trufo

SUBSCRIBER AGREEMENT

THIS SUBSCRIBER AGREEMENT (this "Agreement") is entered into by and between Trufo Inc., operating the Trufo Certificate Authority (the "TCA"), and the individual or legal entity applying for, accepting, or using a digital certificate issued hereunder (the "Subscriber").

BY APPLYING FOR, ACCEPTING, OR USING A TRUFO CERTIFICATE, THE SUBSCRIBER ACKNOWLEDGES THAT IT HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE CONTACT TCA AT CA@TRUFO.AI.

1. DEFINITIONS

In addition to capitalized terms defined elsewhere in this Agreement, the following capitalized words will have their meaning set out below:

"Application" means the Certificate Signing Request (CSR) and related documentation submitted by the Subscriber to the TCA for Certificate issuance.

"C2PA Certificate Policy" means the final, approved version of the document entitled "C2PA Certificate Policy" as made available publicly on the C2PA's website.

"C2PA Generator Product Conforming Requirements" means the final, approved version of the document entitled "C2PA Generator Product Conforming Requirements" as made available publicly on the C2PA's website.

"C2PA Specifications" means version 2.1 or later of the C2PA normative requirements, available at https://c2pa.org/specifications/, as amended from time to time.

"Certificate" means a digitally signed electronic data file issued by the TCA to the Subscriber under this Agreement.

"Certificate Beneficiaries" means any Relying Party, Application Software Vendor (e.g., browser or validator vendors), or Root CA partner that relies on the Certificate.

"Compromise" means a loss, theft, disclosure, modification, unauthorized use, or other breach of security related to a Private Key.

"CPS" means the Trufo Certification Practice Statement (OID 1.3.6.1.4.1.62524.1.1, available at https://trufo.ai/tca/repository/cpcps), as amended from time to time.

"Generator Product" means the specific software or hardware product used to create C2PA manifests, which must be registered on the C2PA Conforming Products List.

"Private Key" means the secret key kept by the Subscriber that corresponds to the Public Key in a Certificate.

"Relying Party" means an entity that acts in reliance on a Certificate or a digital signature verified by a Certificate.

"Trustworthy System" means computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; and are suited to performing their intended functions.

2. APPLICATION AND VERIFICATION

2.1. Submission. The Subscriber may request Certificates by submitting an Application in accordance with the CPS. The Subscriber represents that the Generator Product associated with the Application is currently listed on the C2PA Conforming Products List.

2.2. Verification. The TCA will evaluate the Application to verify the Subscriber's identity and authority. Verification is subject to the TCA's sole discretion. The TCA may refuse to issue a Certificate for any reason, including without limitation if the Generator Product fails to meet current C2PA security standards.

2.3. Incorporation of Policies. The CPS, the C2PA Certificate Policy, and the C2PA Generator Product Conforming Requirements are hereby incorporated by reference into this Agreement. The Subscriber agrees that the TCA may amend these documents from time to time to comply with evolving C2PA and CA/Browser Forum standards.

3. GRANT OF RIGHTS AND PERMITTED USAGE

3.1. License. Effective upon Issuance and continuing until the Certificate expires or is revoked, the TCA grants the Subscriber a limited, non-exclusive, non-transferable, revocable license to use the Certificate in a Trustworthy System solely for the purposes described in this Section 3.

3.2. C2PA Claim Signing Usage. For C2PA Claim Signing Certificates, the Subscriber shall:

(a) Use the Certificate solely for signing C2PA Manifests on verified instances of the designated Generator Product; and

(b) Ensure that the implementation of said Generator Product remains faithful to the specifications and security controls submitted in the C2PA Conformance Application, specifically ensuring that visual content displayed to consumers matches the cryptographic bindings in the manifest (preventing "context separation").

3.3. Identity Usage. For CAWG Identity Certificates, the Subscriber shall use the Certificate solely to assert the identity of the Subscriber as validated by the TCA. The Subscriber shall not use the Certificate to sign on behalf of any other entity.

3.4. Timestamping Usage. Usage must comply with RFC 3161, C2PA Specifications regarding secure timestamping, and the operational requirements set forth in the CP/CPS.

4. SUBSCRIBER OBLIGATIONS AND RESTRICTIONS

4.1. Accuracy of Information. The Subscriber represents and warrants that all information provided to the TCA is true, complete, and not misleading. The Subscriber must promptly update the TCA if any such information changes.

4.2. Accuracy of Assertions. The Subscriber represents and warrants that all assertions, metadata, and claims embedded in any content signed with the Certificate are truthful and accurate.

4.3. Implementation Integrity. The Subscriber represents and warrants that all C2PA Manifests generated using the Certificate are created by a Generator Product that is implemented correctly and securely. This includes, but is not limited to, ensuring that the visual content displayed to consumers matches the cryptographic bindings in the manifest (preventing "context separation").

4.4. Protection of Private Key. The Subscriber shall protect the Private Key in a Trustworthy System consistent with C2PA Assurance requirements for the specific Assurance Level the certificate is granted. The Subscriber acknowledges that it is solely responsible for any Compromise of the Private Key, unless it is using the Trufo Key Management Service.

4.5. Prohibited Activities. The Subscriber shall NOT use the Certificates to sign content or provenance information that is:

(a) Misleading Or Incorrect: Containing inaccurate or falsified provenance information;
(b) Illegal/Harmful: Promotes illegal acts, violence, hate speech, or sexually explicit material involving non-consenting individuals;
(c) Impersonation: Imply endorsement by or affiliation with any third party without explicit written permission.

4.6. Monitoring. The Subscriber is responsible for continuously monitoring the usage of its Generator Products and Certificates to detect anomalous signing patterns or potential abuse.

4.7. Reporting and Remediation. Upon suspicion or discovery of any data quality issue, security vulnerability, or policy violation, the Subscriber must immediately cease using the affected Certification and notify the TCA within twenty-four (24) hours of such occurrence.

4.8. OCSP Usage. To avoid excessive load on the TCA's infrastructure, and to follow the best practices recommended by the C2PA Specifications, the Subscriber should embed OCSP responses directly into C2PA Manifests at the time of signing (e.g. according to 14.5.2 of C2PA Spec v2.3), and should further implement OCSP stapling in the Generator Product so that the Generator Product does not need to query the OCSP endpoint at each signing event. If the Subscriber generates more than one million (1,000,000) signing requests per month without implementing these recommended practices, the TCA reserves the right to charge an overage fee of up to $1.00 USD per one hundred thousand (100,000) requests to cover operational costs.

5. REVOCATION

5.1. Revocation Rights. The TCA reserves the right to revoke any Certificate immediately if the TCA reasonably believes that:

(a) The Subscriber has breached any material term of this Agreement, including the Acceptable Use Policy;
(b) The Private Key has been Compromised or is not stored in a Trustworthy System;
(c) The Generator Product has been removed from the C2PA Conforming Products List;
(d) The Certificate contains inaccurate or misleading information; or
(e) Revocation is necessary to protect the rights, operations, or reputation of the TCA or the C2PA ecosystem.

5.2. Effect of Revocation. Upon revocation or expiration, the Subscriber shall immediately cease using the Certificate and corresponding Private Key.

6. FEES AND PAYMENT

6.1. Fees. The Subscriber shall pay all fees set forth in the applicable Order Form.

6.2. Taxes. The Subscriber is responsible for all applicable taxes, duties, and levies resulting from this Agreement, excluding taxes based on the Trufo's income.

7. INTELLECTUAL PROPERTY RIGHTS

7.1. TCA Ownership. The TCA and its licensors retain all right, title, and interest in and to the Certificates (excluding the Subscriber's data contained therein), the Certificate revocation lists (CRLs), OCSP responses, and the CA infrastructure and Documentation.

7.2. Subscriber Ownership. The Subscriber retains all right, title, and interest in and to its Private Keys and any trademarks or trade names included in the Certificate Subject Distinguished Name (DN).

8. WARRANTIES AND DISCLAIMERS

8.1. TCA Limited Warranty. The TCA warrants solely to the Subscriber that: (a) it has issued the Certificate in material accordance with the CPS; and (b) there are no material misrepresentations of fact in the Certificate known to the TCA at the time of Issuance.

8.2. Subscriber Warranties. The Subscriber warrants that: (a) it owns or has the right to use the Generator Product; (b) it will protect the Private Key from Compromise; and (c) all assertions regarding content provenance made via the Certificate are truthful.

8.3. DISCLAIMER. EXCEPT FOR THE EXPRESS WARRANTIES IN SECTION 8.1, THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE." THE TCA DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THE TCA DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE.

9. INDEMNIFICATION

The Subscriber shall indemnify, defend, and hold harmless the TCA, its affiliates, directors, officers, employees, and Certificate Beneficiaries (collectively, the "Indemnified Parties") from and against all claims, liabilities, damages, and costs (including reasonable attorneys' fees) arising from:

(a) The Subscriber's breach of this Agreement;
(b) Any falsehood or misrepresentation of fact by the Subscriber in the Application or within signed content;
(c) The Compromise of the Subscriber's Private Key; or
(d) An allegation that the Subscriber used the Certificate to infringe on the rights of a third party or to validate illegal or harmful content.

10. PRIVACY AND CONFIDENTIALITY

10.1. Confidentiality. The information collected by the TCA from the Subscriber through the OV and PV processes that are not published in the Certificate or otherwise published publicly will be kept confidential.

10.2. Public Information. The Subscriber acknowledges that Certificates and Certificate Status Information (CRL/OCSP) are public records and consents to their publication by the TCA in accordance with the CPS.

11. TERM AND TERMINATION

11.1. Term. This Agreement is effective as of the Effective Date and remains in effect until the expiration or revocation of the last Certificate issued hereunder, unless earlier terminated.

11.2. Termination. Either party may terminate this Agreement immediately upon written notice if the other party breaches a material term and fails to cure such breach within thirty (30) days of notice.

11.3. Survival. The sections titled Intellectual Property Rights, Warranties and Disclaimers, Indemnification, Limitation of Liability, and Miscellaneous shall survive termination.

12. MISCELLANEOUS

12.1. Governing Law. This Agreement is governed by the laws of the State of New York, without regard to its conflict of laws principles. The parties submit to the exclusive jurisdiction of the state and federal courts located in New York, New York.

12.2. Entire Agreement. This Agreement, together with the CPS, MSA, and the applicable Order Form, constitutes the entire agreement between the parties regarding the subject matter hereof and supersedes all prior agreements.

12.3. Third Party Beneficiaries. Certificate Beneficiaries are express third-party beneficiaries of the Subscriber's obligations and representations under this Agreement. Except for Certificate Beneficiaries, no other third party has any rights under this Agreement.

12.4. Severability. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.