TrustAsia

Subscriber Agreement

V1.2.2

TrustAsia Technologies, Inc.

March 24, 2023

NOTICE: This Subscriber Agreement ("Agreement") is a legal contract between you and TrustAsia. Before proceeding, please carefully read this Agreement and TrustAsia's legally established Certificate practice Statement ("CPS"), which contains the terms and conditions under which you will be granted limited rights to use the Certificate Service and TrustAsia's disclaimers.

Dear certificate users,

TrustAsia Technologies, Inc. ("TrustAsia") is a Certification Authority approved and established by the relevant state management authorities. As an authoritative third-party security certification authority, TrustAsia issues certificates to certificate users ("Subscribers") through a Registration Authority ("RA") to provide information security protection for Subscribers' online transactions. TrustAsia acts as RA on its own and does not establish another RA.

By clicking the "Accept" icon below or submitting the certificate application information, you are deemed to have agreed to accept and be willing to abide by all the terms of this Agreement. If you do not agree to all or part of the terms of this Agreement, please do not apply for a TrustAsia Certificate.

一、 Rights and Obligations of Subscriber Certificates

1. Certificate order

Subscribers can purchase specific services from TrustAsia through written agreements such as purchase contracts, framework agreements or by placing orders through the portal, and TrustAsia will provide the term of each service and the relevant payment terms for that service. Each purchase order confirmed by the Client and TrustAsia is governed by the terms of this Agreement.

2. Certificate application

Subscribers shall follow the principles of honesty and trustworthiness and shall provide true, complete and accurate information and materials when applying for a certificate from TrustAsia and shall promptly notify TrustAsia of any changes in such information and materials. Subscribers agree that TrustAsia shall keep records of such information. If the Subscriber intentionally or negligently provides information that is untrue, incomplete, or inaccurate, or fails to notify TrustAsia in a timely manner when the information changes, the Subscriber shall be responsible for any damages caused. In accordance with the provisions of the Electronic Signature Law of the People's Republic of China, if the applicant fails to provide TrustAsia with true, complete and accurate information or is otherwise at fault and causes damage to the relying party of the electronic signature or TrustAsia, the Subscriber shall be liable for the corresponding legal and compensation responsibilities.

3. Certificate issuance and acceptance

After passing TrustAsia's audit and information registration, Subscribers will receive a certificate download credential, which they should keep safe and personally use to download the certificate from the relevant website in a secure container. The Subscriber can also delegate or authorize others to obtain the certificate through other secure means. The Subscriber shall confirm the information of the obtained certificate, and the first time it is used, the confirmation shall be regarded as effective.

4. The use and management of the certificate

1) The Subscriber shall use the relevant software obtained through legal channels.
2) The Subscriber shall legally use the certificate issued by TrustAsia and shall be responsible for the use of the certificate.
    a) The act of using the certificate shall be in accordance with all

applicable laws and regulations.

b) The use of the certificate shall be in accordance with the Subscriber's true intention or only for the purpose of handling authorized transactions.

c) The use of the certificate shall conform to the scope and conditions of use agreed in this Agreement.

3) When a Subscriber signs with a code signing certificate, it is recommended that the Subscriber use TrustAsia's timestamp service to perform another timestamp signature.

5. Protection of certificate private key

1) The Subscriber shall take necessary measures to ensure the secure storage and backup of the private key and relevant password of the certificate; the EV code signing certificate must be stored in a security medium with a certain security level; the initial default password shall be modified if the smart password key is used for the first time. If the Subscriber intentionally or negligently causes others to steal or use the private key and password of the certificate fraudulently, the Subscriber shall bear the responsibility arising from it.

2) If the private key and password of the certificate used by the Subscriber are leaked or lost, or if the Subscriber does not wish to continue using the certificate, or if the subject of the Subscriber does not exist, the Subscriber or the legal right holder shall immediately apply to TrustAsia for revocation of the certificate, and the related procedures shall follow the regulations of TrustAsia, and TrustAsia shall process the certificate revocation within 24 hours after receiving the revocation application. The request will be processed within 24 hours after TrustAsia receives the revocation request.

6. Subscriber responsibilities and obligations

1) Subscribers who damage TrustAsia's interests are required to

compensate TrustAsia for all losses. These circumstances include, but are not limited to:

a) The Subscriber intentionally, negligently or maliciously provides untrue information when applying for a certificate, causing TrustAsia or a third party to suffer damage.
b) The Subscriber intentionally or negligently causes the leakage or loss of its private key, or fails to stop using the certificate when the Subscriber is aware that the private key has been leaked, lost or is in danger and fails to inform TrustAsia and the relying party in a timely manner, and improperly delivers the certificate to another person for use, causing TrustAsia or the third party to suffer damage.
c) The Subscriber's use of the certificate violates the TrustAsia CPS and related operational specifications, or uses the certificate for business purposes other than those specified in the TrustAsia CPS.
d) After the Subscriber of the certificate or other entities entitled to revoke the certificate submits a revocation request, until TrustAsia releases the revocation information of the certificate, if the certificate is used for illegal transactions or disputes arise in the course of transactions, the Subscriber of the certificate must bear all the liability for damages if TrustAsia has carried out the relevant operations in accordance with the CPS specifications.
e) Changes in the information in the certificate but fails to stop using the certificate and notify TrustAsia and the relying party in a timely manner.
f) Failure to take effective protection measures for the private key, resulting in the loss or damage, theft or leakage of the private key, etc.
g) Certificate expiration but still using the certificate.
h) The Subscriber's certificate information infringes the intellectual property rights of a third party.
i) Using the certificate outside the stipulated scope, such as engaging in illegal and criminal activities.
j) The Subscriber has other faults or fails to fulfill the relevant

agreements of this Agreement.

2) TrustAsia reserves the right to request the Subscriber to replace the certificate due to security risk factors. After receiving the notice of certificate replacement, the Subscriber shall replace it within the specified period.
3) After applying for a code signing certificate, the Subscriber should apply to TrustAsia for revocation of this certificate as soon as one of the following is discovered:
   a) Evidence that this code signing certificate has been used to sign suspicious code, including but not limited to viruses, Trojan horses, or other inappropriate programs.
   b) The contents of the certificate are no longer correct or accurate.
   c) The private key information of this certificate has been leaked, lost, or other relevant parts have been used incorrectly.
4) If a Subscriber discovers or suspects that the authentication service provided by TrustAsia has caused the disclosure or tampering of the Subscriber's online transaction information, the Subscriber shall submit a dispute resolution request to TrustAsia within 3 months and notify the relevant party.
5) If a Subscriber wants to delete certain private information within the validity of a certificate, the Subscriber shall first submit a request for certificate revocation, and the consequences and risks arising therefrom shall be borne by the Subscriber. For more information about the privacy policy, please refer to TrustAsia Privacy Policy.
6) For code signing certificates, EV code signing certificates and document signing certificates, the Subscriber shall guarantee that the private key is generated, stored and used in an unexportable manner in a cryptographic device that meets or exceeds the following standards:
   a) FIPS 140-2 Level 2; or
   b) Common Criteria EAL 4+.
7) When using code signing certificates, Subscribers should not intentionally sign suspicious code and should promptly notify TrustAsia if the signed code is found to contain malware or serious vulnerabilities.

7. Certificate fee

Subscribers are obligated to pay the certificate service fee on a regular basis. Please consult TrustAsia for the fee schedule.

8. Certificate deactivation

1) Once the certificate is revoked, the Subscriber will not be able to use the certificate again.
2) The Subscriber expressly understands that TrustAsia has the right to revoke the Subscriber Certificate directly if TrustAsia discovers that the Subscriber Certificate has been improperly used or that the Subscriber Certificate has been used for illegal or criminal purposes.

二、 TrustAsia's Services, Limitation of Liability, Exclusion of Liability and Indemnity

1. Intellectual property rights

1) TrustAsia enjoys and retains all intellectual property rights to the certificate and all software provided by TrustAsia.
2) TrustAsia has the ownership, name right and benefit sharing right of the certificate system software.
3) TrustAsia has the right to decide which software system to use.
4) All information published on TrustAsia's website is the property of TrustAsia and cannot be reproduced for commercial use by others without TrustAsia's written permission.
5) The certificates and CRLs issued by TrustAsia are the property of TrustAsia.
6) External operational management policies and practices are the property of TrustAsia.
7) The Distinguished Names (DNs) used to represent entities in the

TrustAsia domain in the directory and the certificates issued to end entities in that domain are the property of TrustAsia.

2. Service

1) TrustAsia has formulated the Certificate Practice Statement (CPS) in accordance with the law and published them on the TrustAsia website (www.trustasia.com) to clarify the functions of TrustAsia certificates, the rights and obligations of the parties using the certificates, and the scope of TrustAsia's responsibilities, and the relevant provisions of this agreement are derived from the CPS.
2) TrustAsia provides Subscribers with customer service support hotline service 400-880-8600; 7*24 hours technical support hotline service 86-21-58895880 ext. 2, +86-18916822880. To ensure the quality of our services, TrustAsia has set up a complaint hotline 86-21-58895880 and will respond to Subscribers' suggestions within 1 working day.
3) Certificate problem report can be sent to revoke-cn@trustasia.com or call 400-880-8600. Certificate revocation requests must be sent to revoke-cn@trustasia.com in writing.
4) TrustAsia will review the information submitted by the Subscriber when applying for a certificate, provide services related to the life cycle of the certificate, and provide query services to relevant parties. TrustAsia is obliged to protect the security of the Subscriber's private information.
5) TrustAsia will guarantee the confidentiality, integrity and non-repudiation of the transaction information under the condition that the Subscriber encrypts and signs the transaction information using a certificate through a security tool. In the event of a dispute, TrustAsia shall have the following obligations depending on the circumstances:
   a) Providing the CA certificate that issued the Subscriber's certificate.
   b) Providing proof that the Subscriber's certificate is or is not in the list of revoked certificates issued by TrustAsia at the time of the transaction.
   c) Technical confirmation of the authenticity and validity of the

certificate and signature.

3. Representations and warranties

TrustAsia operates in compliance with the Electronic Signature Law of the People's Republic of China and other legal provisions, accepts the guidance of the competent industry authorities, and assumes corresponding legal responsibilities for the certificates issued.

In accordance with the requirements of the Measures for the Administration of Electronic Certification Services, TrustAsia will perform audits from time –to time to evaluate whether the electronic certification business of its registrars is in compliance with this CPS covenant and revise the CPS as business adjustments are made.

TrustAsia is not responsible for evaluating whether the certificate is used within its proper scope, and Subscribers and relying parties ensure that the certificate is used for the purposes for which it is permitted in accordance with the Subscriber agreement and relying party agreement.

4. Disclaimer

1) Customer acknowledges that none of the warranties, service levels or specifications in this Agreement with respect to the Services shall apply to any Services on a trial basis. Both parties acknowledge that the services provided on a trial basis are provided "as is" without warranty of any kind and that TrustAsia makes no warranties, express, implied or statutory, including, but not limited to, warranties of merchantability, fitness for a particular purpose or non-infringement of third-party rights.
2) TrustAsia disclaims all warranties and obligations of any kind other than those expressly promised in this Agreement:
    a) Does not guarantee the content of statements made by certificate Subscribers, relying parties, and other participants.
    b) Does not guarantee any software used in certification activities.
    c) Does not assume any responsibility for the application of the

certificate beyond the specified purpose.

d) Does not assume responsibility for service interruptions due to force majeure, such as war, natural disasters, etc., and the resulting customer losses.

e) Not to be responsible for errors, delays, interruptions, inability to issue digital certificates, or suspension or termination of all or part of the certificate service due to technical failures such as equipment or network failures of TrustAsia. The reasons for "technical failures" specified in this subparagraph include but are not limited to: associated units such as electricity, telecommunications, communication departments, hacker attacks, TrustAsia's equipment or network failures.

f) In the event that a Subscriber breaches the TrustAsia CPS commitment, or a relying party breaches the commitment, TrustAsia is released from liability.

g) TrustAsia has carefully followed the rules of the Certificate Practice Statement as stipulated by national laws and regulations, but losses are still incurred.

5. Limitation of liability

If the Subscriber of the certificate suffers direct losses by using the certification services provided by TrustAsia for civil activities in accordance with the law, TrustAsia will bear the limited liability of compensation not exceeding that stipulated in TrustAsia CPS and this Agreement, and TrustAsia will only bear the liability of compensation for losses during the validity period of the certificate.

6. Compensation

In accordance with the relevant provisions of the Electronic Signature Law, Subscribers may apply to TrustAsia to assume liability for direct losses incurred as a result of using the certification services provided by TrustAsia

for civil activities (except for statutory or contractual exemptions). The upper limit of legal liability for direct loss is: in any case, the compensation amount for each server certificate shall not exceed 10 times the market purchase price of the certificate.

7. Certificate revocation right

The Subscriber has the right to propose to TrustAsia to revoke the issued certificate and provide relevant evidence or explanation when the following circumstances occur:

1) keyCompromise (RFC 5280 CRLReason #1)
   The certificate Subscriber must select the "keyCompromise" reasonCode as the CRLReason when they realize or have evidence to believe that the private key of its certificate has been compromised. For example, an unauthorized person has accessed the private key of the certificate.
2) affiliationChanged (RFC 5280 CRLReason #3)
   The certificate Subscriber must select the "affiliationChanged" reasonCode as the CRLReason when the subject's name or other subject identity information in the certificate has changed.
3) superseded (RFC 5280 CRLReason #4)
   The certificate Subscriber must select the "superseded" reasonCode as the CRLReason when requesting a new certificate to replace an existing certificate.
4) cessationOfOperation（RFC 5280 CRLReason #5）
   The certificate Subscriber must select the "cessationOfOperation" reasonCode as the CRLReason when they no longer own or control all the domains in the certificate, or no longer use the certificate due to discontinuation of the website.
5) unspecified (RFC 5280 CRLReason #0)
   The certificate Subscriber must select the "unspecified" reasonCode as the CRLReason when the reasonCodes mentioned above are not applicable to the revocation request.
   The option is set by default to revoke a certificate in TrustAsia, and the

Subscriber is not required to provide evidence or state a reason.
The privilegeWithdrawn (RFC 5280 CRLReason #9) reasonCode will not be made available to the Subscriber. The use of this reason is determined by TrustAsia.

TrustAsia revokes the certificate within the period specified in the CPS and uses the corresponding CRLReason if the following occurs:

1) The Subscriber requests in writing that the certificate be revoked (if there is no revocation reason, then use CRLReason #0);
2) Subscriber notifies TrustAsia that the original certificate request was not authorized and cannot retroactively grant authorization (CRLReason #9);
3) TrustAsia obtains evidence that the Subscriber's private key corresponding to the certificate's public key has been compromised or no longer meets the relevant requirements of Sections 6.1.5 and 6.1.6 of the Baseline Requirements (CRLReason #1);
4) TrustAsia obtains evidence that the verification of control of the domain name or IP address contained in the certificate is no longer reliable (CRLReason #4);
5) TrustAsia obtains evidence that the Certificate has been misused (CRLReason #9);
6) TrustAsia is made aware that the Subscriber has breached one or more of its material responsibilities under the Subscriber Agreement, CP/CPS (CRLReason #9);
7) TrustAsia learns of any indication that the use of the FQDN or IP address is no longer permitted by law (e.g., a court or arbitrator has revoked the domain name registrant's authority to use the domain name, the relevant license and service agreement between the domain name registrant and the applicant has been terminated, or the domain name registrant has not successfully renewed the domain name) (CRLReason #5);
8) TrustAsia learns that a wildcard certificate has been used to identify a deceptively misleading sub-domain (CRLReason #9);
9) TrustAsia learns of a significant change in the information contained in

the certificate (CRLReason #9);

10) TrustAsia learns that the issuance of the certificate fails to meet the Baseline Requirements, or TrustAsia's CP/CPS (CRLReason #4);
11) TrustAsia considers any information appearing in the Certificate to be inaccurate, untrue or misleading (CRLReason #9);
12) TrustAsia ceases operations for any reason and has not reached an agreement with another CA to provide certificate revocation services (CRLReason #9);
13) TrustAsia's authority to issue certificates in accordance with Baseline Requirements lapses or is revoked or terminated unless it continues to maintain the CRL/OCSP information base (CRLReason #0);
14) TrustAsia's CP/CPS requests revocation of a Subscriber certificate (CRLReason #4);
15) TrustAsia is informed of the emergence of empirically verified methods that can compromise a Subscriber's private key, where such methods can easily calculate private key values based on public keys (e.g., Debian weak keys, see: http://wiki.debian.org/SSLkeys), or where there is clear evidence that the method used by the Subscriber to generate the private key is flawed (CRLReason #1);
16) The performance of duties in the CPS is delayed or impeded by force majeure; natural disasters; computer or communications failures; changes in laws, regulations, or other laws; governmental actions; or other causes beyond the control of the individual and that pose a threat to the information of others (CRLReason #4);
17) The Subscriber has not paid the Service Fee after TrustAsia has fulfilled its reminder obligations (CRLReason #9);
18) The application software vendor requests revocation (CRLReason #4);
19) TrustAsia detects that the code signing is used for malware signing, or receives a report that it is used for malware signing (CRLReason #9).

8. Information sharing

Subscribers acknowledge and accept that TrustAsia has the right to share

information about applicants, signature requests, certificates and surrounding circumstances with other CA authorities, industry groups, including the CA/B Forum, in the event that

1) The certificate or applicant is identified as the source of the suspect code.
2) The authority to request the certificate cannot be verified.
3) The certificate is revoked for reasons other than the Subscriber's request (e.g., forced revocation due to discovery of malware, etc.).

三、 Others

1. Confidentiality

1) Each party shall keep confidential all Confidential Information (including but not limited to information, documents, systems or processes) received from the other party. The Parties will use the Confidential Information disclosed only for the purpose of exercising and performing their rights and obligations under this Agreement and will use no less than reasonable care to protect all Confidential Information from disclosure.
2) Subscriber acknowledges that the Certificate Services (and any information contained or provided therein) contain TrustAsia's confidential information. Subscriber shall not use any Confidential Information from TrustAsia for the purpose of reverse engineering, decompiling, disassembling or developing competing Certificate Services, etc.
3) If the Parties are compelled by law to disclose Confidential Information pursuant to legal, judicial, administrative proceedings or other relevant requirements, they shall use reasonable efforts to seek confidential treatment of such Confidential Information and notify the other Party in advance to the maximum extent possible.

2. Commencement and termination

This Agreement shall become effective upon Subscriber's click on the "Accept" icon or submission of the certificate application materials. This Agreement shall terminate upon the expiration of the Subscription Period or upon the revocation of all certificates issued under this Agreement by TrustAsia prior to the expiration of the Subscription Period. Upon the expiration of the Subscription Period or upon termination of the Agreement due to breach of this Agreement (including CPS) by the Subscriber, the Subscriber shall immediately cease using the Certificate Services and remove any Certificates issued under this Agreement from the equipment or software on which the Certificate Services have been installed. The provisions of this Agreement relating to Subscriber's Responsibilities and Obligations, Intellectual Property Rights, Representations and Warranties, Disclaimers, Limitations of Liability, Confidentiality, and the surviving provisions specified in the CPS shall survive termination or expiration of this Agreement. All payment obligations of Subscriber shall not terminate upon termination of this Agreement.

3. Update maintenance

Subscribers are advised to frequently visit TrustAsia's website (www.trustasia.com) to keep abreast of TrustAsia's information regarding certificate management, CPS and the announcement of changes to this Agreement.

TrustAsia reserves the right to amend this Agreement and the revised Agreement will be posted on the TrustAsia website (www.trustasia.com). By continuing to use the certificate services provided by TrustAsia after one month from the date of posting of the amendments to this Agreement, Subscriber agrees to be bound by such amendments. If the Subscriber does not accept the restrictions contained in this Agreement, the Subscriber may unilaterally apply in writing to TrustAsia to discontinue the use of the Certificate within the above-mentioned period.

4. Dispute resolution

Disputes arising from TrustAsia's certification services should first be resolved through friendly consultation between the parties. If the parties cannot agree, either party may apply to the Shanghai Arbitration Commission for arbitration, which will be conducted in Shanghai in accordance with the Commission's rules, and the arbitral award will be final and binding on either party.