

亚洲诚信
依赖方协议
V1.1

亚数信息技术（上海）有限公司

2020年8月25日

注意：亚数信息科技（上海）有限公司（简称“亚洲诚信”）是经过国家有关管理机关审批设立的电子认证服务机构，遵照《中华人民共和国电子签名法》提供电子认证服务。您在依赖或信任一张由亚洲诚信签发的数字证书，或访问、使用亚洲诚信证书撤销列表（CRL）、在线证书状态协议（OCSP）及其他信息（以下简称“信息库”）前，应先阅读并同意《亚洲诚信依赖方协议》（以下简称“本协议”）。在接受本协议之前，请您仔细阅读全部内容。若您不同意本协议全部或部分条款，则不得依赖或使用亚洲诚信所提供的所有电子认证产品或服务。一旦您使用了亚洲诚信的电子认证产品或服务即表明您已接受了本协议全部条款。

一、 关键词

1. **【电子认证服务机构（简称 CA）】：**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。
2. **【电子认证业务规定（简称 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。
3. **【数字证书】：**使用数字签名绑定公钥和身份的电子文档。
4. **【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。
5. **【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。
6. **【依赖方】：**是基于对亚洲诚信签发的证书和（或）数字签名的信赖而从事有关活动的实体。
7. **【依赖方协议】：**在验证、依赖或使用证书或访问或使用亚洲诚信信息库之前必须由依赖方阅读和接受的协议。

二、 亚洲诚信产品服务体系

1. 亚洲诚信签发的数字证书类型如下：
 - 1) TrustAsia 根据公钥算法不同，下设 RSA 和 ECC 两套证书链。

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

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

- 2) TrustAsia Global Root CA G2 为 ECDSA(P-384)withSHA384 算法的根证书,有效期 25 年根据实际业务类型下设不同的 ECDSA 中级证书:
 - a) TrustAsia EV TLS ECC CA ， 签发 ECC 增强型 TLS 服务器证书。
 - b) TrustAsia OV TLS ECC CA, 签发 ECC 企业型 TLS 服务器证书。
 - c) TrustAsia DV TLS ECC CA, 签发 ECC 域名型 TLS 服务器证书。

2. 亚洲诚信将提供 3 种级别的认证产品及服务，每个类别都将提供与之相对应特定和安全功能：

- 1) 域名型证书 (DV)：DV 证书提供一个基本水平的保证，不得用于需要身份验证的场景。DV 证书可以被用来进行数字签名，加密以及不需要身份证明的非商业或低价值交易的访问控制。DV 证书是基于确保使用者域名与公钥关联的程序颁发的。这些证书不会验证证书主题的所有者。
- 2) 企业型证书(OV)：与 DV 证书相比，OV 证书提供了更高级别的保证。OV 证书是颁发给组织的数字签名，加密以及需要身份证明的中等价值交易的访问控制。根据 CPS 的条款，此类证书可以用于组织身份验证。OV 证书认证包括根据身份证明来源验证证书申请人提交的信息。
- 3) 增强型证书 (EV)：EV 证书提供了最高级别的保证。EV 证书是颁发给组织的数字签名，加密以及需要身份证明的高价值交易的访问控制。EV 证书所提供的对主体身份的保证是基于该主体确实存在、主体已请求申请证书并且代表该主体提交证书申请的人被授权这样做。EV 证书还可以对主体有权使用证书中所列域名提供保证。

三、 依赖方的使用与依赖

1. **您保证：**对数字证书的任何依赖都基于已采取合理审慎的措施查证了数字证书与数字签名的有效性后作出的知情决定。
2. **您承诺：**您认可并同意在使用本公司的信息库及依赖或信任本公司颁发的任何证书时，应遵守亚洲诚信 CPS 中相关规定，特别是依赖方的责任和义务条款。
3. 您已经充分知悉并愿意承担依赖或信任证书带来的所有风险，不应以任何方式要求亚洲诚信负责评估使用该证书的适当性。
4. 您应独立评估使用亚洲诚信信息库中包含的信息的适当性，并自行决定是否依赖或信任证书中信息。
5. 您应当在信赖证书之前，确认证书在规定的范围和期限内被使用；对证书的信任链进行验证；通过查询 CRL 或 OCSP 确认证书是否被撤销。
6. 您应仅出于 CPS 中允许的有限目的使用亚洲诚信信息库包含的信息，并应对自身或被授权的其他人员任何非法和未经授权地使用亚洲诚信信息库和数字证书负全部责任。
7. **您认可并同意：**在使用或信赖证书时，因您的故意、过错或疏漏等任何行为而导致的任何损失，均由您自行承担；若您的行为导致其他第三方造成损失的，您应承担赔偿责任并使本公司免于第三方的索赔。若因下述情形而导致亚洲诚信或订户遭受损失的，应当承担赔偿责任：
 - a) 没有履行亚洲诚信与依赖方的协议和亚洲诚信 CPS 中规定的义务；
 - b) 未能依照亚洲诚信 CPS 规范进行合理审核，导致亚洲诚信或第三方遭受损害；
 - c) 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；
 - d) 依赖方没有对证书的信任链进行验证；
 - e) 依赖方没有通过查询 CRL 或 OCSP 确认证书是否被撤销。
8. 您不得拒绝任何来自亚洲诚信公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

四、 亚洲诚信的服务与承诺

1. 亚洲诚信将根据本协议以及 CPS 为您提供电子认证服务（CPS 公布于亚洲诚信网站（www.trustasia.com））。
2. 在证书签发后，亚洲诚信将依据 CPS 相关规定提供证书状态查询服务；在证书被吊销后，亚洲诚信将依据 CPS 相关规定更新 CRL。依赖方都可自行查询。
3. 亚洲诚信承诺其签发的数字证书中载明的订户信息是按照 CPS 的规定验证过的。
4. 为解决您在使用亚洲诚信服务过程中遇到的问题，我们会提供热线服务支持，为了保证我们的服务质量，亚洲诚信设立了服务监督电话：86-21-58895880，并将在 1 个工作日内对您的意见建议作出响应。

五、 亚洲诚信的责任及免责声明

1. 亚洲诚信只承担 CPS 规定的有限责任以及在 CPS 规定的赔偿范围内做出赔偿。
2. 亚洲诚信与依赖方间不是代理人和委托者的关系，依赖方没有权利以合同形式或其他方法让亚洲诚信承担信托责任。
3. 因依赖方的原因造成的损害，亚洲诚信不承担责任，由依赖方自行承担。
4. 订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述，这种行为的后果由订户负责，亚洲诚信不承担相关责任。
5. 除本协议明确承诺担保外，亚洲诚信不承担其他任何形式的保证和义务：
 - a) 不保证证书订户、信赖方、其他参与者的陈述内容；
 - b) 不对电子认证活动中使用的任何软件做出保证；
 - c) 不对证书在超出规定目的以外的应用承担任何责任；
 - d) 不对由于不可抗力，如战争、自然灾害等造成的服务中断，并由此造成的客户损失承担责任；
 - e) 不对因亚洲诚信的设备或网络故障等技术故障而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务承担责任。本项所规定之“技术故障”引起原因包括但不

限于：关联单位如电力、电信、通讯部门而致、黑客攻击、亚洲诚信的设备或网络故障；

- f) 订户违反亚洲诚信 CPS 承诺时，或依赖方违反承诺时，得以免除亚洲诚信之责任；
- g) 亚洲诚信已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

六、 知识产权

1. 亚洲诚信享有并保留对证书以及亚洲诚信提供的所有软件的全部知识产权。
2. 亚洲诚信对数字证书系统软件具有所有权、名称权、利益分享权。
3. 亚洲诚信有权决定采用何种软件系统。
4. 亚洲诚信网站上公布的一切信息均为亚洲诚信财产，未经亚洲诚信书面允许，他人不能转载用于商业行为。
5. 亚洲诚信发行的证书和 CRL 均为受亚洲诚信支配的财产。
6. 对外运营管理策略和规范为亚洲诚信财产。
7. 用来表示目录中亚洲诚信域中的实体的甄别名（简称 DN）以及该域中颁发给终端实体的证书，均为亚洲诚信的财产。

七、 法律适用与管辖

本协议之效力、解释、变更、执行与争议解决均适用中华人民共和国法律。因本协议而发生的争议，双方应当先通过友好协商的方式解决，双方不能达成一致意见的，任何一方可以向上海仲裁委员会申请仲裁，按照该会的规则在上海进行仲裁，仲裁裁决是终局的，对任何一方均有约束力。

八、 其他

1. 亚洲诚信可以随时更新本协议的条款，更新后的协议即替代原来的协议条款。本协议的修订恕不另行通知，建议依赖方经常浏览亚洲诚信网站（www.trustasia.com），以便及时了解亚洲诚信有关证书管理、CPS 和

本协议变更公示等方面的信息。

2. 如本协议中的任何条款无论因何种原因完全或部分无效，本协议的其余条款仍应有效。
3. 本协议中的标题仅为方便而设，不具有任何单独的法律效力。
4. 本协议自依赖方使用了亚洲诚信的任何电子认证产品或服务之日起立即生效，直至依赖方不再使用亚洲诚信任何产品或服务为止。但因违反本协议或 CPS 的规定被迫终止使用亚洲诚信任何产品或服务的，并不因协议终止而免责。
5. 亚洲诚信对本协议享有最终解释权。