DIGITAL CERTIFICATE SUBSCRIBER AGREEMENT

For Entities Ordering Through GSA Schedule 70

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A DIGICERT DIGITAL CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING A DIGICERT DIGITAL CERTIFICATE OR BY CHECKING "I AGREE", YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO IT. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A DIGICERT DIGITAL CERTIFICATE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973.

This digital certificate subscriber agreement ("Agreement") is between DigiCert, Inc., a Utah corporation ("DigiCert") and the entity applying for a Certificate ("Applicant") as identified during the online certificate enrollment process. Pursuant to GSA Contract Number GS-35F-0459X ("GSA Contract") and this Subscriber Agreement (referred to collectively as this "Agreement"), DigiCert agrees to provide the services described herein. The conditions and obligations in the GSA Contract supersede any conflicting condition or obligation in this Subscriber Agreement. Applicant and DigiCert agree as follows:

1. DEFINITIONS.

FAR 52.201-1 applies to all defined terms in this Agreement.

1.1. "Account" means a DigiCert system account that is used by Applicant to order Certificates.

1.2. "Affiliate" means an entity controlling, controlled by or under common control with the Applicant. As used in this definition, "control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of more than fifty percent of the voting shares of such entity or the power to direct the management and affairs of such entity.

1.3. "Application Software Vendors" means a software developer that displays or uses Certificates and distributes root certificates.

1.4. "Certificate" means a digitally signed electronic data file issued by DigiCert to an entity in order to confirm the identity of the entity and perform Digital Signature operations.

1.5. "Certificate Beneficiaries" means any Application Software Vendor, Relying Parties, or Cross-certified Entity.

1.6. "Code Signing Certificate" means a Certificate used to sign objects such that the Relying Party is assured that the object has not been modified since being signed.

1.7. "Confidential Information" means any information that is (i) designated as confidential (or a similar designation) by DigiCert, (ii) is disclosed in circumstances of confidence, or (iii) understood by the parties, exercising reasonable business judgment, to be confidential. Confidential Information does not include information that (w) was lawfully known or received by the receiving party prior to disclosure; (x) is or becomes part of the public domain other than as a result of a breach of this Agreement; (y) was

disclosed to the receiving party by a third party, provided such third party, or any other party from whom such third party receives such information, is not in breach of any confidentiality obligation in respect of such information; or (z) is independently developed by the receiving party as evidenced by independent written materials.

1.8. "CPS" refers to DigiCert's written statements of the policies and procedures used to operate its PKI infrastructure. DigiCert's CPS documents are available at http://www.digicert.com/ssl-cps-repository.htm.

1.9. "Cross-certified Entity" means any entity that cross-signed with a DigiCert root certificate, including the Entrust Group and Verizon Business/Cybertrust.

1.10. "Compromise" means evidence that (i) the hardware device used to store a Private Key is missing, (ii) the Private Key was publicly disclosed, (iii) an entity other than the Applicant has control over the Private Key or the Private Key's activation data, or (iv) that a third party is using a Private Key in a manner that does not conform with industry best practices.

1.11. "Digital Signature" means an encrypted electronic data file which is attached to or logically associated with other electronic data and which (i) identifies and is uniquely linked to the signatory of the electronic data, (ii) is created using means that the signatory can maintain under its sole control, and (iii) is linked in a way so as to make any subsequent changes that have been made to the electronic data detectable.

1.12. "EV Certificate" means a Certificate that contains the DigiCert Extended Validation Certificate Policy Object Identifier as set forth in the CPS and is issued in accordance with the EV Guidelines. EV Certificates include both SSL Certificates and Code Signing Certificates.

1.13. "EV Guidelines" means the Guidelines for Extended Validation Certificates as officially published, amended, and updated by the CA/Browser Forum at http://www.cabforum.org.

1.14. "Private Key" means a key that is kept secret by the Applicant that is used to create Digital Signatures and/or decrypt electronic records or files that were encrypted with the corresponding Public Key. Private Keys are Confidential Information.

1.15. "Public Key" means the publicly disclosed key of the Applicant that corresponds to a secret Private Key. The Public Key is used by Relying Parties to verify Digital Signatures created by the Private Key and/or encrypt messages so that they can only be decrypted using the corresponding Private Key.

1.16. "Relying Party" means an entity that acts in reliance on a Certificate or a Digital Signature. An Application Software Vendor is not a Relying Party when the software distributed by the Application Software Vendor merely displays information regarding a Certificate or facilitates the use of the Certificate or Digital Signature.

1.17. "Relying Party Warranty" is a warranty provided by DigiCert against certificate mis-issuance that is available only to Relying Parties who meet the conditions and fulfill all of the terms set forth at http://www.digicert.com/docs/agreements/DigiCert_RPA.pdf.

1.18. "Site Seal" means a logo or trademark provided by DigiCert for use on a website that is associated with a domain using a DigiCert SSL Certificate.

1.19. “SSL Certificate” means a Certificate used to provide TLS/SSL encryption using a Digital Signature.

1.20. “Subject” means the entity identified in the Certificate.

2. CERTIFICATE ISSUANCE AND MANAGEMENT

2.1. **Applicability.** This Agreement covers each Certificate issued by DigiCert to Applicant, regardless of (i) the Certificate type (email, code signing, or TLS/SSL), (ii) when the Applicant requested the Certificate, or (iii) when the Certificate actually issues.

2.2. **Requests**. Applicant may request Certificates from DigiCert by submitting the request electronically through DigiCert’s website, through Applicant’s Account (if one exists), by facsimile, or in writing. Applicant may request SSL Certificates only for domain names registered to (i) Applicant, (ii) an Affiliate of Applicant, or (iii) an entity that expressly authorizes DigiCert to allow Applicant to obtain and manage Certificates for the domain name. All certificate request data is incorporated into this document as part of the subscriber agreement.

2.3. **Certificate Approvers**. During the term of this Agreement, Applicant expressly authorizes the individuals appointed as “Certificate Approvers” in the Account (the designation of which is expressly incorporated into this Agreement) to request and approve EV Certificates on behalf of the Applicant. With respect to DigiCert’s obligations under the EV Guidelines and other industry standards, Applicant expressly authorizes DigiCert to rely on any representations made by a Certificate Approver in connection with an ordered Certificate, including verification of Applicant’s exclusive right to use the domain name listed in the Certificate. The Applicant is responsible for all EV certificates requested by a Certificate Approver until such Certificate Approver’s EV authority is revoked. Applicant may revoke a certificate Approver’s EV Authority by emailing DigiCert at admin@digicert.com. Applicant shall periodically review and update the individuals authorized to approve EV Certificate orders.

2.4. **Verification**. After receiving a Certificate request from Applicant, DigiCert reviews the request and attempts to verify Applicant in accordance with the DigiCert CPS and any applicable industry guidelines (such as the EV Guidelines for EV Certificates). Verification is subject to DigiCert’s sole satisfaction, and DigiCert may refuse to accept a certificate request or issue a Certificate for any reason. DigiCert shall promptly notify Applicant if DigiCert refuses a certificate request; however, DigiCert is not required to provide a reason for the refusal.

2.5. **Certificate Issuance**. If Applicant is successfully verified, DigiCert will issue the requested Certificate and deliver the Certificate to Applicant using a delivery mechanism selected by DigiCert. †Certificates are issued from a DigiCert root or intermediate certificate selected by DigiCert.† DigiCert may change which root or intermediate certificate is used to issue Certificates at any time and without notice to Customer.† DigiCert may deliver the Certificate using any reasonable means of delivery, including via email or as an electronic download in Customer’s account.† DigiCert may modify Certificate lifecycles as necessary to comply with requirements of (i) this Agreement, (ii) industry standards, (iii) a third party with whom DigiCert has cross-certified, (iv) DigiCert’s auditors, or (v) an Application Software Vendor. All Certificates containing internal server names or private IP addresses must expire on or before Nov 1, 2015.

2.6. **Certificate License**. Effective immediately after issuance and continuing until the Certificate either expires or is revoked, DigiCert grants Applicant a revocable, non-exclusive, non-transferable license to

use, for the benefit of the Subject, each issued Certificate in connection with properly licensed cryptographic software to (i) create Digital Signatures and (ii) perform Public Key or Private Key operations. Although DigiCert may send a reminder about expiring Certificates, DigiCert is under no obligation to do so, and Customer is solely responsible for ensuring Certificates are renewed on a timely basis. DigiCert may revoke any Certificates that it deems untrustworthy without prior notice.

2.7. **Certificate Revocation**. DigiCert may revoke a Certificate, without notice, for the reasons stated in the CPS, including if DigiCert reasonably believes that:

(i) Applicant requested revocation of the Certificate or did not authorize the issuance of the Certificate;

(ii) Applicant has materially breached this Agreement or an obligation it has under the CPS;

(iii) Applicant is added to a government list of prohibited persons or entities or is operating from a prohibited destination under the laws of the United States;

(iv) the Certificate contains inaccurate or misleading information;

(v) the Private Key associated with a Certificate was disclosed or Compromised;

(vi) this Agreement terminates;

(vii) industry standards or DigiCert's CPS require Certificate revocation,

(viii) the Certificate was (a) used outside of its intended purpose, (b) used to sign malicious code or software that is downloaded to a computer without the user's consent, (c) used or issued contrary to law, the CPS, or applicable industry standards, or (d) used, directly or indirectly, for illegal or fraudulent purposes; or

(ix) revocation is necessary to protect the rights, confidential information, operations, or reputation of DigiCert or a third party.

2.8. **Obligation on Termination**. Applicant shall promptly cease using the Certificate and corresponding Private Key upon the earlier of (i) revocation of the Certificate or (ii) the date when the allowed usage period for the corresponding Private Key expires.

3. SITE SEALS

3.1. **Site Seal Licenses**. If Applicant purchases an SSL Certificate or Site Seal service, Applicant may display a Site Seal on any websites that are registered with the Applicant's Site Seal service or that are secured using a DigiCert SSL Certificate. If the SSL Certificate or Site Seal service is revoked or expires, Applicant's license to display the Site Seal is also revoked unless Applicant either registers for the Site Seal service or a replacement SSL Certificate is issued. Applicant may not alter the Site Seal in any way, including changing the size of the site seal.

3.2. **Limitations on Use**. Applicant may use only the latest version of the Site Seal and only to indicate that Applicant is a customer of DigiCert's SSL Certificate or Site Seal services. Applicant may not display a Site Seal on any website if (i) the website was not verified as part of DigiCert's SSL Certificate or Site Seal services, (ii) the display would lead a reasonable person to believe that DigiCert guarantees a non-DigiCert product or service, (iii) the site contains content that is misleading, illegal, libelous, or otherwise

objectionable to DigiCert, or (iv) the display could harm or limit DigiCert's rights in the Site Seal or DigiCert's business reputation.

4. OBLIGATIONS AND REPRESENTATIONS

4.1. **Information**. Applicant shall, at all times, provide accurate, complete, and non-misleading information to DigiCert. If any information provided to DigiCert changes or becomes misleading or inaccurate, then Applicant shall promptly inform DigiCert and update the information. If any information included in an issued Certificate becomes inaccurate or misleading, Applicant shall promptly cease using and request revocation of the Certificate. Applicant shall not install or use a Certificate until after Applicant has reviewed and verified the accuracy of the data included in the Certificate.

4.2. **Use**. Applicant is responsible, at Applicant's expense, for (i) all equipment and software required to use the Certificate, (ii) Applicant's conduct, and (iii) Applicant's website. Applicant shall promptly inform DigiCert if it becomes aware of any misuse of a Certificate, including if a Code Signing Certificate is used to sign suspect code.

4.3. **Compliance**. Applicant shall use Certificates in compliance with all applicable laws, for authorized use of the Subject, and in accordance with this Agreement and any applicable standards (such as the EV Guidelines). Applicant shall promptly notify DigiCert if it becomes aware of a breach of this Agreement. Applicant is responsible for obtaining and maintaining any authorization or license necessary to use a Certificate, including any license required under United States' export laws.

4.4. **Restrictions**. Applicant shall only use an SSL Certificate on the servers accessible at the domain names listed in the issued Certificate. Applicant shall not:

(i) use a Certificate or Private Key to operate nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system requiring failsafe operation whose failure could lead to injury, death or environmental damage;

(ii) modify, sub license, reverse-engineer or create a derivative work of any Certificate (except as required to use the Certificate for its intended purpose), Private Key, or Site Seal;

(iii) use or make representations about a Certificate except as allowed in the CPS;

(iv) impersonate or misrepresent Applicant's affiliation with any entity or use a Certificate in a manner that could reasonably result in a civil or criminal action being taken against Applicant or DigiCert;

(v) use a Certificate to (a) send or receive unsolicited bulk correspondence, (b) sign or distribute any files, software, or code that may damage the operation of another's computer or that is downloaded without a user's consent, or (c) breach the confidence of a third party;

(vi) attempt to use a Certificate to issue other Certificates; or

(vii) intentionally create a Private Key that is substantially similar to a DigiCert or third-party Private Key.

4.5. **Compromise**. Applicant shall securely generate its Private Keys and protect its Private Keys from Compromise. Applicant shall protect Private Keys for EV Code Signing Certificates using a device meeting

at least FIPS 140 Level 2. Applicant shall only permit adequately trained individuals to handle the Private Key associated with a Certificate. If Applicant suspects misuse or Compromise of a Private Key, Applicant shall promptly notify DigiCert, cease using the corresponding Certificate, and request revocation of the corresponding Certificate. Applicant is solely responsible for any failure to protect a Private Key.

4.6. **Industry Standards**. Both parties shall comply with all industry and privacy standards applicable to the Certificates. If industry standards change, DigiCert and Customer shall work together in good faith to amend this Agreement to comply with the changes.

4.7. **Representations**. Applicant represents to DigiCert and the Certificate Beneficiaries that:

(i) Applicant has the right to use the domain name listed in the Certificate (if applicable) and is the lawful owner of the common name and organization name that will be included in the Certificate,

(ii) If the Applicant is an organization, the individual accepting this Agreement is expressly authorized by the Applicant to sign this Agreement on behalf of the Applicant,

(iii) Applicant has read, understands, and agrees to the CPS and this Agreement, and

(iv) the organization included in the Certificate and the registered domain name holder (if a domain name is included the Certificate) will be aware of and approve each Certificate request,

5. INTELLECTUAL PROPERTY RIGHTS

5.1. **Ownership**. DigiCert retains sole ownership in (i) the Certificates, Site Seals, and Account, (ii) all documentation provided by DigiCert in connection with the Certificates or Site Seals, (iii) all DigiCert trademarks, copyrights, and other intellectual property rights, and (iv) any derivative works of the Certificates or Site Seals, regardless of who suggested or requested the derivative work. Nothing herein restricts DigiCert's ability to transfer, license, use, or create derivative works of a Certificate or Site Seal.

5.2. **Trademarks**. Except for the limited license to DigiCert's Site Seal as provided in Section 3, DigiCert is not granting Applicant any rights in DigiCert's trademarks. Applicant shall not challenge DigiCert's rights to a trademark or attempt to register a DigiCert trademark or any confusingly similar mark. Except with the express written permission of DigiCert, Applicant shall not use any DigiCert trademark as part of Applicant's trade names or domain names. Applicant shall not use the Account or Certificates in a way that might diminish or damage DigiCert's reputation, including using a Certificate with a website that could be considered associated with crime, defamation, or copyright infringement. Applicant hereby grants DigiCert a non-exclusive, non-transferable, non-sublicenseable, royalty-free license to use Applicant's trademarks to indicate that Applicant is a customer of DigiCert's services.

6. FEES

6.1. **Payment**. Applicant shall pay DigiCert the GSA IT Schedule 70 fees for each ordered Certificate. This fee is for the services provided by DigiCert and is not a royalty or license fee. Applicant may pay the fees using either a credit card or by purchase order. If Applicant is paying by credit card, Applicant authorizes DigiCert to charge the fees to the card prior to issuing the Certificate. If Applicant is paying fees with a purchase order, then Applicant shall pay DigiCert the amount due within thirty days after receiving an accurate invoice from DigiCert.

6.2. **Refunds**. If Applicant's request for a Certificate is canceled or rejected for any reason, DigiCert shall refund the fees already paid for the Certificate. If Applicant wishes to purchase a different type of Certificate from DigiCert ("Replacement Certificate"), and DigiCert is willing to provide the Certificate to Applicant, then DigiCert shall apply the amount already paid to the purchase of the Replacement Certificate. DigiCert shall refund any fees paid for a Certificate if Applicant requests revocation of the Certificate in writing within 30 days after the Certificate issues. No refunds are given after the expiration of the 30-day period.

6.3. **Late Payments**. Applicant shall pay an interest rate as allowed by law on any amount that is not paid on or before the applicable due date.

6.4. **No Offsets or Deductions**. This Agreement is entered into, and all of the services are performed and provided, entirely from the State of Utah, within the United States of America. All fees are exclusive of any taxes, however imposed, e.g. sales tax, income tax, or VAT. Applicant may not withhold or offset any amount owed to DigiCert for any reason. If a withholding or deduction is required by law, then Applicant shall pay an additional fee that is equal to the amount withheld, causing DigiCert to receive a net amount from Applicant that is equal to the amount DigiCert would receive if a withholding or deduction was not required.

7. USE OF INFORMATION

7.1. **Confidentiality**. Each party shall keep confidential all Confidential Information it receives from the other party or its Affiliates. Each party shall use provided Confidential Information only for the purpose of exercising its rights and fulfilling its obligations under this Agreement and shall protect all Confidential Information against disclosure using a reasonable degree of care. Each party may provide Confidential Information to its contractors if the contractor is contractually obligated to confidentially provisions that are at least as protective as those contained herein. If a receiving party is compelled by law to disclose Confidential Information of the disclosing party, the receiving party shall use reasonable efforts to (i) seek confidential treatment for the Confidential Information, and (ii) send sufficient prior notice to the other party to allow the other party to seek protective or other court orders.

7.2. **Publication of Certificate**. Applicant consents to (i) DigiCert’s public disclosure of information embedded in an issued Certificate and (ii) DigiCert’s transfer of Applicant’s information to servers located inside the United States.

7.3. **Storage and Use of Information**. DigiCert shall follow the privacy policy posted on its website when receiving and using information from the Applicant or its Affiliates. DigiCert may modify the privacy policy in its sole discretion. Applicant expressly consents to inclusion on DigiCert’s mailing list. DigiCert may opt-out of having information used for purposes not directly related to DigiCert’s services by emailing a clear notice to privacy@digicert.com. Applicant may not opt-out of receiving important updates related to changes in industry standards that affect Applicant’s digital certificates or the security and use of ordered products.

8. TERM AND TERMINATION

8.1. **Term**. This Agreement is effective upon Applicant’s acceptance and lasts until the earlier of (i) the expiration date of all Certificates issued under this Agreement or (ii) the termination of this Agreement by a party as allowed herein.

8.2. **Termination**. Applicant may terminate this Agreement for convenience by providing notice to DigiCert. DigiCert may terminate this Agreement, after sending notice to Applicant, if (i) Applicant materially breaches this Agreement, (ii) DigiCert cannot satisfactorily verify Applicant's qualifications for a Certificate, (iii) industry standard or regulations change in a way that affects the validity of Certificates issued to Applicant, (iv) Applicant has a receiver, trustee, or liquidator appointed over substantially all of its assets, (v) Applicant has an involuntary bankruptcy proceeding filed against it that is not dismissed within 30 days of filing, (vi) Applicant files a voluntary petition of bankruptcy or reorganization, (vii) Applicant assigns this Agreement, or (viii) Applicant undergoes a change of control where more than fifty percent ownership is transferred to a third party.

8.3. **Effect of Termination**. Upon termination, DigiCert may revoke all Certificates issued under this Agreement, and Applicant shall promptly (i) cease using the Certificates issued under this Agreement and the associated Private Keys and (ii) remove any Site Seals displayed on websites under Applicant's ownership or control. All obligations and claims that are outstanding prior to termination remain outstanding.

8.4. **Survival**. All provisions of this Agreement that, by their nature, are intended to survive the termination of this Agreement, survive termination of the Agreement and continue in full force and effect, including all provisions related to proprietary rights (Section 5.1), use of information (Section 7), disclaimer of warranties and limitations on liability (Section 9), and the miscellaneous provisions (Section 10).

9. DISCLAIMERS AND LIMITATIONS ON LIABILITY

9.1. **Relying Party Warranties**. Applicant acknowledges that any Relying Party Warranty is only for the benefit of Relying Parties. Applicant does not have rights under the warranty, including any right to enforce the terms of the warranty or make a claim under the warranty.

9.2. **Remedy**. Applicant's sole remedy for a defect in a Certificate is to have DigiCert use reasonable efforts to correct the defect. DigiCert is not obligated to correct a defect if (i) the Certificate was misused, damaged, or modified, (ii) Applicant did not promptly report the defect to DigiCert, or (iii) Applicant breached any provision of this agreement.

9.3. **Warranty Disclaimers**. ALL DIGICERT PRODUCTS AND SERVICES, INCLUDING THE CERTIFICATES AND SITE SEALS, ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY PRODUCTS OR SERVICES WILL MEET APPLICANT'S EXPECTATIONS OR THAT ACCESS TO PRODUCTS OR SERVICES WILL BE TIMELY OR ERROR-FREE. DigiCert does not guarantee the availability of any products or services and may modify or discontinue a Certificate or Site Seal offering at any time.

9.4. **Limitation on Liability**. EXCEPT AS PROVIDED UNDER SECTION 9.6, THE LIABILITY OF DIGICERT AND ITS AFFILIATES, AND EACH OF THEIR OFFICERS, DIRECTORS, PARTNERS, EMPLOYEES, CONTRACTORS, AND AGENTS, RESULTING FROM OR CONNECTED TO THIS AGREEMENT IS LIMITED PURSUANT TO THE GSA CONTRACT. APPLICANT WAIVES ALL CLAIMS FOR ANY SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RELATED TO THIS AGREEMENT OR A CERTIFICATE, INCLUDING ALL

DAMAGES FOR LOST PROFITS, REVENUE, USE, OR DATA. THIS WAIVER APPLIES EVEN IF DIGICERT IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES.

9.5. **Force Majeure and Internet Frailties**. DigiCert is not liable for any failure or delay in performing its obligations under this Agreement to the extent that the circumstances causing such failure or delay and DigiCert's response to such circumstances meet the requirements of FAR 52.212-4(f). Applicant acknowledges that the Certificates are subject to the operation and telecommunication infrastructures of the Internet and the operation of Applicant's Internet connection services, all of which are beyond DigiCert's control.

9.6. **Applicability**. The limitations and waivers in this section 9 apply only to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of any claims, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this Agreement have been breached or proven ineffective.

9.7. **Limitation on Actions**. Each party shall commence any claim and action arising from this Agreement within one year from the date when the cause of action occurred. Each party waives its right to any claim that is commenced more than one year from the date of the cause of action.

10. MISCELLANEOUS

10.1. **Independent Contractors**. DigiCert and Applicant are independent contractors and not agents or employees of each other. Neither party has the power to bind or obligate the other. Each party is responsible for its own expenses and employees.

10.2. **Entire Agreement**. This Agreement, along with all documents referred to herein, constitutes the entire agreement between the parties with respect to the issuance and use of requested Certificate(s) and/or Site Seal(s), superseding all other agreements that may exist.

10.3. **Amendments**. DigiCert may amend any of its (i) website and any documents listed thereon, (ii) CPS, (iii) fees, (iv) privacy policy, or (iv) the conditions under which Applicant receives a Certificate, including this agreement. Amendments are effective upon the earlier of DigiCert's posting the amendment on its website or Applicant's receipt of the amendment. Applicant shall periodically review the website to be aware of any changes. Applicant may only amend this Agreement if the amendment is approved in writing by DigiCert. Applicant's continued use of a Certificate after an amendment is posted constitutes Applicant's acceptance of the amendment.

10.4. **Waiver**. A party's failure to enforce or delay in enforcing a provision of this Agreement does not waive (i) the party's right to enforce the same provision later or (ii) the party's right to enforce any other provision of the Agreement. A waiver is only effective if in writing and signed by the party benefiting from the waived provision.

10.5. **Notices**. Applicant shall send all notices in English writing by first class mail with return receipt request to DigiCert, Inc. 2801 North Thanksgiving Way, STE 500, Lehi, UT 84043. DigiCert shall send notices to Applicant using the email address provided by Applicant during the Certificate application process. Notices to DigiCert are effective when received. Notices to Applicant are effective when sent.

10.6. **Assignment**. Applicant shall not assign any of its rights or obligations under this agreement without the prior written consent of DigiCert. Any transfer without consent is void and a material breach of this Agreement. DigiCert may assign its rights and obligations without Applicant's consent.

10.7. **Governing Law and Jurisdiction**. The laws of the state of Utah govern the interpretation, construction, and enforcement of this Agreement and all matters related to it, including tort claims, without regards to any conflicts-of-laws principles. The parties hereby submit to the exclusive jurisdiction of and venue in the state and federal courts located in the State of Utah.

10.8. **Severability**. The invalidity or unenforceability of a provision under this Agreement, as determined by a court or administrative body of competent jurisdiction, does not affect the validity or enforceability of the remainder of this Agreement. The parties shall substitute any invalid or unenforceable provision with a valid or enforceable provision that achieves the same economic, legal, and commercial objectives as the invalid or unenforceable provision.

10.9. **Rights of Third Parties**. The Certificate Beneficiaries are express third party beneficiaries of Applicant's obligations and representations under this Agreement. Except for the Certificate Beneficiaries, no other third party has any rights or remedies under this Agreement.

10.10. **Interpretation**. The definitive version of this Agreement is written in English. If this Agreement is translated into another language and there is a conflict between the English version and the translated version, the English language version controls. Section headings are for reference and convenience only and are not part of the interpretation of this Agreement.

FOR EV CERTIFICATES: By accepting this Subscriber Agreement, you are entering into a legally valid and enforceable agreement to obtain a form of digital identity for the Applicant. You acknowledge that you have the authority to obtain the digital equivalent of a company stamp, seal, or (where applicable) officer's signature to establish the authenticity of the Applicant's website or signed code, and that the Applicant is responsible for all uses of its EV Certificate. By accepting this Agreement on behalf of the Applicant, you represent that you (i) are acting as an authorized representative of the Applicant, (ii) are expressly authorized by Applicant to sign Subscriber Agreements and approve EV Certificate requests on Applicant's behalf, and (iii) if applicable, have confirmed Applicant's exclusive right to use the domain(s) to be included in any issued EV Certificates.

ACCEPTANCE

BY CHECKING "I AGREE", YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT AND THAT YOU AGREE TO COMPLY WITH ITS TERMS. DO NOT CHECK "I AGREE" IF YOU DO NOT ACCEPT THIS AGREEMENT.