UniTrust Global Subscriber Agreement ver1.13

This Subscriber Agreement (“Agreement”) is entered into by and between you and the company, organization, or other entity you represent (“You”) and Shanghai Electronic Certification Authority Co., Ltd. (“SHECA”, “UniTrust”).

By applying for a Certificate, the applicant or the organization and its authorized agent consent to and authorize SHECA to use the Certificate application materials for electronic authentication services and to duly store such materials in accordance with applicable laws, regulations, and supervisory requirements. Applying for a Certificate constitutes acceptance of SHECA’s Personal Information Protection Policy, which is available on the official website: https://www.sheca.com。

This Agreement shall become effective as of the date of the Certificate application. Please read this Agreement carefully. By applying for a Certificate or clicking the Agree button, you signify your consent to and acceptance of the terms of this Agreement. If you do not agree with this Agreement or any of its terms, you must cancel your order within 30 calendar days from the Certificate effective date to obtain a full refund.

If you have any questions regarding this Agreement, you may contact policy@sheca.com for assistance.

1.Definitions and Terminology

AATL : refers to the Adobe Approved Trust List, a root certificate inclusion program maintained by Adobe Inc.
PDF:Portable Document Format, a file format used to present documents independently of application software, hardware, and operating systems.
CA: Refers to a third-party electronic certification authority lawfully established, possessing public trust, and responsible for issuing, revoking, and managing Certificates in accordance with the CP and CPS. For this Agreement, CA refers to UniTrust.
Certificate Applicant: Refers to the natural person or legal entity applying for a Certificate; upon issuance, the Applicant shall be deemed a Subscriber. Subscriber: A natural person or legal entity who accepts the Certificate and complies with the Subscriber Agreement and Terms of Use.
Public Key and Private Key: The Public Key and Private Key form a key pair generated by an algorithm (i.e., one Public Key and one Private Key); the Public Key is the publicly disclosed component of the key pair, The private key constitutes the non-public component.
Certificate/Digital Certificate: An electronic document issued by a Certification

Authority (CA), which binds a public key to subscriber information via a digital signature.

SSL/TLS Certificate : Secure Socket Layer (SSL) is the most prevalent standard for ensuring the security of Internet communications and transactions. An SSL/TLS Certificate adheres to the SSL protocol and is issued by a trusted CA following rigorous validation, providing server identity authentication and data encryption capabilities. SSL/TLS Certificates are categorized by validation level into three types: Domain Validation SSL Certificates (DV SSL), Organization Validation SSL Certificates (OV SSL), and Extended Validation SSL Certificates (EV SSL).

Wildcard Certificate: An SSL/TLS Certificate where the leftmost character of any domain name listed in the Subject Alternative Name contains an asterisk (“*”).

Code Signing Certificate : A Digital Certificate used to digitally sign code, identifying the software source and the developer’s true identity, while ensuring the code remains untampered after signing.

Timestamp Signature: A signature verifying that data existed, remained intact, and was verifiable at or before a specified time. Timestamp signatures are primarily utilized for data integrity protection and subsequent non-repudiation, establishing the exact time of data creation.

Certificate Transparency: also referred to as certificate transparency,it is an experimental IETF open standard and open-source framework designed to monitor and audit digital certi ficates.

Key Leakage: If the Private Key is disclosed to unauthorized persons, and such unauthorized persons can access or use the Private Key, it is deemed that the Private Key has been compromised.

Subject Alternative Name : An extension of X.509 that permits multiple values to be associated with a Certificate via the subjectAltName field in an SSL/TLS Certificate. These values are referred to as Subject Alternative Names.

CRL: The Certificate Revocation List is a list of Digital Certificates revoked by the Certificate Authority prior to their expiration. Certificates included in this list are no longer trusted. Validity.

OCSP: The Online Certificate Status Protocol is an Internet protocol used to obtain the revocation status of X.509 Digital Certificates . Serving as an alternative to the Certificate Revocation List, it addresses Various issues arising from the use of the Certificate Revocation List within Public Key Infrastructure.

Trusted Platform Module (“TPM”): An international standard for secure cryptoprocessors designed to prevent hackers from capturing passwords, encryption keys, and other sensitive data.Trusted Cryptography Module (“TCM”): A hardware module of the Trusted Computing Platform that provides cryptographic operations and features protected storage space. Token : A key storage hardware device approved by the national cryptographic authority or certified to meet FIPS 140-2 Level 2 or higher standards.

Hardware Security Module (“HSM”): A hardware security module approved by the national cryptographic authority or certified to meet FIPS 140-2 Level 2 or higher standards Devices.

CA/Browser Forum : a voluntary consortium comprising certificate authorities, browser software vendors, operating systems, and other PKI-enabled applications, establishing Internet security industry standards for browsers and certificate authorities. UniTrust Certificate Policy ("CP"): the latest version of this policy is accessible at https://www.sheca.com/repository.

UniTrust Certification Practice Statement ("CPS"): the latest version of this policy is accessible at https://www.sheca.com/repository. UniTrust EV Certificate Policy ("EV CP"): The latest version of this policy is available at https://www.sheca.com/repository.

UniTrust EV Certificate Practice Statement ("EV CPS") : The latest version of this practice statement is available at https://www.sheca.com/repository.

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("BR"): The latest version of this docu- ment is available at https://cabforum.org/baseline-requirements-documents.

Guidelines for the Issuance and Management of Extended Validation Certificates ("Guidelines") : The latest version of this document is available at https://cabforum.org/extended-validation.

Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ("MRCS"): The latest version of this document is available at https://aka.ms/csbr.

Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates ("EVCS Guidelines"): The latest version of this document is available at https://cabforum.org/ev-code-signing-certificate-guidelines.

2.Use and Authorization of Certificates

Authorization

From the effective date of the Subscriber Certificate, UniTrust authorizes the Subscriber to exercise the rights to use the Certificate.

Scope of Certificate Usage

The Subscriber shall use the Certificate solely within the authorized scope of use; otherwise, UniTrust shall bear no responsibility for any consequences arising from such use of the Certificate. For S/MIME Certificates, the Subscriber shall use the Certificate only with the email address specified in the Subscriber Certificate.

3. Services Provided by UniTrust

Certificate Revocation Status Query Service

UniTrust provides Certificate Revocation Lists ("CRL") and Online Certificate Status Protocol ("OCSP") services to query the revocation status of Certificates.

Certificate Revocation Service

1.SHECA shall revoke the Subscriber Certificate within 24 hours upon the occurrence of any of the following circumstances:

- The Subscriber (or its authorized agent) requests the revocation of the Certificate and it is confirmed that the requester is indeed the Subscriber;
- Violation of national laws and regulations due to improper use of the Certificate;
- The Subscriber notifies the CA that the original Certificate application was unauthorized and there is no intention to subsequently authorize it;
- The CA possesses evidence indicating that the Private Key corresponding to the Public Key within the Subscriber Certificate is at risk of compromise or no longer complies with the requirements concerning key length, key parameter settings, and quality control as specified in the CPS (please refer specifically to CPS 6.1.5 and 6.1.6);
- The CA discovers a method by which the Private Key corresponding to the Public Key in the Subscriber Certificate can be easily derived;
- The CA possesses evidence indicating that the authentication of Domain Names or IP Addresses within SSL Certificates, or Domain Names or Email Addresses within S/MIME Certificates, is untrustworthy;
- When the CA organization discovers or is notified that the subscriber's signature software contains suspicious code, the CA organization may revoke the Code Signing Certificate.

2. If any of the following situations occur, SHECA shall revoke the Subscriber Certificate within five days:

- SHECA obtains evidence indicating that the Certificate has been misused;
- SHECA discovers that the issuance of the Certificate does not comply with the requirements of the CP/CPS;
- SHECA revokes the Certificate pursuant to the requirements of the CP/CPS;
- Substantive modifications have been made to the information contained in the Subscriber Certificate;
- After issuing the Certificate, SHECA discovers that the Certificate Holder provided false information in their Certificate application;
- The Subscriber breaches obligations, representations, or warranties stipulated in the CP, CPS, and Subscriber Agreement, or the Subscriber is no longer capable of fulfilling the obligations under the relevant agreements;
- The Subscriber has failed to fulfill the payment obligations;
- Continued use of the Subscriber Certificate would undermine SHECA’s commercial reputation and trust framework;
- The legal status of the Subscriber organization changes, is revoked, or is dissolved;
- Technical or standards evolution may impose unacceptable risks on relying parties or application software providers;
- SHECA’s right to issue SSL Certificates under the Baseline Requirements has expired, been revoked, or terminated, unless the CA has arranged for
- the continued maintenance of CRL/OCSP;

- SHECA becomes aware that the Subscriber no longer lawfully uses the email address, domain name, or IP Address contained in the Certificate, such as when a court or arbitration suspends the registrar's right to use a domain name, the usage license or service agreement between the registrar and the Applicant terminates, or the account holder fails to maintain the active status of the email address or domain name;
- SHECA has become aware that a certain wildcard SSL certificate was used to authenticate a domain name involving fraudulent or misleading characteristics;
- SHECA has become aware that a Subscriber's Private Key has been compromised, or there is clear evidence indicating a defect in the specific method used to generate the Private Key;
- Relevant provisions or requirements of laws and regulations.

Certificate Revocation Reason Code (CRL reason Code) Description

Reason Code	Code Value	Description
unspecifed	**0**	Denoted by omitting the reason code. If a CRL Entry pertains to a certificate that is technically unissueable, the reason code must be omitted, except where the CRL Entry concerns Subscriber Certificates subject to these requirements and revoked prior to 15 July 2023.
keyCompromise	1	Indicates that the Subscriber's Private Key is known or suspected to have been compromised.
affliationChanged	3	Indicates that the Subject Name or other subject identity information in the Certificate has changed, but there is no reason to suspect that the Certificate's Private Key has been compromised.
superseded	**4**	Indicates that the Certificate was replaced because the Subscriber requested a new Certificate, or the CA has reasonable evidence indicating that reliance on the authorization or control validation of any fully qualified domain name or IP Address in the Certificate, or the CA revoked the Certificate for compliance reasons (e.g., the

		Certificate does not meet these baseline requirements or the CA's CP or CPS).
cessationOfOperation	**5**	Indicates that, prior to the Certificate's expiration, the website associated with the Certificate was closed, or that, prior to expiration, the Subscriber no longer owns or controls the domain names in the Certificate.
certificateHold	**6**	If a CRL Entry pertains to 1) Certificates subject to these requirements, or 2) Certificates not subject to these requirements, and is A) issued on or after September 30, 2020, or B) not earlier than September 30, 2020, it shall not be included.
privilegeWithdrawn	**9**	Indicates that the Subscriber has engaged in misconduct that has not yet resulted in key compromise, such as the Certificate Subscriber providing misleading information in their certificate request or failing to perform material obligations under the Subscriber Agreement or Terms of Use.

Key Generation Services

UniTrust recommends that Subscribers generate their Key Pairs and perform backups using trusted systems independently whenever feasible. If the Subscriber utilizes UniTrust's key generation service, UniTrust shall generate the Key Pair using a trusted system, with the key length of the RSA Algorithm being no less than 2048 bits and the ECC Algorithm no less than 256 bits. UniTrust does not provide key generation services for publicly trusted SSL/TLS or EV SSL/TLS Certificates.

Timestamp service applicable to code signing or EV code signing.

UniTrust provides free, compliant timestamp services applicable to code signing; UniTrust recommends that Subscribers include timestamp Signatures when signing code. Timestamp services applicable to PDF signatures (AATL).

UniTrust provides chargeable, compliant timestamp services applicable to PDF document signing; Subscribers holding PDF signature Certificates may reasonably utilize this service. However, UniTrust reserves the right to suspend services.

4.Obligations of the Subscriber

Accuracy of Information

The Subscriber hereby represents and warrants that all information provided to UniTrust during the application for the Certificate, as well as any information supplied that is necessary for its issuance, shall be accurate, complete, reliable, and not misleading. If the Subscriber intentionally or negligently fails to provide true, complete, and accurate information to UniTrust, resulting in the erroneous issuance of a Certificate and causing loss to relevant parties,the Subscriber shall bear the corresponding liability.

The Subscriber shall declare and confirm control over the email address contained in the Certificate, as well as the Domain Names or IP Addresses listed in the Subject Alternative Name. If the Subscriber no longer controls such email address, Domain Name, or IP Address, the Subscriber shall promptly notify UniTrust.

Key Pair Generation

If the Subscriber generates the Key Pair independently, the Subscriber shall use a trusted system to generate and safeguard the Key Pair in compliance with the following requirements:

1. The generated Key Pair shall have a minimum key length of 2048 bits for the RSA Algorithm and 256 bits for the ECC Algorithm;
2. The Subscriber shall ensure that the Public Key submitted to UniTrust correctly corresponds to the Private Key.

For Publicly Trusted Code Signing Certificates, the Subscriber shall generate and safeguard the Key Pair by employing one of the following methods:

1. Generating and safeguarding the Key Pair using a Trusted Platform Module;
2. Generating and safeguarding the Key Pair using a Trusted Cryptographic Module;
3. Generating and safeguarding the Key Pair using a Hardware Security Module.

For Publicly Trusted EV Code Signing Certificates or Adobe Document Signing Certificates, the Subscriber shall generate and protect the Key Pair using a Hardware Security Module.During the validity period of the Certificate, the Subscriber must be able to provide UniTrust with proof that the keys associated with the Certificate are stored within a Hardware Security Module; otherwise, UniTrust shall revoke the issued Subscriber Certificate, and the Subscriber shall bear all corresponding liabilities for any losses incurred by related parties.

Private Key Protection

The Subscriber shall take all reasonable and necessary measures to ensure continuous control, non-disclosure, proper safekeeping, and authorized use only of the Private Key corresponding to the Public Key in the Certificate (including any related activation data or devices, such as passwords or tokens). If the Subscriber fails to properly safeguard the Digital Certificate, resulting in its theft, misuse, forgery, or alteration, the Subscriber shall bear the corresponding responsibility.

Reuse of Private Key

Subscribers shall not use a public key that has been or will be used in a non-Code Signing Certificate to apply for a Publicly Trusted Code Signing or EV Code Signing Certificate.

Prevention of Misuse

Subscribers shall implement appropriate network or other security controls to prevent the misuse of Private Keys. In the event of unauthorized access to the Private Key, UniTrust may revoke the Certificate immediately without prior notice.

Acceptance of Certificate

Subscribers shall not use the Certificate before the Applicant or the Applicant's authorized representative has reviewed and verified the accuracy of the Certificate content. If no objection is raised regarding the certificate content within 30 days of receipt, the certificate shall be deemed accepted.

Use of Certificate

The Private Key corresponding to the Public Key contained in the certificate shall be accessed and used exclusively by the Subscriber; the Subscriber shall be responsible for all actions and consequences resulting from the use of the certificate. All online activities involving the use of the certificate in transactions and operations shall be deemed to have been performed by the Subscriber, who shall bear all resulting consequences.

The certificate shall not be transferred, lent, or otherwise assigned. Any consequences arising from transfer, lending, or assignment shall be borne solely by the Subscriber.

Under no circumstances shall the certificate be used for illegal or criminal activities, including phishing attacks, fraud, or signing malware. Subscribers are only permitted to install SSL/TLS or EV SSL/TLS Certificates on servers accessible by the domain names or IP addresses listed in the Subject Alternative Name of the Certificate. Subscribers shall not intentionally use the Certificate to sign software containing suspicious code. If the Certificate is used to sign PDF documents, the user shall retain the approval records at the time the PDF document is signed.

For publicly trusted EV Code Signing Certificates, Subscribers shall also accept the following additional obligations:

1. Sign only code that complies with the latest EV CS Guidelines requirements;
2. Limit use to the authorized company’s business.

Reporting and Revocation

In the event of a certificate revocation under this Agreement, subscribers must promptly cooperate with SHECA to revoke issued certificates within the specified timeframe. Furthermore, the Large-Scale Revocation Plan (MRIP&TP) developed by SHECA in accordance with Cab/From requirements is available on the SHECA resource website at https://www.sheca.com/repository. In the event of a large-scale revocation, subscribers must assist CA in implementing this plan.

Termination of Certificate Usage
The Subscriber shall immediately cease using the Private Key corresponding to the Public Key in the Certificate upon the expiration or revocation of the Certificate.

Responsiveness
The Subscriber shall respond to UniTrust with a statement regarding any Private Key compromise or Certificate misuse within 48 hours.

Acknowledgment and Acceptance
If the Subscriber breaches this Agreement or its terms of use, or if UniTrust determines that the Certificate has been used for illegal activities,criminal activities (such as phishing attacks), fraud,publication, malware or signing of malware, UniTrust is entitled to immediately revoke the Certificate.

Information Sharing
In the case of Publicly Trusted Code Signing or EV Code Signing Certificates, UniTrust may share the Applicant's public information, Subscriber Certificates, signed applications, and related information with other Certification Authorities, industry organizations, and the CA/Browser Forum under the following circumstances:

1. The Certificate or Applicant is identified as a source of suspicious code;
2. The entitlement to the applied Certificate cannot be verified;
3. The reasons for Certificate revocation are not due to the Subscriber's voluntary request (e.g., Private Key compromise, signing of Malware, etc.).

Compliant with industry standards
UniTrust may revise this Agreement as necessary to comply with any changes to the BR 、Guidelines、MRCS or EVCS Guidelines. The revised version of this Agreement shall take effect 30 days after publication on the website. Subscribers may obtain the latest version of the Subscriber Agreement at any time by visiting https://www.sheca.com/repository. Should the Subscriber disagree with the revisions， the Subscriber may terminate this Agreement at any time， and require UniTrust to provide a pro-rata refund from the date of termination of this Agreement until the expiration date of the Certificate Services.If the Subscriber Agreement revision comes into effect

5. Information Disclosure

The Subscriber agrees that UniTrust may disclose the information provided during the Certificate application by the following methods:
1. Embedding the information in the issued Certificate;
2. Publishing the Certificate in the Certificate Transparency logs.

6. Term and Termination

This Agreement shall automatically terminate upon the expiration date of the Certificate Services. This Agreement may be terminated earlier under the following circumstances:

1. Mutual agreement by both parties for early termination;
2. The Subscriber fails to fulfill obligations under this Agreement and fails to effectuate correction within 30 days after receiving notice from UniTrust.

Upon termination of This Agreement, the rights granted to the Subscriber under Article 2 shall be terminated. UniTrust may revoke the Subscriber Certificate in accordance with the certificate revocation procedures, and the Subscriber shall fulfill the obligations to cease use of the Certificate. Termination of This Agreement shall not affect the validity of Article Four、Five、Six、Seven、Eight、Nine and Eleven；the aforementioned provisions shall remain effective to ensure the full execution of necessary obligations.

7. Disclaimer

Except as stated in the CPS，the Certificate Services related to this Agreement shall be subject to the actual services provided. SHECA and its branches、Authorizers do not guarantee the completeness of the Certificate Services.Accurate and without error、Any express warranty regarding content security or any other losses、Implied 、Statutory or other forms of warranty or representation. SHECA and its branches、Authorizer Bear only those obligations prescribed by law，Reject any other warranties，Including merchantability、Quality、Implied warranty of fitness for a particular purpose，Non-infringement warranty，Right to confidentiality，And warranties arising from commercial management or trade customs.

8.Limitation of Liability

Neither SHECA nor SHECA Branches or Authorizers shall be liable to you for any indirect, incidental, special, consequential, or punitive damages (including but not limited to loss of profits, goodwill, use, or data), even if such party has been advised of the possibility of such damages, and even if such damages were foreseeable . Furthermore, SHECA, SHECA Branch, or the Authorizer shall not be liable for any compensation, indemnification, or losses arising from the following:

1. Your inability to use the Certificate, which may result from the following causes;

a. Termination or suspension of This Agreement, or where the Certificate remains under the approval process or has been revoked;
b. SHECA ceases operation of part or all of the services provided under This Agreement;
c. Any total or partial cessation of Certificate Services due to any cause, including

power outages, system failures, or other interruptions.

2. Expenses incurred in purchasing replacement goods or services;
3. Other investments, expenditures, or obligations you incur in connection with This Agreement arising from the use of UniTrust Certificate Services or the exercise of related rights;
4. Any unauthorized access, alteration, deletion, destruction, damage, loss, or failure to store any of your content or other data.Under no circumstances shall the aggregate liability of SHECA, the SHECA Branch, or the Authorizer with respect to Certificates under this Agreement exceed the amount you paid for the Certificate during its issuance. To avoid disputes, notwithstanding the foregoing, the total liability of SHECA, the SHECA Branch, or the Authorizer for any enhanced Certificate issued under this Agreement shall be limited to RMB 20,000 per enhanced Certificate.

9. Intellectual Property

Neither party to this Agreement shall acquire any Intellectual Property rights (including but not limited to trademarks, logos, patents, copyrights, trade secrets, data, etc.) of the other party by virtue of signing or performing this Agreement; Unless the party owning the Intellectual Property grants a written license to use such Intellectual Property, the other party shall have no right to use such Intellectual Property. The Subscriber shall not, under this Agreement, in any manner、assert、 claims against SHECA regarding all software provided thereby、 programs 、documentation 、 systems 、or any Intellectual Property rights in data. Any Intellectual Property arising during the provision of services by SHECA 、shall be considered as、protected by law. Without the written authorization of SHECA, no person shall use, create derivative works of, or commercialize such Intellectual Property in any form.

10.Entire Agreement

The following policies and their updated versions are incorporated into this Agreement by reference:

- UniTrust Certificate Authentication Business Rules;
- UniTrust EV Certificate Authentication Business Rules;
- Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates;
- Guidelines for the Issuance and Management of EV Certificates;
- Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates;
- Guidelines for the Issuance and Management of EV Code Signing Certificates.

11. Governing Law, Jurisdiction, and Other Provisions

Formation of this Agreement、 Effective Date、 Interpretation、 Amendments、 Supplements、Termination、The enforcement of this Agreement and the resolution of disputes shall be governed by the laws of the Mainland of the People's Republic of China. Any disputes arising from this Agreement shall first be resolved through amicable negotiations. If negotiation fails, either party may submit the dispute to the People's Court having jurisdiction over UniTrust's domicile.

If any provision of this Agreement is held to be invalid, void, or unenforceable, such provision shall be deemed severable and shall not affect the validity or enforceability of the remaining provisions.

The final and binding version of this Agreement shall be the Chinese text. In the event of any conflict between the Chinese version of this Agreement and any translated version, the Chinese version shall prevail. (End of text)