IdenTrust
part of HID Global

TrustID®
Extended Validation SSL Certificate
Forms Packet

IdenTrust Services, LLC | 5225 W. Wiley Post Way, Suite 450 | Salt Lake City, UT 84116

www.IdenTrust.com

Sponsoring Organization Authorization Form

This Server (EV SSL) TrustID® Certificate Subscriber Agreement ("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 Server (EV SSL) TrustID® Certificate Issuance

IdenTrust is a Certification Authority that issues digital certificates to employees, agents and other individuals (e.g., licensed professionals) affiliated with the Sponsoring Organization ("Certificate Requestor"). Each TrustID® Server (EV SSL) certificate supplies trustworthy confirmation of the identity of the organization controlling the domain name(s) listed in the subject common name (CN) and subject alternative name (SAN) fields. However, TrustID® Server (EV SSL) certificates establish trustworthiness, not authority, and therefore 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 Server (EV SSL) TrustID® certificate to the Sponsoring Organization listed below. Prior to issuing a Server (EV SSL) TrustID® certificate, IdenTrust must confirm that the Certificate Requestor is indeed affiliated with the Sponsoring Organization, and Sponsoring Organization agrees that the information it provides to IdenTrust concerning a Certificate Requestor'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 Server (EV SSL) TrustID® Agreement that is presented to the Certificate Requestor on IdenTrust’s web site during the application process. Sponsoring Organization further acknowledges and agrees that the act or omission by the Certificate Requestor with respect to a Server (EV SSL) TrustID® 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 Server (EV SSL) TrustID® certificate issued to Sponsoring Organization identified below will expire after its stated period of validity, and that prior to expiration the Certificate Requestor may apply for and receive a renewal Server (EV SSL) TrustID® certificate to replace the expiring certificate. Sponsoring Organization hereby authorizes the Certificate Requestor to apply for and receive, and authorizes IdenTrust to issue, successive renewal Server (EV SSL) TrustID® certificates, provided that the Certificate Requestor applies for the renewal Server (EV SSL) TrustID® certificate within the required time frames for such renewal. Sponsoring Organization acknowledges and agrees that IdenTrust may require the Certificate Requestor 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. Server (EV SSL) certificates can also be revoked by the Sponsoring Organization at any time for any other reason.

4. Term and Termination

The terms of this Authorization Agreement shall run from the date indicated below until all Server (EV SSL) TrustID® certificates issued to the Sponsoring Organization 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 Server (EV SSL) TrustID® 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 Server (EV SSL) TrustID® 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 Certificate Requestor’s legal first and last name	Certificate Requestor’s email address
Print Sponsoring Organization name	Contract Signer’s signature
Address line 1	Contract Signer’s first and last name
Address line 2	Contract Signer’s title
City, State/Province, Country, Postal Code	Date Contract Signer signed

Server (EV SSL) TrustID® 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 Server Certificates.

3. Application. The contents of the Server Certificate requested as part of the Application will be based on information provided to IdenTrust in the Application. The contents of any Server 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. 1. 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.

IdenTrust and Subscriber acknowledge that this Agreement is a legally valid and enforceable agreement that creates extensive obligations on Subscriber. A Server Certificate serves as a form of digital identity for Subscriber. The loss or misuse of the Server Certificate can result in great harm to the Subscriber. 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 Server 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; (iii) is expressly authorized by Subscriber to approve requests for Server Certificates on Subscriber's behalf; and (iv) has confirmed Subscriber's right to use the domain(s) to be included in Server Certificates.

4.2. Representations and Warranties Relating to 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 and domain names) is accurate, current, complete, and not misleading; (ii) Subscriber owns the right to use such organization and domain names; 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 Server Certificate requested from IdenTrust pursuant to this Agreement.

By accepting a Server 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 Server 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 Server 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 Server Certificate, (d) all information in the Server 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 Server Certificate that has not been previously communicated to IdenTrust, and (f) Subscriber has kept secret its Private Key related to the Server Certificate.

4.3. Contract Signer as Certificate Approver. With respect to the request that is for a TrustID® 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 TrustID® 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 TrustID® 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 TrustID® Certificates; and (v) approve requests for TrustID® 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 on 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 TrustID® Certificates from Certificate Requestors, it is understood that if a Certificate Requestor desires to request a TrustID® 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. Server 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 Server Certificate, the Public Key submitted as part of the request for such TrustID® Certificate that part of the Application will be included in such Server Certificate. IN NO EVENT WILL IDENTRUST EVER HAVE ACCESS TO A PRIVATE KEY OF ANY KEY PAIR GENERATED BY CUSTOMER FOR A SERVER CERTIFICATE.

5.2. Verification of Identity and Authorization. Subscriber authorizes IdenTrust to engage in Identification and Authentication relative to the TrustID® Certificate requested in the Application and any further TrustID® 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 TrustID® Certificate, IdenTrust will create a Server Certificate in the name of Subscriber and the domain name(s) provided by Subscriber, and will notify Subscriber how and where to retrieve such Server Certificate. When Subscriber retrieves a Server Certificate, Subscriber will be deemed to have been issued and accepted the Server 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 TrustID® Certificate requested under this Agreement is not satisfied, then IdenTrust may refuse to issue such TrustID® Certificate without any liability to any Individual or other entity.

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

By accepting a Server Certificate, Subscriber: (i) accept its contents and the responsibilities identified in this Agreement;(ii) represents, warrants and agrees that all information in the Server Certificate that identifies Subscriber or the domain name(s) of Subscriber included in the Server Certificate are accurate, current, complete; (iii) all representations made by and on behalf of Subscriber in connection with its applying for the Server 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 Server Certificate that has not been previously communicated to IdenTrust; and (v) the Individual retrieving the Server Certificate was authorized to complete the registration and application for the Server 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 Server Certificate is issued by IdenTrust hereunder, then (a) the term of this Agreement shall terminate when the Server Certificate ceases to be valid, and (b) the Server Certificate will be valid for the Validity Period specified in the Server 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 Server 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 Server Certificate, and authorizes the billing as indicated during the application process. If the Application for a Server 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 Server Certificate is not paid, IdenTrust may

revoke the Server Certificate without any liability to any person or entity. Once a Server Certificate is issued by IdenTrust, refunds are not provided in relation to the Server Certificate.

7.2. Use of the Server Certificate. Server Certificates may be used by servers and other Internet devices to establish secure communications sessions with third parties. Server 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) on any server or other Internet device that is not located on the Internet at a domain name owned or lawfully controlled by Subscriber and contained in the Server Certificate; or (vii) to issue any other Certificate.

7.3. Protect Private Key. Subscriber is responsible for protecting its Private Key(s). Subscriber represents, warrants and agrees that, in regard to each Server Certificate, Subscriber: (i) has kept and will keep its corresponding Private Key (and any associated Activation Data) private, and (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.

Subscriber may change its employee(s) or agent(s) who are authorized to use and administer on behalf of Subscriber Server Certificates, without requesting revocation of current Server Certificates, but Subscriber shall bear the security and control risks associated with making such changes without revoking any Server Certificates. In the alternative, Subscriber may request revocation of current Server Certificates and apply for new TrustID® Certificates, subject to the fees and other requirements associated with the issuance of new TrustID® Certificates. Subscriber agrees that the act or omission of any employee or agent of Subscriber who has access to use any given Server Certificate or the corresponding Private Key, in using or administering the Server 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 must respond to IdenTrust within twelve (12) hours if IdenTrust sends instructions to Subscriber regarding any actual or possible compromise of any Private Key corresponding to a Server Certificate or misuse of a Server Certificate.

7.5. Revoking the Server Certificate -- When. Subscriber must immediately request that a Server 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 Server Certificate is no longer accurate, current, or complete or becomes misleading. Subscriber may also revoke any Server Certificate at any time for any other reason.

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

> **(i)** sending an email to Support@identrust.com, which email contains the reason for revocation and is signed using the Private Key corresponding to such Server Certificate;
>
> **(ii)** calling IdenTrust Support at 1-888-248-4447;
>
> **(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 Server Certificate. Subscriber must immediately cease using a Server Certificate in the following circumstances: (i) the Private Key corresponding to the Public Key listed in the Server 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 Server Certificate is no longer accurate, current, or complete or becomes misleading; (iii) upon the revocation or expiration of the Server 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 Server 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 Server Certificate(s) and proven Subscriber's authority and identity to IdenTrust as part of such request; or (iv) Subscriber's misuse of any Server Certificate(s), including without limitation any use of any Server 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 Server Certificates and related status information shall not be considered or deemed Private Information – that would defeat the purpose of each Server Certificate, which is to establish a trusted, secure communication link between Subscriber's server(s) located at the domain names of Subscriber included in that Server Certificate and third parties, and to confirm the identity of Subscriber and Subscriber's control of the domain names(s) of Subscriber identified in that Server Certificate. 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 TrustID® Certificates (including, as applicable, Server Certificates), and (ii) a CRL or online database indicating the status, whether valid, suspended or revoked, of TrustID® Certificates. When Subscriber accepts any Server Certificate hereunder, IdenTrust will publish that Server 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 Server Certificates when any party makes a claim to or against IdenTrust that indicates that a Server Certificates is invalid or has been compromised. IdenTrust will promptly investigate any such claim. If IdenTrust suspends any Server Certificate, then with respect to each such Server Certificate separately and as IdenTrust reasonably deems appropriate, IdenTrust will revoke the Server Certificate or the Server Certificates to valid status.

With respect to each Server Certificate separately, IdenTrust will revoke the Server 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 Server Certificate, IdenTrust will accept the request as valid.

With respect to each Server Certificate separately, IdenTrust may revoke the Server Certificate without advance notice if IdenTrust, in its sole discretion, determines that: (i) the Server Certificate was not properly issued or was obtained by fraud; (ii) the security of the Private Key corresponding to the Server Certificate has or may have been lost or otherwise compromised; (iii) the Server Certificate has become unreliable; (iv) material information in the application or the Server 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 Server 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 Server Certificate revoked as provided in the immediately preceding sentence, IdenTrust will notify Subscriber when the Server Certificate has been revoked.

8.4. Warranties. With respect to each Server 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 Server Certificate shall be issued and managed in accordance with the applicable terms of the CP, CPS and this Agreement; and (ii) that the Server 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 SERVER 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 SERVER CERTIFICATE AND ANY IDENTRUST SERVICE. IDENTRUST MAKES NO WARRANTY THAT ANY SERVER 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 THE CONTENT OF ANY WEBSITE OR SERVER USING AN IDENTRUST SECURED SSL 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 THE SERVER CERTIFICATE FOR WHICH CUSTOMER APPLIED FOR IN CONNECTION WITH THIS AGREEMENT. NOTWITHSTANDING THE FOREGOING SENTENCE AND WITH RESPECT TO EACH SERVER CERTIFICATE SEPARATELY, IN THE EVENT THE SERVER CERTIFICATE IS AN "EV 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 THAT SINGLE SERVER 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
6623 Dumbarton Circle
Freemont, CA 94555

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 Server 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 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.

19. Third Party Beneficiaries. Each Application Software Vendors and 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 Server 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 them 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 SERVER (EV SSL) TrustID® CERTIFICATE SUBSCRIBER AGREEMENT signed by the Contract Signer.

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

Application Software Vendor (ASV): A developer of Internet browser software or other software that displays or uses certificates, including but not limited to KDE, Microsoft, Mozilla Corporation, Nokia Corporation, Opera Software ASA, and Red Hat, Inc.

CAB Forum Document: The current version of the "CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates" document published by The CA/Browser Forum and available at: http://www.cabforum.org, which document 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.

Contract Signer: The Individual who made the Application and accepts the terms of this Agreement.

CP: The most recent version of the Certificate Policy for TrustID® 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.

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.

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.

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

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.

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 Subscriber provides or that IdenTrust obtains, during the application and Identification and Authentication processes, that is not included in the Server 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.

Relying Party: Any person or entity that reasonably relies on the Server Certificate during its Validity Period. For avoidance of doubt, an ASV is not a "Relying Party" when software distributed by such ASV merely displays information regarding a Certificate.

Repository: The information and data repository of IdenTrust located at

https://secure.identrust.com/certificates/policy/ts/, which may be amended from time to time by IdenTrust in its sole discretion.

Server 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 "Server Certificate" is used herein, such use is to be constructed to include an "if issued" condition.

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 Server 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 Server Certificate, beginning with the date of issuance ("Valid From" or "Activation" date), and ending on the expiration date indicated in the Server Certificate ("Valid To" or "Expiry" date).