# TrustID®
## Code Signing | Organization Identity | Certificate
### Forms Packet



TrustID® CERTIFICATE PROGRAM

# Instructions for completing the Form

Thank you for choosing IdenTrust Services, LLC ("IdenTrust"), a subsidiary of IdenTrust, Inc., to issue you a TrustID | Code Signing | Organization Identity certificate. TrustID | Code Signing | Organization Identity certificates are issued to business entities that have been validated by IdenTrust.

If using a Hardware Security Module (HSM) to generate, store and use the private key related to your TrustID | Code Signing | Organization Identity certificate you are required to complete and return the TrustID Code Signing HSM IT Audit Form available in Appendix A of the TrustID | Code Signing | Organization Identity CERTIFICATE SUBSCRIBER AGREEMENT.

Follow these instructions to successfully apply and complete paperwork for the TrustID | Code Signing | Organization Identity certificate.

## Form

Please apply for the TrustID | Code Signing | Organization Identity certificate:
https://www.identrust.com/digital-certificates/trustid-code-signing
Fill out all of the fields on the form:

- Contract Signer – Your name, title and signature are required.
- Subscriber – The name of the subscribing organization.

In addition, if using an HSM for key storage, fill out all fields on the TrustID | Code Signing | Organization Identity certificate HSM IT Audit Form by consulting with your IT and/or InfoSec personnel that are in charge of installing, and operating the HSM storing the private key associated with all of your TrustID | Code Signing | Organization Identity certificate(s). Please note that your organization maybe using multiple HSMs from multiple different vendors installed at different times. Working with your IT and/or InfoSec personnel please take account of all those HSM(s). Once the form has been completed and signed, please follow the instructions for submitting the completed form to IdenTrust.

Please review the published validation for each HSM module and confirm that the 'Standard' is FIPS 140-2 and 'Overall Level' is 2 or higher. https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules

## Submitting the Completed Form

Choose one of the following:

- Send the original, 'wet-signature' (pen to paper) forms packet to IdenTrust for processing. It is advised you select a traceable shipping method such as FedEx or UPS, but you may also submit the originals using US Mail.

  Registration Department
  IdenTrust Services
  5225 W. Wiley Post Way, Ste 450
  Salt Lake City, UT 84116-2898

- Submit the forms packet to IdenTrust via email. Signatures on the forms must be handwritten or a digital signature that can be traced to an IdenTrust Certificate Root with a Human Subscriber digital certificate specified for Document Signing (excluding certificates used exclusively for S/MIME) and may not be a stamp or electronic signature.

  Email to Processing@IdenTrust.com

Processing and approval of your application will begin once valid, accurate and complete forms have been received.

# TrustID | Code Signing | Organization Identity Certificate Subscriber Agreement

CONTRACT SIGNER: _____

SUBSCRIBER: _____

The natural person who signs below in this TrustID | Code Signing | Organization Identity Certificate Subscriber Agreement warrants, represents, and attests that:

(i) he or she is the person who made the online application for a TrustID Certificate to which this agreement relates;

(ii) his or her name is the name of the "CONTRACT SIGNER" as entered above and such name is the same name he or she used to identify his or herself, respectively, in the online application for a TrustID Certificate to which this agreement relates;

(iii) with respect to the name of the "SUBSCRIBER" as entered above, he or she entered the same name in the online application for a TrustID Certificate to which this agreement relates as the name of the organization for which a TrustID Certificate is requested in such application; and

(iv) he or she has read, understood, and accepts the terms and conditions set forth in Schedule 1 **(attached and incorporated by reference).**

Unless otherwise defined herein, capitalized terms used herein shall have the meanings ascribed to them in Schedule 1.

ACCEPTED AND AGREED:

_____
(Print SUBSCRIBER name)

By:_____
(Signature of CONTRACT SIGNER)

Name: _____
(Print CONTRACT SIGNER name)

Title: _____
(Print CONTACT SIGNER title)

THE AGREEMENT BELOW SETS FORTH TERMS AND CONDITIONS THAT GOVERN THE APPLICATION FOR AND USE OF ANY TRUSTID™ CERTIFICATE THAT MAY BE ISSUED AS A RESULT OF SUCH AN APPLICATION.

TO AGREE TO SUCH TERMS AND CONDITIONS, THEN ON THE PRIOR SCREEN, CLICK ON THE BOX NEXT TO "By clicking in the box to the left, you indicate that you have read and that you accept the terms and conditions of the Subscriber Agreement and Privacy Policy."

IF YOU DO NOT AGREE TO SUCH TERMS AND CONDITIONS, CLICK ON "X CANCEL" AT THE BOTTOM LEFT OF THE PRIOR SCREEN AND DO NOT PROCEED WITH AN APPLICATION FOR A TRUSTID™ CERTIFICATE.

# TRUSTID® | CODE SIGNING | ORGANIZATION IDENTITY CERTIFICATE SUBSCRIBER AGREEMENT

**1. Definitions.** Unless otherwise defined herein, capitalized terms used herein shall have the meanings ascribed to them in Section 22 of this Agreement.

**2. Scope.** This Agreement establishes Subscriber's rights, duties, and obligations as an Applicant for one or more TrustID® Certificates and, if issued by IdenTrust pursuant in response to such application, one or more Code Signing Certificates.

**3. Application.** The contents of the Code Signing Certificate requested as part of the Application will be based on information provided to IdenTrust in the Application. The contents of any Code Signing Certificate requested by any Certificate Requester shall be based on information provided to IdenTrust in the Application and in the applicable request of the Certificate Requestor, with the information in such request becoming part of the Application for purposes hereof.

**4. Identity and Authorization.**

**4.1. Representations and Warranties Relating to Contract Signer.**

The Contract Signer represents and warrants that: (i) he or she is the Subscriber, is employed by the Subscriber, or is an authorized agent of the Subscriber; and (ii) he or she has express authority to represent the Subscriber; and (iii) all information entered in the Application is accurate, current, and complete.

By signing this Agreement, the Contract Signer acknowledges that he or she has the authority to obtain the digital equivalent of a Subscriber stamp, seal, or (where applicable) officer's signature to establish the authenticity of the Subscriber's website, and that Subscriber is responsible for all uses of the Code Signing Certificate. By signing this Agreement on behalf of Subscriber, the Contract Signer represents that the Contract Signer: (i) is acting as an authorized representative of Subscriber; (ii) is expressly authorized by Subscriber to sign this Agreement and such other documents that may be signed by Contract Signer in connection with this Agreement; and (iii) is expressly authorized by Subscriber to approve requests for Code Signing Certificates on Subscriber's behalf.

**4.2. Representations and Warranties Relating to Subscriber.**

IdenTrust and Subscriber acknowledge that this Agreement is a legally valid and enforceable agreement that creates extensive obligations on Subscriber. A Code Signing Certificate serves as a form of digital identity for Subscriber. The loss or misuse of the Code Signing Certificate can result in great harm to the Subscriber.

By entering into this Agreement, Subscriber represents and warrants that: (i) all of the information submitted to IdenTrust in the Application (including without limitation organization names) is accurate, current, complete, and not misleading; (ii) Subscriber owns the right to use any organization name submitted to IdenTrust in the Application; and (iii) Subscriber has provided all facts material to confirming its identity and to establishing the reliability of the information Subscriber has provided to IdenTrust for incorporation into any Code Signing Certificate requested from IdenTrust pursuant to this Agreement.

By accepting a Code Signing Certificate, Subscriber: (i) accepts its contents and the responsibilities identified in this Agreement; and (ii) represents and warrants to IdenTrust and to each Relying Party that, (a) Subscriber rightfully holds the Private Key corresponding to the Public Key listed in the Code Signing Certificate, (b) all representations made and information submitted by or on behalf of Subscriber to IdenTrust in the Application and as part of the Identification and Authentication related to the Code Signing Certificate, such representations are and such information is current, complete, true, and not misleading, (c) Subscriber has provided all facts material to confirming Subscriber's identity and to establishing

the reliability of the Code Signing Certificate, (d) all information in the Code Signing Certificate that identifies Subscriber is current, complete, true, and not misleading, (e) Subscriber is not aware of any fact material to the reliability of the information in the Code Signing Certificate that has not been previously communicated to IdenTrust, (f) Subscriber has generated, stored, and used the private key in either IdenTrust provided key storage mechanism related to the Code Signing Certificate or in Subscriber controlled crypto module that meets or exceeds the requirements of FIPS 140-2 level 2, and (g) Subscriber has kept secret its Private Key related to the Code Signing Certificate.

**4.3. Contract Signer as Certificate Approver.**

With respect to the request that is for a Code Signing Certificate and that is part of the Application, Subscriber authorizes the Contract Signer to submit such request to IdenTrust, which such authorization and request are hereby acknowledged as and deemed to be made during the term of this Agreement.

For the duration of the term of this Agreement, the Subscriber authorizes the Contract Signer to: (i) submit requests for Code Signing Certificates to IdenTrust; (ii) with respect to the Application, to provide to IdenTrust the information in such Application and requested from Subscriber in connection with such Application; (iii) authorize one or more Certificate Requestors to submit requests for Code Signing Certificates on behalf of Subscriber; (iv) authorize one or more Certificate Requestors to provide information requested from the Subscriber by IdenTrust in connection with the issuance of Code Signing Certificates; and (v) approve requests for Code Signing Certificates submitted by any Certificate Requestor.

With respect to authorizing any Certificate Requestors as provided for above, it is understood that if Contract Signer desires to so authorize one or more Certificate Requestors, Contact Signer will contact IdenTrust at Support@IdenTrust.com and IdenTrust will send the Contract Signer the applicable IdenTrust form(s) for such authorization(s) to be presented to IdenTrust.

With respect to requests for Code Signing Certificates from Certificate Requestors, it is understood that if a Certificate Requestor desires to request a Code Signing Certificate from IdenTrust, such Certificate Requestor will contact IdenTrust at Support@IdenTrust.com and IdenTrust will send the Certificate Requestor the applicable IdenTrust form(s) to make such request to IdenTrust.

**5. Code Signing Certificate Issuance.**

**5.1. Key Pair Generation.** Subscriber shall generate a Key Pair (Public and Private Keys) and submit the Public Key of such Key Pair with the Application. When IdenTrust creates a Code Signing Certificate, the Public Key submitted as part of the request for such Code Signing Certificate that part of the Application will be included in such Code Signing Certificate. IN NO EVENT WILL IDENTRUST EVER HAVE ACCESS TO A PRIVATE KEY OF ANY KEY PAIR GENERATED BY SUBSCRIBER FOR A CODE SIGNING CERTIFICATE.

**5.2. Verification of Identity and Authorization.** Subscriber authorizes IdenTrust to engage in Identification and Authentication relative to the Code Signing Certificate requested in the Application and any further Code Signing Certificate requested by a Contract Signer or a Certificate Requestor as provided for in this Agreement. IdenTrust may consult public or private databases or other sources as part of such Identification and Authentication. Subscriber agrees to provide such further information as IdenTrust may reasonably require in connection with Identification and Authentication processes, which such further information shall be deemed part of the Application. In the event IdenTrust contacts Subscriber or Contract Signer or a Certificate Requestor as part of Identification and Authentication, Subscriber represents and warrants that any responses provided to IdenTrust by Subscriber as part of such contact shall be complete and accurate when given. IdenTrust will not request a credit report without Subscriber's express written prior consent, and this Agreement will not be construed as express written prior consent to obtain a credit report. Subscriber also authorizes IdenTrust to store and use, in accordance with this Agreement, the Application, any information provided to IdenTrust during the Identification and Authentication process, and any information disclosed to IdenTrust during the process described in Section 5.3.

**5.3. Issuance.** If IdenTrust approves the Application in relation to a given request for a Code Signing Certificate, IdenTrust will create a Code Signing Certificate in the name of Subscriber and will notify Subscriber how and where to retrieve such Code Signing Certificate. When Subscriber retrieves a Code Signing Certificate, Subscriber will be deemed to have been issued and accepted the Code Signing Certificate by IdenTrust. If IdenTrust determines through Identification and Authentication that any requirement of the CP and CPS applicable to issuance by IdenTrust of a Code Signing Certificate requested under this Agreement is not satisfied, then IdenTrust may refuse to issue such Code Signing Certificate without any liability to any Individual or other entity.

**5.4. Acceptance.** When Subscriber downloads a Code Signing Certificate described in Section 5.3 above, the contents of such Code Signing Certificate will be presented, and Subscriber agrees to (a) review again the information in the Code Signing Certificate and (b) immediately notify IdenTrust of any inaccuracies, errors, defects or other problems with the Code Signing Certificate. Subscriber agrees that it will have accepted the Code Signing Certificate: (i) when it uses the Code Signing Certificate or the corresponding Key Pair after downloading that Code Signing Certificate; or (ii) if it fails to notify IdenTrust of any inaccuracies, errors, defects or other problems with the Code Signing Certificate within a reasonable time after downloading it. Subscriber agrees not to install or use the Code Signing Certificate until it has reviewed and verified the accuracy of the data in the Code Signing Certificate.

By accepting a Code Signing Certificate, Subscriber: (i) accept its contents and the responsibilities identified in this Agreement;(ii) represents, warrants and agrees that all information in the Code Signing Certificate that identifies Subscriber is accurate, current, complete; (iii) all representations made by and on behalf of Subscriber in connection with its applying for the Code Signing Certificate and during any contact with IdenTrust as provided for under Section 5.2 above, are true and not misleading; (iv) that Subscriber is not aware of any fact material to the reliability of the information in the Code Signing Certificate that has not been previously communicated to IdenTrust; and (v) the Individual retrieving the Code Signing Certificate was authorized to complete the registration and application for the Code Signing Certificate and provide information to IdenTrust during any contact with IdenTrust as provided for under Section 5.3 above.

**6. Term**. The term of this Agreement commences upon Subscriber's acceptance hereof. If the Application is not approved by IdenTrust, this Agreement will terminate upon such event. In the event a Code Signing Certificate is issued by IdenTrust hereunder, then (a) the term of this Agreement shall terminate when the Code Signing Certificate ceases to be valid, and **(b)** the Code Signing Certificate will be valid for the Validity Period specified in the Code Signing Certificate unless it ceases to be valid at an earlier time due to it being revoked as provided for herein. Subscriber hereby requests and authorizes IdenTrust to send e-mail messages to Subscriber relating to lifecycle events of Code Signing Certificates (e.g., revocation events, reminding Subscriber of the renewal process).

**7. Subscriber's Rights and Responsibilities.**

**7.1. Fee.** Subscriber will be responsible for the applicable certificate issuance fee for each Code Signing Certificate, and authorizes the billing as indicated during the process of the making of the Application. If the Application for a Code Signing Certificate is not approved by IdenTrust, payment of the relevant fee will be refunded where payment has actually been received by IdenTrust or not collected where payment information was provided to IdenTrust but not yet fully processed by IdenTrust. If the certificate issuance fee for a given Code Signing Certificate is not paid, IdenTrust may revoke the Code Signing Certificate without any liability to any person or entity. Once a Code Signing Certificate is issued by IdenTrust, refunds are not provided in relation to the Code Signing Certificate.

**7.2. Use of the Code Signing Certificate.** Subscriber will limit Subscriber's use of the Code Signing Certificate to the following uses: (i) use to verify the identity of the Subscriber; and (ii) use to verify the integrity of Subscriber's computer Code.

Code Signing Certificates may not be used: (i) for any application requiring fail-safe performance, such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system whose failure could lead to injury, death or environmental damage; (ii) for transactions where applicable law prohibits its use or where otherwise prohibited by law; (iii) for fraud or any other illegal scheme or unauthorized purpose; (iv) to present, send or otherwise transfer hostile code, including spyware or other malicious software; (v) in any software or hardware architectures that provide facilities for interfering with encrypted communications; (vi) to issue any other Certificate; (vii) to identify a particular software object; (xi) to make any determination that any computer code is free of vulnerabilities, malware, bugs, or other problems; (xii) to make any determination that it is "safe" to install code distributed by the CertSubject named in the Code Signing Certificate; or (xiii) to make any determination that the CertSubject named in the Code Signing Certificate is (a) actively engaged in business, (b) complies with applicable laws, (c) is trustworthy, honest, or reputable in its business dealings.

**7.3. Protect Private Key.** Subscriber is responsible for protecting its Private Key(s). Subscriber represents, warrants and agrees that, in regard to each Code Signing Certificate, Subscriber: (i) has kept and will keep its corresponding Private Key (and any associated Activation Data) private, (ii) will take reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, its corresponding Private Key (and associated Activation Data), as well as any computer system, device, or media on which its corresponding Private Key (or associated Activation Data) is stored, (iii) Subscriber has generated, maintained storage of, and used its private key in either IdenTrust provided key storage mechanism related to the Code Signing Certificate or in Subscriber acquired crypto module that meets or exceeds the requirements of FIPS 140-2 level 2, and (iv) Subscriber will confirm the operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 2 or Common Criteria EAL 4+ and communicate audit compliance via a completed TrustID Code Signing HSM IT Audit Form included in the Appendix A of this Subscriber Agreement and also posted for reference on the IdenTrust TrustID Repository.

Subscriber may change its employee(s) or agent(s) who are authorized to use and administer on behalf of Subscriber Code Signing Certificates, without requesting revocation of current Code Signing Certificates, but Subscriber shall bear the security and control risks associated with making such changes without revoking any Code Signing Certificates. In the alternative, Subscriber may request revocation of current Code Signing Certificates and apply for new Code Signing Certificates, subject to the fees and other requirements associated with the issuance of new Code Signing Certificates. Subscriber agrees that the act or omission of any employee or agent of Subscriber who has access to use any given Code Signing Certificate or the corresponding Private Key, in using or administering the Code Signing Certificate or such Private Key, will be deemed for all purposes to be the act or omission of Subscriber.

Failure to protect the Private Key or to notify IdenTrust of the theft, compromise, or misuse of the Private Key may cause Subscriber serious adverse legal and financial consequences.

**7.4. Responsiveness to Instructions.** Subscriber shall respond to IdenTrust within twelve (12) hours if IdenTrust provides notice to Subscriber containing instructions regarding any actual or possible compromise of any Private Key corresponding to a Code Signing Certificate or misuse of a Code Signing Certificate.

**7.5. Revoking the Code Signing Certificate -- When.** Subscriber must immediately request that a Code Signing Certificate be revoked if: (i) the Subscriber's corresponding Private Key has actually been, or is suspected of being, lost, disclosed, compromised, or subjected to unauthorized use in any way: or (ii) any information in the Code Signing Certificate is no longer accurate, current, or complete or becomes misleading. Subscriber may also revoke any Code Signing Certificate at any time for any other reason.

**7.6. Revoking the Code Signing Certificate -- How.** Subscriber can initiate a revocation request for a given Code Signing Certificate by:

**(i)** sending an e-mail to Support@IdenTrust.com which email contains the reason for revocation and is signed using the Private Key corresponding to such Code Signing Certificate;

**(ii)** calling IdenTrust Support at 1-888-248-4447, 1-801-384-3477 (International);

**(iii)** online-request via IdenTrust's online certificate management interface systems, if such systems are made available to Subscriber and Subscriber has signed up for access to such IdenTrust online systems, which such availability and access, if any, are outside the scope of this agreement; or

**(iv)** such other means as may be provided by IdenTrust.

**7.7. Cease Using a Code Signing Certificate.** Subscriber must immediately cease using a Code Signing Certificate in the following circumstances: (i) the Private Key corresponding to the Public Key listed in the Code Signing Certificate has actually or is suspected of being lost, disclosed, compromised, or subjected to unauthorized use in any way; (ii) when any information in the Code Signing Certificate is no longer accurate, current, or complete or becomes misleading; (iii) upon the revocation or expiration of the Code Signing Certificate; or (iv) upon termination of this Agreement.

**7.8. Indemnification.** Subscriber agrees to indemnify and hold IdenTrust and its directors, officers, employees, agents and affiliates harmless from any and all liabilities, costs, and expenses, including reasonable attorneys' fees, related to: (i) any misrepresentation or omission of material fact by Subscriber or its employees or agents to IdenTrust, whether or not such misrepresentation or omission was intentional; (ii) Subscriber's violation of this Agreement; (iii) any compromise or unauthorized use of one or more Code Signing Certificates (or the applicable corresponding Private Key(s)) caused by Subscriber's negligence, intentional misconduct, or breach of this Agreement, unless prior to such unauthorized use Subscriber has appropriately requested revocation of the applicable Code Signing Certificate(s) and proven Subscriber's authority and identity to IdenTrust as part of such request; or (iv) Subscriber's misuse of any Code Signing Certificate(s), including without limitation any use of any Code Signing Certificate(s) that is not permitted by this Agreement.

**8. IdenTrust's Rights and Responsibilities.**

**8.1. Privacy.** With respect to Private Information provided by Subscriber to IdenTrust in connection with this Agreement, IdenTrust will care for and process such information in accordance with the Privacy Policy.

Subscriber acknowledges that information contained in Code Signing Certificates and related status information shall not be considered or deemed Private Information – that would defeat the purpose of each Code Signing Certificate, which purpose consists of those uses provided for in Section 7.2 hereof. Subscriber authorizes the use of such information in furtherance of the purposes of this Agreement and in conformity with the requirements of the CP and CPS.

**8.2. Certificate Repository.** During the term of this Agreement, IdenTrust will operate and maintain a secure online repository that contains (i) all current, valid Code Signing Certificates (including, as applicable, Code Signing Certificates), and (ii) a CRL or online database indicating the status, whether valid, suspended or revoked, of Code Signing Certificates. When Subscriber accepts any Code Signing Certificate hereunder, IdenTrust will publish that Code Signing Certificate in the repository and will indicate its valid status until it is suspended, revoked, or expired.

**8.3. Suspension and Revocation.** IdenTrust may suspend one or more Code Signing Certificates when any party makes a claim to or against IdenTrust that indicates that a Code Signing Certificates is invalid or has been compromised. IdenTrust will promptly investigate any such claim. If IdenTrust suspends any Code Signing Certificate, then with respect to each such Code Signing Certificate separately and as IdenTrust reasonably deems appropriate, IdenTrust will revoke the Code Signing Certificate or the Code Signing Certificates to valid status.

With respect to each Code Signing Certificate separately, IdenTrust will revoke the Code Signing Certificate upon request of Subscriber and update the Repository as soon as practical after IdenTrust has adequately confirmed that the Individual making the revocation request is authorized to do so on behalf of Subscriber. If such request is signed using the Private Key corresponding to the Code Signing Certificate, IdenTrust will accept the request as valid.

With respect to each Code Signing Certificate separately, IdenTrust may revoke the Code Signing Certificate without advance notice if IdenTrust, in its sole discretion, determines that: (i) the Code Signing Certificate was not properly issued or was obtained by fraud; (ii) the security of the Private Key corresponding to the Code Signing Certificate has or may have been lost or otherwise compromised; (iii) the Code Signing Certificate has become unreliable; (iv) material information in the Application or the Code Signing Certificate has changed or has become false or misleading; (v) Subscriber has violated any applicable agreement or obligation; (vi) Subscriber requests revocation; (vii) a governmental authority has lawfully ordered IdenTrust to revoke the Code Signing Certificate; (viii) this Agreement terminates; or (ix) there are other reasonable grounds for revocation, including any violation of a provision of the CP or CPS by Subscriber. With respect to any Code Signing Certificate revoked as provided in the immediately preceding sentence, IdenTrust will notify Subscriber when the Code Signing Certificate has been revoked.

**8.4. Warranties.** With respect to each Code Signing Certificate separately and subject to the provisions CP, CPS and this Agreement, and Subscriber's fulfillment of its duties and obligations under the same, IdenTrust warrants: (i) that the Code Signing Certificate shall be issued and managed in accordance with the applicable terms of the CP, CPS and this Agreement; and (ii) that the Code Signing Certificate meets all requirements of the CP, CPS and this Agreement.

**8.5. Disclaimer of Warranties and Limitations of Liability.** EXCEPT AS PROVIDED IN SECTION 8.4 ABOVE, EVERY CODE SIGNING CERTIFICATE IS PROVIDED BY IDENTRUST "AS-IS" AND IDENTRUST DISCLAIMS ANY AND ALL WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, CORRECTNESS OR ACCURACY OF INFORMATION PROVIDED, OR FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO EVERY CODE SIGNING CERTIFICATE AND ANY IDENTRUST SERVICE. IDENTRUST MAKES NO WARRANTY THAT ANY CODE SIGNING CERTIFICATE OR ANY IDENTRUST SERVICE WILL MEET ANY EXPECTATIONS, OR THAT ANY FUNCTION OR AVAILABILITY THEREOF WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE, OR THAT DEFECTS WILL BE CORRECTED. IDENTRUST MAKES NO WARRANTY REGARDING ANY COMPUTER CODE SIGNED WITH THE CODE SIGNING CERTIFICATE.

IDENTRUST WILL NOT BE LIABLE TO CUSTOMER UNDER ANY CIRCUMSTANCES WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES OF ANY KIND (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUE OR GOODWILL OR ANTICIPATED PROFITS OR LOST BUSINESS), REGARDLESS OF WHETHER IDENTRUST KNEW OR HAD REASON TO KNOW OF THE POSSIBILITY THEREOF.

IN NO EVENT SHALL IDENTRUST'S TOTAL AGGREGATE LIABILITY ARISING FROM OR RELATED TO THIS AGREEMENT EXCEED AN AMOUNT EQUAL TO THE AMOUNT CUSTOMER ACTUALLY PAID IDENTRUST FOR THEOV CODE SIGNING CERTIFICATE FOR WHICH SUBSCRIBER APPLIED FOR IN CONNECTION WITH THIS AGREEMENT. NOTWITHSTANDING THE FOREGOING SENTENCE AND WITH RESPECT TO EACH CODE SIGNING CERTIFICATE SEPARATELY, IN THE EVENT THE CODE SIGNING CERTIFICATE IS A "CERTIFICATE" AS PROVIDED FOR UNDER THE CP AND CPS, THEN IN NO EVENT SHALL IDENTRUST'S TOTAL AGGREGATE LIABILITY ARISING FROM OR RELATED TO THIS AGREEMENT AS IT APPLIES AND RELATES TO THE CODE SIGNING CERTIFICATE EXCEED AN AMOUNT EQUAL TO $2,000 UNITED STATES DOLLARS.

THE PARTIES AGREE THAT THE FOREGOING LIMITATION OF WARRANTIES AND LIABILITY ARE AN ESSENTIAL INDUCEMENT TO IDENTRUST TO ENTER INTO THIS AGREEMENT, AND THAT THE FOREGOING LIMITATIONS SHALL APPLY TO THE GREATEST EXTENT PERMITTED BY LAW.

**9. Governing Law.** The parties hereto agree that the United Nations Convention on Contracts for the International Sale of Goods will not apply to this Agreement. This Agreement shall be governed by and construed under the laws of the State of Utah, without regard to its conflicts of law principles.

**10. Force Majeure.** If IdenTrust's performance of any obligation under this Agreement is prevented or delayed by an event beyond such IdenTrust's reasonable control, including without limitation, crime, fire, flood, war, terrorism, riot, acts of civil or military authority (including governmental priorities), severe weather, strikes or labor disputes, or by disruption of telecommunications, power or Internet services not caused by such IdenTrust, then IdenTrust will be excused from such performance to the extent it is necessarily prevented or delayed thereby.

**11. Assignment.** Subscriber may not assign this Agreement or delegate any obligations hereunder. Any attempt by Subscriber to assign this Agreement or delegate any obligations hereunder shall render this Agreement voidable by IdenTrust, in its sole discretion. IdenTrust may assign this Agreement or delegate all or part of its obligations hereunder upon: (i) notice to Subscriber; or (ii) assignment of all rights and obligations hereunder to a successor in interest, whether by merger, sale of assets or otherwise.

**12. Notice.** Notice from Subscriber to IdenTrust shall be effective upon actual receipt by IdenTrust and shall be made by either internationally recognized overnight courier service or by certified mail addressed to:

IdenTrust Services, LLC
Attn: Legal Department
5225 W. Wiley Post Way, Ste 450
Salt Lake City, UT 84116-2898

Notices from IdenTrust to Subscriber shall be made by posting on the Repository, or by mail or email in the event IdenTrust receives an email or mailing address for Subscriber in the course of communications made in connection with this Agreement. Except as otherwise provided herein, notices to Subscriber posted on the Repository shall be deemed effective three (3) days after being so posted, notices to Subscriber sent by mail shall be deemed effective seven (7) days after being sent, and notices to Subscriber sent by email shall be deemed effective when sent.

**13. Dispute Resolution.** In the event of any dispute or disagreement between the parties hereto ("Disputing Parties") arising out of or related to this Agreement or any Code Signing Certificate, the Disputing Parties will use their best efforts to settle the dispute or disagreement through mediation or good faith negotiations following notice from one Disputing Party to the other. If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice, then the Disputing Parties will submit the dispute to binding arbitration, as provided below.

Except for a controversy, claim, or dispute involving the federal government of the United States or a "Core Proceeding" under the United States Bankruptcy Code, the parties agree to submit any controversy, claim, or dispute, whether in tort, contract, or otherwise arising out of or related in any way to this Agreement, that cannot be resolved by mediation or negotiations between the parties, for resolution by binding arbitration by a single arbitrator, and judgment upon the award rendered by the arbitrator may be entered in any court having jurisdiction over the parties. The arbitrator will have no authority to impose penalties or award punitive damages. Binding arbitration will: (i) proceed in Salt Lake County, Utah; (ii) be governed by the Federal Arbitration Act (Title 9 of the United States Code); and (iii) be conducted in accordance with the Commercial Arbitration rules of the American Arbitration Association ("AAA"). Each party will bear its costs for the arbitration; however, upon award of any judgment or conclusion of arbitration, the arbitrator will award the prevailing party the costs it expended in such arbitration. Unless the arbitrator otherwise directs, the parties, their representatives, other participants, and the arbitrator will hold the existence, content, and result of the arbitration in confidence. This arbitration requirement does not limit the right of any party to obtain provisional ancillary remedies such as injunctive relief or the appointment of a receiver, before, during, or after the pendency of any arbitration proceeding. This exclusion does not constitute a waiver of the right or obligation of any party to submit any dispute to arbitration.

**14. Relationship of the Parties.** Nothing in this Agreement shall be deemed to create a partnership or joint venture or fiduciary relationship, and neither party is the other's agent, partner, employee, or representative.

**15. Headings and Titles.** The headings and titles contained in this Agreement are included for convenience only and will not limit or otherwise affect the terms of this Agreement.

**16. Waiver.** No waiver by either party of any default will operate as a waiver of any other default, or of a similar default on a future occasion. No waiver of any term or condition by either party will be effective unless in writing and signed by the party against whom enforcement of such waiver is sought.

**17. Severability.** In case one or more of the provisions of this Agreement should be held invalid, illegal or unenforceable in any respect for any reason, the same will not affect any other provision in this Agreement, which will be construed to give maximum effect to the extent of the parties as evidenced by this original Agreement as originally drafted save to the extent of such invalid, illegal or unenforceable provision.

**18. Entire Agreement.** This Agreement, including the CP and CPS as referenced herein, represents the entire agreement of the parties, and supersedes all other agreements and discussions relating to the subject matter hereof. Except as expressly provided otherwise in this Agreement, this Agreement may not be amended except in writing signed by both parties.

**19. Third Party Beneficiaries.** Each Relying Party is an intended third party beneficiary of Subscriber's representations, warranties, and obligations made herein.

**20. Amendment.** You agree that this Agreement, the CP, and the CPS can be amended from time to time by IdenTrust, in its sole discretion. Any such modifications shall be effective immediately upon a revised version of the applicable document being posted by IdenTrust to the Repository. If Subscriber uses the Code Signing Certificate hereunder after such a posting, Subscriber shall be deemed to have accepted the most recent versions of the Agreement, the CP and the CPS posted on the Repository and be bound thereunder. You are responsible for periodically checking the Repository for the latest version of the Agreement, the CP, and the CPS posted on the Repository.

**21. Survival.** Sections governing confidentiality of information, indemnification, disclaimer of warranties, limitations of liability, governing law, and dispute resolution will survive any termination or expiration of this Agreement.

**22. Definitions and Terms.** Capitalized terms used in these Terms and Conditions have the meaning given below.

**Activation Data:** User IDs, pass-phrases or shared secrets used to safeguard the Private Key from unauthorized viewing or use.

**Agreement:** refers to these Terms and Conditions as incorporated into the (TRUSTID | CODE SIGNING | ORGANIZATION IDENTITY CERTIFICATE SUBSCRIBER AGREEMENT signed by the Contract Signer.

**Applicant:** An Individual or Organization that submits application information to an RA or an Issuing CA for the purpose of obtaining or renewing a TrustID Certificate.

**Application:** means the online application for a TrustID® Certificate made in connection with this Agreement, and, if any, each request for a Code Signing Certificate made by a Certificate Requestor.

**CAB Forum Document:** The current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" document. Such document is understood to be as (a) published by The CA/Browser Forum and available via the website located at "https://cabforum.org/working-groups/code-signing/" and (b) may amended from time to time by its publisher.

**Certificate:** A computer-based record or electronic message issued by an entity that: (i) identifies the entity issuing it; (ii) names or identifies a Certificate holder; (iii) contains the Public Key of the Certificate holder; (iv) identifies the Certificate's Validity Period; and (v) is digitally signed by the issuing entity. A Certificate includes not only its actual content but also all documents expressly referenced or incorporated in it.

**Certificate Requestor:** has the meaning provided such term in the CAB Forum Document and which is an Individual authorized by the Contract Signer as contemplated in the provisions of Section 4.3 relating to authorization of Certificate Requestors.

**CertSubject:** means the entity named in the "subject:organizationName" field of a given Certificate.

**Code Signing Certificate:** Refers to any TrustID Certificate issued to Subscriber pursuant to this Agreement, with the terms hereof being applicable to each such TrustID Certificate independently of any other such TrustID Certificate. Also, when "Code Signing Certificate" is used herein, such use is to be constructed to include an "if issued" condition.

**Contract Signer:** A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

**CP:** The most recent version of the TrustID® Certificate Policy posted on the Repository.

**CPS:** The most recent version of the TrustID® Certificate Practice Statement posted on the Repository.

**CRL:** A database or other list of Certificates that have been revoked prior to the expiration of their Validity Period.

**Digital Signature/Digitally Sign:** The transformation of an electronic record by one person, using a Private Key and Public Key Cryptography, so that another person having the transformed record and the corresponding Public Key can accurately determine (i) whether the transformation was created using the Private Key that corresponds to the Public Key, and (ii) whether the record has been altered since the transformation was made. It need not involve a handwritten signature.

**HSM:** A hardware security module storing certificate private keys meeting standard security equivalent to FIPS 140-2 level 2 or Common Criteria EAL 4+

**Identification and Authentication:** The process by which IdenTrust ascertains and confirms through appropriate inquiry and investigation the identity, authorizations, and qualifications of the Subscriber and Contract Signer, and, if applicable, Certificate Requestors. Certain aspects and activities within this process are prescribed by the CP and CPS.

**Individual:** A natural person.

**Issuing Certification Authority /Issuing CA:** An entity authorized by the PMA to issue and sign Certificates in accordance to the CP and CPS.

**Key Pair:** Two mathematically related keys (a Private Key and its corresponding Public Key), having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

**Policy Management Authority (PMA):** The Organization responsible for setting, implementing and administering policy decisions regarding the CP and CPS.

**Privacy Policy:** The policy posted at http://www.identrust.com/privacy.html, which policy may be amended from time to time by IdenTrust in its sole discretion.

**Private Information:** Non-public information that Subscriber provides or that IdenTrust obtains, during the application and Identification and Authentication processes, that is not included in the Code Signing Certificate and that identifies Subscriber.

**Private Key:** The key of a Key Pair kept secret by its holder and used to create Digital Signatures and to decrypt messages or files that were encrypted with the corresponding Public Key.

**Public Key:** The key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and used by the recipient to validate Digital Signatures created with the corresponding Private Key and to encrypt messages or files to be decrypted with the corresponding Private Key.

**Public Key Cryptography:** A type of cryptography (a process of creating and deciphering communications to keep them secure) that uses a Key Pair to securely encrypt and decrypt messages. One key encrypts a message, and the other key decrypts the message. One key is kept secret (Private Key), and one is made available to others (Public Key). These keys are,

in essence, large mathematically-related numbers that form a unique pair. Either key may be used to encrypt a message, but only the other corresponding key may be used to decrypt the message.

**Registration Authority (RA):** An entity contractually delegated by an Issuing CA to accept and process Certificate applications, and to verify the identity of potential End Entities and authenticate information contained in Certificate applications, in conformity with the provisions of the CP, CPS and related agreements.

**Relying Party:** Any person or entity that reasonably relies on the TrustID | Code Signing | Organization Identity Certificate during its Validity Period.

**Repository:** The information and data repository of IdenTrust located at https://www.identrust.com/support/documents/trustid, https://secure.identrust.com/certificates/policy/ts/, which may be amended from time to time by IdenTrust in its sole discretion.

**Subscriber:** The entity for which the Application is made (which entity is not the Contract Signer), and which is identified to IdenTrust in such Application, and which is identified within the “subject:organizationName” (as defined in the CAB Forum Document) field of the Code Signing Certificate that is the subject of this Agreement.

**TrustID Certificate:** A Certificate issued by IdenTrust under the TrustID brand.

**Validity Period:** The intended term of validity of a Code Signing Certificate, beginning with the date of issuance ("Valid From" or "Activation" date), and ending on the expiration date indicated in the Code Signing Certificate ("Valid To" or "Expiry" date).

# TrustID Code Signing Certificate HSM IT Audit Form

## *** For Subscriber Provided HSM Only ***

### Terms and Conditions

The undersigned warrants, represents, and attests that all facts and information provided in this form, to the best of the undersigned auditor's knowledge, accurate, current and complete and that he or she: a) Is authorized by the Organization identified in this form to conduct an audit for the HSM(s) used to generate, store, and use related to all TrustID Code Signing Certificates in use by the Organization; b) Has evaluated each TrustID Code Signing Certificate in use to validate that the corresponding private key was generated, stored and used in HSM that meets or exceeds FIPS 140-2 level 2; c) Has confirmed the operating environment of HSM(s) achieves a level of security at least equivalent to that of FIPS 140-2 level 2; d) Has requisite qualifications, credentials, and experience to conduct this audit; and e) agrees that this TrustID Code Signing HSM IT Audit Form is for exclusive reliance by IdenTrust Services, LLC ("IdenTrust"), a subsidiary of IdenTrust, Inc, and will not be quoted in whole or in part, used, published or otherwise referred to or relied upon in any manner, including, without limitation, in any financial statement or other document.

Organization Name: _____ ("Organization")

Organization Address: _____

Organization Phone: _____

Organization E-mail: _____

After reviewing the Organization's records, processes, procedures, security controls and based on my investigation, my professional opinion is that:

1. Organization stores its private keys associated with TrustID Code Signing Certificate securely in an HSM that prevents removal of the private key.
2. The private key(s) associated with TrustID Code Signing Certificate has not been used outside of the HSM.
3. In addition to technical controls, there exists procedurals and/or security controls that prevents use of private key(s) associated with TrustID Code Signing Certificate outside of HSM.

The information on this form should be verified and signed by someone responsible for security within your organization, such as a director, officer or other member of management.

Signature _____

Name _____ ("auditor")

Organization Name _____

Title _____

Phone: _____

E-mail: _____

Date: _____

# Code Signing Certificate

## IdenTrust Attestation Letter for Organization Authorization



Dear Professional,

You have been asked by your client ("Organization") to provide a legal attestation to aid them in obtaining an IdenTrust Code Signing digital certificate ("Certificate"). All issuing Certification Authorities (CAs) must comply with certain vetting processes to ensure a uniform standard for certificate issuance. As a CA, IdenTrust must follow the guidelines as detailed in the current version of the industry standard CA/Browser Forum Code Signing Certificate guidelines located at: https://cabforum.org/working-groups/code-signing/.

Accordingly, certain information must be verified by you, as a professional representing the Organization. Once the attached attestation letter is submitted, IdenTrust may contact the legal/accounting board/association that issued your license to verify your professional standing. Using the contact information in the attestation letter, IdenTrust may also contact you to confirm the accuracy of the attestation.

Wet signature or signature via digital certificate issued to you to sign electronically are both acceptable. Should you have any questions, please contact IdenTrust by emailing: Processing@IdenTrust.com.

**Instructions for Completion of Attestation Letter**

This attestation letter may be completed by either:

(a) The Organization's legal counsel (or an in-house legal counsel employed by the Organization), who must be properly registered with the appropriate authorizing agency in the location of the Organization's Jurisdiction of Incorporation or any jurisdiction where the Organization maintains an office or physical facility.

(b) An independent professional accountant retained by and representing the Organization (or an in-house professional accountant employed by the Organization), who is a certified public accountant, chartered accountant, or equivalent licensed by a full member of the International Federation of Accountants (IFAC) to practice accounting in the location of the Organization's Jurisdiction of Incorporation or any jurisdiction where the Organization maintains an office or physical facility.

If you are unable to attest to any fact below, you may indicate so by striking a line through the relevant section.

As used in the Attestation Letter, "Demand Deposit Account" shall mean a deposit account held at a bank or other financial institution; the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, or a current account.

**PLEASE COMPLETE AND EXECUTE PROFESSIONAL ATTESTATION LETTER ON THE FOLLOWING PAGE**

IdenTrust, Inc. Attn: Registration Department

5225 Wiley Post Way, Ste
450 Salt Lake City, UT
84116-2898
VIA COURIER MAIL OR VIA EMAIL TO: processing@identrust.com

**IdenTrust Attestation Letter for Organization Authorization**

Re: Code Signing Certificate Application to IdenTrust Certificate Authority

Organization: _____[Enter exact Organization name[1]] ("The Organization")

Organizational Representative: _____[Enter exact name of Organizational Representative who signed the application submitted to IdenTrust[2]]

Application Date: _____ [Insert date of Organization's Code Signing Certificate Application]

I represent that the above Organization, that submitted the Application to IdenTrust Certificate Authority as of the Application Date shown above ("Application"). I have been asked by the Organization to present you with my attestation as stated in this letter. My attestation below is based on my familiarity with the relevant facts and the exercise of my professional judgment and expertise.

On this basis, I hereby offer the following attestation:

1. Organizational Representative is employed by the Organizations _____[Enter job title] and has the necessary authority to act on behalf of the Organization to: (a) provide the information about the Organization required for issuance of Code Signing Certificates, (b) request one or more Code Signing Certificates and to designate other persons to request Code Signing Certificates, (c) agree to the relevant contractual obligations on behalf of Organization.

2. The Organization has a physical presence and its principal place of business at the following location: Address: _____

_____

_____

3. The Organization can be contacted at its stated place of business at the following telephone number: Telephone Number: _____

4. That the Organization has the right to use the following Domain Name(s) in identifying itself on the Internet:

_____.

5. The Organization has an active current Demand Deposit Account with a regulated financial institution. [Optional: Insert customary limitations and disclaimers for attestation letters in your jurisdiction.]

Name: _____License Number: _____

Email Address: _____

Signature: _____Date: _____

Professional Capacity (check one): ☐ Lawyer ☐ Accountant

Contact information for the authorizing agency where IdenTrust may verify your authority to practice (e.g., a bar association or a board of accountancy):

_____

_____

cc: Organization

[1] The Organization listed in the Attestation Letter must be the exact corporate name, as registered with the relevant Incorporating Agency in the Organization's Jurisdiction of Incorporation. This is the name that will be included in the Code Signing Certificate. Please attach copy of supporting documents to establish the Organization's active legal existence such Certificate of Formation, Articles of Formation or Organization, Company formation documents.

[2] If necessary, to establish the Organizational Representative's actual authority, you may rely on a Power of Attorney from an officer of the Organization who has authority to delegate the authority to the Organizational Representative.