**IGTF CERTIFICATE SUBSCRIBER AGREEMENT**

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PROCEEDING. A GLOSSARY APPEARS AT THE END.

BY CHECKING "I AGREE" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO IT. THE PURPOSE OF A DIGITAL CERTIFICATE IS TO BIND AN IDENTITY (TYPICALLY YOURS) TO A PUBLIC-PRIVATE KEY PAIR. BY OBTAINING OR USING A CERTIFICATE ISSUED BY DIGICERT, YOU AGREE TO THE TERMS HEREIN. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT CHECK ACCEPT OR SUBMIT YOUR CERTIFICATE ORDER. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973.

This IGTF certificate subscriber agreement (**"Agreement"**) is between DigiCert, Inc., a Utah corporation (**"DigiCert"**) and you, the individual applying for a Certificate ("**You**"). DigiCert and your sponsor have previously entered into an agreement ("**Sponsor Agreement**") that allows You to order and use an IGTF certificate. This Agreement contains the terms and conditions applicable to the issuance and your use of the IGTF certificate. You and DigiCert agree as follows:

## 1. YOUR OBLIGATIONS

1.1. Protect your Private Key. You shall keep your Private Keys confidential and use all reasonable measures to protect your Private Keys from disclosure or misuse. In addition to your adherence to any Private Key protection requirements of your sponsor, You shall generate, protect, and use your Private Key as follows:

(i) inside a PIN-protected secure hardware token or inside a computer system that cryptographically protects the Private Key with at least a 12-character passphrase;

(ii) the PIN or passphrase and Private Key must never be disclosed or transmitted by You or the system unencrypted or in plain text, either during transmission, in data storage, or in memory for longer than 24 hours;

(iii) the data used to decrypt or use your Private Key may be active in the system only as a result of your action and only for as long as You are using the system;

(iv) any system storing your Private Key must be located in a secure environment where access is controlled and limited to only authorized personnel, and all such persons with access to the system must be subject to and aware of applicable privacy rules, codes of professional conduct, and data security requirements, and any third party involved in the generation or storage of your Private Key must also have a similarly defined data privacy and security policy that meets industry best practices; and

(v) You shall promptly (within one working day) notify DigiCert or your sponsor, cease using the Certificate, and request Certificate revocation if You suspect misuse or Compromise of your Private Key. You are solely responsible for any failure to protect your Private Keys.

1.2. Information. You shall, at all times, provide accurate, complete, and true information to DigiCert. If any information provided to DigiCert changes or becomes misleading or inaccurate, then You shall (i) promptly update the information and (ii) within one working day after the information changes, cease using and request the revocation of any Certificate including such information.

You shall not install or use a Certificate until after You have reviewed and verified the accuracy of the Certificate data.

1.3. Use. You may not share your Private Key with another user, including co-workers. You are responsible for any use of your Private Key, including any equipment or software that relies on the use of your Private Key and Certificate. You shall use Certificates in compliance with applicable laws and policies (including the CPS, which is incorporated by reference within the Certificate). You shall promptly notify DigiCert if You become aware of a breach of this Agreement. You are responsible for obtaining and maintaining any additional authorizations or licenses necessary to use the Private Key or Certificate for any specific or particular purpose.

1.4. Restrictions. You shall not use your Private Key or Certificate to:

(i) 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) send, upload, distribute or deliver unsolicited bulk correspondence, malicious code, code that is downloaded without a user's consent, or any files or software that may damage the operation of another's computer;

(iii) make misrepresentations about your Certificate, yourself, or your affiliation with any entity, or breach the confidence of a third party;

(iv) modify, sub license, reverse-engineer, or create a derivative work of any Certificate or Private Key or take any action to attack or attempt to disrupt the trustworthy operation of any Public Key Infrastructure in which your Key Pair or Certificate participates; or

(v) act in a manner that could reasonably result in a civil or criminal action being taken against You, your sponsor, or DigiCert.

## 2. CERTIFICATE ISSUANCE AND REVOCATION

2.1. Verification. DigiCert verifies certificate information with you and your sponsor in accordance with DigiCert's Certification Practices Statement (CPS) and applicable industry guidelines. Verification is subject to DigiCert's sole satisfaction, and DigiCert may refuse to issue a Certificate for any reason. DigiCert is not required to provide a reason for the refusal.

2.2. Certificate License. Effective immediately after issuance and continuing until the Certificate either expires or is revoked, DigiCert grants You a revocable, non-exclusive, non-transferable license to use the Certificate, for the benefit of the subject identified therein, and in connection with properly licensed and operating cryptographic software, to (i) create Digital Signatures, (ii) encrypt and decrypt communications, and/or (iii) perform other Public Key or Private Key operations. You are solely responsible for any failure to renew or replace a Certificate prior to its expiration.

2.3. Certificate Revocation and Termination. DigiCert may revoke a Certificate, without notice, for the reasons stated in the CPS, including if DigiCert believes revocation is necessary to protect its reputation or business. You shall promptly cease using the Certificate and corresponding Private Key (except to lawfully decrypt previously encrypted communications) upon: (i) revocation of the Certificate, (ii) termination of this Agreement, or (iii) the date when the allowed usage period for the corresponding Private Key expires.

## 3. INTELLECTUAL PROPERTY AND INFORMATION

3.1. Ownership. DigiCert retains sole ownership in (i) any Certificates it issues, (ii) all DigiCert trademarks, copyrights, and other intellectual property rights, (iii) the information collected by DigiCert, and (iv) any derivative works of the Certificates, regardless of who suggested or requested the derivative work.

3.2. Publication of Certificate. You consent to (i) DigiCert's public disclosure of information embedded in an issued Certificate, and (ii) DigiCert's transfer of your personal information to DigiCert's servers, which are located inside the United States.

3.3. Storage and Use of Information. DigiCert shall follow the privacy policy posted on its website when receiving and using information from You. DigiCert may modify the privacy policy in its sole discretion.

## 4. TERM AND TERMINATION

4.1. Term. This Agreement is effective on acceptance and lasts until the earlier of (i) the expiration date of the corresponding Certificate or (ii) the termination of this Agreement by a party as allowed herein.

4.2. Termination. You may terminate this Agreement for convenience by providing 30 days prior notice to DigiCert. DigiCert may immediately terminate this Agreement if (i) You materially breach this Agreement, (ii) DigiCert cannot satisfactorily verify your information, (iii) the Sponsor Agreement terminates, or (iv) if industry standards or regulations change in a way that affects the validity or security of the Certificates. Upon termination, DigiCert may revoke any Certificates issued under this Agreement.

4.3. Survival. All provisions of this Agreement related to proprietary rights (Section 3.1), disclaimer of warranties and limitations on liability (Section 5), and the miscellaneous provisions (Section 6) survive the termination of the Agreement and continue in full force and effect.

## 5. DISCLAIMERS AND LIMITATIONS ON LIABILITY

5.1. Remedy. Your 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) You did not promptly report the defect to DigiCert, or (iii) You breached a provision of this agreement.

5.2. Warranty Disclaimers. ALL DIGICERT PRODUCTS AND SERVICES, INCLUDING CERTIFICATES, 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 YOUR 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-related offering at any time.

5.3. Limitation on Liability. EXCEPT AS PROVIDED UNDER SECTION 5.5, YOU WAIVE ALL LIABILITY OF DIGICERT AND ITS AFFILIATES, AND EACH OF THEIR OFFICERS, DIRECTORS, PARTNERS, EMPLOYEES, CONTRACTORS, AND AGENTS, RESULTING FROM OR CONNECTED TO THIS AGREEMENT. YOU ALSO WAIVE ALL LIABILITY FOR ANY DIRECT, 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.

5.4. Force Majeure and Internet Frailties. Neither party is liable for any failure or delay in performing its obligations under this Agreement to the extent that the circumstances causing such failure or delay are beyond a party's reasonably control. You acknowledge that the Certificates are subject to the operation and telecommunication infrastructures of the Internet and the operation of your Internet connection services, all of which are beyond DigiCert's control.

5.5. Applicability. The limitations and waivers in this section 5 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.

5.6. Limitation on Actions. Each party shall commence any claim and action arising from this Agreement within one year from the occurrence of events giving rise to a cause of action. Each party waives its right to any claim that is commenced more than one year from the first date on which the cause of action accrued.

## 6. MISCELLANEOUS

6.1. Liability for Breach. You are liable for any claims (including damages, costs, and defense expenses) that are brought by third parties against DigiCert, its agents, or assigns that are based on your intentional or grossly negligent breach of this Agreement. This includes claims related to the unauthorized use of your Private Key, unless prior to the unauthorized use You notified DigiCert of the compromise and requested revocation of the Certificate.

6.2. Conflict Resolution. All provisions for governing law, jurisdiction, and venue for any arbitration, mediation, or other conflict dispute resolution process shall be as specified in the Sponsor Agreement and such provisions apply equally to this Agreement.

6.3. Independent Contractors. Neither party has the power to bind or obligate the other. Each party is responsible for its own expenses.

6.4. Amendments. DigiCert may amend any of its website and any documents listed thereon, including its CPS and privacy policy, provided that such amendments are adopted and implemented in accordance with the Sponsor Agreement and standard industry practices. Your use of a Certificate after the date an amendment is posted to the website constitutes your acceptance of the amendment.

6.5. Waiver. A party's failure to enforce, or its 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 against whom the waiver is claimed.

6.6. Notices. Unless otherwise specified in the Sponsor Agreement: You shall send all notices in English by first class mail with return receipt request to DigiCert, Inc., 355 South 520 West, Suite 200, Lindon, UT 84042; DigiCert shall send notices to You using the email address provided during the Certificate application process. Notices to DigiCert are effective when received; notices to You are effective when sent.

6.7. Assignment. You may not assign your 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 your consent.

6.8. Severability. The invalidity or unenforceability of a provision under this Agreement, as determined by an arbitrator, 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.

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

6.10. 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.

## 7. GLOSSARY OF TERMS

**"Application Software Vendor"** means a software developer that displays or uses Certificates and distributes root certificates

**"Certificate"** means a digitally signed electronic data file issued by DigiCert to a person, group, or role in order to confirm the identity of that entity as possessing the Private Key that corresponds to the Public Key contained in the certificate.

**"Certificate Beneficiaries"** means your sponsor and any Application Software Vendor or Cross-certified Entity.

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

**"Cross-certified Entity"** means any entity that is cross-signed with any DigiCert CA certificate that an issued Certificate chains to, which may include the Entrust Group, Verizon Business/Cybertrust, the U.S. Federal Bridge CA, or other bridge CAs.

**"Compromise"** means evidence that (i) the hardware device used to store a Private Key is missing, (ii) the Private Key was publicly disclosed, or (iii) that a third party is using a Private Key without authorization.

**"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.

**"Key Pair"** means two mathematically related cryptographic keys—a Private Key and a Public Key.

**"Private Key"** means the key that is kept secret by You that is used to create Digital Signatures and/or decrypt electronic records or files that were encrypted with the corresponding Public Key.

"**Public Key"** means your publically disclosed key that is contained in your Certificate and corresponds to the secret Private Key that You use. The Public Key is used by Relying Parties to verify Digital Signatures created by the Private Key and/or to encrypt messages so that they can only be decrypted by You using the corresponding Private Key.

**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" AND DO NOT PROCEED IF YOU DO NOT ACCEPT THIS AGREEMENT.