

TrustID<sup>®</sup>  
Medium Assurance | Business Identity  
Certificate  
Forms Packet



Copyright © 2022 IdenTrust Services, LLC. All rights reserved.

## Instructions for the Applicant

Thank you for choosing IdenTrust Services, LLC (“IdenTrust”), a subsidiary of IdenTrust, Inc., to issue you a TrustID® | Business Identity certificate. TrustID | Business Identity certificates are issued to individuals such as employees, officers, and agents authorized to act on behalf of business entities that have been validated by IdenTrust.

Enrollment for a TrustID | Business Identity certificate requires that you complete an online application as well as complete and return the following forms:

1. Part 1 – Sponsoring Organization Authorization Form
2. Part 2 – Notary Form – U.S. Applicants, or Notary Form – Non-U.S. Applicants

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

### The Online Application

Please apply for the TrustID | Business Identity certificate: <https://www.identrust.com/certificates/publicly-trusted>

**Apply with your legal first and last name, full organization name and headquarters’ address, and a valid email address.**

### Part 1 Form

Fill out all of the fields on the form, then take the Part 1 form to an officer in your Organization who can sign on behalf of the Organization, representing to IdenTrust that you are an authorized representative of the Organization. Once the form has been signed, request the Organization officer return the Part 1 to you.

### Part 2 Form

Take the Part 2 form to a licensed notary to verify your identity credentials. You must present 2 forms of valid ID for verification, of which one must be a verifiable government-issued photo ID.

#### Acceptable government-issued Photo ID Must be valid, not expired

- Passport
- Drivers’ license
- State or government-issued ID card
- Federal employee ID card
- Military photo ID
- Certificate of citizenship with photo
- Concealed weapons permit

#### Other acceptable forms of ID

- Original or certificated birth certificate
- Social security card
- Student ID from a state/government college or university
- Government-issued pilots’ license
- CAC card
- Other pre-approved ID

**IdenTrust offers Remote Identity Proofing services.** Contact our Support team at (888) 339-8904 for details

### Complete the Registration Process

Choose one of the following:

- **Send the original, ‘wet-signature’ (pen to paper) Part 1 and Part 2 forms to IdenTrust for processing.** It is advised you select a traceable ship 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 Part 1 and Part 2 forms to IdenTrust via email.** Signatures on the forms must be handwritten and may not be a stamp or electronic signature. The signature of the Notary or Trusted Agent may be either a handwritten signature or a digital signature that can be traced to a certificate root. Electronic signatures are not accepted.

Email to [Processing@IdenTrust.com](mailto:Processing@IdenTrust.com)

This email inbox is monitored for forms packets only.

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

**Part 1 – Sponsoring Organization Authorization Form**

This TrustID | Business Identity Certificate Authorization Agreement (this "Authorization Agreement") is made by and between IdenTrust Services, LLC, ("IdenTrust") a Delaware limited liability company with its principal place of business at 5225 Wiley Post Way, Suite 450, Salt Lake City, UT 84116-2898 U.S.A (www.IdenTrust.com), and the Organization identified at the bottom of this Authorization Agreement ("Sponsoring Organization").

**1. Effect of TrustID | Business Identity Certificate Issuance**

IdenTrust is a Certification Authority that issues digital certificates to employees, agents and other individuals (e.g., licensed professionals) affiliated with Sponsoring Organization ("Affiliated Individuals"). Each TrustID | Business Identity Certificate identifies its named holder (i.e., its "Subject") as employed, associated or otherwise affiliated with the Organization. However, TrustID | Business Identity Certificates establish identity, not authority, and do not establish authority to bind the Organization—such authority would be established by other means between the parties relying on the digital certificate and Sponsoring Organization. Sponsoring Organization authorizes IdenTrust to issue a TrustID | Business Identity Certificate to the Affiliated Individual listed below. Prior to issuing a TrustID | Business Identity Certificate that identifies a person as affiliated with Sponsoring Organization, IdenTrust must confirm that the person is indeed affiliated with the Sponsoring Organization, and Sponsoring Organization agrees that the information it provides to IdenTrust concerning an Affiliated Individual's status with the Sponsoring Organization will be accurate, current and complete. Sponsoring Organization agrees to be bound by and accepts the terms and conditions of the attached TrustID | Business Identity Certificate Agreement that is presented to the Affiliated Individual on IdenTrust's web site during the application process. Sponsoring Organization further acknowledges and agrees that the act or omission of the Affiliated Individual with respect to a TrustID | Business Identity Certificate authorized hereunder will be deemed for all purposes to be the act or omission of Sponsoring Organization.

**2. Certificate Renewal**

Sponsoring Organization understands and acknowledges that the TrustID | Business Identity Certificate issued to the Affiliated Individual identified below will expire after its stated period of validity, and that prior to expiration the Affiliated Individual may apply for and receive a renewal TrustID | Business Identity Certificate to replace his or her expiring certificate. Sponsoring Organization hereby authorizes the Affiliated Individual to apply for and receive, and authorizes IdenTrust to issue, successive renewal TrustID | Business Identity Certificates, provided that the Affiliated Individual applies for the renewal TrustID | Business Identity Certificate within the required time frames for such renewal. Sponsoring Organization acknowledges and agrees that IdenTrust may require the Affiliated Individual to execute a new Certificate Agreement each time he or she applies for a renewal Certificate, and the Sponsoring Organization will be bound by the terms of each such Certificate Agreement.

**3. Certificate Revocation**

Sponsoring Organization must immediately request that the Certificate be revoked if: (i) it ever discovers or suspects that the Private Key corresponding to the Certificate has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way, or (ii) any information in the Certificate is no longer accurate, current, or complete or becomes misleading, including if the Affiliated Individual is no longer affiliated with Sponsoring Organization.

**4. Term and Termination**

The terms of this Authorization Agreement shall run from the date indicated below until all TrustID | Business Identity Certificate issued to the Affiliated Individual, and all subsequent renewal Certificates, have been revoked, have expired or are no longer valid. If Sponsoring Organization desires to terminate this Authorization Agreement and all corresponding Certificate Agreements, then it must give notice to IdenTrust, in which case IdenTrust shall revoke all outstanding TrustID Business Certificates authorized hereunder.

**5. Interpretation**

Irrespective of the place of performance, this Authorization Agreement shall be construed, interpreted, and enforced in accordance with the substantive laws of the State of Utah, without regard to its conflicts of law principles. Capitalized terms used but not defined here in shall have the meanings indicated in the TrustID | Business Identity Certificate Agreement. If any provision hereof is found invalid, illegal or unenforceable, then the remaining provisions shall be construed to give maximum effect to the intent of the parties as evidenced by this Agreement.

\_\_\_\_\_  
Print Applicant's legal first and last name

\_\_\_\_\_  
Applicant's email

\_\_\_\_\_  
Print Organization name

\_\_\_\_\_  
Authorized signer's signature

\_\_\_\_\_  
Address line 1

\_\_\_\_\_  
Authorized signer's first and last name

\_\_\_\_\_  
Address line 2

\_\_\_\_\_  
Authorized signer's title

\_\_\_\_\_  
City, State/Province, Country, Postal Code

\_\_\_\_\_  
Date authorized signer signed

## Part 2 - Notary Form – U.S. Applicants

### Terms and Conditions

The undersigned applicant warrants, represents, and attests that all facts and information provided in Parts 1 and 2 are, to the best of the undersigned applicant's knowledge, accurate, current and complete and that he or she: a) Is authorized by his or her Organization to receive and use an TrustID | Business Identity certificate to be issued by IdenTrust; b) Has read and accepts the personal identifying information set forth herein; c) Is who he or she represents himself or herself to be; and d) Has read, understood, and agrees to the responsibilities associated with being a Subscriber of an TrustID | Business Identity Certificate, including the terms and conditions found in the on-line TrustID | Business Identity Certificate Agreement. The applicant agrees to: 1) accurately represent him or herself in all communications with IdenTrust and Relying Parties; 2) protect his or her private key at all times; 3) immediately notify IdenTrust if he or she suspects his or her private key to have been compromised, stolen or lost; and 4) use his or her key only for authorized business as allowed by the TrustID Program.

Signed By: \_\_\_\_\_ (Subscriber to sign only in the presence of notary)

Print Legal Name: \_\_\_\_\_ Email Address: \_\_\_\_\_  
First Name MI Last Name (Must match email address provided online)

**Identification – Present two (2) forms of verifiable ID, one of which must be a valid government-issued photo ID**

#### PHOTO ID

#### 2<sup>nd</sup> ID

Doc. Type/Title: \_\_\_\_\_

Doc. Type/Title: \_\_\_\_\_

Doc. Issuer: \_\_\_\_\_

Doc. Issuer: \_\_\_\_\_

Serial/Unique #: \_\_\_\_\_

Serial/Unique #: \_\_\_\_\_

Full Name: \_\_\_\_\_

Full Name: \_\_\_\_\_

Issue Date: \_\_\_\_\_

Issue Date: \_\_\_\_\_

Expire Date: \_\_\_\_\_

Expire Date: \_\_\_\_\_

**\*Note:** If the name on your Photo ID is different from the name on your Second ID, please send a copy of the document showing the name change (E.g., A copy of your marriage license or certificate of marriage, official seal must be visible on document).

I \_\_\_\_\_ (name of notary/officer), registered in the state of \_\_\_\_\_, county of \_\_\_\_\_ do hereby certify under PENALTY OF PERJURY under the laws of the State of \_\_\_\_\_ that the following information is true and correct:

1. On \_\_\_\_\_ (MM/DD/YY), before me personally appeared \_\_\_\_\_ (name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

2. I have seen and verified the forms of identification for which information is written above and hereby assert that said forms of ID do not appear to be altered, forged or modified in any way.

WITNESS my hand and official seal

(Seal)

Signature \_\_\_\_\_

## Part 2 - Notary Form – Non-U.S. Applicants

### Terms and Conditions

The undersigned applicant warrants, represents, and attests that all facts and information provided in Parts 1 and 2 are, to the best of the undersigned applicant's knowledge, accurate, current and complete and that he or she: a) Is authorized by his or her Organization to receive and use an TrustID | Business Identity certificate to be issued by IdenTrust; b) Has read and accepts the personal identifying information set forth herein; c) Is who he or she represents himself or herself to be; and d) Has read, understood, and agrees to the responsibilities associated with being a Subscriber of an TrustID | Business Identity Certificate, including the terms and conditions found in the on-line TrustID | Business Identity Certificate Agreement. The applicant agrees to: 1) accurately represent him or herself in all communications with IdenTrust and Relying Parties; 2) protect his or her private key at all times; 3) immediately notify IdenTrust if he or she suspects his or her private key to have been compromised, stolen or lost; and 4) use his or her key only for authorized business as allowed by the TrustID Program.

Signed By: \_\_\_\_\_ (Subscriber to sign only in the presence of notary)

Print Legal Name: \_\_\_\_\_ Email Address: \_\_\_\_\_  
First Name MI Last Name (Must match email address provided online)

**Identification – Present two (2) forms of verifiable ID, one of which must be a valid government-issued photo ID**

PHOTO ID	2 <sup>nd</sup> ID
Doc. Type/Title: _____	Doc. Type/Title: _____
Doc. Issuer: _____	Doc. Issuer: _____
Serial/Unique #: _____	Serial/Unique #: _____
Full Name: _____	Full Name: _____
Issue Date: _____	Issue Date: _____
Expire Date: _____	Expire Date: _____

**\*Note:** If the name on your Photo ID is different from the name on your Second ID, please send a copy of the document showing the name change (E.g., A copy of your marriage license or certificate of marriage, official seal must be visible on document).

### Notarial Acknowledgement

1. On \_\_\_\_\_ (DD/MM/YY), before me personally appeared \_\_\_\_\_ (name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

2. I have seen and verified the forms of identification for which information is written above and hereby assert that said forms of ID do not appear to be altered, forged or modified in any way.

WITNESS my hand and official seal

<b>Notary Public Name:</b>	
<b>Notary Public Signature:</b>	
<b>Office Street Address</b>	
<b>Residing in: (City, Country)</b>	
<b>My Commission Expires on: (DD/MM/YY), if applicable</b>	

Space Reserved for Notary Seal  
Use back page if needed

## TrustID® | Business Identity Certificate Agreement

**1. Scope.** This Agreement governs your rights, duties and liabilities as the Holder of a TrustID® | Business Identity Certificate ("Your Certificate") issued to You by IdenTrust Services LLC ("IdenTrust"), using terms as defined below in Section 12.

### 2. TrustID Business Certificate Issuance

**2.1 Application.** The contents of Your Certificate will be based on the information You entered on the previous screens as part of your completed application. By entering into this Agreement, You represent and warrant that: (i) all of the information You submit in your application form - including but not limited to Your Organization's name - is accurate, current, complete, and not misleading; (ii) You have provided all facts material to confirming your identity and to establishing the reliability of Your Certificate; and (iii) Your Organization has authorized You to apply for, obtain and use a TrustID | Business Identity Certificate that identifies Your Organization and the fact of your affiliation with Your Organization. You also agree to inform Your Organization that You have applied for a TrustID | Business Identity Certificate and bound Your Organization to this Agreement. If You are uncertain whether the information You provided is accurate, You should now click "BACK" and correct it. You agree to provide such further information as IdenTrust may reasonably require in connection with your application and the Identification and Authentication process.

**2.2 Key Pair Generation.** Your Key Pair (Public and Private Keys) will be generated by You, and the corresponding Public Key will be submitted to IdenTrust, incorporated into Your Certificate, and stored by IdenTrust in its Certificate Repository. IN NO EVENT WILL IDENTRUST EVER HAVE ACCESS TO YOUR PRIVATE KEY.

**2.3 Verification of Identity and Authorization.** As part of application process, IdenTrust will provide You with a form entitled "TrustID | Business Identity Certificate Authorization Agreement" that Your Organization must sign (the "Authorization Agreement"). Follow the instructions accompanying the Authorization Agreement and send it to IdenTrust. You and Your Organization authorize IdenTrust to verify your and Your Organization's identity and relationship. IdenTrust may consult public or private databases or other sources for the purpose of verifying submitted information. IdenTrust will not request a credit report without your express written prior consent. In no way shall this Agreement be construed as any express consent from you to obtain a credit report. If, based on the information available, IdenTrust is unable to identify and authenticate You and your certificate request to its satisfaction, IdenTrust may refuse to issue You a certificate or seek your permission to obtain additional information. You and Your Organization also authorize IdenTrust to store and use in accordance with this Agreement any information generated during the application, identification, and certificate issuance processes. At all times, IdenTrust agrees to protect your personal privacy in accordance with Section 4.1 below

**2.4 Issuance.** If IdenTrust accepts your application and confirms the information submitted during the application process, IdenTrust will create Your Certificate and notify You how and where to retrieve Your Certificate. If IdenTrust is unable to confirm your identity or authorization, IdenTrust may refuse to approve your application or refuse to issue You a TrustID | Business Identity Certificate without incurring liability for any loss You or Your Organization may incur as a result.

**2.5 Acceptance.** When You enter the activation code, as provided to You by IdenTrust, in order to download Your Certificate, You will once again be presented with the Certificate's proposed contents. You agree to review the proposed contents of Your Certificate, and immediately notify IdenTrust of any errors, defects or problems with Your Certificate. You agree that You will have accepted Your Certificate: (i) when You use Your Certificate or the corresponding Private Key after downloading Your Certificate, or (ii) if You fail to notify IdenTrust of any errors, defects or problems with Your Certificate within a reasonable time after downloading it.

By accepting Your Certificate, You (i) accept its contents and the responsibilities identified in this Agreement, and (ii) represent, warrant and agree that all information in Your Certificate that identifies You or Your Organization is accurate, current, complete and not misleading, and that You and Your Organization are not aware of any fact material to the reliability of the information in Your Certificate that has not been previously communicated to IdenTrust.

### 2.6 Addition Provision for Types of Certificates that include Hardware.

If the TrustID | Business Identity Certificate is purchased with an IdenTrust approved Hardcryptomodule, Customer will be sent a Hardcryptomodule by IdenTrust along with instructions regarding how to activate such Hardcryptomodule.

If Customer is sent a Hardcryptomodule and if a TrustID | Business Identity Certificate is issued to Customer, then in connection with the download process that is part of such issuance (see Section 2.3), Customer will be required to activate the Hardcryptomodule as required by IdenTrust in connection with the download process provided for in Section 2.5. In the event that Customer does not so activate a Hardcryptomodule when required to do so pursuant to the foregoing provisions set forth in the immediately preceding sentence, it is understood that IdenTrust will revoke the TrustID | Business Identity Certificate.

ANY HARDCRYPTOMODULE PROVIDED BY IDENTRUST UNDER THIS AGREEMENT IS PROVIDED SUBJECT TO THE PROVISIONS OF SECTION 4.4. Without derogating from or forming a limitation or exception on the provisions of Section 4.4: (i) with respect to any Hardcryptomodule sent by IdenTrust under this Agreement, Customer shall rely only on such representations and warranties as may be provided by the applicable original equipment manufacturer(s); (ii) IdenTrust will use commercially reasonable efforts to facilitate return of any defective Hardcryptomodule to the original equipment manufacturer(s) provided that all risks of such returns are borne solely by the Customer.

**2.7 Term.** Once issued, Your Certificate will be valid for the Validity Period specified therein. This Agreement will be coterminous with Your Certificate and will, therefore, terminate on the specified date. At the expiration of Your Certificate, You may renew Your Certificate in accordance with IdenTrust's renewal procedures, unless (a) Your Certificate has been revoked or (b) You or Your Organization have notified IdenTrust to cancel this Agreement. You hereby request and authorize IdenTrust to send You email messages reminding You of the renewal process. If You elect to renew, You will be charged for a renewal Certificate, and You will be responsible for complying with IdenTrust's then-current procedures to receive your renewal Certificate.

### **3. Your and Your Organization's Rights and Responsibilities**

**3.1 Fee.** You and Your Organization will be responsible for the applicable certificate issuance fee, which you authorize may be billed to Your credit card (or pursuant to other payment arrangements agreed upon between IdenTrust and You or someone acting on your behalf). If the certificate issuance fee is not paid, IdenTrust may revoke Your Certificate. You agree that if Your Certificate is purchased with funds provided by an employer or governmental entity (the "Purchaser"), the Purchaser may act either on your behalf or on behalf of the Purchaser (without cause and without Your prior consent) for the purposes of requesting certificate revocation in accordance with Section 3.7 and 4.3.

**3.2 Representations and Warranties.** By accepting Your Certificate, You: (i) accept its contents and the responsibilities identified in this Agreement, and (ii) represent and warrant to IdenTrust and to all who reasonably rely on the information contained in Your Certificate that: (a) You rightfully hold the Private Key corresponding to the Public Key listed in Your Certificate; (b) all representations You made and information You submitted to IdenTrust in the application process were current, complete, true and not misleading, (c) You have provided all facts material to confirming your identity and to establishing the reliability of Your Certificate, (d) all information in Your Certificate that identifies You is current, complete, true and not misleading, (e) You are not aware of any fact material to the reliability of the information in Your Certificate that has not been previously communicated to IdenTrust, and (f) You have kept your Private Key secret.

**3.3 Use of Your Certificate.** The purpose of Your Certificate is to identify You and the fact that You are employed or otherwise affiliated with Your Organization-not to certify any authority or capacity to act on behalf of or bind Your Organization. You may use Your Certificate to establish your identity with third-parties, sign and file documents electronically, obtain access to certificate-enabled online sources of information, and make secure and/or encrypted communications. You may not use Your Certificate for (i) 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) transactions where applicable law prohibits its use; or (iii) fraud or any other illegal scheme or unauthorized purpose.

**3.4 Legal Effect.** You and Your Organization agree that (i) a Digital Signature created using your Private Key shall be considered a "signature" for all intents and purposes; (ii) such Digital Signature, or any contract or other document or record Digitally Signed using your Private Key, will not be denied legal effect, validity or enforceability merely because such Digital Signature, contract, document or record is in electronic form or created using electronic processes; and (iii) neither You nor Your Organization will deny or contest such legal effect, validity or enforceability on such grounds.

**3.5 Protect Your Private Key.** You and Your Organization are responsible for protecting your Private Key. You and Your Organization represent, warrant and agree that, in regard to Your Certificate: (i) You have kept and will keep your Private Key (and any Activation Data used to protect your Private Key) private, and (ii) You and Your Organization will take reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, your Private Key and the computer system or media on which your Private Key is stored.

Failure to protect your Private Key or to notify IdenTrust of the theft, compromise, or misuse of your Private Key, or continued use of the Key or Certificate after they have been compromised, may cause You or Your Organization serious adverse legal consequences.

If You or Your Organization ever suspect or discover that the security of your Private Key has been or is in danger of being compromised in any way, You or Your Organization must immediately notify IdenTrust, as provided in Section 3.7 below, and request that Your Certificate be revoked.

If your Private Key has been compromised, You should notify anyone who may use Your Certificate to send encrypted messages to You that such encrypted messages may not be secure.

**3.6 Changes in Certificate Information.** If any of your information changes, you should immediately notify IdenTrust. You may update your information at the Certificate Management Center (located at <https://www.identrust.com/manage/certificates>) using your TrustID | Business Identity Certificate and selecting "View/Update Contact Information." NOTE: If IdenTrust does not have current information for You, it may not be able to fully perform its obligations to You and Your Organization, including but not necessarily limited to, sending Certificate renewal notices, revocation and suspension notices, and providing other information You may need to know about Your Certificate and its use. An incorrect e-mail address in Your Certificate may also prevent You from using it for signing and securing your e-mail, and may cause other technical problems or limitations on the use of Your Certificate.

### **3.7 Revoke Your Certificate.**

When to Revoke Your Certificate. You or Your Organization must immediately request that Your Certificate be revoked if: (i) You or Your Organization ever discover or suspect that your Private Key has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way, or (ii) any information in Your Certificate (other than your email address) is no longer accurate, current, or complete or becomes misleading, including if You are no longer affiliated with Your Organization. You or Your Organization may also revoke Your Certificate at any time for any other reason.

How to Revoke Your Certificate. You or Your Organization can initiate a revocation request by: accessing the TrustID Certificate Management Center (located at <https://www.identrust.com/manage/certificates>) using Your Certificate and selecting "Revoke My Certificate"; sending a signed e-mail (containing the reason for revocation and using the Private Key for which revocation is requested) to [Support@IdenTrust.com](mailto:Support@IdenTrust.com); calling IdenTrust Support at 1-888-248-4447; or such other means as may be provided by IdenTrust.

**3.8 Cease Using Your Certificate.** You must immediately cease using Your Certificate in the following circumstances: (i) when You or Your Organization suspects or discovers that the Private Key corresponding to Your Certificate has been or may be compromised or subjected to unauthorized use in any way; (ii) when any information in Your Certificate (other than your e-mail address) is no longer accurate, current, or complete or becomes misleading; (iii) upon the revocation or expiration of Your Certificate; or (iv) upon termination of this Agreement.

**3.9 Consequences of Breach.** If You act in any manner counter to Your obligations under this Agreement, You will forfeit any claims You may have against IdenTrust.

**3.10 Indemnification.** You and Your Organization agree 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 You to IdenTrust, whether or not such misrepresentation or omission was intentional; (ii) your violation of this Agreement; (iii) any compromise or unauthorized use of Your Certificate (or the corresponding Private Key) caused by Your or Your Organization's negligence, intentional misconduct or failure to fulfill your obligations under this Agreement, unless prior to such unauthorized use You or Your Organization has appropriately requested revocation of Your Certificate and proven your or its authority to request revocation; or (iv) your misuse of Your Certificate, including without limitation any use of Your Certificate that is not permitted by this Agreement; PROVIDED, however, that nothing herein shall require You or Your Organization to indemnify IdenTrust for any consequences caused by the fault of IdenTrust, or IdenTrust's failure to fulfill any of its obligations.

## **4. IdenTrust's Rights and Responsibilities**

**4.1 Your Privacy Is Important.** IdenTrust will take reasonable care to ensure that the Private Information will be kept confidential. IdenTrust will: (i) comply with all applicable laws and regulations regarding privacy of information; (ii) protect the confidentiality of the Private Information; and (iii) use such information only for the purpose of providing certificate services and carrying out the provisions of this Agreement. The Private Information that identifies You will not be sold, rented, leased, or disclosed in any manner to any person without your prior consent, except (i) as required by law, or (ii) as may be necessary for the performance of Certificate and Repository services or for auditing requirements. IdenTrust also agrees to protect the Private Information in a manner designed to ensure its integrity and to make it available to You or Your Organization, following an appropriate request. However, Your TrustID | Business Identity Certificate and any information contained therein, including Your and Your Organization's identity, must be seen by others and is not private--that would defeat the purpose of Your Certificate, which is to allow third parties to establish you and Your Organization's identity. Personal information included in Your Certificate that allows third parties to confirm your identity and/or Digital Signature must be disclosed in order to make Your Certificate effective. Information that may be disclosed includes, but is not limited to: (i) your name and e-mail address, (ii) your Public Key; (iii) Your Organization's name, address and telephone number; and (iv) the Certificate serial number and expiration date. However, your address and telephone number and other personally identifying information, other than name and e-mail address, will not appear in Your Certificate and will not be disclosed to third parties except as provided in this Agreement.

**4.2 Certificate Repository.** During the term of this Agreement, IdenTrust will operate and maintain a secure online Repository that is available to Authorized Relying Parties and that contains (i) all current, valid TrustID Certificates (including, as applicable, Your Certificate), and (ii) a CRL or online database indicating the status, whether valid, suspended or revoked, of TrustID Certificates. When You accept Your Certificate, IdenTrust will publish Your Certificate in the Repository and will indicate its valid status until it is suspended, revoked or expired. IdenTrust will provide nonexclusive access to the Repository to Authorized Relying Parties to check the validity and status of Your Certificate.

**4.3 Suspension and Revocation.** IdenTrust may suspend Your Certificate when any party makes a claim against IdenTrust that Your Certificate is invalid or has been compromised. IdenTrust will promptly investigate any such claim, and either revoke Your Certificate or restore it to valid status, as IdenTrust reasonably deems appropriate. If You, or someone else with authority, request/s that your Certificate be revoked, IdenTrust will revoke Your Certificate and update the Repository as soon as practical after it has adequately confirmed that the person making the revocation request is authorized to do so. If the request is signed using your Private Key, the request will be accepted as valid. IdenTrust may also revoke Your Certificate without advance notice if it determines, in its sole discretion, that: (i) Your Certificate was not properly issued or was obtained by fraud; (ii) the security of the Private Key corresponding to Your Certificate has or may have been lost or otherwise compromised; (iii) Your Certificate has become unreliable; (iv) material information in your application or Your Certificate has changed or has become false or misleading (e.g., You are no longer affiliated with Your Organization); (v) You or Your Organization have violated any applicable Agreement



or obligation; (vi) You, Your Organization or the Purchaser requests revocation; (vii) a governmental authority has lawfully ordered IdenTrust to revoke Your Certificate; (viii) this Agreement terminates; or (ix) there are other reasonable grounds for revocation. IdenTrust will notify You when Your Certificate has been revoked.

**4.4 Disclaimer of Warranties and Limitation of Liability.** Disclaimer of Warranties. IDENTRUST DISCLAIMS ANY AND ALL OTHER WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO THE SERVICES PROVIDED OR THE TRUSTID | BUSINESS IDENTITY CERTIFICATE ISSUED HEREUNDER. Limitations of Liability. YOUR AND YOUR ORGANIZATION'S SOLE REMEDY FOR DAMAGES ARISING UNDER, OUT OF OR RELATED IN ANY WAY TO THIS AGREEMENT OR YOUR CERTIFICATE WILL BE A REFUND OF YOUR CERTIFICATE ISSUANCE FEE. IDENTRUST WILL NOT BE LIABLE TO YOU OR YOUR ORGANIZATION FOR ANY DAMAGES-WHETHER SUCH DAMAGES ARE DIRECT, CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR PUNITIVE, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND WHETHER SUCH DAMAGES ARE BASED IN CONTRACT, WARRANTY, TORT OR ANY OTHER LEGAL THEORY.

**5. 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.

**6. Dispute Resolution.** In the event of any dispute or disagreement between two or more parties hereto ("Disputing Parties") arising out of or related to this Agreement or Your 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(s). 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 among 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.

**7. Entire Agreement.** This Agreement and the Authorization Agreement, together with any other documents referred to and/or incorporated in any of the foregoing, constitute the entire Agreement among You, Your Organization, and IdenTrust with the respect to Your Certificate.

**8. Third Party Beneficiaries.** It is not the parties' intent that this Agreement (except for Section), or any of the other documents mentioned in the preceding paragraph, should confer, and they shall not confer, any rights on any third party.

**9. Amendment.** You and Your Organization agree that IdenTrust may modify this Agreement from time to time during the term of this Agreement. Minor modifications shall become effective when posted to IdenTrust's Web site. Any modification to this Agreement that substantially alters your or Your Organization's rights or obligations will become effective when You use or renew Your Certificate, whichever occurs first, after You or Your Organization have received notice of such modification. You and Your Organization will be deemed to have received notice of any modification when (i) either You or Your Organization actually receive written notice of such modification, or (ii) when notice of such modification is received at the e-mail address that You have provided to IdenTrust as your e-mail address.

**10. Severability.** If any provision of this Agreement is found to be invalid or unenforceable, then this Agreement will be deemed amended by modifying such provision to the extent necessary to make it valid and enforceable while preserving its intent or, if that is not possible, by striking the provision and enforcing the remainder of this Agreement.

**11. 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.

## **12. Definitions and Terms**

**Activation Data:** Any account number, password, or shared secret used to safeguard the Private Key from unauthorized viewing or use.

**Authorized Relying Party:** An individual or entity that has entered into an agreement with IdenTrust allowing the party to rely on TrustID Certificates.

**Agreement:** This Subscriber Agreement for TrustID | Business Identity Certificate.

**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.

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

**Customer:** The natural person accepting this agreement, except in the case where the natural person accepting this agreement is acting on behalf an entity that is not a natural person, in which case "Customer" is such entity.

**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.

**Hardcryptomodule:** a hardware device, typically in the form of a USB token or other smartcard, that: (i) generates Key Pairs; (ii) stores cryptographic information (such as the Private Key); and (iii) performs cryptographic functions. Such device is deemed and construed for purposes hereof to include any device reader hardware provided along with such device, as well as any software embedded in the hardware device or reader.

**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 (i.e., create a Digital Signature) that can only be decrypted using the other key (i.e., verify the Digital Signature), and (ii) even knowing one key (e.g., the Public Key), it is computationally infeasible to discover the other key (e.g., the Private Key).

**Private Information:** Non-public information that You or Your Organization provide or that IdenTrust obtains, during the application and identification processes, that is not included in Your Certificate and that identifies You or Your Organization.

**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.

**Repository:** An online system maintained by IdenTrust for storing and retrieving TrustID Certificates and other information relevant to TrustID Certificates, including information relating to TrustID Certificate validity or revocation. **TrustID Certificate:** A Certificate issued by IdenTrust under the TrustID brand. **Validity Period:** The intended term of validity of Your Certificate, beginning with the date of issuance ("Valid From" or "Activation" date), and ending on the expiration date indicated in Your Certificate ("Valid To" or "Expiry" date). **Your Certificate:** The TrustID | Business Identity Certificate issued to You pursuant to this Agreement.