SUBSCRIBER AGREEMENT FOR
TRUSTID
SECURE EMAIL SOFTWARE CERTIFICATE

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

TO AGREE TO SUCH TERMS AND CONDITIONS, CLICK ON THE BOX NEXT TO THE TEXT THAT READS "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" ON THE PRIOR SCREEN. CLICKING SUCH BOX SHALL FOR ALL PURPOSES CONSTITUTE CUSTOMER'S ACCEPTANCE OF THE TERMS AND CONDITIONS SET FORTH BELOW.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS SET FORTH BELOW, CLICK ON "CANCEL" ON THE PRIOR SCREEN, AND DO NOT PROCEED WITH AN APPLICATION FOR A TRUSTID SECURE EMAIL CERTIFICATE.

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 Customer's rights, duties, and obligations as the applicant for a TrustID Secure Email Certificate and, if issued by IdenTrust pursuant in response to such application, then also to the TrustID Secure Email Certificate issued in connection herewith.

3. TrustID Secure Email Certificate Application, Issuance, and Term

3.1. Authority. In the event Customer is a natural person entering this agreement on behalf of himself or herself, then such person represents and warrants that they have full power and authority to accept this Agreement and understand that by accepting this Agreement they will be fully bound by the terms of this Agreement. In the event Customer is an entity other than a natural person, then the natural person accepting this agreement (such natural person, "You") represents and warrants that he or she has full power and authority to accept this Agreement on behalf of such entity and to thereby fully bind such entity to the terms of this Agreement.

3.2. Application. The contents of the TrustID Secure Email Certificate, if issued, will be based on the information provided by Customer (or You) on the previous screens as part of the registration and application process. By entering into this Agreement, Customer represents and warrants that: (i) all of the information provided to IdenTrust in the registration and application process, including but not limited to the email address(es) provided as part of such process, is accurate, current, complete, and not misleading; (ii) Customer owns or has lawful control of the email address(es) provided to IdenTrust in the registration and application process; (iii) Customer has provided all facts material to establishing the reliability of the information Customer has provided to IdenTrust in the registration and application process, including but not limited to information so provided for incorporation into a TrustID Secure Email Certificate by IdenTrust pursuant to this Agreement; and (iv) the information contained in the email address(es) provided to IdenTrust in the registration and application process, if included by IdenTrust in a TrustID Secure Email Certificate issued to Customer, will not infringe or otherwise violate any copyright, trademark, or any other proprietary right of any third party. If Customer is uncertain whether information provided to IdenTrust during the aforementioned registration and application process is accurate or correct, Customer must now click "BACK" in their Web browser application and (a) correct it, or (b) if correction is not feasible, cancel the application. Customer agrees to provide such further information as IdenTrust may reasonably require in connection with the registration and application process.

3.3. Fee. IdenTrust will begin processing the application made in connection herewith as soon as IdenTrust has received the following in connection herewith: (i) a completed application; and (ii) a (a) purchase order in the amount of the fee specified by IdenTrust to Customer in connection with the TrustID Secure Email Certificate applied for, (b) Customer's submission to IdenTrust of a valid IdenTrust voucher number that Customer rightfully holds, or (c) preauthorization to charge a credit card identified to IdenTrust in connection with such application. In the event IdenTrust approves

Customer's application for a TrustID Secure Email Certificate in connection herewith, IdenTrust will, and Customer hereby irrevocably authorizes IdenTrust to, bill against such purchase order, fulfil such voucher, or charge credit card, as applicable, for the applicable TrustID Secure Email Certificate fee specified by IdenTrust in connection with application for a TrustID Secure Email Certificate made in connection herewith. Once such billing, fulfillment, or charge occurs, unless otherwise required by law, no refunds will be provided by IdenTrust. If a TrustID Secure Email Certificate is issued to Customer hereunder, IdenTrust will revoke such TrustID Secure Email Certificate if IdenTrust does not actually receive payment for the Certificate within sixty (60) days of such issuance without any liability to any person or entity.

3.4. Verification. Customer authorizes IdenTrust to verify Customer's control of email address(es) provided to IdenTrust in application made by Customer in connection herewith. IdenTrust may consult public or private databases or other sources for the purpose of verifying information submitted to IdenTrust in connection herewith. In the event IdenTrust contacts Customer as part of such verification activities, Customer represents and warrants that any responses provided to IdenTrust by Customer as part of such contact shall be complete and accurate when given. Customer also authorizes IdenTrust to store and use in accordance with this Agreement any information (a) submitted to IdenTrust by or on behalf of Customer or (b) generated by or on behalf of IdenTrust during IdenTrust's application process, registration process, verification process, and TrustID Secure Email Certificate issuance process. If IdenTrust is unable to verify Customer's control of email address(es) provided to IdenTrust in the application made in connection herewith, then notwithstanding any other provision hereof IdenTrust may refuse to issue a TrustID Secure Email Certificate to Customer without any liability to any person or entity.

3.5. Creation and Availability for Download.

If IdenTrust accepts and approves the application for a TrustID Secure Email Certificate made in connection herewith, notice thereof will be sent to Customer at an email address submitted to IdenTrust in the application information. Such notice will include instructions to Customer for Customer to connect with IdenTrust computer systems via the Internet as part of the TrustID Secure Email Certificate issuance process. As part of such process, Customer shall generate a Key Pair and submit the Public Key of such Key Pair to IdenTrust pursuant to the IdenTrust instructions relating to the issuance process. If IdenTrust creates a TrustID Secure Email Certificate for Customer, the Public Key so submitted to IdenTrust will be included in such TrustID Secure Email Certificate, along with other information of Customer as provided for in the CPS, including but not limited to at least one email address submitted by Customer to IdenTrust among the application and registration information submitted by Customer to IdenTrust in connection herewith. IN NO EVENT WILL IDENTRUST EVER HAVE ACCESS TO THE PRIVATE KEY OF THE KEY PAIR GENERATED BY CUSTOMER. After IdenTrust creates such TrustID Secure Email Certificate for Customer, it will be made available to Customer to download.

If Customer has not downloaded a TrustID Secure Email Certificate that is made available for download as described above in this Section 3.5 within thirty (30) days of IdenTrust sending Customer a notice of acceptance and approval of the application as described above in this Section 3.3, then the associated approval from IdenTrust will become void and this Agreement shall terminate without any liability to any person or entity, including but not limited to there being no obligation for IdenTrust to refund any fees paid IdenTrust in connection herewith.

3.6. Issuance and Acceptance.

When Customer downloads the TrustID Secure Email Certificate made available as described in Section 3.5 above, Customer will be deemed to have been issued the TrustID Secure Email Certificate by IdenTrust. When Customer downloads the TrustID Secure Email Certificate made available as described in Section 3.5 above, the contents of such TrustID Secure Email Certificate will be presented and Customer agrees to: (i) review again the information in the TrustID Secure Email Certificate; and (ii) immediately notify IdenTrust of any inaccuracies, errors, defects, or other problems with the TrustID Secure Email Certificate.

Customer agrees that it will be deemed to have accepted the TrustID Secure Email Certificate: (a) when Customer uses the TrustID Secure Email Certificate or either key of the corresponding Key Pair after downloading the TrustID Secure Email Certificate; or (b) if Customer fails to notify IdenTrust of any inaccuracies, errors, defects, or other problems with the TrustID Secure Email Certificate promptly after downloading and reviewing it as provided above in this Section 3.6. By accepting the TrustID Secure Email Certificate, Customer accepts the contents of the TrustID Secure Email Certificate and reaffirms Customer's acceptance of Customer's of this Agreement.

Customer agrees to install and use the TrustID Secure Email Certificate only on computer systems owned or controlled by Customer and not to use such TrustID Secure Email Certificate until Customer has reviewed and verified the accuracy and correctness of the information in such Certificate.

3.7. Addition Provisions for Types of Certificates that include Hardware.

If the definition of TrustID Secure Email Certificate set forth in Section 22 below includes the phrase "TrustID Secure Email Software Certificate", no Hardcryptomodule will be provided by IdenTrust under this Agreement and the provisions below in this Section 3.7 do not apply.

If the definition of TrustID Secure Email Certificate set forth in Section 22 below includes the phrase "TrustID Secure Email Hardware Certificate" and if IdenTrust approves the issuance of a TrustID Secure Email Certificate to Customer, 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 Secure Email Certificate is issued to Customer, then in connection with the download process that is part of such issuance (*see* Section 3.4), Customer will be required to activate the Hardcryptomodule as required by IdenTrust in connection with the download process provided for in Section 3.6. 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 Secure Email Certificate.

ANY HARDCRYPTOMODULE PROVIDED BY IDENTRUST UNDER THIS AGREEMENT IS PROVIDED SUBJECT TO THE PROVISIONS OF SECTION 6.2. Without derogating from or forming a limitation or exception on the provisions of Section 6.2: (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.

3.8. Term. Once issued, the TrustID Secure Email Certificate will be valid for the term specified in the TrustID Secure Email Certificate unless revoked earlier as provided for herein. This Agreement will be coterminous with the TrustID Secure Email Certificate and will, therefore, terminate when the TrustID Secure Email Certificate ceases to be valid. At the expiration of the TrustID Secure Email Certificate, Customer may request a new or renewal TrustID Secure Email Certificate in accordance with IdenTrust's then current procedures and such new or renewal TrustID Secure Email Certificate shall be subject to the then-applicable terms and conditions for TrustID Secure Email Certificates. Customer hereby requests and authorizes IdenTrust to send e-mail messages to Customer relating to lifecycle events of the TrustID Secure Email Certificate (e.g. issuance process, revocation events, reminding Customer of the renewal process).

4. Customer's Responsibilities.

4.1. Representations and Warranties.

By accepting the TrustID Secure Email Certificate as provided for in Section 3.6, Customer represents and warrants to IdenTrust and to each Relying Party that: (i) Customer rightfully holds the Private Key corresponding to the Public Key listed in the TrustID Secure Email Certificate; (ii) all representations made and information submitted by and on behalf of Customer to IdenTrust during the application process for the TrustID Secure Email Certificate and, separately, during any subsequent contact with IdenTrust as provided for under Section 3.4 above, were current, complete, true, and not misleading; (iii) Customer has provided all facts material to confirming Customer's control over the email address(es) provided to IdenTrust in application made by Customer in connection herewith and to establishing the reliability of the TrustID Secure Email Certificate; (iv) all information in the TrustID Secure Email Certificate that identifies Customer is current, complete, true, and not misleading; (v) Customer is not aware of any fact material to the reliability of the information in the TrustID Secure Email Certificate that has not been previously communicated in writing by Customer to IdenTrust; and (vi) Customer has kept its Private Key secret.

Without forming any limitation on any other provision hereof, with respect to each use of the TrustID Secure Email Certificate, Customer represents and warrants to IdenTrust and each Relying Party that (a) such use shall be in conformity with the provisions of Section 4.2 below, and (b) any Digital Signature made with the TrustID Secure Email Certificate is made by and attributable to Customer.

4.2. Use of the TrustID Secure Email Certificate.

The TrustID Secure Email Certificate may be used only to: (i) encrypt email; (ii) Digitally Sign email in compliance with the provisions hereof and the CPS.

The TrustID Secure Email Certificate 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 where 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) on any computing or other electronic device that is not owned or lawfully controlled by Customer; (vi) to issue any other Certificate; or (vii) to Digitally Sign any email that if sent to a recipient in the United States would be subject to (and not exempted from) the CAN-SPAM Act.

4.3. Protect Private Key. Customer is responsible for protecting its Private Key. Customer represents, warrants and agrees that, in regard to the TrustID Secure Email Certificate, Customer: (i) has kept and will keep its Private Key (and any Activation Data used to protect Customer's Private Key) private, and (ii) will take all reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, its Private Key and the computer system or media on which its Private Key is stored. Failure to protect the Private Key or to notify IdenTrust of the theft, compromise, or misuse of the Private Key may cause Customer serious adverse legal and financial consequences.

4.6. Responsiveness to Instructions. Customer must respond to IdenTrust within twelve (12) hours if IdenTrust sends instructions to Customer regarding any actual or possible compromise of Customer's Private Key or misuse of the TrustID Secure Email Certificate.

4.7. Customer Requests to Revoke the TrustID Secure Email Certificate.

When to Revoke the TrustID Secure Email Certificate. Customer must immediately request that the TrustID Secure Email Certificate be revoked if: (i) the Private Key corresponding to the Public Key listed in the TrustID Secure Email Certificate is suspected of or has actually been lost, disclosed, compromised, or subjected to unauthorized use in any way; or (ii) any information in the TrustID Secure Email Certificate becomes misleading or is no longer accurate, current, or complete. Customer may also revoke the TrustID Secure Email Certificate at any time for any other reason.

How to Revoke the TrustID Secure Email Certificate. Customer can initiate a revocation request by:

(i) delivery of an e-mail (containing the reason for revocation and using the Private Key for which revocation is requested) to helpdesk@IdenTrust.com;

(ii) contact with the IdenTrust Help Desk at +1.801.924.8140;

(iii) submitting a request via IdenTrust's online Certificate management interface systems, if such systems are made available to Customer and Customer 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.

4.8. Cease Using the TrustID Secure Email Certificate. Customer must immediately cease using the TrustID Secure Email Certificate in the following circumstances: (i) the Private Key corresponding to the Public Key listed in the TrustID Secure Email Certificate is suspected of or has actually been lost, disclosed, compromised, or subjected to unauthorized use in any way; (ii) when any information in the TrustID Secure Email Certificate becomes misleading or is no longer accurate,

current, or complete; (iii) upon the revocation or expiration of the TrustID Secure Email Certificate; or (iv) upon termination of this Agreement.

4.9. Indemnification. Customer 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 Customer to IdenTrust, whether or not such misrepresentation or omission was intentional; (ii) Customer's violation of this Agreement; (iii) any compromise or unauthorized use of the TrustID Secure Email Certificate or the corresponding Private Key caused by Customer's negligence, intentional misconduct, or breach of this Agreement, unless prior to such unauthorized use Customer has appropriately requested revocation of the TrustID Secure Email Certificate and proven its authority to request revocation; (iv) Customer's misuse of the TrustID Secure Email Certificate, including without limitation any use of the TrustID Secure Email Certificate that is not permitted under Section 4.2 of this Agreement; (v) the content of any communication made wherein the TrustID Secure Email Certificate is used to encrypt or Digitally Sign such communication; or (vi) any entity (natural or otherwise) relying on the TrustID Secure Email Certificate, encryption resulting from the use of such Certificate, or a Digital Signature made using such Certificate.

5. IdenTrust's Responsibilities.

5.1. Privacy.

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

Notwithstanding the foregoing provisions of this Section 5.1, Customer acknowledges that information contained in any TrustID Secure Email Certificate issued in connection herewith and related status information shall not be considered or deemed Private Information, for that would defeat the purpose of the TrustID Secure Email Certificate (which purpose is the use described in Section 4 above). Customer authorizes the disclosure of such information by IdenTrust in connection with IdenTrust fulfilling its duties and obligations hereunder and as may otherwise be provided for under the CP or CPS.

5.2. Certificate Repository. During the term of this Agreement, IdenTrust will maintain at least one secure online repository that contains (a) the TrustID Secure Email Certificate, if issued to Customer, and (b) a CRL or online database indicating the status, whether valid or revoked, of the TrustID Secure Email Certificate, if issued to Customer. Such repository will be updated by IdenTrust from time to time in conformity with the applicable requirements of the CPS.

5.3. Revocation.

IdenTrust will revoke the TrustID Secure Email Certificate upon request by Customer (such request to be made in conformity with the provisions of Section 4.5 above) as soon as practical after IdenTrust has determined, in its sole discretion, that the person making the revocation request is authorized to do so. If the request is signed using the Private Key corresponding to the TrustID Secure Email Certificate, IdenTrust will accept the request as valid.

IdenTrust may also revoke the TrustID Secure Email Certificate without advance notice if it determines, in its sole discretion, that: (i) the TrustID Secure Email Certificate was not properly issued or was obtained by fraud; (ii) the security of the Private Key corresponding to the TrustID Secure Email Certificate has or may have been lost or otherwise compromised; (iii) the TrustID Secure Email Certificate has become unreliable; (iv) material information in the application or the TrustID Secure Email Certificate has changed or has become false or misleading; (v) Customer has violated any applicable duty or obligation; (vi) Customer requests revocation; (vii) a governmental authority has lawfully ordered IdenTrust to revoke the TrustID Secure Email Certificate; (viii) this Agreement terminates; (ix) there are other reasonable grounds for revocation, including any violation of a provision of the CP or CPS by Customer; or (x) requests for IdenTrust to validate such Certificate or Digital Signatures made with such Certificate result in demands on the applicable validation operations of IdenTrust provided per the CPS that (a) materially reduce or (b) otherwise cause a serious problem affecting performance of such IdenTrust validation operations or related IdenTrust computer systems, in each case as determined by IdenTrust in its sole discretion. IdenTrust will send notice to Customer when the TrustID Secure Email Certificate has been revoked.

6. Warranties and Disclaimers of Warranties and Limitations of Liability

6.1. Warranties. Subject to the provisions CP, CPS, and this Agreement, and Customer's fulfillment of its duties and obligations under the same, IdenTrust warrants to Customer that the TrustID Secure Email Certificate shall be issued and managed by IdenTrust in accordance with the terms of the CP, CPS, and this Agreement that are applicable to IdenTrust.

6.2. Disclaimer of Warranties and Limitations of Liability.

EXCEPT AS PROVIDED IN SECTION 5.4 ABOVE, THE TRUSTID SECURE EMAIL 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 THE TRUSTID SECURE EMAIL CERTIFICATE AND ANY IDENTRUST SERVICE.

ANY HARDCRYPTOMODULE PROVIDED BY IDENTRUST UNDER SECTION 3.7 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 THE TRUSTID SECURE EMAIL CERTIFICATE AND ANY IDENTRUST SERVICE

IDENTRUST MAKES NO WARRANTY THAT THE TRUSTID SECURE EMAIL CERTIFICATE, ANY HARDCRYPTOMODULE, 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.

IN NO EVENT SHALL IDENTRUST'S LIABILITY ARISING FROM OR RELATED TO THIS AGREEMENT EXCEED AN AMOUNT EQUAL TO THE AMOUNT CUSTOMER ACTUALLY PAID IDENTRUST FOR THE TRUSTID SECURE EMAIL CERTIFICATE FOR WHICH CUSTOMER APPLIED FOR IN CONNECTION WITH THIS AGREEMENT.

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 HAVE ANY LIABILITY FOR THE CONTENT OF ANY COMMUNICATION MADE USING A TRUSTID SECURE EMAIL CERTIFICATE, ANY HARDCRYPTOMODULE, OR ANY IDENTRUST SERVICE.

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

7. 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.

8. 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.

9. Assignment. Customer will not assign this Agreement or delegate any obligations hereunder. Any attempt by Customer 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 Customer; or (ii) assignment of all rights and obligations hereunder to a successor in interest, whether by merger, sale of assets, or otherwise.

10. Notice. Notice from Customer 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
55 Hawthorne Street, Suite 400
San Francisco, CA 94105

Notices from IdenTrust to Customer shall be made by posting on the Repository, or, provided a TrustID Secure Email Certificate is issued by IdenTrust hereunder, sending such notice to an email address for Customer set forth in such TrustID Secure Email Certificate. Except as otherwise provided herein, notices to Customer posted on the Repository shall be deemed effective three (3) days after being so posted and notices to Customer sent by email shall be deemed effective when sent.

11. 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 TrustID Secure Email 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.

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 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.

The provisions of this Section 11 are subject to the terms and conditions set forth in the other Sections of this Agreement, including but not limited to Sections 6.4 and 6.5.

12. Export.

With respect to Customer's application for, receipt of, custody of, and use of (a) the TrustID Secure Email Certificate if such Certificate issued by IdenTrust to Customer hereunder and (b) any Hardcryptomodule sent to Customer per Section 3.7, Customer (and You if Customer is not a natural person) will (y) comply with all applicable laws, ordinances, rules and regulations and (z) obtain any and all permits, licenses, authorization, and certificates that may be required in connection with such application, receipt, custody, and use.

Regardless of any disclosure made by Customer (or on behalf of Customer by You) to IdenTrust of the ultimate destination of the TrustID Secure Email Certificate that Customer applies for in connection herewith or any Hardcryptomodule sent to Customer per Section 3.7, Customer (and You if Customer is not a natural person) will not to export, either directly or indirectly, such TrustID Secure Email Certificate or such Hardcryptomodule without complying with all applicable export control laws, including, without limitation, United States export regulations as applicable.

Customer (and You if Customer is not a natural person) represents and warrants that Customer (and You if Customer is not a natural person) is not a citizen, national, or resident of any country which is subject to U.S. export prohibitions (all such countries, collectively, the "Prohibited Countries"), including without limitation Cuba, Iran, North Korea, Sudan, and Syria.

Customer (and You if Customer is not a natural person) represents and warrants that Customer (and You if Customer is not a natural person) is not among those persons and entities listed by the government of the United States of America in any of: (i) the *Denied Persons List* published by the Department of Commerce of the United States of America, (ii) the *Entity List*, or the *Unverified List*, each as published by the Department of Commerce, Bureau of Industry and Security, or (iii) the *Specially Designated Nationals List*, the *Non-SDN, Palestinian Legislative Council List*, the *Part 561 List*, the *Non-SDN Iran Sanctions Act List*, the *Foreign Sanctions Evaders List*, the *Sectoral Sanctions Identifications List*, or *the List of Persons Identified as Blocked Solely Pursuant to Executive Order 13599,* each as published by the Department of the Treasury of the United States of America (all lists described in this paragraph, collectively, the "Exclusion Lists").

Customer (and You if Customer is not a natural person) covenants that Customer (an You if Customer is not a natural person) will not transfer or otherwise provide, directly or indirectly, the TrustID Secure Email Certificate that Customer applies for in connection herewith or any Hardcryptomodule sent to Customer per Section 3.7 to (a) any citizen, national, or resident of any Prohibited Countries or (b) any person or entity listed in any of the Exclusion Lists.

13. Trademark Notice. "IdenTrust" and "TrustID" are registered trademarks of IdenTrust, Inc., used by IdenTrust with permission**.**

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 supercedes 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. Additional or different terms set forth on acceptance orders, purchase orders, confirmations and similar documents shall not modify the terms of this Agreement unless the same are specifically assented to in a writing that (a) expressly refers to this specific Agreement (and not, for example, to any agreement inconsistent therewith), (b) expressly states that this Agreement is amended or supplemented by such additional or different terms, and specifically refers to the sections or provisions that are so amended or supplemented, and (c) is signed by an authorized representative (in the case of IdenTrust, an officer thereof) of the party against whom enforcement of such terms is sought.

19. Third Party Beneficiaries. Each Relying Party is an intended third party beneficiary solely with respect to Customer's representations, warranties, duties, 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 Customer uses the TrustID Secure Email Certificate hereunder after such a posting, Customer shall be deemed to have accepted the most recent versions of the Agreement, CP, and CPS

posted on the Repository and be bound thereunder. Customer is 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.

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

Agreement: This Subscriber Agreement for TrustID Secure Email Software Certificate.

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

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

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

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 (such as Customer), using a Private Key and Public Key Cryptography, so that another person (or a person acting on behalf of an entity) having the transformed record and the corresponding Public Key can accurately determine (a) whether the transformation was created using the Private Key that corresponds to the Public Key, and (b) whether the record has been altered since the transformation was made. It need not involve a handwritten signature.

Exclusion Lists: defined in Section 12.

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.

Identification and Authentication: The process by which IdenTrust ascertains and confirms through appropriate inquiry and investigation the identity of the Customer. Certain aspects and activities within this process are prescribed by the CP and CPS.

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

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

Private Information: Non-public information that Customer provides or that IdenTrust obtains, during the application and Identification and Authentication processes, that is not included in the TrustID Secure Email Certificate and that identifies any of Customer.

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.

Prohibited Countries: defined in Section 12.

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.

Relying Party: Any person or entity that reasonably relies (in conformity with the CP and CPS) on the TrustID Secure Email Certificate during its Validity Period.

Repository: The information and data repository of IdenTrust located at:

https://secure.identrust.com/certificates/policy/ts/

TrustID Secure Email Certificate: a Certificate of the "TrustID Secure Email Software Certificate" type as provided in for in the CPS and subject to the terms hereof, and which is applied for by Customer in connection with this Agreement. Also, when "TrustID Secure Email Certificate" is used herein, such use is deemed and construed as including an "if issued" condition unless expressly provided otherwise.

Validity Period: The intended term of validity of a TrustID Secure Email Certificate, beginning with the date of issuance (for example, the "Valid From", "Begins On", "Not Before", or "Activation" date set forth in the TrustID Secure Email Certificate), and ending on the expiration date indicated in the TrustID Secure Email Certificate (for example, the "Valid To", "Expires On", "Not After", or "Expiry" date set forth in the TrustID Secure Email Certificate).

You: defined in Section 3.1.