 CPS 或依赖方协议的 URL 地址，也可能包含证书使用条款的文字。
数字证书	使用数字签名绑定公钥和身份的电子文档
电子签名	具有识别签名人身份和表明签名人认可签名数据功能的技术手段。
数字签名	通过使用非对称密码加密系统对电子记录进行加密、解密变换来实现的一种电子签名。
电子签名人	是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的人。
电子签名依赖方	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。
订户	从电子认证服务机构接收证书的实体，也被称为证书持有人。在电子签名应用中，订户即为电子签名人。
订户协议	申请人在收到证书前必须阅读和接受的证书的签发和使用的协议。
依赖方	依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。
依赖方协议	在验证、依赖或使用证书或访问或使用亚洲诚信CA信息库之前必须由依赖方阅读和接受的协议。
WebTrust	CPA 加拿大针对认证服务机构的 WebTrust项目的当前版本。
P-Label	一种 XN-Lable，从第五个及其后位置的包含 Punycode 算法（RFC3492 第 6.3 节所定义）的有效输出。
Persistent DCV TXT Record	一种申请人用于使用第3.2.2.4.22章节方法申请域名验证的DNS TXT记录。
LDH-Label	由ASCII字母、数字和连字符组成的字符串，连字符不能出现在字符串的开头或结尾。与所有DNS标签一样，其总长度不得超过63个八位字节。（摘RFC5890 http://tools.ietf.org/html/rfc5890 ）

术语	定义
Linting	检查数字签名数据或待签名数据对象的内容是否符合BRs要求中定义的配置文件和要求的过程。
多视角签发确证(Multi-Perspective Issuance Corroboration)	在证书签发之前，由其他网络视角对主网络视角在域名验证和CAA检查过程中所做出的决定进行确证的过程。
网络视角(Network Perspective)	与多视角签发确证相关。用于发送与域名控制验证方法和（或）CAA检查相关的出站互联网流量的系统（如，云托管服务器实例）或网络组件集合（如，VPN及其相应的基础设施）。网络视角的位置取决于未封装的出站互联网流量在首次被传递给为该视角提供互联网连接的网络基础设施的地点。
主网络视角(Primary Network Perspective)	证书认证机构（CA）使用的网络视角，用于确定以下两点： 1) CA是否有权为请求的域名或IP地址签发证书； 2) 申请人是否具有对所请求的域名或IP地址的授权和(或)控制权。
地址和路由参数域名名称(Address and Routing Parameter Area Name)	顶级域名为“arpa”的域名。
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 (https://tools.ietf.org/html/rfc8499)，顶级域是比根域名低一级的区域，如“com”或“cn”。

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
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
MPIC	Multi-Perspective Issuance Corroboration	多视角签发确证
OCSP	Online Certificate Status Protocol	在线证书状态协议
OID	object identifier	对象标识符
OSCCA	State Cryptography Administration Office of Security Commercial Code Administration of China	中国国家商用密码管理办公室
PIN	Personal Identification Number	个人身份识别码
PKCS	Public KEY Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公钥基础设施
RA	Registration Authority	注册机构
RFC	Request for Comments	请求评注标准 (一种互联网建议标准)
SSL	Secure Sockets Layer	安全套接字
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

- http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf 互联网工程任务组（IETF）发布的 RFC3647 标准
- CA/Browser 论坛（https://cabforum.org/）发布的以下最新版要求（自本 CP&CPS 发布前）：
  - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.
  - Network and Certificate System Security Requirements
  - Guidelines for the Issuance and Management of Extended Validation Certificates
  - Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
  - Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
- Mozilla Root Store Policy
- Microsoft Trusted Root Program
- AATL Technical Requirements
- Apple Root Certificate Program
- Chrome Root Program
- 360 Browser Root Certificate Program
- Oracle 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”、“不应”、“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 365 天发布一次 CP&CPS。

亚洲诚信 CA 会定期跟进 CA/Browser 论坛标准的变化，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 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 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、基线要求和 EVG。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。

对于 SSL/TLS 服务器证书，所有的域名或 IP 地址都添加到主题别名中，而通用名称为主域名或 IP 地址，必须是一个出现在主题别名中的域名或 IP 地址。对于国际化域名（IDNs），亚洲诚信 CA 会将 IDN 的 punycode 格式的编码包含在主题名称或主题别名中。

在 SSL/TLS 服务器证书，所有的域名或 IP 地址都添加到主题别名中，而通用名为主域名或 IP 地址，必须是一个出现在主题别名中的域名或 IP 地址。在 TLS/SSL 证书的 subjectAltName 扩展名或 subject：commonName 字段中，不能包含保留私有 IP 地址或内部名称。在证书的 dNSName 条目中，不能带有下划线（_）字符。

在 DV 及 EV SSL/TLS 服务器证书的 subjectAltName 扩展名或 subject：commonName 字段中不能包含 IP 地址，且 EV SSL/TLS 服务器证书还不能包含通配符。

所有证书的命名规则和要求都被记录在本 CP&CPS 中，并符合 CA/Browser 论坛的要求。

亚洲诚信 CA 证书签发机构的主体甄别名命名规则如下：

属性	**值**
国家(C)	CN
省(ST)	证书签发者所在省份，或者不用
地区(L)	证书签发者所在城市，或者不用
机构(O)	TrustAsia Technologies, Inc.
通用名(CN)	此属性为 CA 名

亚洲诚信CA证书订户的主体甄别名命名规则如下：

属性	**值**
国家(C)	订户所属的国家地区代码
省(ST)	订户所在省份，或者不用
地区(L)	订户所在城市，或者不用
组织(O)	订户的机构名称
部门(OU)	订户的机构部门名称（企业型文档签名证书）

属性	值
组织标识(OI)	订户的机构注册编码（企业型邮件安全证书）
名字(givenName)	个人的法定名字(个人型证书、包含个人信息的企业型证书)
姓氏(surname)	个人的法定姓氏(个人型证书、包含个人信息的企业型证书)
化名(pseudonym)	个人化名(包含个人信息的企业型证书)
电子邮件(E)	订户的电子邮件地址，或不用
通用名(CN)	域名(SSL/TLS服务器证书)，或机构名(机构类型证书)，或个人姓名(个人类型证书)，或其他可识别的名称

亚洲诚信CA EV证书订户地主体甄别名命名规则如下：

属性	值
国家(C)	订户所属的国家地区代码
省(ST)	订户所在省份，或者不用
地区(L)	订户所在城市，或者不用
机构(O)	订户的法定机构名称
商业类别	订户的商业类别：私营组织，政府实体，商业实体以及非商业实体
组织注册所在国家	订户注册地所在国
组织注册成立的州/省	订户注册地所在州/省
组织注册成立的地点	订户注册地
序列号	订户注册号/订户成立或注册日期
通用名(CN)	域名(SSL/TLS服务器证书)，或机构名(机构类型证书)，或其他可识别的名称

3.1.2 对名称意义化的要求

亚洲诚信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。

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

1. 域名型SSL/TLS服务器证书、基础型邮件安全证书的甄别名通常包含：订户所拥有的域名、公网IP或是电子邮件地址，作为标识订户的关键信息被鉴别与验证。
2. 个人型文档签名证书、个人型邮件安全证书的甄别名通常包含：订户所拥有的电子邮件地址（邮件安全证书），订户的个人身份信息，作为标识订户的关键信息被鉴别与验证。

3. 企业型SSL/TLS服务器证书、普通代码签名证书、企业型文档签名证书、企业型邮件安全证书的甄别名通常包含:订户所拥有的域名、公网IP（SSL/TLS服务器证书）或是电子邮件地址（邮件安全证书），订户机构的企业身份信息，订户的个人身份信息（包含个人信息的企业型文档签名证书、Sponsor-validated邮件安全证书）作为标识订户的关键信息被鉴别与验证。
4. 增强型SSL/TLS服务器证书、增强型代码签名证书的甄别名通常包含:订户所拥有的域名（增强型SSL/TLS服务器证书），订户机构的企业身份信息作为标识订户的关键信息被鉴别与验证。

3.1.3 订户的匿名或伪名

本CP&CPS所述证书的订户在进行证书申请时必须提供真实名称和/或姓名。但在Sponsor-validated邮件安全证书DN中的组织名称可以显示化名，个人信息可以显示化名；在Organization-validated邮件安全证书DN中的组织名称可以显示化名。无论是组织化名或者是个人化名都须经过亚洲诚信CA严格的身份验证。

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。

证书中每一个主题名称的唯一性规定如下:

SSL/TLS服务器证书	域名的唯一性由互联网名称与数字地址分配机构(ICANN)控制。
邮件安全证书	要求唯一的电子邮件地址或申请人姓名（化名）或组织名称与唯一的序列号相组合或关联。
代码签名证书	要求唯一的组织名称与唯一的序列号相组合或关联。
文档签名证书	要求唯一的组织名称或申请人姓名与唯一的序列号相组合或关联。
时间戳证书	要求唯一的组织名称与唯一的序列号分配给时间戳。

3.1.6 商标的识别、鉴别和角色

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

证书申请者必须证明其正当地持有与包含在证书中的公钥相对应的私钥，其证明方法可以是提交经过数字签名的PKCS#10格式证书签名请求(CSR)或者通过签署提供给RFC 8555第7.4节中定义的ACME协议的Finalize方法的CSR来证明拥有与证书请求中的公钥相对应的私钥。

3.2.2 组织和域名鉴别

3.2.2.1 组织机构的身份鉴别

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

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

1. 通过政府机构签发的有效文件（包括但不限于工商营业执照、事业单位法人证书、统一社会信用代码证书等）或通过签发有效文件的权威第三方数据库以确认组织是真实存在的、合法的实体。
2. 通过可信的第三方数据库获取组织的地址及联系方式，以电话、电子邮件、邮政信函等方式与组织进行联络，以确认申请者所提供的信息的真实性。
3. 通过有执业资格的律师、会计师等出具的证明函件来验证信息。
4. 通过物业账单、银行对账单、政府签发的税单或其他亚洲诚信CA认可的验证方式来确认组织的地址信息。
5. 委托第三方对组织进行调查，或要求申请者提供额外的信息及证明材料。

此外，必要时，亚洲诚信CA还可以设定其它所需要的鉴别方式和资料。申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

对于亚洲诚信CA签发的订户证书，亚洲诚信CA会建立评估标准用于识别存在潜在高风险欺诈情况的证书请求。对于被识别为“高风险”的证书请求，亚洲诚信CA可直接予以拒绝。

3.2.2.1.1 EV证书的组织机构的身份鉴别

1. EV证书申请要求

   亚洲诚信CA不为IP地址、通配符域名，不为个人签发EV证书。申请EV证书的组织必须安排如下角色配合亚洲诚信CA完成审核：

   a. 证书经办人：EV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。
   b. 证书审批人：EV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。
   c. 合同签署人：EV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. EV证书主题字段要求

   a. subject:organizationName (OID 2.5.4.10)字段：亚洲诚信CA仅接受通过注册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获取的法定组织名称。该字段文本长度不得超过64个字符，如若超过亚洲诚信CA将缩写部分组织名称或省略其中的非实质性词，以使其满足该字段字符限制；但前提是使用的缩写不会在组织注册的司法辖区内产生误导，不会让依赖方产生误解以为是在和不同的组织打交道。

b. subject:commonName (OID 2.5.4.3)字段：对于服务器证书，亚洲诚信CA仅接受证书主体拥有或控制的单个域名，并与主体的服务器相关联；但不允许使用IP地址或通配符。对于代码签名证书，该字段的内容应与subject:organizationName (OID 2.5.4.10)保持一致。

c. subject:businessCategory (OID: 2.5.4.15)字段：亚洲诚信CA将对申请人的组织业务类型划分为四类并在证书主题中标识，分别为：私营组织，政府实体，商业实体以及非商业实体。亚洲诚信CA将按照业务划分来对申请人的合法存续以及身份进行区别验证。

d. subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)；subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)；subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)字段：亚洲诚信CA已将这些字段中的值在官网公开的"Audit and Validate Data Sources"中披露。与注册机构级别无关的信息不允许填入该字段。例如：

   组织的注册机构是国家级别的则只填写subject:jurisdictionCountryName，不得填写subject:jurisdictionStateOrProvinceName和subject:jurisdictionLocalityName；

   如果注册机构是州/省一级的，则必须填写subject:jurisdictionCountryName和subject:jurisdictionStateOrProvinceName，不得填写subject:jurisdictionLocalityName；

   如果是地方一级的，这上述三个字段都必须填写。

e. subject:serialNumber (OID: 2.5.4.5)字段：该字段中的值也在亚洲诚信CA的官网公开的"Audit and Validate Data Sources"中披露。亚洲诚信CA仅登记组织注册管辖区的注册号，若该司法管辖区未提供注册号将登记组织成立或注册日期。

   对于d和e字段的鉴别，亚洲诚信CA仅接受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获取的信息。

f. subject:localityName (OID: 2.5.4.7)；subject:stateOrProvinceName (OID: 2.5.4.8) Country: subject:countryName (OID: 2.5.4.6)字段：上述字段亚洲诚信CA将登记组织注册地或经营地的物理地址。对于申请组织物理地址的确认，亚洲诚信CA将使用章节3.2.2.1的规则来验证。

g. 亚洲诚信CA的EV证书主题不包含subject:organizationalUnitName (OID: 2.5.4.11)字段。

除了EVG第9.2章节规定的主题名称，亚洲诚信CA证书主题不包含其他任何主题名称属性。

3. EV证书验证要求

   a. 申请组织相关角色人员的验证

      对于EV证书，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，以确认信息的准确性。

   b. 订户协议和证书请求的签名验证

      对于EV证书，亚洲诚信CA要求订户协议和证书请求必须有签名，证书请求必须由证书经办人签署，

订户协议必须由授权的合同签署人签署，授权的证书审批人必须完成证书请求的批准。对于证书请求以及订户协议的签名，亚洲诚信CA将要求订户在下单页面完成；对于证书审批人证书请求的批准，亚洲诚信CA将通过电子邮件的方式发送在线批准链接。亚洲诚信CA也将在审核过程中确认签名行为的真实性。

c. 申请组织业务能力的验证

对于EV证书，亚洲诚信CA不仅要确认其是否合法存续以及物理存在，还须验证申请人是否具备参与业务的能力。亚洲诚信CA将通过验证申请人，或联署机构、母公司或子公司的运营存在，验证申请人具备参与业务的能力，验证方式如下：

i. 根据注册或登记机关的纪录，验证申请人、联署机构、母公司或子公司已存在至少3年时间；

ii. 验证申请人、联署机构、母公司或子公司在QIIS或QTIS中收录；

iii. 通过收到受监管的金融机构关于申请方、联署机构、母公司或子公司的确认性文件，以验证申请方、联署机构、母公司或子公司在该金融机构有一个有效的活期金融账户；或

iv. 通过已验证的专业意见函验证申请人在受监管的金融机构有一个有效活期存款账户。

d. 商业实体中的“主要个人”的验证

对于申请EV证书的商业实体，亚洲诚信CA则要求证书审批人必须为该组织的“主要个人”参与验证。主要个人可以是该实体所有者、法定代表人、投资人、负责人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会参照EVG第11.11.3章节的要求为其安排“面对面审核”。面对面审核（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，可接受的证明文件参照EVG第11.2.2章节的要求。“主要个人”需要按审核人员的要求出示上述证明文件的原件，并当场签署关于个人信息陈述的申请文件以完成审核。

3.2.2.1.2 企业型邮件安全证书的组织机构的身份鉴别

1. 证书申请要求

申请Organization-validated邮件安全证书或Sponsor-validated邮件安全证书都需要进行组织机构身份的鉴别，鉴别要求的等级等同于其他企业型证书。亚洲诚信CA将通过第3.2.2.1章节所列举的方式对申请组织进行相应的审核。

2. 证书主题字段要求（组织机构身份鉴别部分）

a. subject:commonName（OID:2.5.4.3）字段：对于Organization-validated邮件安全证书，亚洲诚信CA仅接受登记subject:organizationName (OID:2.5.4.10)字段的内容；对于Sponsor-validated邮件安全证书，亚洲诚信CA接受自然人使用法定姓名或者化名来作为该字段的内容。

b. subject:organizationName (OID:2.5.4.10)字段：亚洲诚信CA接受该字段登记申请组织的完整法定名称和/或根据第3.2.2.1章节验证的假定名称。假定名称与法定名称同时出现的，应先显示假定名称，然后括号里填写完整法定名称。该字段文本长度不得超过64个字符，如若超过亚洲诚信CA将缩写部分组织名称或省略其中的非实质性词，以使其满足该字段字符限制；但前提是使用的缩写不会在组织注册的司法辖区内产生误导，不会让依赖方产生误解以为是在和不同的组织打交道。

c. subject:organizationIdentifier (OID:2.5.4.97)字段：该字段应包含根据确定的注册方案分配的法人实体的注册参考。具体内容由3个字符的Registration Scheme identifier、2个字符的country code、2个字符的identifier for the subdivision of the nation以及组织注册编号组成。 Registration Scheme identifier分为：NTR（国家登记处）、VAT（国家税务机关）、PSD（欧盟）、LEI（全球法人识别编码）、GOV（政府机构）以及INT（国际组织）。

d. subject:emailAddress (OID:1.2.840.113549.1.9.1)字段：亚洲诚信CA将在该字段登记申请组织所要申请的电子邮件地址。该电子邮件地址将通过章节3.2.2.9所述的方式进行验证。

e. subject:stateOrProvinceName（OID:2.5.4.8）字段；subject:localityName（OID:2.5.4.7）字段；subject:countryName（OID:2.5.4.6）字段：上述字段亚洲诚信CA将登记组织注册地或经营地的物理地址。对于申请组织物理地址的确认，亚洲诚信CA将使用章节3.2.2.1的规则来验证。

3. 证书验证要求

a. 组织信息验证

无论申请组织是否使用化名来申请证书，亚洲诚信CA都须验证组织机构的法定名称、经营状态、注册机构及编码，以及经营地址等相关组织信息。验证方式及验证数据来源与其他企业型证书相同。

b. LEI全球法人识别编码的使用

在验证Organization-validated邮件安全证书或Sponsor-validated邮件安全证书的组织信息时，可以使用LEI全球法人识别编码作为验证数据来源，且无地域限制。但在使用LEI全球法人识别编码时，其RegistrationStatus须为ISSUED且EntityStatus为ACTIVE，ValidationSources为FULLY_CORROBORATED；若ValidationSources为PARTIALLY_CORROBORATED、PENDING或ENTITY_SUPPLIED_ONLY则不可用。

c. 组织假定名称的验证

亚洲诚信CA接受申请组织在申请Organization-validated邮件安全证书或Sponsor-validated邮件安全证书时使用企业假定名称。但亚洲诚信CA对组织的假定名称做了严格的限制，仅接受申请组织使用上市公司的证券简称或国家知识产权局商标局注册的商标名称（仅接受文字，不接受图形）作为企业假定名称。且若亚洲诚信CA发现该假定名称存在歧义或者重名的可能，则有权拒绝申请组织使用该假定名称来申请证书。

d. 组织唯一标识符的验证

亚洲诚信CA须验证申请组织的注册机构及编码信息作为subject:organizationIdentifier (OID:2.5.4.97)字段的内容依据。亚洲诚信CA将通过可信验证数据来源获取相关信息，并按照SMIME BR的要求填写相应编码。具体的验证数据来源已在亚洲诚信CA的官网公开的“Validation Resources”中披露。

e. 申请授权的验证

在审核企业型邮件安全证书的过程中，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申请人联系，获得足够肯定的答复，以确认信息的准确性。

3.2.2.1.3 企业型文档签名证书的组织机构的身份鉴别

1. 证书申请要求

申请企业型文档签名证书的鉴别要求的等级等同于其他企业型证书。亚洲诚信CA将通过第3.2.2.1章节所列举的方式对申请组织进行相应的审核。除常规验证外，对于申请企业型文档签名证书的组织，亚洲诚信CA还将与其申请经办人进行面对面审核。

2. 证书主题字段要求（组织机构身份鉴别部分）

a. subject:commonName（OID:2.5.4.3）字段：对于普通企业型文档签名证书，亚洲诚信CA仅接受登记subject:organizationName (OID:2.5.4.10)字段的内容；对于包含个人信息的企业型文档签名证书

，亚洲诚信CA仅接受登记subject:givenName (OID:2.5.4.42)
加subject:surname(OID:2.5.4.4)字段的内容。

b. subject:organizationName (OID:2.5.4.10)字段：亚洲诚信CA仅接受通过注册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获取的法定组织名称。该字段文本长度不得超过64个字符，如若超过亚洲诚信CA将缩写部分组织名称或省略其中的非实质性词，以使其满足该字段字符限制；但前提是使用的缩写不会在组织注册的司法辖区内产生误导，不会让依赖方产生误解以为是在和不同的组织打交道。

c. subject:stateOrProvinceName（OID:2.5.4.8）字段；subject:localityName（OID:2.5.4.7）字段；subject:countryName（OID:2.5.4.6）字段：上述字段亚洲诚信CA将登记组织注册地或经营地的物理地址。对于申请组织物理地址的确认，亚洲诚信CA将使用章节3.2.2.1的规则来验证。

d. subject:organizationalUnitName（OID：2.5.4.11）字段：上述字段亚洲诚信CA可以登记subject:organizationName的附属机构的完整法定名称，亚洲诚信CA将使用章节3.2.2.1的规则来验证；也可以登记subject:organizationName的合规部门名称，部门名称需要申请组织提供相关证明文件。

3. 证书验证要求

a. 组织信息验证

亚洲诚信CA将对组织机构的法定名称、经营状态、注册机构及以及经营地址等相关组织信息。验证方式及验证数据来源与其他企业型证书相同。

b. 申请授权的验证

在审核企业型文档签名证书的过程中，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联系，获得足够肯定的答复，以确认信息的准确性。

c. 面对面审核

在申请授权验证完后，亚洲诚信CA还将与证书经办人进行一次“面对面审核”，审核方式及要求参考EVG第11.11.3章节所述内容。面对面审核（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，证书经办人需要按审核人员的要求出示身份证件原件，并当场签署关于个人信息陈述的申请文件以完成审核。若订户申请是Sponsor-validated文档签名证书，则由证书中的个人配合审核部完成面对面审核。

3.2.2.2 机构商业名称的验证

不适用。

3.2.2.3 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。

3.2.2.4 域名的确认和鉴别

用户在申请TLS服务器证书或者S/MIME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不支持最右端为.onion的域名的验证，且不提供该证书的签发。

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BR版本号。

对于DNSSEC验证，参考本CP&CPS第3.2.2.8.1节内容。

3.2.2.4.1 验证申请人为域名联系人

亚洲诚信CA不支持此方法。

3.2.2.4.2 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。

3.2.2.4.3 域联系人电话联系

亚洲诚信CA不支持此方法。

3.2.2.4.4 构造电子邮件到域联系人

按照TLS基线要求第3.2.2.4.4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。

证书请求中的唯一随机值由亚洲诚信CA生成，并在生成之日起有效期不超过30 天。此验证方式同时适用于通配符域名的验证。

3.2.2.4.5 域名授权文件

亚洲诚信CA不支持此方法。

3.2.2.4.6 商定的网站变更

亚洲诚信CA不支持此方法。

3.2.2.4.7 DNS 变更

按照TLS基线要求第3.2.2.4.7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。

证书请求中的唯一随机值由亚洲诚信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。此验证方式同时适用于通配符域名的验证。

亚洲诚信CA按照第3.2.2.9节的规定实施多视角签发确证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。

3.2.2.4.8 IP地址

亚洲诚信CA不支持此方法。

3.2.2.4.9 测试证书

亚洲诚信CA不支持此方法。

3.2.2.4.10 使用TLS随机数

亚洲诚信CA不支持此方法。

3.2.2.4.11 任何其他方法

亚洲诚信CA不支持此方法。

3.2.2.4.12 验证申请人为域名联系人

亚洲诚信CA不支持此方法。

3.2.2.4.13 向 DNS CAA 联系人发送电子邮件

亚洲诚信CA不支持此方法。

3.2.2.4.14 向 DNS TXT 联系人发送电子邮件

按照TLS基线要求第3.2.2.4.14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。

证书请求中的唯一随机值由亚洲诚信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。此验证方式同时适用于通配符域名的验证。

亚洲诚信CA按照第3.2.2.9节的规定实施多视角签发确证（MPIC）。为了计入验证结果，网络视角必须监测主网络视角所监测到的用于域名验证的选定联系地址。

3.2.2.4.15 电话验证域名联系人

亚洲诚信CA不支持此方法。

3.2.2.4.16 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。

3.2.2.4.17 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。

3.2.2.4.18 商定的网站变更v2

按照TLS基线要求第3.2.2.4.18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。

证书请求中的唯一随机值由亚洲诚信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。此验证方式不适用于通配符域名的验证。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。

亚洲诚信CA按照第3.2.2.9节的规定实施多视角签发确证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。

3.2.2.4.19 使用ACME方式的网站变更

按照TLS基线要求第3.2.2.4.19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。

亚洲诚信CA按照第3.2.2.9节的规定实施多视角签发确证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。

3.2.2.4.20 使用TLS的ALPN扩展

亚洲诚信CA不支持此方法。

3.2.2.4.21 使用ACME acount ID的DNS验证

亚洲诚信CA不支持此方法。

3.2.2.4.22 使用DNS TXT记录的持久验证

通过验证特定的持久性域名控制验证（Persistent DCV）TXT记录是否存在，以确认申请者对某个完全限定域名（FQDN）的控制权。该TXT记录必须放置在待验证的授权域名（Authorization Domain Name）前，以 _validation-persist作为主机名标签（即格式为 _validation-persist.[授权域名]）。采用此方法时，亚洲诚信CA不会将DNS CNAME查询返回的FQDN用作域名验证的FQDN。此项禁止规定优先于授权域名的定义。但在解析持久性DCV TXT记录时，可以遵循CNAME记录。

该持久性DCV TXT记录的RDATA值满足以下要求：

1. RDATA值必须符合RFC 8659第4.2节中定义的 issue-value语法。
2. issuer-domain-name的值必须是亚洲诚信CP/CPS中4.2节中披露的颁发者域名（Issuer Domain Name）。
3. issue-value必须包含一个accounturi参数，该参数的值是一个唯一URI（遵循RFC 8657第3节描述），用于标识为此FQDN请求验证的申请者账户。
4. issue-value可以包含一个 persistUntil参数。如果存在此参数，其值必须是一个以十进制编码的整数，代表UNIX时间戳（自1970-01-01T00:00:00Z起忽略闰秒的秒数）。
5. issue-value可以包含其他参数。亚洲诚信CA忽略任何未知的参数键。

如果存在persistUntil参数，亚洲诚信CA会评估其值。如果检查时间晚于persistUntil参数值所指定的时间，则亚洲诚信CA不会将该记录用作申请者对完全限定域名（FQDN）拥有控制权的证据。

例如，一个持久性 DCV TXT 记录可能如下所示： _validation-persist.example.com IN TXT "authority.example; accounturi=https://authority.example/acct/123; persistUntil=1782424856" 就第4.2.1 节而言，认证机构（CA）必须将使用此方法完成的验证的最大验证数据重用期限视为 10 天。 亚

洲诚信CA按照第3.2.2.9节的规定实施多视角签发确证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。此方法适用于通配符证书。

3.2.2.5 IP地址的确认和鉴别

亚洲诚信CA接受订户使用公有IP申请SSL证书，不为IP签发域名型和增强型证书。用于申请证书的IP需符合IANA规范且不可为保留IP。

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

3.2.2.5.1 商定的网站变更

按照TLS基线要求第3.2.2.5.1节中的定义，订户通过在待验证IP站点指定目录 /.well-known/pki-validation/ 下放置指定的验证文件和随机值。

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。

亚洲诚信CA按照第3.2.2.9节的规定实施多视角签发确证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。

3.2.2.5.2 向IP地址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 反向地址查找

亚洲诚信CA不支持此方法。

3.2.2.5.4 任何其他方法

亚洲诚信CA不支持此方法。

3.2.2.5.5 电话联系IP地址联系方式

亚洲诚信CA不支持此方法。

3.2.2.5.6 IP 地址的 ACME“http-01”方法

亚洲诚信CA通过执行RFC 8738中记录的“http-01”挑战程序，确认申请人对IP地址的控制权。

亚洲诚信CA按照第3.2.2.9节的规定实施多视角签发确证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的令牌。

3.2.2.5.7 IP 地址的 ACME“tls-alpn-01”方法

亚洲诚信CA不支持此方法。

3.2.2.5.8 反向地址查找域名中具有持久的DNS TXT记录

亚洲诚信CA不支持此方法。

3.2.2.6 通配符域名的确认和鉴别

亚洲诚信CA对通配符右侧的域名进行控制权验证，验证规则遵循本CP&CPS第3.2.2.4节中的规定。通配符域名右侧若为顶级域名或公共后缀，亚洲诚信CA则拒绝为其签发证书。亚洲诚信CA不为通配符签发EV证书。

3.2.2.7 数据源的准确性

亚洲诚信CA在鉴别过程中使用的数据源会在官网信息库中公布，在采用任何数据源作为可靠数据源之前，亚洲诚信CA会对数据源的可靠性、准确性、防篡改及防伪造能力进行评估。并遵循CA/Browser论坛对数据源的要求考虑以下因素：

1. 信息的时效性
2. 信息的更新频率
3. 信息提供方及信息收集的目的
4. 信息的可公开访问性及可用性
5. 信息伪造和篡改的难度

3.2.2.8 认证机构授权记录

作为证书签发过程的一部分，亚洲诚信CA根据RFC 8659的规定，检索并处理每个subjectAltName扩展中不包含“.onion”域名的dNSName的CAA记录。亚洲诚信CA关于CAA记录的策略见第4.2.4节，其中包括明确规定CA在CAA的“issue”或“issuewild”或“issuemail”记录中认可的允许其签发证书的发行者域名集。

某些用于验证申请人对将在证书中列出的主题域名（参见第3.2.2.4节）或IP地址（参见第3.2.2.5节）的所有权或控制权的方法，要求在证书签发前从额外的远程网络视角检索并处理CAA记录（参见第3.2.2.9）。为了确证主网络视角，无论两个视角的响应是否完全逐字节相同，远程网络视角的CAA检查响应必须被解释为允许签发证书。此外，如果一个或两个视角在CAA记录查询中出现了本节定义的可接受的失败，亚洲诚信CA可以将远程网络视角的响应视为有效验证。

亚洲诚信CA可以在任何适合的时间检查CAA记录。

亚洲诚信CA在处理CAA记录后签发证书，会在CAA记录的TTL（生存时间）或8小时内完成签发，以时间较长者为准。

3.2.2.8.1 DNSSEC对CAA记录的验证

自2026年3月15日起，亚洲诚信CA所有与主网络视角执行的CAA记录查找相关的DNS查询均会向IANA DNSSEC根信任锚进行DNSSEC验证。亚洲诚信CA不会使用本地策略禁用任何DNS查询CAA记录的DNSSEC。主网络视角观察到的验证错误（如SERVFAIL）时，不会视为有效验证。

作为MPIC的一部分，可以对远程网络视角执行CAA记录查询相关的DNS查询返回到IANA DNSSEC根信任锚进行DNSSEC验证。亚洲诚信CA对DNSSEC验证进行内部审计。

3.2.2.9 多视角签发确证（MPIC）

多视角签发确证尝试在证书签发前，从多个远程网络视角确证主网络视角所做的判定（即域名验证通过/失败、CAA允许/禁止）。这一过程可以提高对具有相同特定前缀的边界网关协议（BGP）攻击或劫持的防护能力。

亚洲诚信CA在执行多视角签发确证时既可以使用相同的网络视角集，也可以使用不同的网络视角集，来进行

所需的域名授权/控制和CAA记录检查。

所依赖的网络视角集向亚洲诚信CA提供以下必要的信息，以便其能够明确评估：

1. 根据第3.2.2.4节和第3.2.2.5节中指定的验证方法要求，存在预期的:1) 随机值、2) 请求令牌、3) IP地址、4) 联系地址或5) 持久的DNS TXT记录；
2. 根据第3.2.2.8节中所规定的，亚洲诚信CA是否有权向请求的域名签发证书。

第3.2.2.4节和第3.2.2.5节描述了需要使用多视角签发确证（MPIC）的域名验证方法，以及网络视角如何确证主网络视角判定的结果。

从一个网络视角获得的结果或信息不得在随后的网络视角验证时被重复使用或缓存。为网络视角提供互联网连接的网络基础设施可以由提供运营网络视角所需计算服务的同一组织管理。远程网络视角与亚洲诚信CA之间的所有通信必须通过经过身份验证和加密的通道进行，且该通道依赖现代协议（如HTTPS）。

网络视角可以使用与网络视角不在同一地点的递归DNS解析器。但网络视角使用的DNS解析器必须与依赖它的网络视角位于相同的互联网注册服务区域。此外，对于在多视角签发确证（MPIC）尝试中使用的任何一对DNS解析器，这两个DNS解析器所在的州、省或国家之间的直线距离至少为500千米。DNS解析器的位置取决于未封装的出站DNS查询首次传递给为其提供互联网连接的网络基础设施的地点。

亚洲诚信CA可以立即通过相同的验证方法或替代方法来重试多视角签发确证（MPIC）。在重试多视角签发确证（MPIC）时，亚洲诚信CA不依赖之前尝试的验证结果。对任何时间段内可以执行的最大确证尝试次数没有明确要求。

“网络视角集要求”表描述了与多视角签发确证（MPIC）相关的网络视角集要求。如果亚洲诚信CA在域名授权/控制和CAA记录检查中不依赖相同的网络视角集，则两套网络视角集（即域名授权或控制集和CAA记录检查集）必须满足网络视角集要求。当两套网络视角集所在的两个州、省或国家之间的直线距离至少为500千米时，则两者被认为是不同的。当网络视角与主网络视角及网络视角集中包含的其他网络视角不同时，则两者被认为是“远程”的。

“网络视角集要求”表：

使用的不同远程网络视角数量	允许的非确证数量
2-5	1
6+	2

亚洲诚信CA的远程网络视角在执行多视角签发确证（MPIC）时符合：

- 网络强化：
  - 依靠网络（例如互联网服务提供商或云提供商网络）实施措施来缓解全球互联网路由系统中的BGP路由事件，从而为网络视角提供互联网连接。
  - 为每个网络边界控制（防火墙、交换机、路由器、网关或其他网络控制设备或系统）配置仅支持运营所需的服务、协议、端口和通信的规则。
  - 依赖于以下网络（如，互联网服务提供商）：1) 使用基于安全跨域路由（RFC 6480）的机制，如BGP前缀源验证（RFC 6811），2) 使用其他非RPKI路由泄漏预防机制（如RFC 9234），3) 应用BCP 194中描述的当前最佳实践。
- 设施和服务供应商要求：

- 托管在通过ISO/IEC 27001认证的设施或经过独立审计和认证（或报告）的同等安全框架中。
- 依赖于以下报告之一所覆盖的服务：System and Organization Controls 2（SOC 2）、IASE 3000、ENISA 715、FedRAMP Moderate、C5:2020、CSA STAR CCM或经过独立审计和认证（或报告）的同等服务框架。

- 漏洞检测和补丁管理：
  - 至少每三个月进行一次漏洞扫描.
  - 实施入侵检测和防御控制，以防范常见的网络和系统威胁。
  - 记录并遵循漏洞修复流程，涵盖漏洞的识别、审查、响应和修复。
  - 在安全补丁发布后六个月内应用推荐的安全补丁，除非亚洲诚信CA能证明该安全补丁会带来额外的漏洞或不稳定性，超过应用安全补丁的好处。
- 系统强化：
  - 禁用所有不使用的账户、应用、服务、协议和端口。
  - 对所有用户的账户实施多因素认证。

分段实施时间表：

时间	亚洲诚信CA使用的最少网络视角数量	决定主网络视角的远程网络视角至少在两个不同互联网注册机构服务区	法定确证人数符合“法定人数要求”表
2024-09-15	2	非必须	非必须
2025-03-15	2	非必须	非必须
2025-09-15	2	非必须	必须
2026-03-15	3	必须	必须
2026-06-15	4	必须	必须
2026-12-15	6	必须	必须

3.2.2.10 电子邮件地址的验证

当邮件地址被作为证书主题内容或备用名称申请证书时，亚洲诚信CA会对该邮件地址的有效性进行检查，并审核申请者对邮件地址的使用权，只有通过验证后才可在证书中签入Email项。

1. 通过域名验证电子邮件地址控制权

   亚洲诚信CA可以通过验证证书中使用的电子邮件地址的域名部分的控制权，以验证申请人对该电子邮件地址的控制权。亚洲诚信CA仅使用章节3.2.2.4规定的验证方式来执行此验证。

2. 通过电子邮件验证电子邮件地址控制权

   亚洲诚信CA可以通过电子邮件发送随机值，然后收到使用该随机值的确认回复，以验证申请人对该电子邮件地址的控制权，具体的验证步骤如下：

   a. 亚洲诚信CA系统向需要验证的电子邮件地址发送一封邮件地址控制权验证邮件，该邮件中会包含一个附带唯一随机值的批准链接；

b. 申请人收到邮件并通过带随机值的链接进行批准操作；

c. 亚洲诚信CA系统收到用户批准后，比对批准中的随机值与发送的随机值，若结果一致，则电子邮件地址验证通过。

随机值在每封电子邮件中都是唯一的，带随机值的验证邮件有效期仅为24小时，随机值会在每次由亚洲诚信CA向电子邮件地址发送电子邮件时被重置。

3.2.3 个人身份的鉴别

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

申请者需要证明其对请求中包含的某些身份属性有控制权，例如其包含在证书请求中证书涉及的电子邮件地址或域名。申请者还可能被要求提交有效的政府签发的带照片的证件（如居民身份证、护照、驾驶证、军官证或其他同等证件）的清晰副本。亚洲诚信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。

亚洲诚信CA通过以下一种或多种方式来鉴别和验证：

1. 采用发送相关校验码电子邮件或通过电话、手机短信等其他可靠的方式来鉴别和验证申请者证书请求的真实性。亚洲诚信CA不确认、不担保所签发的证书中除验证信息以外的其他身份信息是真实的、可靠的、属于申请者本人的；
2. 检查申请者所提交的证件副本是否有任何篡改或伪造的痕迹，必要时通过查询权威第三方数据库等可靠的方式对申请者提供的身份信息进行核实验证，以确保申请者所提供的信息与核查结果一致；
3. 通过物业费账单、银行卡对账单或信用卡账单等核实申请者的地址或直接依赖政府签发的身份证明文件来确认地址。
4. 当申请信息包含组织信息时，可要求申请者提交任职证明文件、或查询第三方数据库、或发送确认电子邮件等方式来确认该组织是否存在，以及申请者是否是该组织成员。

此外，必要时，亚洲诚信CA还可以设定其它所需要的鉴别方式和资料。申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

对于亚洲诚信CA签发的订户证书，亚洲诚信CA会建立评估标准用于识别存在潜在高风险欺诈情况的证书请求。对于被识别为“高风险”的证书请求，亚洲诚信CA可直接予以拒绝。

3.2.3.1 Individual-validated邮件安全证书的个人身份鉴别

1. 证书申请要求

   亚洲诚信CA仅接受具有完全民事行为能力的自然人申请Individual-validated邮件安全证书。申请人需向亚洲诚信CA提供身份证明文件，亚洲诚信CA将对其身份证明文件进行核实，并验证其申请行为的真实性。

2. 证书主题要求

   a. subject:commonName（OID:2.5.4.3）字段：亚洲诚信CA仅接受申请人的法定姓名作为该字段的内容。申请人的姓名必须跟其所提供的证件上的姓名一致。

   b. subject:givenName (OID:2.5.4.42)和subject:surname(OID:2.5.4.4)字段：亚洲诚信CA仅接受申请人的法定姓名。

c. subject:emailAddress(OID:1.2.840.113549.1.9.1)字段：亚洲诚信CA将在该字段登记申请人所要申请的电子邮件地址。该电子邮件地址将通过章节3.2.2.9所述的方式进行验证。

d. subject:countryName（OID:2.5.4.6）字段：亚洲诚信CA将在该字段登记申请人提供的身份证件上的国籍的国家代码。

3. 证书验证要求

除了对出现在Individual-validated邮件安全证书DN中的每一个字段进行相应的审核验证外，亚洲诚信CA会收集申请人的身份证明文件，与申请人本人确认申请行为。

a. 申请人身份信息验证

关于收集个人身份属性的方法，亚洲诚信CA仅接受物理身份证明文件。亚洲诚信CA可接受的个人证件类型为：居民身份证/临时居民身份证、军官证、驾驶证、护照、港澳台居民居住证、港澳居民往来内地通行证、台湾居民往来大陆通行证以及外国人永久居留证等国家为个人签发的身份证明文件。身份证证明文件上必须有清晰可见的面部照片，否则不可作为身份验证使用。若身份证明文件上无地址信息，申请人还需提供载明申请人姓名、身份编码以及地址的物业账单、银行对账单、信用卡账单或政府签发的税单等亚洲诚信CA认可的证明文件来证明申请人的住址。

b. 申请人申请行为确认

亚洲诚信CA将通过“面对面审核”的方式来完成身份信息的核对以及申请人申请行为的确认，审核方式及要求参考EVG第11.11.3章节所述内容。面对面审核（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，申请人需要按审核人员的要求出示身份证件原件，并当场签署关于个人信息陈述的申请文件以完成审核。

3.2.3.2 Sponsor-validated邮件安全证书的个人身份鉴别

1. 证书申请要求

亚洲诚信CA允许Sponsor-validated邮件安全证书中包含个人信息，但个人信息必须经过相应验证。该证书信息中的个人不仅须具有完全民事行为能力，还须获得申请组织的授权。申请组织除了完成第3.2.2.1章节要求的组织验证外，还需向亚洲诚信CA提供个人信息中个人身份证明文件，亚洲诚信CA将对其身份证明文件进行核实，并验证申请及授权行为的真实性。

2. 证书主题要求（个人身份鉴别部分）

a. subject:commonName（OID:2.5.4.3）字段：亚洲诚信CA接受自然人使用法定姓名或者化名来作为该字段的内容。使用法定姓名的必须跟其所提供的证件上的姓名一致；若使用化名则需申请组织提供相应的证明文件。

b. subject:givenName (OID:2.5.4.42) 和subject:surname(OID:2.5.4.4)字段：亚洲诚信CA仅接受申请人的法定姓名。该字段不与subject: pseudonym (OID:2.5.4.65)同时出现在证书DN中。

c. subject: pseudonym (OID:2.5.4.65)字段：亚洲诚信CA接受Sponsor-validated邮件安全证书中的个人使用化名，但申请组织必须出具相应证明，以证明该个人的化名与其真实身份信息相关联。该字段不与subject:givenName (OID:2.5.4.42) 和subject:surname(OID:2.5.4.4)同时出现在证书DN中。

3. 证书验证要求

在Sponsor-validated邮件安全证书DN中出现的个人信息都需要按照本章节的要求进行验证，亚洲诚信CA会收集其身份证明文件，并与本人确认申请行为。

a. 个人身份信息验证

关于身份证明文件的收集方式同第3.2.3.1章节所述。除此之外，若证书DN需要显示个人的化名，则申请组织还须提供相应的证明文件。证明文件可以是授权书、证明函等亚洲诚信CA认可的，可以明确证明个人的化名与其真实身份信息相关联的文件。

b. 个人申请及授权行为确认

亚洲诚信CA除了通过第3.2.2.1章节验证的组织联系方式确认证书中个人的授权行为外，还须通过“面对面审核”的方式来核对个人身份证明材料，审核方式及要求参考EVG第11.11.3章节所述内容。面对面审核（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，申请人需要按审核人员的要求出示身份证件原件，并当场签署关于个人信息陈述的申请文件以完成审核。

3.2.3.3 Individual-validated文档签名证书的个人身份鉴别

1. 证书申请要求

亚洲诚信CA仅接受具有完全民事行为能力的自然人申请Individual-validated文档签名证书。申请人需向亚洲诚信CA提供身份证明文件，亚洲诚信CA将对其身份证明文件进行核实，并验证其申请行为的真实性。

2. 证书主题要求

   a. subject:commonName（OID:2.5.4.3）字段：亚洲诚信CA接受申请人的法定姓名作为该字段的内容。申请人的姓名必须跟其所提供的证件上的姓名一致。

   b. subject:givenName(OID:2.5.4.42)和subject:surname(OID:2.5.4.4)字段：亚洲诚信CA仅接受申请人的法定姓名。

   c. subject:countryName（OID:2.5.4.6）字段：亚洲诚信CA将在该字段登记申请人提供的身份证件上的国籍的国家代码。

3. 证书验证要求

除了对出现在Individual-validated文档签名证书DN中的每一个字段进行相应的审核验证外，亚洲诚信CA会收集申请人的身份证明文件，与申请人本人确认申请行为。

a. 申请人身份信息验证

关于收集个人身份属性的方法，亚洲诚信CA仅接受物理身份证明文件。亚洲诚信CA可接受的个人证件类型为：居民身份证/临时居民身份证、军官证、驾驶证、护照、港澳台居民居住证、港澳居民往来内地通行证、台湾居民往来大陆通行证以及外国人永久居留证等国家为个人签发的身份证明文件。身份证证明文件上必须有清晰可见的面部照片，否则不可作为身份验证使用。若身份证明文件上无地址信息，申请人还需提供载明申请人姓名、身份编码以及地址的物业账单、银行对账单、信用卡账单或政府签发的税单等亚洲诚信CA认可的证明文件来证明申请人的住址。

b. 申请人申请行为确认

亚洲诚信CA将通过“面对面审核”的方式来完成身份信息的核对以及申请人申请行为的确认，审核方式及要求参考EVG第11.11.3章节所述内容。面对面审核（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，申请人需要按审核人员的要求出示身份证件原件，并当场签署关于个人信息陈述的申请文件以完成审核。

3.2.3.4 包含个人信息的企业型文档签名证书的个人身份鉴别

1. 证书申请要求

   亚洲诚信CA允许企业型文档签名证书中包含个人信息，但个人信息必须经过相应验证。该证书信息中的个人不仅须具有完全民事行为能力，还须获得申请组织的授权。申请组织除了完成第3.2.2.1章节要求的组织验证外，还需向亚洲诚信CA提供个人信息中个人身份证明文件，亚洲诚信CA将对其身份证明文件进行核实，并验证申请及授权行为的真实性。

2. 证书主题要求（个人身份鉴别部分）

   a. subject:commonName（OID:2.5.4.3）字段：亚洲诚信CA仅接受自然人使用法定姓名来作为该字段的内容，法定姓名的必须跟其所提供的证件上的姓名一致。

   b. subject:givenName (OID:2.5.4.42) 和subject:surname(OID:2.5.4.4)字段：亚洲诚信CA仅接受申请人的法定姓名。

3. 证书验证要求

   在企业型文档签名证书DN中出现的个人信息都需要按照本章节的要求进行验证，亚洲诚信CA会收集其身份证明文件，并与本人确认申请行为。

   a. 个人身份信息验证

      关于身份证明文件的收集方式同第3.2.3.1章节所述。

   b. 个人申请及授权行为确认

      亚洲诚信CA除了通过第3.2.2.1章节验证的组织联系方式确认证书中个人的授权行为外，还须通过“面对面审核”的方式来核对个人身份证明材料，审核方式及要求参考EVG第11.11.3章节所述内容。面对面审核（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，申请人需要按审核人员的要求出示身份证件原件，并当场签署关于个人信息陈述的申请文件以完成审核。

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

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

此外，亚洲诚信CA允许申请者指定独立个人来申请证书。若申请者以书面形式指定了可以进行证书申请的独立个人，则亚洲诚信CA不接受任何超出该授权的证书请求。在收到申请者已核实的书面请求时，亚洲诚

信CA应向申请者提供其已授权人员的清单。

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。

截至目前，亚洲诚信CA未签发任何交叉证书。

3.3 密钥更新请求的标识与鉴别

在证书到期之前，订户可以请求更新密钥。在收到更新密钥的请求后，亚洲诚信CA将创建一个含有新公钥但证书主题内容与原证书相同的新证书，并且可选择地延长证书有效期。亚洲诚信CA可根据实际情况选择对申请者进行重新确认，或者依赖之前提供或获得的信息。

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

3.3.1 常规密钥更新的标识与鉴别

亚洲诚信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。

证书密钥更新一般有两种情况：补发和换发。

1. **证书补发**

   补发是指证书在有效期内，订户申请更新证书密钥的操作。

   以下情况订户需要申请证书补发：

   - 订户证书（文件）丢失或损坏或订户认为原有证书和密钥不安全；
   - 订户一张证书多处部署，需要使用不同的密钥对；
   - 订户需要获取多种算法的证书（RSA、ECC）；
   - 订户需要增加域名（仅限于多域名SSL/TLS服务器证书）；
   - 其他经亚洲诚信CA认可的原因。

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

2. **证书换发**

   换发是指在证书将要过期的30日（含）内，订户申请更新密钥的操作。

   在订户证书到期前的30日（含）内，亚洲诚信CA将通过适当的方式通知订户对证书进行换发操作。若订户已验证的证书注册信息在CA/Browser论坛BR规定验证有效期内，亚洲诚信CA将基于其原有的信息对

其重新签发证书。若已验证的证书注册信息距离初次验证已超过CA/Browser论坛BR规定验证有效期，则需对订户身份进行重新验证，验证流程及要求与初次申请相同。新证书有效期将从证书换发之日起至原证书到期为止再另加一个证书有效周期。

3.3.2 撤销后密钥更新的标识与鉴别

亚洲诚信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，也可以来自亚洲诚信CA。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。

3.5 授权服务机构的标识与鉴别

亚洲诚信CA自行担任证书RA，不再另行设立RA。

4. 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

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

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

4.1.2 注册过程和责任

1. 注册过程包括：
    - 提交证书申请；
    - 生成密钥对；
    - 向亚洲诚信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。

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

亚洲诚信CA会对待签发证书主题别名扩展项中的每一个DNSName做CAA记录检查，并按照4.2.4中的检查方法和结果判定是否批准该证书申请。

亚洲诚信CA验证团队在执行身份识别与鉴别时，将实施严格的职责分离控制程序，以确保没有任何一个人可以单独完成验证签发个人型、企业型及增强型证书。审核人员将严格执行本章节3.2的相关要求，完成证书的

申请的初次审核，包括但不限于：使用可信数据库进信息比对，完成对申请人、合同签署人、证书经办人、证书审批人所需的验证，收集与验证相关信息和文件。复审人员将审查审核人员所收集的审核资料，核对每个验证项目以及检查审核人员的验证流程。复审人员不得参与审核环节的信息采集工作。唯有经过复核人员复核通过，证书才能被批准签发证书。亚洲诚信CA验证团队执行身份识别与鉴别的过程都会留下相应记录，供审计人员检查。

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

验证完成后，亚洲诚信CA验证团队会根据验证结果决定接受、拒绝申请或要求申请者补充递交相关材料。

在鉴别个人型、企业型与增强型证书中的信息时，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；根据本CP&CPS第3.2.2.4章节以及第3.2.2.5章节验证过的域名及IP地址按照下表时间可以不用重复验证。

颁发日期在此日或之后	颁发日期在此日之前	复用时长
	2026-03-15	398天
2026-03-15	2027-03-15	200天
2027-03-15	2029-03-15	100天
2029-03-15		10天

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。

亚洲诚信CA不再签发顶级域名为arpa相关的证书。

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 处理证书身申请的时间

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SSL/TLS服务器证书，亚洲诚信CA遵循CA/Browser 论坛BR 3.2.2.8规定，在证书签发前，对证书申请中的所有主题名称和备用名称中的域名进行DNS CAA记录检查。

亚洲诚信CA根据RFC8659中的规定处理CAA记录中”issue”，”issuewild”，”issuemail”，"iodef"属性标签。

在使用ACME客户端进行证书申请时，CAA支持“accounturi”和“validationmethods”配置，其中accounturi为亚洲诚信CA维护的，可以用于请求签发证书并代表特定实体或相关实体组织的对象标识；validationmethods支持http-01以及dns-01两种方法。

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尊重关键标签，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”issue”,"issuewild" ，"issuemail"标签，且”issue”,"issuewild" 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，以便向CA/Browser论坛提供有关情况反馈。

CAA记录对于代码签名、文档签名证书、时间戳签名证书均不适用。

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。

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

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

在证书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阅服务器。

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。

4.3.1.2 使用Linting工具检测待签名证书内容

对于SSL/TLS服务器证书，在证书签名之前，对TBS证书进行lint检测并结合错误信息进行人工复核，以防止签发违反BR要求。

4.3.1.3 使用Linting工具检测已签发的证书

亚洲诚信CA使用lint工具检测所有签发的TLS/CS/SMIME等证书。

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，同时会根据谷歌、苹果的要求，选择将证书发布在多个CT日志服务器中。

亚洲诚信CA遵照本CP&CPS中2.4和2.5章节中关于信息库机制的规定，向订户签发证书。该信息库只有CA被授权的角色人员才能监控并管理该高风险数据库或备用签发机制，同时，被授予权限的角色人员应维护并管理其完整性。若保密法等相关法律法规有要求，亚洲诚信CA将遵照相关要求，在获得订户同意后，再让其证书处于可检索状态。

4.4.3 CA对其他实体的通告

亚洲诚信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

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

订户应按协议规定、法律法规、CP&CPS的范围内使用密钥对。

4.5.2 依赖方公钥和证书的使用

依赖方应在依赖证书前考虑总体情况和损失风险。

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

1. 获得数字签名对应的证书及信任链；
2. 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30日（含）起可以进行证书更新。订户选择保留原有密钥对重新签发证书,则订户需要保证其密钥对的安全性没有受到威胁。在证书到期前30日（含）起，亚洲诚信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，且其证书剩余有效期少于30日（含）。

4.6.3 证书更新请求的处理

对于证书更新，其处理过程包括申请识别和鉴别、证书信息验证及签发证书。

1. 对于申请的识别和鉴别须基于以下几个方面：
    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）丢失或损坏或订户认为原有证书和密钥不安全；
2. 订户一张证书多处部署，需要使用不同的密钥对；
3. 订户需要获取多种算法的证书（RSA、ECC）；
4. 订户需要增加域名（仅限于多域名SSL/TLS服务器证书）；
5. 订户证书即将到期且认为更新证书时需要更新密钥。

6. 其他可能导致密钥更新的情形。

4.7.2 请求证书密钥更新的实体

请求证书更新的实体为已经申请过亚洲诚信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

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

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

4.8.2 请求证书变更的实体

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

4.8.3 证书变更请求的处理

当订户提交证书信息变更申请后，亚洲诚信CA会对证书信息进行重新验证，若原证书的申请资料可用且未过期（验证有效期参考第4.2.1章），则可以参考原资料进行审核验证，若上述资料不可用或已超期，则亚洲诚信CA会按照初次申请证书流程和要求进行审核验证，审核通过后，亚洲诚信CA将重新签发新的证书。

4.8.4 签发新证书时对订户的通告

同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

除非CRLReason为“unspecified（0)”，否则CRL条目的“reasonCode”扩展中需包含CRLReason。

只有以下CRLReasons可以出现在CRL条目的“reasonCode”扩展中：

1. keyCompromise (RFC 5280 CRLReason #1)：

   表示已知或怀疑订户的私钥已被泄露；

2. affiliationChanged (RFC 5280 CRLReason #3)：

   旨在用于表明证书中的主题名称或其他主题身份信息已更改，但没有理由怀疑证书的私钥已泄漏；

3. superseded（RFC 5280 CRLReason #4）：

   旨在用于指示证书订户何时请求新证书来替换现有证书，或者亚洲诚信CA获得合理的证据表明域授权的验证不依赖证书中任何FQDN或IP地址的控制，或者亚洲诚信CA出于合规性原因撤销了证书。

4. cessationOfOperation（RFC 5280 CRLReason 5）：

   它旨在在证书到期前停止运营该证书对应的网站时使用，或者订户在证书过期前不再拥有证书中域名的控制权；

5. privilegeWithdrawn（RFC 5280 CRLReason #9）：

   它旨在用于没有私钥泄漏的订户方违规行为。此为特权撤销，不提供给订户。

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（CRLReason“unspecified(0)”，或订户指定另一个原因）；
   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（CRLReason # 9

“privilegeWithdrawn”）；

c. 亚洲诚信CA获得了证据，证明与证书公钥对应的订户私钥遭到了损害(CRLReason # 1“keyCompromise”)；

d. 亚洲诚信CA具有验证订户私钥泄露的方法，此方法可根据公钥轻易计算私钥值(如Debian弱密钥，见https://wiki.debian.org/SSLkeys) ,或者有明确的证据证明订户用来生成私钥的方法是有缺陷的(CRLReason # 1“keyCompromise”)；

e. 亚洲诚信CA获得证据，证书中所包含的域名或IP地址的控制权验证已不再可靠(CRLReason # 4“superseded”)。

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，或不再符合依赖方当前根证书策略如 Mozilla、Google、Microsoft、Apple、Adobe、Oracle、360等(CRLReason # 4“superseded”)；

b. 亚洲诚信CA获得了证书遭到误用的证据（CRLReason # 9 “privilegeWithdrawn”）；

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（CRLReason # 9 “privilegeWithdrawn”）；

d. 亚洲诚信CA获悉任何表明 FQDN 或 IP 地址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）（CRLReason # 5 “cessationOfOperation”）；

e. 亚洲诚信CA获悉某通配符证书被用于鉴别具有欺骗误导性的子域名（CRLReason # 9 “privilegeWithdrawn”）；

f. 亚洲诚信CA获悉证书中所含信息出现重大变化（CRLReason # 9 “privilegeWithdrawn”）；

g. 亚洲诚信CA获悉证书的签发未能符合BR要求、或亚洲诚信CA的CP&CPS(CRLReason # 4“superseded”)；

h. 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（CRLReason # 9 “privilegeWithdrawn”）；

i. 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（CRLReason“unspecified(0)”）；

j. 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（CRLReason“unspecified(0)”）；

k. 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(CRLReason # 1 “keyCompromise”)；

l. 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（CRLReason # 9 “privilegeWithdrawn”）；

m. 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(CRLReason # 4“superseded”)；

n. 亚洲诚信CA已经履行催缴义务后，订户仍未缴纳服务费（CRLReason # 9 “privilegeWithdrawn”）；

o. 证书的技术内容或格式对应用程序软件供应商或依赖方构成不可接受的风险（例如，CA/Browser

论坛可能会确定已弃用的加密/签名算法或密钥大小会带来不可接受的风险，因此应将此类证书在给定的时间内撤销并由CA取代）(CRLReason # 4 “superseded”)；

p. CA 获得证据证明或被告知订户在其签名的软件对象中具有可疑代码（CRLReason # 9 “privilegeWithdrawn”）。

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。
10. 证书的技术内容或格式给应用软件供应商或依赖方带来了不可接受的风险（例如，CA/Browser论坛可能确定不赞成使用的加密/签名算法或密钥大小带来不可接受的风险。

4.9.2 请求证书撤销的实体

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

涉及恶意软件的事件，亚洲诚信CA将按照以下方式处理：

1. 在获悉事件后的1个工作日内，与软件发行商联系，并在72小时内请求答复。
2. 在了解到事件的72小时内，确定受影响的依赖方的数量。
3. 如果收到发行商的答复，则CA和发布者确定撤销的“合理日期”
4. 如果未从发行商处收到任何答复，则CA会通知发布者，CA将在7天内撤销证书，除非它有书面证据证明这将对公众产生重大影响。

4.9.3 撤销请求的流程

4.9.3.1 订户主动提出撤销申请

1. 订户向亚洲诚信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、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，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4天更新并发布新的CRL;
2. 在证书撤销后的24小时内更新并发布新的CRL。

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：

- 自2025年1月15日起，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。

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。

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。

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。如果OCSP响应器的CA未根据第7.1.2.3或第7.1.2.5节进行技术约束，则响应器不对此类请求作出“good”状态的响应。

4.9.10 在线撤销检查要求

与RFC6960一致。

4.9.11 其他形式的撤销公告

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EV CS、EV SSL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

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

CA/Browser论坛的网络和证书系统安全要求通过引用并入，如同在本文中完整阐述一样。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；
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；
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；
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是能够提供正常的服务。另外，还采用专用柴油机，可满足新建机房所有机架满负载可续航12小时以上。

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

5.1.4 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期初始化并进行特理销毁。

在处理作废内容时，至少2名可信人员在场。

5.1.8 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. 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。针对EV型证书，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EV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，每年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. CA/Browser论坛要求及本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;

g. 从每个网络视角进行多视角签发确证（MPIC）尝试，记录以下信息:

- 可唯一标识所使用网络视角的标识符;
- 尝试验证的域名和/或IP地址;
- 尝试的结果（如，“域名验证通过/失败”，“CAA允许/禁止”）

h. 每个尝试的域名或IP地址在证书请求中的多视角签发确证（MPIC）法定人数结果（即“3/4”应解释为“在4个尝试的网络视角中，3个网络视角确证了主网络视角的判定”）。

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每月进行一次检查和汇总。

对系统安全日志，每月进行一次跟踪处理，检查违反策略和规范的重大事件。

5.4.3 审计日志的保存期限

亚洲诚信CA及其时间戳机构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（如第5.4.1—1规定）。
    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（如第5.4.1-2节所述）。
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（如第5.5.5节所述）。
4. 当有事件发生后的任何安全事件记录（如第5.4.1-3条规定，对于时间戳机构的安全事件记录，如第5.5.5-3条规定）。

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，归档以SVN服务器进行备份。

对于纸质资料，不需要进行备份，但采取严格的安全措施保证其安全性，防止非授权访问、修改删除等行为的发生。

5.5.5 记录时间戳要求

亚洲诚信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

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

5.7.1.1 事件响应和灾难恢复计划

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。

5.7.1.2 大规模证书撤销计划

亚洲诚信CA为大规模证书撤销事件制定了全面且可行的计划，此计划每年进行测试演练，并且不断总结和完善该计划。

此计划包含明确定义、可操作且全面的程序，旨在确保快速、一致且可靠地响应大规模证书撤销情况。亚洲诚信CA 不公开此计划，但会提供给第三方审计人员进行审计。亚洲诚信CA 每年会测试、审查和更新此计划。

此大规模证书撤销计划包含：

1. 启动标准——根据CA的风险状况、发证量、运营能力，制定触发大规模撤销计划的具体、客观、可衡量的阈值；
2. 客户联系信息——如何存储、维护和更新订户和客户的联系方式；
3. 自动化——已经自动化或者可以自动化的流程，以及需要人工干预的流程；
4. 目标和时间表——事件分类、撤销启动、证书替换和事件后审查；
5. 订户通知方法——通知受影响订户的机制；
6. 角色分配——负责发起、协调和执行计划的人员的角色和职责；
7. 培训和教育——为负责或支持该计划的人员提供培训、认识和准备活动；
8. 计划测试——每年进行运营测试，以评估准备情况并证明实施的可行性，使用一种或多种桌面演习、模拟、并行测试或受控测试环境，这些测试不涉及撤销有效订户证书；以及
9. 测试后分析和更新计划——如何将从测试或现场事件中获得的经验教训纳入计划，以及审查和更新的频率。

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 私钥损害处理程序

1. 当证书订户发现证书私钥损害时，订户必须立即停止使用其私钥，并立即访问亚洲诚信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CP&CPS第4.9节发布证书撤销信息。
2. 当亚洲诚信CA证书订户的证书私钥受到损害时，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CP&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出现私钥损害时，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，如：Microsoft、Mozilla、Google、Apple、Adobe、Oracle、360。

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（如：Microsoft、Mozilla、Google、Apple、Adobe、Oracle、360。）；
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

订户密钥对由订户自身的服务器或其他设备内置的密钥生成机制生成，亚洲诚信CA不替订户生成服务器证书密钥对。

对于代码签名、EV代码签名和文档签名证书，订户应确保其的私钥应在符合或高于以下标准的密码设备中生成：

- FIPS140-2 Level 2，或
- CC EAL 4+

如果存在以下情况亚洲诚信CA会拒绝订户的证书申请：

1. 密钥对不满足本CP&CPS 6.1.5或6.1.6 中的要求
2. 有明确的证据表明，订户用于生成私钥的特定方法是有缺陷的
3. 亚洲诚信CA通过一种已验证的方法可表明订户的私钥已遭泄露
4. 亚洲诚信CA已事先获知订户的私钥已遭泄露（例如通过本CP&CPS 4.9.1.1中规定的情形获知）
5. 亚洲诚信CA通过一种已验证的方法可以根据订户公钥轻易地计算出私钥(如Debian弱密钥,见: https://wiki.debian.org/SSLkeys ）

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	SHA256, SHA384	SHA256, SHA384	SHA256, SHA384
RSA密钥长度	4096	2048,3072,4096（对于代码签名和EV代码签名证书密钥长度至少为4096位）	2048,3072,4096（对于代码签名和EV代码签名证书密钥长度至少为3072位）
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，使用lint工具进行公钥参数检测，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。

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；

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

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

6.2 私钥保护和密码模块工程控制

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。

用于代码签名、EV代码签名和文档签名证书的密码模块符合或高于以下标准：

- FIPS140-2 Level 2，或
- CC EAL 4+

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

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CP&CPS第6.2.7.1节要求。

6.2.7.3 签名服务的私钥存储

对于签名服务使用的EV代码签名、代码签名以及文档签名私钥，在生成、存储、使用时所用到的硬件加密模块需符合FIPS140-2 Level3或者CC EAL 4+级别或以上，订户应使用以下条件之一来满足签名服务的要求：

1. 使用的HSM可用制造商证书进行验证；
2. 基于云的密钥生成和保护解决方案：
    a. 私钥的密钥创建、存储和使用保持在符合指定要求的云解决方案硬件加密模块的安全边界内；
    b. 必须在管理私钥级别上配置订阅，以记录所有访问、操作和对保护私钥的资源配置更改；
3. 由亚洲诚信CA提供的签名服务。

6.2.7.4 4 订户私钥保护和验证

6.2.7.4.1 订户私钥的保护

对于代码签名、EV代码签名和文档签名证书，订户需向亚洲诚信CA表明使用以下方法之一来满足私钥保护的要求：

1. 订户需向亚洲诚信CA提供可受审计的声明，以表明生成和保护其私钥的硬件加密模块符合以下条件：
    - FIPS140-2 Level 2，或
    - CC EAL 4+
2. 基于云的密钥生成和保护解决方案：
    a. 私钥的密钥创建、存储和使用保持在符合指定要求的云解决方案硬件加密模块的安全边界内；
    b. 必须在管理私钥级别上配置订阅，以记录所有访问、操作和对保护私钥的资源配置更改；
3. 订户使用符合本CP&CPS第6.2.7.3节要求的签名服务。

6.2.7.4.2 订户私钥的验证

亚洲诚信CA通过以下可选的方式来验证订户私钥的保护满足上述要求：

- 订户提供由HSM设备厂商产生的密钥证明，以证明订户CSR对应的私钥是以不可导出的方式在合适的HSM设备中生成的。
- 订户使用亚洲诚信CA指定的加密库、软件和HSM设备来生成和存储密钥对。
- 亚洲诚信CA依赖申请人提供的报告，该报告由经亚洲诚信CA批准并接受过IT和安全培训的审核员签署，或者是CISA，见证在合适的硬件加密模块解决方案（包括基于云的硬件加密模块）中创建密钥对。
- 订户同意他们使用符合本CP&CPS 6.2.7.3要求的签名服务。

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

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
公开信任的根CA	无规定	25年
公开信任的子CA	无规定	20年
DV SSL/TLS服务器证书	无规定	见TLS订户证书期限表
OV SSL/TLS服务器证书	无规定	见TLS订户证书期限表
EV SSL/TLS服务器证书	无规定	见TLS订户证书期限表
文档签名证书	无规定	39个月
代码签名证书	无规定	不超过460天
EV代码签名证书	无规定	不超过460天
邮件安全证书	无规定	27个月
时间戳证书	15个月	135个月

TLS订户证书期限表：

颁发日期在此日期或之后	颁发日期在此之前	证书期限
	2026-03-15	不超过397天
2026-03-15	2027-03-15	不超过199天
2027-03-15	2029-03-15	不超过99天
2029-03-15		不超过46天

对于时间戳证书相关的私钥，签发超过15个月后该私钥不再使用，并且在签发时间戳证书18个月内从保护私钥的硬件加密模块中删除。亚洲诚信CA将委派至少有两名可信人员见证和签署的密钥删除仪式来记录从硬件加密模块中删除私钥的情况。

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码保护私钥匙，订户应妥善保管，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户应注意防止其生物特征被人非法窃取。

6.4.3 激活数据的其他方面

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

当私钥的激活数据不需要时将销毁，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。

考虑到安全因素，对于申请证书的订户激活数据的生命周期，规定如下：

1. 订户用于申请证书的口令，申请成功后失效。
2. 用于保护私钥或者IC卡、USB Key的口令，建议订户根据业务应用的需要随时予以变更，使用期限超过3个月后应要进行修改。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

CA系统的信息安全管理，按照国标《证书认证系统密码及其相关安全技术规范》、工业和信息化部公布的《电子认证服务管理办法》，参照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维护并更新Linting工具，以确保其在发布后的三个月内完成更新，每当Linting工具更新后，会用更新后工具检测所有未过期、未撤销的TLS/CS/SMIME订户证书。

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。

亚洲诚信CA根据风险评估制定以下时间表来进行审查、响应和修复所有已识别的漏洞，并严格按照此时间表执行。

级别	响应时间	补丁/缓解措施	验证和关闭
关键	24小时	72小时	7天
高危	7天	15天	30天
一般	15天	90天	120天
低危	30天	180天	210天

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

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
- 7.1.2.3 技术受限的非TLS中级证书配置
- 7.1.2.6.TLS中级CA证书配置
- 7.1.2.7 订户证书配置
- 7.1.2.8 OCSP响应程序证书配置
- 7.1.2.9 预证书配置

7.1.2.1 根CA证书配置

见第11.1节。

7.1.2.1.1 根CA有效性

见第11.1节。

7.1.2.1.2 根CA扩展

见第11.1节。

7.1.2.1.3 根CA机构密钥标识符

见第11.1节。

7.1.2.1.4 根CA基本约束

见第11.1节。

7.1.2.2.交叉认证的中级CA证书配置

不适用。

7.1.2.2.1 交叉认证的中级CA有效性

不适用。

7.1.2.2.2 交叉认证的中级CA命名

不适用。

7.1.2.2.3 交叉认证的中级CA扩展

不适用。

7.1.2.2.4 交叉认证的中级CA扩展密钥用法-无约束

不适用。

7.1.2.2.5 交叉认证的中级CA扩展密钥用法-受约束

不适用。

7.1.2.2.6 交叉认证的从属CA证书证书策略

不适用。

7.1.2.3 技术受限的非TLS中级CA证书配置

亚州诚信CA除了TLS证书以外，还会签发代码签名证书、邮件安全证书、AATL证书、时间戳证书、OCSP应用程序响应证书。配置可见附件11.2。

7.1.2.3.1 技术受限的非TLS中级CA扩展

见第11.2节。

7.1.2.3.2 技术受限的非TLS中级CA证书策略

见第11.2节。

7.1.2.3.3 技术受限的非TLS中级CA扩展密钥用法

见第11.2节。

7.1.2.4 技术受限的预证书签名CA证书配置

不适用。

7.1.2.4.1 技术受限的预证书签名CA扩展

不适用。

7.1.2.4.2 技术受限的预证书签名CA扩展密钥用法

不适用。

7.1.2.5 技术受限的TLS中级CA证书配置

不适用。

7.1.2.5.1 技术受限的TLS中级CA扩展

不适用。

7.1.2.5.2 技术受限的TLS中级CA名称约束

不适用。

7.1.2.6 TLS中级CA证书配置

见第11.2节.

7.1.2.6.1 TLS中级CA扩展

见第11.2节。

7.1.2.7 订户证书配置

亚洲诚信CA签发TLS证书可以见附件11.3，另外也签发代码签名证书、邮件安全证书、文档签名证书用的订户证书，以及其它作用的时间戳签名证书和OCSP应用程序响应证书，可以见附件11.3。

7.1.2.7.1 订户证书类型

TLS证书包括：域名验证型（DV），组织验证型（OV），增强验证型（EV）。目前暂不签发个人验证（IV）。

代码签名证书包括：代码签名（CS），增强型验证代码签名（EVCS）。

邮件安全签名证书包括：邮箱验证型（MV），个人验证型（IV），组织验证型（OV），Sponsor-验证型（SV）。

其它包括：文档签名证书（DS）、时间戳签名证书以及OCSP应用程序响应证书。

7.1.2.7.2 域名验证

见第11.3.1节。

7.1.2.7.3 个人验证

不适用

7.1.2.7.4 组织验证

见第11.3.2节。

7.1.2.7.5 增强验证

见第11.3.3节。

7.1.2.7.6 订户证书扩展

见第11.3节。

7.1.2.7.7 订户证书签发机构信息访问

见第11.3节。

7.1.2.7.8 订户证书基本约束

见第11.3节。

7.1.2.7.9 订户证书证书策略

见第11.3节。所有保留的证书策略标识符均在本CPS第1.2.1中定义与记录。若订户证书存在policyQualifiers（id-qt-cps:1.3.6.1.5.5.7.2.1），为本CPS的URL地址。

7.1.2.7.10 订户证书扩展密钥用法

见第11.3节。

7.1.2.7.11 订户证书密钥用法

见第11.3节。

7.1.2.7.12 订户证书主题备用名称

见第11.3节。dNSName不包含代表互联网域名系统根区域的零长度域标签。

7.1.2.8 OCSP应用程序响应证书配置

见第11.3.11节。

7.1.2.8.1 OCSP应用程序响应证书有效期

见第11.3.11节。

7.1.2.8.2 OCSP应用程序响应证书扩展

见第11.3.11节。

7.1.2.8.3 OCSP应用程序响应证书权限信息访问

不适用。

7.1.2.8.4 OCSP应用程序响应证书基本约束

见第11.3.11节。

7.1.2.8.5 OCSP应用程序响应证书扩展密钥用法

见第11.3.11节。

7.1.2.8.6 OCSP应用程序响应证书id-pkix-ocsp-nocheck

见第11.3.11节。

7.1.2.8.7 OCSP应用程序响应证书密钥用法

见第11.3.11节。

7.1.2.8.8 OCSP应用程序响应证书证书策略

不适用。

7.1.2.9 预证书配置

预证书是一个由RFC 6962定义的数据结构，可以提交到证书透明度日志中。在结构上，Precertificate与证书完全相同，唯一的区别是在扩展字段中具有特殊的关键性扩展Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)。该扩展确保预证书不会被符合RFC 5280的客户端接受为证书。签署的预证书的存在可以被视为相应证书也存在的证据，因为签名代表亚洲诚信CA的承诺，他可以签发这样的证书。

预证书在CA决定签发证书之后，但在实际签署证书之前创建。亚洲诚信CA可以构建和签发与证书对应的预证书，用于提交到证书透明度日志。亚洲诚信CA可以使用返回的签名证书时间戳来修改证书的扩展字段，在签署证书之前添加一个签名证书时间戳列表，如第7.1.2.11.3节中定义的，并根据相关配置文件允许的内容进行。

一旦签署了预证书，依赖方可以将其视为亚洲诚信CA意图签发相应证书的有约束力承诺，或更常见的是，相应证书已经存在。证书是否与预证书相对应是根据待签名证书内容的值来确定的，该值经过RFC 6962第3.2节定义的转换过程。

亚洲诚信CA在愿意签发相应证书时，才会签发预证书。预证书由签名CA直接签发。

预证书配置中的字段中的编码与证书内容逐字逐句匹配，字段与11.3中TLS证书配置中的字段一致，序列号与相应证书字段相同。扩展部分见7.1.2.9.1。

7.1.2.9.1 预证书扩展配置-直接签发

扩展	是否存在	关键	描述
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	是	是	
签名证书时间戳列表	不	-	
其它扩展	-	-	与证书一致

7.1.2.9.2 预证书扩展配置-预签名CA签发

不适用。

7.1.2.9.3 预证书扩展

预证书包含预证书扩展（OID：1.3.6.1.4.1.11129.2.4.3）。

此扩展有一个extnValue OCTET STRING，它正好是RFC 6962第3.1节规定的ASN.1 NULL值的编码表示，即十六进制编码字节0500。

7.1.2.9.4 预证书授权密钥标识符

预证书由签名CA直接签发，预证书的授权密钥标识与签名CA的证书的主题密钥标识符一致。

7.1.2.10 CA通用字段

亚洲诚信CA在签发CA证书之前，确保证书内容，包括每个字段的内容，完全符合第7.1.2节中至少一个证书配置文件的所有要求。

7.1.2.10.1 CA证书有效期

见第11.2节。

7.1.2.10.2 CA证书命名

见第11.2节。

7.1.2.10.3 CA证书签发机构信息访问

见第11.2节。

7.1.2.10.4 CA证书基本约束

见第11.2节。

7.1.2.10.5 CA证书证书策略

见第11.2节。若证书存在policyQualifiers（id-qt-cps:1.3.6.1.5.5.7.2.1），为本CPS的URL地址。

7.1.2.10.6 CA证书扩展密钥用法

见第11.2节。

7.1.2.10.7 CA证书密钥用法

见第11.2节。

7.1.2.10.8 CA证书名称约束

不适用。

7.1.2.11 通用证书字段

亚洲诚信CA在签发证书之前，确保证书内容，包括每个字段的内容，完全符合第7.1.2节中至少一个证书配置文件的所有要求。

7.1.2.11.1 授权密钥标识符

见第11.3节。

7.1.2.11.2 CRL分发点

见第11.3节。

7.1.2.11.3 签名证书时间戳列表

如果存在签名时间戳列表扩展，其内容是一个OCTET STRING，其中包含根据RFC 6962第3.3节规定编码的签名时间戳列表。

签名时间戳列表中包含的每个签名时间戳对应于与当前证书相关的预证书的LogEntryType。

7.1.2.11.4 主题密钥标识符

见第11.3节。

7.1.2.11.5 其它扩展

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。

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。
- 如果存在多个相对甄别名，则它们按照它们在第7.1.4.2节中出现的顺序编码在RDNSequence内，可以参考附录B。
- 每个名称在所有相对甄别名中不包含多个给定的AttributeTypeAndValue实例。

7.1.4.2 主题属性编码

亚洲诚信CA签发的TLS/CS证书主体中属性顺序以及编码遵循如下表，其它证书参考附录B中对应的证书模版。通用名称包含一个IP地址或者FQDN的值，这个值存在于使用者备用名称扩展中。

属性	OID	规范	编码要求	最大长度
国家	2.5.4.6	RFC5280	PrintableString	2
省份	2.5.4.8	RFC5280	UTF8String 或PrintableString	128
城市	2.5.4.7	RFC5280	UTF8String 或PrintableString	128
组织	2.5.4.10	RFC5280	UTF8String 或PrintableString	64
通用名称	2.5.4.3	RFC5280	UTF8String 或PrintableString	64

EV相关属性顺序以及编码如下表。

属性	OID	规范	编码要求	最大长度
businessCategory	2.5.4.15	X.520	UTF8String 或PrintableString	128
jurisdictionCountry	1.3.6.1.4.1.311.60.2.1.3	EVG	PrintableString	2
jurisdictionStateOrProvince	1.3.6.1.4.1.311.60.2.1.2	EVG	UTF8String 或PrintableString	128
jurisdictionLocality	1.3.6.1.4.1.311.60.2.1.1	EVG	UTF8String 或PrintableString	128
serialNumber	2.5.4.5	RFC 5280	PrintableString	64

7.1.4.3 订户证书通用名称属性

通用名称包含的条目存在与使用者备用名称中，该字段值的编码如下：

- 如果该值是IPv4地址，则该值必须编码为IPv4地址，如RFC 3986第 3.2.2节中指定。
- 如果该值是IPv6地址，则该值必须以RFC 5952第4节中指定的文本表示形式进行编码。
- 如果dNSName值是完全限定域名或通配符域名，则该值编码与使用者备用名称中条目值逐字逐句匹配。完全限定域名或通配符域名的FQDN部分的所有域标签编码为LDH-Label，并且P-Label不使用其Unicode表示形式。

7.1.4.4 其他主题属性

见第11.3节。

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			
	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	撤销原因代码参考下表CRLReasons。 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。

CRLReasons：

RFC5280原因代码	值	描述
未指定	0	默认项
密钥泄漏	1	确认订户私钥泄漏时使用，如果与下面其它原因有重复时，使用此原因
隶属关系变更	3	证书主体名称或者其他主体身份信息变更
被取代	4	表示证书正在被替换，因为：订户已请求新证书，亚洲诚信CA有合理证据表明证书中任何FQDN或IP地址的域授权或控制的验证不被证实，或出于合规原因（例如证书不符合这些基准要求或CPS）而撤销了证书。
停止运营	5	表示持有证书的网站在证书到期前被关闭，或者订户在证书到期前不再拥有或控制证书中的域名。
证书挂起	6	不适用
特权撤销	9	表示订户方存在未导致密钥泄露的违规行为，例如证书订户在其证书请求中提供了误导性信息，或者未履行订户协议或使用条款下的重大义务。

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CA/Browser论坛的BR和指南要求；
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，抽取至少3%的证书样本。
4. 每年根据CA/Browser论坛上BR的要求，进行一次BR自评估工作。
5. 每年对物理控制、密钥管理、操作控制、鉴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。
6. 每年进行一次运营风险评估工作，识别内部与外部的威胁，评估威胁事件发生的可能性及造成的损害，并根据风险评估结果，制定并实施处置计划。
7. 除了内部审计和评估外，亚洲诚信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

内部审计工作涉及以下内容：

1. 运营工作流程和制度是否得到严格遵守；
2. 是否严格按CP&CPS、业务规范和安全要求开展认证业务；
3. 各种日志、记录是否完整，是否存在问题；
4. 是否存在其他可能存在的安全风险。

第三方审计师事务所按照WebTrust CA规范的要求，对亚洲诚信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。审计报告也将在7个工作日内同步到CCADB中。

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该期间签发证书总数的3%。

亚洲诚信CA使用包含与之前证书签发系统不同的Linting工具流程来验证所选样本集内的证书的技术准确性。

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

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. 遵守《中华人民共和国电子签名法》等法律法规，接受行业主管部门的指导，对签发的数字证书承担相应法律责任。
2. 根据《电子认证服务管理办法》要求，对其注册机构电子认证业务是否符合本CP&CPS约定进行审计。
3. 签发给订户的证书符合本CP&CPS的所有实质性要求。

4. 不会签发具有误导依赖方相关CA验证的证书信息的证书。
5. 将向证书订户通报任何已知的，将在本质上影响订户的证书的有效性和可靠性事件。
6. 将根据CP&CPS的要求及时撤销证书。
7. 根据CP&CPS的要求验证申请人的身份。
8. 若亚洲诚信CA与订户无关联，则亚洲诚信CA与订户是合法有效且可执行的订户协议双方，该订户协议符合CA/Browser论坛发布的BRs等要求；若亚洲诚信CA与订户为同一实体或有关联，则申请人代表已认可使用条款。
9. 针对所有未过期的证书的当前状态信息(有效或已撤销)建立及维护24*7公开的信息库。

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

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

9.6.2 注册机构的陈述与担保

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

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. 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，订户就应当承担如下责任：始终保持对其私钥的控制，使用可信的系统，采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用。
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。
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。
10. 对于SSL/TLS服务器证书，订户有责任和义务保证只在证书中列出的主题别名对应的服务器中部署证书。

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

9.6.4 依赖方的陈述与担保

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承担责任。
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将承担不超过本CP&CPS第9.9节规定的有限赔偿责任。

9.9 赔偿

尽管对订户和依赖方承担的责任存在限制，亚洲诚信CA理解并确认，已与亚洲诚信CA签署根证书分发协议的应用程序软件供应商，并不承担认证机构根据这些要求本应承担的任何义务或潜在责任，也不承担因证书的签发、维护或依赖方及其他方对证书的依赖而可能产生的任何其他责任。因此，对于因亚洲诚信CA签发的证书而导致该应用程序软件供应商遭受的任何及所有索赔、损害赔偿和损失，无论涉及何种诉讼原因或法律理论，亚洲诚信CA应为每一家应用程序软件供应商进行辩护、予以赔偿并使其免受损害。但是，这不适用于以下情况：应用程序软件供应商遭受的与亚洲诚信CA签发的证书相关的索赔、损害赔偿或损失，是直接由该应用程序软件供应商的以下行为造成的：将仍然有效的证书显示为不可信，或将以下证书显示为可信：(1) 已过期的证书，或 (2) 已被撤销的证书（但仅限于当前可从亚洲诚信CA在线获取撤销状态，且应用程序软件未能检查此状态或忽略了撤销状态指示的情况）。

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：

- 在任何情况下，每张服务器证书赔偿额，不得超过该证书市场购买价格的10倍。
- 每张 EV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 CP&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。

亚洲诚信CA（在根据修改后的要求签发证书之前）将本CP&CPS中新增的相关信息通知CA/B论坛，方式是向 questions@cabforum.org 发送消息，并收到确认信息已发布到公共邮件列表且在 https://cabforum.org/pipermail/public/ （或在论坛可能指定的其他电子邮件地址和链接）的公共邮件档案中建立索引，以便CA/Browser论坛可以考虑对这些要求进行相应修订。

如果法律不再适用，则停止根据本节启用的对CA实践的任何修改，或者修改这些要求以使其能够同时遵守这些要求和法律。如上所述，亚洲诚信CA在90天内对实践进行适当的改变、调整CP&CPS进行修改并向CA/Browser论坛发出通知。

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/IP验证	依据CSP 3.2.2.4 验证域名控制权 依据CPS 3.2.2.5 验证IP控制权
CAA 验证	依据CPS 3.2.2.8 & CPS 4.2.4 验证CAA
邮箱验证	依据CPS 3.2.2.9 验证电子邮件地址控制权
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 遵循CPS 3.2.2.1及BR、EVG要求
企业扩展验证	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 遵循CPS 3.2.2.1及BR、 EVG要求
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。

鉴别条目	鉴别要求
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代码签名证书。 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EV SSL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。

10.2 订户证书及验证项

各类订户证书需要验证的项目：

	DV SSL/TLS服务器证书	OV SSL/TLS服务器证书	EV SSL/TLS服务器证书	代码签名	EV代码签名	文档签名	MV Strict S/MIME	OV Strict S/MIME	IV Multipurpose S/MIME	SV Multipurpose S/MIME
CSR 验证	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
域名/IP验证	Y	Y	Y	N	N	N	O	O	O	O
CAA 验证	Y	Y	Y	N	N	N	O	O	O	O
邮箱验证	N	N	N	N	N	N	O	O	O	O
组织验证	N	Y	Y	Y	Y	O	N	Y	N	Y
企业扩展验证	N	N	Y	N	Y	N	N	N	N	N
个人身份验证	N	N	N	N	N	O	N	N	Y	Y
经办人验证	N	Y	Y	Y	Y	Y	N	Y	N	Y
高风险验证	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

	DV SSL/TLS服务器证书	OV SSL/TLS服务器证书	EV SSL/TLS服务器证书	代码签名	EV代码签名	文档签名	MV Strict S/MIME	OV Strict S/MIME	IV Multipurpose S/MIME	SV Multipurpose S/MIME
律师身份验证 [1]	N	O	O	O	O	O	N	O	N	O

备注：

Y: 执行此项验证

N: 不需要执行此项验证

O: 根据情况决定是否需要执行此项验证，对于 SMIME 类型证书，可选择使用 1）“域名/IP验证”类型中的域名 结合“CAA 验证”的方式或者，2）“邮箱验证”

[1] 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

多用途根证书字段		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 Global Root CA G3:sha384withRSA TrustAsia Global Root CA G4: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 Global Root CA G3	G4
	组织（O）		TrustAsia Technologies, Inc.
	国家（C）		CN
公钥信息			G3:RSA4096 (OID: 1.2.840.113549.1.1.1) G4:secp384r1 (OID: 1.3.132.0.34)
签名算法			与TBSCertificate签名匹配
扩展: authorityKeyIdentifier		非关键	与subjectKeyIdentifier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

专用CA根证书字段		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			见本CP&CPS第1.1.2节
有效期:notBefore			生成仪式当天
有效期:notAfter			见第1.1.2章
主题	通用名称（CN）		见第1.1.2章
	组织（O）		TrustAsia Technologies, Inc.
	国家（C）		CN
公钥信息			见本CP&CPS第1.1.2节
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

多用途PKI中级证书字段		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			由G3签名：sha384withRSA 由G4签名：sha384withECDSA
有效期:notBefore			生成仪式当天
有效期:notAfter			不晚于签名证书的notAfter
主题	通用名称(CN)		见第1.1.2章中所述
	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	• 用于签发代码签名的中级CA，该扩展为： Policy Identifier=2.23.140.1.4.1 Policy Identifier=1.3.6.1.4.1.44494.2.2.1 • 用于签发EV代码的中级CA，该扩展为： Policy Identifier=2.23.140.1.3 Policy Identifier=1.3.6.1.4.1.44494.2.2.2 • 用于签发除上述之外的中级CA，该扩展为 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	digitalSignature, keyCertSign，cRLSign

多用途PKI中级证书字段	关键扩展项	内容
扩展: extKeyUsage	非关键	必须存在 • 用于签发SSL/TLS类型，该扩展为： 服务器验证 1.3.6.1.5.5.7.3.1 客户端验证 1.3.6.1.5.5.7.3.2 • 用于签发代码签名证书类型，该扩展为： 代码签名 1.3.6.1.5.5.7.3.3 • 用于签发邮件安全证书类型，该扩展为： 安全电子邮件 1.3.6.1.5.5.7.3.4 客户端验证 1.3.6.1.5.5.7.3.2 微软文档签名 1.3.6.1.4.1.311.10.3.12 • 用于签发文档签名证书，该扩展为： PDF 签名 1.2.840.113583.1.1.5 微软文档签名 1.3.6.1.4.1.311.10.3.12 • 用于签发时间戳证书，该扩展为： 时间戳 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 URL= http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>
扩展: cRLDistributionPoints	非关键	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl

专用中级证书字段		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			sha384withRSA或sha384withECDSA
有效期:notBefore			生成仪式当天
有效期:notAfter			不晚于签名证书的notAfter，其中： • TLS/SMIME有效期小于或等于10年 • CS/TSA有效期为20年
主题	通用名称(CN)		见第1.1.2章中所述
	组织（O）		组织机构名称
	国家（C）		国家地区代码
公钥算法			RSA2048 | 4096 (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	• 用于签发 TLS 的中级CA，可用的 Policy Identifier 或组合为： ◦ 2.23.140.1.2.1 ◦ 2.23.140.1.2.2 ◦ 2.23.140.1.1 ◦ 1.3.6.1.4.1.44496.2.1.1 ◦ 2.5.29.32.0（与其他值不能同时存在） • 用于签发时间戳的中级CA，该扩展为：Policy Identifier=2.23.140.1.4.2 • 用于签发代码签名的中级CA，该扩展为：Policy Identifier=2.23.140.1.4.1 • 用于签发邮件安全证书的中级CA，该扩展为：Policy Identifier=Any Policy（2.5.29.32.0）
扩展: basicConstraints		关键	Subject Type=CA Path Length Constraint=0

专用中级证书字段	关键扩展项	内容
扩展: keyUsage	关键	keyCertSign，cRLSign，digitalSignature（可选，仅当 CA 需要签发OCSP响应时设置）
扩展: extKeyUsage	非关键	• 用于签发SSL/TLS类型，该扩展为： 服务器验证 1.3.6.1.5.5.7.3.1 客户端验证 1.3.6.1.5.5.7.3.2（可选） • 用于签发代码签名证书类型，该扩展为： 代码签名 1.3.6.1.5.5.7.3.3 • 用于签发邮件安全证书类型，该扩展为： 安全电子邮件 1.3.6.1.5.5.7.3.4 客户端验证 1.3.6.1.5.5.7.3.2 • 用于签发时间戳证书，该扩展为： 时间戳 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 URL= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1（可选） URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints	非关键	CRL HTTP URL= <CRL 下载地址 HTTP 链接>

11.3 订户（终端实体）证书

11.3.1 域名型SSL/TLS服务器证书

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 or sha384withRSA or 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397天
主题	通用名称（CN）		必须包含在subjectAltName的派生值中
公钥信息			RSA2048 | 3072 | 4096 or 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	Policy Identifier=2.23.140.1.2.1
扩展: basicConstraints		关键	Subject Type=End Entity Path Length Constraint=None
扩展: subjectAltName		非关键	允许 dNSName类型。该条目包含根据第3.2.2.4所验证的完全限定域名或者通配符域名，不得使用内部域名。
扩展: keyUsage		关键	digitalSignature, keyEncipherment (只RSA时可选择设置)
扩展: extKeyUsage		非关键	服务器验证（1.3.6.1.5.5.7.3.1）
扩展：Signed Certificate Timestamp List		非关键	可选扩展，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= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1（可选） URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints		非关键	CRL HTTP URL= <CRL 下载地址的 HTTP 链接>

11.3.2 企业型SSL/TLS服务器证书

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 or sha384withRSA or 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397天
主题	国家（C）		受第3.2章验证的组织机构注册地/经营地所在国家地区代码
	省份（ST）		受第3.2章验证的组织机构注册地/经营地所在省份名称
	城市（L）		受第3.2章验证的组织机构注册地/经营地所在城市名称
	组织（O）		受第3.2章验证的组织机构名称
	通用名称（CN）		必须包含在subjectAltName的派生值中
公钥信息			RSA2048 | 3072 | 4096 or 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	Policy Identifier=2.23.140.1.2.2
扩展: basicConstraints		关键	Subject Type=End Entity Path Length Constraint=None
扩展: subjectAltName		非关键	只能是dNSName或iPAddress类型。为dNSName时，该条目包含根据第3.2.2.4所验证的完全限定域名或者通配符域名，不得使用内部名称；为iPAddress时，如果该值是IPv4地址，则该值必须编码为RFC 3986第3.2.2节中指定的IPv4Address。如果该值是IPv6地址，则该值必须以RFC 5952第4节中指定的文本表示形式编码。
扩展: keyUsage		关键	digitalSignature, keyEncipherment (只RSA时可选择设置)
扩展: extKeyUsage		非关键	服务器验证（1.3.6.1.5.5.7.3.1）
扩展：Signed Certificate Timestamp List		非关键	可选扩展，与预证书LogEntryType匹配

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 URL= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1（可选） URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints	非关键	CRL HTTP URL= <CRL 下载地址的 HTTP 链接>

11.3.3 增强型SSL/TLS服务器证书

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 or sha384withRSA or 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397天
主题	商业类别		受第3.2章验证的组织机构商业类别
	司法管辖区国家名称		受第3.2章验证的组织机构注册地所在司法管辖区国家地区代码
	司法管辖区省份/州		受第3.2章验证的组织机构注册地所在司法管辖区省份/州
	司法管辖区地点		受第3.2章验证的组织机构注册地所在司法管辖区地点
	序列号		受第3.2章验证的组织机构注册编号
	国家（C）		受第3.2章验证的组织机构注册地/经营地所在国家地区代码
	省份（ST）		受第3.2章验证的组织机构注册地/经营地所在省份名称
	城市（L）		受第3.2章验证的组织机构注册地/经营地所在城市名称
	组织（O）		受第3.2章验证的组织机构名称
	通用名称（CN）		必须包含在subjectAltName的派生值中
公钥信息			RSA2048 | 3072 | 4096 or 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=2.23.140.1.1 [2] Policy Identifier=1.3.6.1.4.1.44494.2.1.1
扩展: basicConstraints		关键	Subject Type=End Entity Path Length Constraint=None

证书字段	关键扩展项	内容
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: keyUsage	关键	digitalSignature, keyEncipherment (只RSA时可选择设置)
扩展: extKeyUsage	非关键	服务器验证（1.3.6.1.5.5.7.3.1）
扩展：Signed Certificate Timestamp List	非关键	可选扩展，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= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1（可选） URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints	非关键	CRL HTTP URL= <CRL 下载地址的 HTTP 链接>

11.3.4 企业型代码签名证书

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			sha256withRSA or sha384withRSA or 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460天
主题	国家（C）		受第3.2章验证的组织机构注册地/经营地所在国家地区代码
	省份（ST）		受第3.2章验证的组织机构注册地/经营地所在省份名称
	城市（L）		受第3.2章验证的组织机构注册地/经营地所在城市名称
	组织（O）		受第3.2章验证的组织机构名称
	通用名称（CN）		受第3.2.2章验证的主体合法名称
公钥信息			RSA 3072 | 4096 or 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	Policy Identifier=2.23.140.1.4.1
扩展: basicConstraints		关键	Subject Type=End Entity Path Length Constraint=None
扩展: keyUsage		关键	digitalSignature
扩展: extKeyUsage		非关键	代码签名（1.3.6.1.5.5.7.3.3）
扩展: authorityInfoAccess		非关键	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints		非关键	CRL HTTP URL= <CRL 下载地址的 HTTP 链接>

11.3.5 增强型代码签名证书

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			sha256withRSA or sha384withRSA or 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460天
主题	商业类别		受第3.2章验证的组织机构商业类别
	司法管辖区国家名称		受第3.2章验证的组织机构注册地所在司法管辖区国家地区代码
	司法管辖区省份/州		受第3.2章验证的组织机构注册地所在司法管辖区省份/州
	司法管辖区地点		受第3.2章验证的组织机构注册地所在司法管辖区地点
	序列号		受第3.2章验证的组织机构注册编号
	国家（C）		受第3.2章验证的组织机构注册地/经营地所在国家地区代码
	省份（ST）		受第3.2章验证的组织机构注册地/经营地所在省份名称
	城市（L）		受第3.2章验证的组织机构注册地/经营地所在城市名称
	组织（O）		受第3.2章验证的组织机构名称
	通用名称（CN）		受第3.2.2章验证的主体合法名称
公钥信息			RSA 3072 | 4096 or 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	Policy Identifier=2.23.140.1.3
扩展: basicConstraints		关键	Subject Type=End Entity Path Length Constraint=None
扩展: keyUsage		关键	digitalSignature
扩展: extKeyUsage		非关键	代码签名（1.3.6.1.5.5.7.3.3）

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 URL= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints	非关键	CRL HTTP URL= <CRL 下载地址的 HTTP 链接>

11.3.6 基础型邮件安全证书

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 or sha384withRSA or 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825天
主题	通用名称（CN）		受3.2章验证的rfc822Name电子邮件地址
	Email（E）		受3.2章验证的rfc822Name电子邮件地址
公钥信息			RSA2048 | 3072 | 4096 or 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	Policy Identifier=2.23.140.1.5.1.3
扩展: basicConstraints		关键	Subject Type=End Entity Path Length Constraint=None
扩展: subjectAltName		非关键	包括rfc822Name电子邮件地址
扩展: keyUsage		关键	digitalSignature,nonRepudiation（可选）， keyEncipherment(Only RSA),keyAgreement(Only ECC)
扩展: extKeyUsage		非关键	安全电子邮件（1.3.6.1.5.5.7.3.4）
扩展: authorityInfoAccess		非关键	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints		非关键	CRL HTTP URL= <CRL 下载地址的 HTTP 链接>

11.3.7 个人型邮件安全证书

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 or sha384withRSA or 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825天
主题	通用名称（CN）		受第3.2章验证的申请人的个人法定姓名
	名字（givenName）		受第3.2章验证的申请人的个人法定名字
	姓氏（surname）		受第3.2章验证的申请人的个人法定姓氏
	邮箱（Email）		受第3.2章验证的 rfc822Name电子邮件地址
	国家（C）		受第3.2章验证的申请人国籍的国家地区代码
公钥信息			RSA2048 | 3072 | 4096 or 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	Policy Identifier=2.23.140.1.5.4.2
扩展: basicConstraints		关键	Subject Type=End Entity Path Length Constraint=None
扩展: subjectAltName		非关键	包括rfc822Name电子邮件地址
扩展：keyUsage		关键	digitalSignature,nonRepudiation（可选）， keyEncipherment(Only RSA),keyAgreement(Only ECC)
扩展: extKeyUsage		非关键	安全电子邮件（1.3.6.1.5.5.7.3.4） 客户端验证（1.3.6.1.5.5.7.3.2）

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 URL= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints	非关键	CRL HTTP URL= <CRL 下载地址的 HTTP 链接>

11.3.8 企业型邮件安全证书

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 or sha384withRSA or 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825天
主题	通用名称（CN）		受第3.2章验证的组织机构名称
	组织（O）		受第3.2章验证的组织机构名称
	组织标识（OI）		受第3.2章验证的组织机构注册编码（参照S/MIME BR编写）
	邮箱（Email）		受第3.2章验证的 rfc822Name电子邮件地址
	城市（L）		受第3.2章验证的组织机构注册地/经营地所在城市名称
	省份（ST）		受第3.2章验证的组织机构注册地/经营地所在省份名称
	国家（C）		受第3.2章验证的组织机构注册地/经营地所在国家地区代码
公钥信息			RSA2048 | 3072 | 4096 or 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	Policy Identifier=2.23.140.1.5.2.3
扩展: basicConstraints		关键	Subject Type=End Entity Path Length Constraint=None
扩展: subjectAltName		非关键	包括rfc822Name电子邮件地址
扩展：keyUsage		关键	digitalSignature,nonRepudiation（可选）， keyEncipherment(Only RSA),keyAgreement(Only ECC)
扩展: extKeyUsage		非关键	安全电子邮件（1.3.6.1.5.5.7.3.4）

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 URL= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints	非关键	CRL HTTP URL= <CRL 下载地址的 HTTP 链接>

11.3.9 企业型邮件安全证书高级版

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 or sha384withRSA or 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825天
主题	通用名称（CN）		受第3.2章验证的申请人姓名或pseudonym (2.5.4.65)，以上两者择其一
	组织（O）		受第3.2章验证的组织机构名称
	组织标识（OI）		受第3.2章验证的组织机构注册编码（参照S/MIME BR编写）
	名字(givenName)		受第3.2章验证的申请人的个人法定名字
	姓氏(surname)		受第3.2章验证的申请人的个人法定姓氏
	化名（pseudonym）		受第3.2章验证的申请人的个人化名，此字段不与申请人姓名同存于证书DN中
	邮件(Email)		受第3.2章验证的 rfc822Name电子邮件地址
	城市（L）		受第3.2章验证的组织机构注册地/经营地所在城市名称
	省份（ST）		受第3.2章验证的组织机构注册地/经营地所在省份名称
	国家（C）		受第3.2章验证的组织机构注册地/经营地所在国家地区代码
公钥信息			RSA2048 | 3072 | 4096 or 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	Policy Identifier=2.23.140.1.5.3.2
扩展: basicConstraints		关键	Subject Type=End Entity Path Length Constraint=None

证书字段	关键扩展项	内容
扩展: subjectAltName	非关键	必须包括rfc822Name电子邮件地址
扩展：keyUsage	关键	digitalSignature,nonRepudiation（可选）, keyEncipherment(Only RSA),keyAgreement(Only ECC)
扩展: extKeyUsage	非关键	安全电子邮件（1.3.6.1.5.5.7.3.4） 客户端验证（1.3.6.1.5.5.7.3.2）
扩展: authorityInfoAccess	非关键	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints	非关键	CRL HTTP URL= <CRL 下载地址的 HTTP 链接>

11.3.10 文档签名证书

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			sha256withRSA or sha384withRSA or 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39个月
主题	通用名称（CN）		受第3.2章验证的申请人姓名或受第3.2章验证的组织机构名称
	serialNumber		如果存在，为申请者加密的身份信息
	名字(givenName)		受第3.2章验证的申请人的个人法定名字（个人型和包含个人信息的企业型）
	姓名(surname)		受第3.2章验证的申请人的个人法定姓氏（个人型和包含个人信息的企业型）
	组织（O）		受第3.2章验证的组织机构名称（企业型和包含个人信息的企业型）
	部门(OU)		受第3.2章验证的组织附属机构/组织部门名称（企业型和包含个人信息的企业型）
	城市（L）		受第3.2章验证的组织机构注册地/经营地所在城市名称（企业型和包含个人信息的企业型）
	省份（ST）		受第3.2章验证的组织机构注册地/经营地所在省份名称（企业型和包含个人信息的企业型）
	国家（C）		受第3.2章验证的组织机构注册地/经营地、国籍（个人型）所在国家地区代码
公钥信息			RSA2048 | 3072 | 4096 or 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	Policy Identifier=1.3.6.1.4.1.44494.2.3.1

证书字段	关键扩展项	内容
扩展: basicConstraints	关键	Subject Type=End Entity Path Length Constraint=None
扩展: keyUsage	关键	digitalSignature, nonRepudiation
扩展: extKeyUsage	非关键	PDF 签名（1.2.840.113583.1.1.5） 微软文档签名（1.3.6.1.4.1.311.10.3.12）
扩展: authorityInfoAccess	非关键	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL= <签发者CA下载地址的 HTTP 链接> OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= <OCSP 查询地址的 HTTP 链接>
扩展: cRLDistributionPoints	非关键	CRL HTTP URL= <CRL 下载地址的 HTTP 链接>
扩展：timeStamping	非关键	TimeStamping URL RSA： http://tsa.wt.trustasia.com/aatl-rsag3/<TSCert's SerialNumber> TimeStamping URL ECC： http://tsa.wt.trustasia.com/aatl-eccg4/<TSCert's SerialNumber>
扩展：ArchiveRevInfo	非关键	支持此扩展

11.3.11 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 or 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398天
主题	通用名称（CN）		<CA Common Name>-OCSP Responder
	组织（O）		TrustAsia Technologies, lnc.
	国家（C）		CN
公钥信息			RSA 2048 | 3072 | 4096 or 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 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