Relying Party Agreement

DIGICERT, INC. AND/OR ITS SUBSIDIARIES ("DIGICERT") IS WILLING TO PROVIDE THE SERVICES TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE RELYING ON A DIGICERT SITE SEAL, SSL CERTIFICATE, OR OTHER SITE AUTHENTICATION PRODUCT OR SERVICE ("YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS RELYING PARTY AGREEMENT. YOU ARE REQUIRED TO READ THIS AGREEMENT CAREFULLY BEFORE RELYING ON A DIGICERT SITE SEAL, SSL CERTIFICATE, OR OTHER SITE AUTHENTICATION PRODUCT OR SERVICE. IF YOU DO NOT AGREE TO THE TERMS HEREIN, YOU MAY NOT RELY ON OR USE A DIGICERT SITE AUTHENTICATION PRODUCT OR SERVICE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1.800.896.7973.

You agree as follows:

1. DEFINITIONS

1.1. "Certificate" means an X.509v-3 formatted data structure that is signed by DigiCert.

1.2. "Certificate Chain" means an ordered list of Certificates.

1.3. "CPS" means the written statement of the policies and procedures used to operate DigiCert's PKI infrastructure. The CPS is available on the Repository.

1.4. "Non-verified Subject Information" means information submitted by a Subject and included within a Certificate, that has not been confirmed by DigiCert and for which DigiCert provides no assurances other than the information was submitted by the Subject.

1.5. "Relying Party" means an entity that acts in reliance on the information provided by DigiCert in a Site Seal, Certificate, or other site authentication product or service.

1.6. "Repository" means the collection of documents located on the DigiCert website or the website related to the brand of the issued Certificate; specifically, www.digicert.com, www.websecurity.symantec.com, www.thawte.com, www.geotrust.com, or www.rapidssl.com.

1.7. "Site Seal" means a hyperlinked graphic provided by DigiCert to a Verified Identity for display on the Subject's website.

1.8. "Subject" means the entity that is listed in a DigiCert product or service as the authorized user of the product or service.

1.9. "Verified Identity" means the identity of the Subject as displayed by or listed in a DigiCert site authentication product or service.

2. USE

2.1. Applicability. This agreement is effective immediately upon your use of or reliance on a DigiCert site authentication product or service, such as when your SSL-enabled device is presented with a Certificate or when you access a website displaying an authentic DigiCert Site Seal. The agreement lasts for as long as you assert that you have reasonably relied on a DigiCert site authentication product or service.

2.2. Reliance. Subject to the conditions herein, you may rely on DigiCert's products and services for their intended purpose as described on DigiCert's website and in its CPS.

2.3. Limitations on Use. You may not rely on a DigiCert site authentication product or service to control equipment in hazardous circumstances, or with any system where a failure could lead to death, personal injury, or severe environmental damage.

3. CLASSES

3.1. Classes. DigiCert offers three (3) classes of site authentication products or services, with each class providing specific functionality and security features corresponding to a specific level of trust:

(i) DV Certificates. Domain Validated ("DV") Certificates offer a basic level of assurance and should not be used for authentication purposes or to support non-repudiation. DV Certificates can be used for digital signatures, encryption, and access control for non-commercial or low-value transactions where proof of identity is not necessary. DV Certificates are issued based on procedures that assure that the Subject's domain name is associated with a public key. These Certificates do not verify the owner of the Subject.

(ii) OV Certificates. Organization Validated ("OV") Certificates offer a higher level of assurance in comparison with DV Certificates. OV Certificates are issued to individuals and organizations for digital signatures, encryption, and access control, including proof of identity in medium value transactions. Such Certificates may be used for organization authentication under the terms of the CPS. OV Certificate authentication includes verification of information submitted by the Certificate applicant against identity proofing sources.

(iii) EV Certificates. Extended Validation ("EV") Certificates provide the highest level of assurance. EV Certificates are issued to individuals and organizations for digital signatures, encryption, and access control, including proof of identity in high-value transactions. EV Certificates may be issued to devices to provide authentication; message and content integrity; and confidentiality through encryption. EV Certificates provide assurance of the identity of the Subject based on a confirmation that the Subject individual or organization does in fact exist, that the individual or organization has requested the Certificate, and that the person submitting the Certificate application on behalf of the Subject was authorized to do so. EV Certificates also provide assurance that the Subject is entitled to use the domain listed in the Certificate.

4. LIMITED WARRANTY

4.1. Limited Warranty. DigiCert warrants to Relying Parties that: (i) all information in the Certificate, except for Non-verified Subject Information, is accurate as of the date the validation process was complete; (ii) the Certificate has been issued to the individual, organization, or device named in the Certificate as the Subject; and (iii) DigiCert exercised reasonable care to perform the validation process set forth in the CPS for the Certificate. This warranty does not apply to Client Certificates, Code Signing Certificates, intranet Certificates (such as Certificates that do not include a fully qualified domain name), the transaction of non-financial sensitive or private information, or any actions or omissions of a third party, including the Subject. This warranty is void if you breach the terms of this agreement.

4.2. Qualifications. The warranty provided herein only applies if all of the following are true:

(i) Prior to relying on the site authentication product or service, you checked all status information provided by DigiCert related to the site authentication product or service to confirm that the information was still valid and that the product or service had not expired or been revoked. For Certificates, this includes checking to ensure that each Certificate in the Certificate Chain is valid, unexpired, and non-revoked (by using any CRL or OCSP information available). For Site Seals, this includes verifying the Site Seal's authenticity and validity directly with DigiCert and receiving a clear confirmation that the Subject was and remains authorized to display or use the Site Seal.

(ii) Prior to relying on a site authentication product or service, you gathered sufficient information to make an informed decision about the proper use of the authentication product or service and whether your intended reliance on the authentication product or service was reasonable in light of the circumstances. This includes evaluating the risks associated with your intended use and the limitations associated with the site authentication product or service provided by DigiCert.

(iii) Your reliance on the site authentication product or service is reasonable based on the circumstances. Your reliance is not reasonable if (i) there was information reasonably available, or if information was known by or presented to you, that would have led a reasonable person not to conduct business through the site or (ii) you used software or hardware that did not satisfactorily perform the technological procedures required to verify the validity of the relied upon site authentication product or service.

(iv) You relied on the site authentication product or service when conducting an online transaction with the Subject during an SSL/TLS encrypted session and that transaction resulted in a fraudulent charge.

(v) You disputed the unauthorized charge with any applicable service provider in accordance with the conditions and terms of the service provider, but the service provider refused to reverse the transaction, issue a refund, or provide other reimbursement for the unauthorized charge.

(vi) You submit the claim via email to support@digicert.com within 60 days after the transaction occurs. A failure to submit the claim via email within the required 60-day period constitutes a conclusive waiver of the claim. The email claim must include your contact information (name, street address, phone number and e-mail address); the date of loss and a detailed description of the events and circumstances related to the loss; the website URL and Subject name through which the loss occurred; the amount of the loss; information about the service providers involved in the financial transaction (credit card issuer, bank providing the wire transfer, etc.); and a description of any additional information, logs, records or supporting information that you have.

(vii) You cooperate fully with any investigation of your claim, including providing additional information and granting rights of subrogation, if requested.

4.3. Processing. Within 30 days after receiving your email and all supporting documentation (including a determination from any applicable service provider concerning any reversal, reimbursement, or refund of the charge), DigiCert will determine the amount eligible for reimbursement. If you do not receive a response from DigiCert within 60 days of submitting all supporting documentation, then the claim is deemed denied. If you are not satisfied with DigiCert's initial determination of your claim, then, within 30 days of the denial or partial denial, you must send a notice by certified mail to DigiCert requesting a legal review of your claim. Your failure to send such notice under this mandatory procedure within 30 days after initial denial of the claim constitutes waiver of appeal and DigiCert's initial determination is final, binding, and a complete defense and bar to any attempt at judicial review on the ground of failure to exhaust administrative remedies.

5. DISCLAIMERS AND LIMITATIONS ON LIABILITY

5.1. Warranty Disclaimers. DIGICERT'S SITE AUTHENTICATION PRODUCTS AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". THE USE OF A PRODUCT AND/OR SERVICE IS AT YOUR OWN RISK. EXCEPT FOR THE LIMITED WARRANTY UNDER SECTION 4.1, DIGICERT DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, AND ANY WARRANTY ARISING OUT OF A COURSE OF PERFORMANCE, DEALING OR TRADE USAGE. 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 WARRANT ANY THIRD PARTY PRODUCT OR SERVICE, INCLUDING ANY WEBSITE THAT IS SECURED BY A DIGICERT CERTIFICATE OR DISPLAYING A DIGICERT SITE SEAL.

5.2. Limitations on Reimbursement. If DigiCert breaches the warranty made in Section 4.1, and if you meet the requirements in Section 4.2, and if you are in compliance with this agreement, then DigiCert will reimburse you for the actual unreimbursed unauthorized charge according to the class of the certificate relied upon and limited, per Relying Party and in the aggregate, to the amounts set forth below:

Class	Liability Cap
DV	$100 USD (or the local currency equivalent thereof) per Relying Party per certificate. $1,000 USD (or the local currency equivalent thereof) aggregate per certificate.
OV	$5,000 USD (or the local currency equivalent thereof) per Relying Party per certificate. $50,000 USD (or the local currency equivalent thereof) aggregate per certificate.
EV	$10,000 USD (or the local currency equivalent thereof) per Relying Party per certificate. $100,000 USD (or the local currency equivalent thereof) aggregate per certificate.

DigiCert's total liability for all damages sustained by all Relying Parties is $2,000,000 USD in the aggregate ("Aggregate Limit"). DigiCert administers all claims on a first-come, first-serve basis. You may only make one warranty claim related to a transaction regardless of whether you relied on multiple products and services on the same website (e.g., you may not make a warranty claim for both a Site Seal and Certificate used on the same site or with the same transaction). Payments made to you or another Relying Party by DigiCert will decrease the amount available to all other Relying Parties under the applicable aggregate limit in the table in this Section 5.2 or the Aggregate Limit. If the applicable aggregate limit in the table in this Section 5.2 or the Aggregate Limit is met then you waive DigiCert of any liability for all remaining unreimbursed unauthorized charges, regardless of whether any amount was actually paid to you.

5.3. Limitation on Liability. EXCEPT FOR CLAIMS UNDER SECTION 4 (WHICH ARE SUBJECT TO THE LIMITS SET FORTH IN SECTION 5.2), YOU HEREBY WAIVE ALL LIABILITY OF DIGICERT AND ITS OFFICERS, DIRECTORS, PARTNERS, EMPLOYEES, CONTRACTORS, AND AGENTS, RESULTING FROM OR CONNECTED TO THE RELIANCE ON OR USE OF DIGICERT'S SITE AUTHENTICATION PRODUCTS AND SERVICES, INCLUDING ANY LOSS RELATED TO THE ACTIONS OR OMISSIONS OF A SUBJECT OR OTHER THIRD PARTY. YOU WAIVE ALL LIABILITY FOR ANY SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RELATED TO THIS AGREEMENT OR A DIGICERT PRODUCT OR SERVICE, 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 reasonable control. You acknowledge that DigiCert's products and services 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 waivers and limitations 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.

6. INDEMNIFICATION

6.1. Indemnification. You agree to indemnify, defend, and hold harmless DigiCert and its contractors, agents, employees, officers, directors, shareholders, affiliates, and assigns against all liabilities, claims, damages, costs, and expenses, including reasonable attorney's fees, related to (i) your failure to comply with this agreement, (ii) your improper use of, or unreasonable reliance on, a DigiCert product or service, or (iii) your failure to check the status of a Certificate to determine if the Certificate is expired or revoked.

6.2. Indemnification Procedure. DigiCert will promptly notify you of any such claim, and you will bear full responsibility for the defense of such claim (including any settlements), provided that (i) you inform and consult with DigiCert about the progress of any litigation or settlement; (ii) any settlement does not stipulate any liability or wrong-doing by DigiCert, and (iii) any settlement does not require specific performance by DigiCert. DigiCert may elect to participate in the defense of a claim using counsel of its choice at its own expense. The terms of this Section 6 will survive any termination of this agreement.

7. MISCELLANEOUS

7.1. Entire Agreement. This agreement constitutes the entire agreement between the parties with respect to your reliance on DigiCert's products and services, superseding all other agreements that may exist. DigiCert may, without notice, amend this agreement and the conditions under which you may rely on a DigiCert site authentication product or service. Amendments are effective when posted to DigiCert's website. You must periodically review the website to be aware of any changes.

7.2. Notices. Other than your claim made under this agreement, which will be submitted in accordance with Section 4.2(vi), you will send all notices in English writing by mail with return receipt request to DigiCert, Inc., Attn: Legal Department, 2801 North Thanksgiving Way, Suite 500, Lehi, UT 84043. DigiCert will post notices to you on its website.

7.3. Assignment. You will not assign any of 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.

7.4. Dispute Resolution. At least 60 days before filing a suit or initiating an administrative claim, you will notify DigiCert and any other party to the dispute and attempt to settle the dispute in good faith via a business discussion.

7.5. Governing Law and Jurisdiction. This agreement and any disputes relating to the performance hereunder will be governed, interpreted, and enforced in accordance with the laws of the State of Utah, USA, without regards to any conflict-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, USA. The United Nations Convention on Contracts for the International Sale of Goods does not apply to this agreement.

7.6. 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 will 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.

7.7. Rights of Third Parties. No third party has any rights or remedies under this agreement.

7.8. Compliance with Law. Each party will comply with all applicable federal, state, and local laws and regulations in connection with its performance under this agreement. You hereby acknowledge and agree that the technology you are accessing may be subject to applicable export control, trade sanction, and physical or electronic import laws, regulations, rules and licenses. DigiCert reserves the right to suspend performance of any of its obligations under this agreement, without any prior notice being required and without any liability to you, if you fail to comply with this provision.

7.9. 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.

Last updated on 17th September 2018