

亚洲诚信
订户协议
V1.2.2

亚数信息科技（上海）有限公司

2023年3月24日

注意事项：本订户协议（以下简称“协议”）是您与亚洲诚信签署的法律合同。在继续之前，请仔细阅读本协议以及亚洲诚信依法制定的《电子认证业务规则》（简称 CPS），其中包含了您将获得使用证书服务的有限权利的条款和细则以及亚洲诚信的免责条款。

尊敬的数字证书用户：

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构审批设立的电子认证服务机构，作为权威的第三方安全认证机构，通过数字证书注册机构（以下简称“RA”）向数字证书用户（以下简称“订户”）发放数字证书，为订户网上交易提供信息安全保障。亚洲诚信自行承担 RA，不再另行设立 RA。

您在单击下面“接受”图标或提交证书申请资料后，即视为表明同意接受并愿意遵守本协议的所有条款。若您不同意本协议全部或部分条款，请勿申请使用亚洲诚信数字证书。

一、 订户证书的权利和义务

1、证书订购

订户可以通过签订采购合同、框架协议等书面协议或通过门户网站下单的方式从亚洲诚信购买特定服务，亚洲诚信将会提供每种服务的期限以及该服务的相关付款条款。客户与亚洲诚信所确认的每一张订购单均受本协议条款的管辖。

2、证书申请

订户应遵循诚实、信用原则，在向亚洲诚信申请证书时，应当提供其真实、完整、准确的信息和资料，并在这些信息、资料发生改变时及时通知亚洲诚信。订户同意亚洲诚信对上述信息保留相关记录。如因订户故意或过失提供的资料不真实、不完整、不准确或资料改变后未及时通知亚洲诚信，造成的损失由订户自己承担。根据《中华人民共和国电子签名法》的规定，申请者未向亚洲诚信提供真实、完整和准确的信息，或者有其他过错，给电子

签名依赖方、亚洲诚信造成损失的，订户应承担相应的法律及赔偿责任。

3、证书签发与验收

在通过亚洲诚信的审核、信息注册后，订户即可获得数字证书的下载凭证，订户应妥善保管下载凭证，亲自用该凭证从相关网站将数字证书下载到安全的容器里。订户也可以委托或授权他人通过其他安全的方式获得数字证书。订户应对获得的数字证书信息进行确认，首次使用，视为确认生效。

4、证书的使用与管理

- 1) 订户须使用经合法途径获得的相关软件。
- 2) 订户应合法使用亚洲诚信发放的数字证书，并对使用数字证书的行为负责：
 - a) 使用证书的行为应符合全部适用的法律法规；
 - b) 使用证书的行为应符合订户真实意愿或者仅为了处理已获得授权的事务；
 - c) 使用证书的行为应符合本协议约定的使用范围和条件。
- 3) 当订户使用代码签名证书进行签名时，推荐订户使用亚洲诚信的时间戳服务再次进行时间戳签名。

5、证书私钥的保护

- 1) 订户应采取必要手段来保障证书的私钥和相关密码的安全存储、使用备份等。EV 代码签名证书必须被保存在一定安全级别的安全介质中；如初次使用智能密码钥匙时，应修改初始的缺省密码。订户如因故意或过失导致他人盗用、冒用数字证书私钥和密码时，订户应自行承担由此产生的责任。
- 2) 如订户使用的数字证书私钥和密码泄漏、丢失，或者订户不希望继续使用数字证书，或者订户主体不存在，订户或法定权利人应当立即向亚洲诚信申请撤销该数字证书，相关手续遵循亚洲诚信的规定。亚洲诚信收到撤销申请后，24 小时内处理证书撤销请求。

6、订户责任与义务

- 1) 订户损害亚洲诚信利益的，须向亚洲诚信赔偿全部损失。这些情形包

包括但不限于：

- a) 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致亚洲诚信或第三方遭受损害；
 - b) 订户因故意或者过失造成其私钥泄漏、遗失，或明知私钥已经泄漏、遗失或存在危险而未停止使用证书且未及时告知亚洲诚信和依赖方，以及不当交付他人使用导致亚洲诚信或第三方遭受损害；
 - c) 订户使用证书的行为，有违反亚洲诚信 CPS 及相关操作规范，或者将证书用于非亚洲诚信 CPS 规定的业务范围；
 - d) 证书订户或者其他有权提出撤销证书的实体提出撤销请求后，到亚洲诚信将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果亚洲诚信按照 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赔偿责任；
 - e) 证书中的信息发生变更但未停止使用证书并及时通知亚洲诚信和依赖方；
 - f) 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；
 - g) 证书到期但仍在使用证书；
 - h) 订户的证书信息侵犯了第三方的知识产权；
 - i) 在规定的范围外使用证书，如从事违法犯罪活动。
 - j) 订户有其他过错或未履行本协议的相关约定。
- 2) 亚洲诚信有权因安全风险因素要求订户更换数字证书。订户在收到数字证书更换通知后，应在规定期限内更换。
 - 3) 订户申请代码签名证书后，一旦发现如下情况之一时，应当立即向亚洲诚信申请吊销此证书：
 - a) 证据表明，此代码签名证书被用于签署可疑代码，包括但不限于病毒，木马，或者其他不恰当的程序。
 - b) 证书中内容不再正确或不再准确。
 - c) 此证书私钥信息已被泄露、丢失，或者其他相关部分已被错误使用。
 - 4) 订户在发现或怀疑由亚洲诚信提供的认证服务造成订户的网上交易信息的泄露或篡改时，应在 3 个月内向亚洲诚信提出争议处理请求并通知相关方。

- 5) 订户在证书有效期内如需要删除相关隐私信息，应先提交吊销证书申请，由此产生的后果及风险由订户自行承担。关于更多的隐私政策请参阅《TrustAsia 隐私政策》。
- 6) 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以不可导出的方式生成、存储和使用：
 - a) FIPS140-2 Level 2，或；
 - b) CC EAL 4+。
- 7) 订户在使用代码签名证书时，不得故意为可疑代码签名，若发现已签名的代码包含恶意软件或严重漏洞应及时告知亚洲诚信。

7、证书费用

订户有按期缴纳数字证书服务费的义务，费用标准请咨询亚洲诚信。

8、证书停用

- 1) 证书一旦被吊销，订户将不能再使用该证书。
- 2) 订户明确了解，如果亚洲诚信发现了订户证书的不当使用，或订户证书被用于违法犯罪行为，亚洲诚信有权直接吊销订户证书。

二、 亚洲诚信的服务、责任限制、免责条款和赔偿

1. 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。

2. 服务

- 1) 亚洲诚信依法制定《电子认证业务规则》(简称 CPS)，并公布于亚洲诚信网站 (www.trustasia.com)，明确亚洲诚信数字证书的功能、使用证书各方的权利、义务以及亚洲诚信的责任范围，本协议的相关条款源自 CPS。
- 2) 亚洲诚信为订户提供客服支持热线服务 400-880-8600；7*24 小时技术支持热线服务 86-21-58895880 转 2，+86-18916822880。为了保证我们的服务质量，亚洲诚信设立了投诉电话 86-21-58895880，并将在 1 个工作日内对订户的意见建议作出响应。
- 3) 证书问题报告可发送邮件至 revoke-cn@trustasia.com 或致电 400-880-8600，证书撤销请求必须以书面形式发送至 revoke-cn@trustasia.com。
- 4) 亚洲诚信将对订户申请数字证书时提交的信息进行审核，提供证书生命周期内的相关服务，同时向相关方提供查询服务。亚洲诚信有义务保护订户隐私信息安全性。
- 5) 在订户通过安全工具使用数字证书对交易信息进行加密和签名的条件下，亚洲诚信将保证交易信息的保密性、完整性、抗抵赖性。如果发生纠纷，亚洲诚信将依据不同情形承担下述义务：
 - a) 提供签发订户数字证书的 CA 证书；
 - b) 提供订户数字证书在交易发生时，在或不在亚洲诚信发布的数字证书废止列表内的证明；
 - c) 对数字证书、数字签名的真实性、有效性进行技术确认。

3. 陈述与担保

亚洲诚信的运作遵守《中华人民共和国电子签名法》等法律规定，接受行业主管部门的指导，对签发的数字证书承担相应法律责任。

根据《电子认证服务管理办法》要求，亚洲诚信将不定期对其注册机构电子认证业务是否符合本 CPS 约定进行审计，并随着业务的调整对 CPS 进行修订。

亚洲诚信不负责评估证书是否在适当的范围内使用，订户和依赖方依照

订户协议和依赖方协议确保证书用于允许使用的目的。

4. 免责声明

- 1) 客户确认：本协议中关于服务的担保、服务等级或规格均不适用于基于试用的任何服务。双方确认：试用提供的服务是“按原样”提供的，没有任何保证。亚洲诚信不做任何包括但不限于对适销性，特定用途适用性或不侵犯第三方权利的明示、暗示或法定保证。
- 2) 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。

5. 限制责任

证书订户依法使用亚洲诚信提供的认证服务进行民事活动而遭受直接损失的，亚洲诚信将承担不超过亚洲诚信 CPS 及本协议规定的有限赔偿责任。亚洲诚信只在证书有效期内承担损失赔偿责任。

6. 赔偿

根据《电子签名法》的相关规定，如订户依法使用亚洲诚信提供的认证服务进行民事活动而遭受直接损失的，证书订户可以申请亚洲诚信承担赔偿责任。

责任（法定或约定免责除外）。对于直接损失所负法律责任的上限为：在任何情况下每张服务器证书赔偿额不得超过证书市场购买价格的 10 倍。

7. 证书撤销权

当有以下原因时，订户有权向亚洲诚信提出撤销所签发的数字证书，并提供相关证据或者说明：

1) 密钥泄漏 (RFC 5280 CRLReason #1)

当证书订户知道或有证据相信其证书的私钥已被泄露时，证书订户必须选择“keyCompromise”撤销原因。例如，未经授权的人已经访问了他们证书的私钥。

2) 附属关系已更改 (RFC 5280 CRLReason #3)

当证书中的组织名称或其他组织信息发生更改时，证书订户应该选择“affiliationChanged”撤销原因。

3) 被取代 (RFC 5280 CRLReason #4)

证书订户在请求新证书替换其现有证书时应该选择“superseded”撤销原因。

4) 证书停用 (RFC 5280 CRLReason #5)

当证书订户不再拥有证书中的所有域名或由于停止网站而不再使用证书时，证书订户应选择“cessationOfOperation”撤销原因。

5) 未提供或未指定原因 (RFC 5280 CRLReason #0)

当上述其它原因代码不适用于撤销请求时，订户需选择“unspecified”原因代码，不能使用其它。此项为亚洲诚信撤销证书的默认选项，用户无需提供证据或者说明原因。

特权撤销 (RFC 5280 CRLReason #9) 不提供给订户选择，为亚洲诚信保留使用的撤销方式。

有下列原因的，亚洲诚信将依据 CPS 所表明时间范围内撤销证书并使用相应的 CRLReason：

1) 订户以书面形式请求撤销证书（如果指名撤销原因，则使用 CRLReason #0）；

2) 订户通知亚洲诚信最初的证书请求未得到授权且不能追溯到授权行为（CRLReason #9）；

- 3) 亚洲诚信获得了证据，证明与证书公钥对应的订户私钥遭到了损害，或不再符合 Baseline Requirements 第 6.1.5 节及第 6.1.6 节的相关要求（CRLReason #1）；
- 4) 亚洲诚信获得证据，证书中所包含的域名或 IP 地址的控制权验证已不再可靠（CRLReason #4）；
- 5) 亚洲诚信获得了证书遭到误用的证据（CRLReason #9）；
- 6) 亚洲诚信获悉订户违反了订户协议、CP/CPS 中的一项或多项重大责任（CRLReason #9）；
- 7) 亚洲诚信获悉任何表明 FQDN 或 IP 地址的使用不再被法律许可（例如，某法院或仲裁员已经吊销了域名注册人使用域名的权力，域名注册人与申请人的相关许可及服务协议被终止，或域名注册人未成功更新域名）（CRLReason #5）；
- 8) 亚洲诚信获悉某通配符证书被用于鉴别具有欺骗误导性的子域名（CRLReason #9）；
- 9) 亚洲诚信获悉证书中所含信息出现重大变化（CRLReason #9）；
- 10) 亚洲诚信获悉证书的签发未能符合 Baseline Requirements 要求，或亚洲诚信的 CP/CPS（CRLReason #4）；
- 11) 亚洲诚信认为任何出现在证书中的信息不准确、不真实或具有误导性（CRLReason #9）；
- 12) 亚洲诚信由于任何原因停止运营，且未与另一家 CA 达成协议以提供证书撤销服务（CRLReason #9）；
- 13) 亚洲诚信依据 Baseline Requirements 签发证书的权力失效，或被撤销或被终止，除非其继续维护 CRL/OCSP 信息库（CRLReason #0）；
- 14) 亚洲诚信的 CP/CPS 要求撤销订户证书（CRLReason #4）；
- 15) 亚洲诚信被告知出现了可使订户私钥泄露的经验验证的方法，此类方法可根据公钥轻易地计算私钥值（例如 Debian 弱密钥，见：<http://wiki.debian.org/SSLkeys>），或者有明确的证据证明订户用来生成私钥的方法是有缺陷的（CRLReason #1）；
- 16) CPS 中职责的履行被延迟或受不可抗力的阻碍；自然灾害；计算机或通信失败；法律、规章或其它法律的改变；政府行为；或其它超过个人控制的原因并且对他人信息构成威胁的（CRLReason #4）；
- 17) 亚洲诚信已经履行催缴义务后，订户仍未缴纳服务费（CRLReason #9）；

- 18) 应用软件供应商请求撤销 (CRLReason #4);
- 19) 亚洲诚信检测到代码签名用于恶意软件签名到或者收到用于恶意软件签名的报告 (CRLReason #9)。

8. 亚洲诚信检测到代码签名用于恶意软件签名到或者收到用于恶意软件签名的报告。信息共享

订户确认并接受在以下情况发生时亚洲诚信有权与其他 CA 机构、行业团体、包括 CA/B 论坛共享有关申请人、签名申请、证书和周围情况的信息：

- 1) 证书或申请人被确定为可疑代码的来源；
- 2) 请求证书的权力无法核实；
- 3) 证书因订户请求以外的原因而被撤销（例如：发现恶意软件等而被强制撤销）。

三、 其他

1. 保密性

- 1) 双方均应保密从另一方收到的所有保密信息（包括但不限于信息、文档、系统或流程）。双方仅出于行使和履行本协议下的权利义务之目的而使用所披露的保密信息，并会通过不低于合理谨慎程度来保护所有保密信息免于泄露。
- 2) 订户确认证书服务（以及其中包含或提供的任何信息）包含了亚洲诚信的保密信息。订户不得使用任何来自于亚洲诚信的保密信息进行逆向工程、反编译、反汇编或开发竞争性证书服务等。
- 3) 若根据法律、司法、行政程序或其他相关要求，双方被强制要求依法披露密信息时，应尽合理努力寻求对此类保密信息进行保密处理，并尽最大可能事先通知另一方。

2. 生效与终止

本协议在订户单击“接受”图标或提交证书申请资料后即为生效。本协议将在认购期届满时终止，或在认购期届满前亚洲诚信撤销本协议项下签发的所有数字证书时终止。当认购期届满或证书订户因违反本协议（包括 CPS）

而导致协议终止时，订户须立即停止使用证书服务，并从已经安装了证书服务的设备或软件中移除本协议项下颁发的任何证书。本协议中关于“订户责任与义务”、“知识产权”、“陈述和担保”、“免责声明”、“限制责任”、“保密性”以及 CPS 中指定的存续条款，即使在本协议终止或期满后仍将继续有效。订户的所有付款义务不因本协议终止而终止。

3. 更新维护

建议订户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。

亚洲诚信有权对本协议进行修订，修订后的本协议将公布于亚洲诚信网站 (www.trustasia.com)。如订户在本协议公布修订的 1 个月后继续使用亚洲诚信提供的数字证书服务，即表明同意接受此等修订的约束。如果订户不予接受本协议中的约束，订户可以在上述期限内单方以书面形式向亚洲诚信申请停止使用证书。

4. 争议解决

因依据亚洲诚信的电子认证服务而发生的争议，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。