digicert®

ENTERPRISE MANAGED PKI ACCESS AGREEMENT

This enterprise managed PKI access agreement is effective on 23 December 2013 ("Effective Date") and is between DigiCert, Inc., a Utah corporation ("**DigiCert**") and the entity indicated below ("**Customer**").

Background

DigiCert is a trusted third party certification authority and experienced provider of ITU X.509 v.3 digital certificates ("**Certificates**"). DigiCert operates a web-based interface and related API that facilitates and simplifies management of Certificates. Customer desires to use a DigiCert system account and API (collectively, "**Account**") to manage Certificates on domain names owned or controlled by Customer.

Agreement

DigiCert agrees to provide, and Customer agrees to use, the Account in accordance with DigiCert's *Terms and Conditions for Use of Managed PKI Services*, attached, which are hereby incorporated by reference as part of this agreement (this agreement, the attached terms, and all schedules, if any, are referred to collectively as the "**Agreement**").

This Agreement commences on the Effective Date and lasts for a term of three years. At the end of the Agreement, the Agreement automatically renews, without notice, for successive one year terms unless either (i) this Agreement is terminated in accordance with the attached *Terms and Conditions for Use of Managed PKI Services* or (ii) a party gives 30 days notice prior to the end of the then-current term to the other party that the Agreement will terminate without renewal.

INITIAL PRIMARY ADMINISTRATOR:	
Name	Thomas Morse
Title	Senior Director of IT and SaaS Operations
Address	303 2nd St., North Tower, 8th floor
Address	San Francisco, CA 94107
Phone	
Email	ops@appdynamics.com
Fax	

Other Administrators (Attach list if needed)	
Name	
Email	
Phone	
Name	
Email	
Phone	

CUSTOMER BILLING INFORMATION	
Attn:	Tom Pham
Address	303 2nd St., North Tower, 8th floor
Address	San Francisco, CA 94107
Phone	415-442-3070
Email	accountspayable@appdynamics.com
Fax	

CUSTOMER CONTACT INFORMATION	
Attn:	Thomas Morse
Address	303 2nd St., North Tower, 8th floor
Address	San Francisco, CA 94107
Phone	
Email	ops@appdynamics.com
Fax	

AppDynamics ("CUSTOMER")	
By:	DocuSigned by: Dan Wright
Name	Dan Wright
Title	Director of Legal
Date	23 December 2013

DIGICERT, INC.	
By:	
Name	Nicholas E Hales
Title	CEO
Date	26 December 2013

Terms and Conditions for Use of Managed PKI Services

1. Definitions.

1.1. **"Administrator"** means an individual with access rights that grant authorization to (i) manage Authentication Mechanisms, (ii) approve Certificate requests, and (iii) designate other individuals either as Administrators or as general Account users without full control over the Account.

1.2. **"Affiliate"** means a parent, subsidiary, or present or future company that controls, is controlled by, or is under common control with Customer. As used in this definition, 'control' (and its correlative meanings, 'controlled by' and 'under common control with') means possession, directly or indirectly, of the power to: (i) direct the management, personnel, finances, or plans of such entity; (ii) control the election of a majority of the directors; or (iii) vote that portion of voting shares required for "control" under law but in no case less than 10%.

1.3. **"Application Software Vendors"** means an entity that displays or uses Certificates in connection with a distributed root store in which DigiCert participates or will participate.

1.4. **"Authentication Mechanism"** means any method of authenticating an individual's right to access the Account, including any username, login ID, password, code, number, or cryptographic key.

1.5. **"Business Day"** means Monday to Friday inclusive, excluding U.S. Federal Holidays, which are set forth in 5 U.S.C. § 6103.

1.6. **"Certificate"** has the meaning assigned to it on the first page of the Agreement and includes both SSL Certificates and Client Certificates.

1.7. **"Certificate Beneficiary"** means an Application Software Vendor or Relying Party.

1.8. **"Certificate Practices Statement"** or **"CPS"** means DigiCert's written statement of the policies and practices used to operate its PKI infrastructure. DigiCert's CPS documents are available at http://www.digicert.com/ssl-cps-repository.htm.

1.9. **"Client Agreement"** means a DigiCert agreement with the subject of a Client Certificate that dictates the terms of use for Client Certificates.

1.10. **"Client Certificate"** means an S/MIME certificate used by agents, employees, and contractors of the Customer to encrypt and add a Digital Signature to emails.

1.11. **"Compromise"** means evidence that (i) a hardware device used to store a Private Key is missing, (ii) the Private Key was publicly disclosed, or (iii) a third party is using a Private Key in a manner that does not conform with industry standards.

1.12. **"Confidential Information"** means any information, documentation, system, or process disclosed by a party or a party's affiliates that is (i) designated as confidential (or a similar designation) at the time of disclosure, (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.

1.13. **"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.

1.14. **"EV Certificate"** means a Certificate that contains the DigiCert Extended Validation Certificate Policy Object Identifier of 2.16.840.1.114412.2.1 and is issued in accordance with the EV Guidelines.

1.15. **"EV Guidelines"** means the Extended Validation Guidelines published by the CA/Browser Forum and made public through the www.cabforum.org website.

1.16. **"Key Set"** means a set of two or more mathematically related keys, referred to as Private Keys or key shares along with a Public Key, having the properties that (i) the Public Key can encrypt a message which only the Private Key(s) can decrypt, and (ii) even knowing the Public Key, it is computationally infeasible to discover the Private Key(s).

1.17. **"Private Key"** means the key or key share of a Key Set that is used to create a Digital Signature and is kept secret.

1.18. **"Public Key"** means the key of a Key Set that is used to verify a Digital Signature and is publicly disclosed.

1.19. **"Relying Party"** means an entity other than Customer 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.

1.20. **"Relying Party Warranty"** means a warranty offered to a Relying Party that meets the conditions found in the *Relying Party Warranty Agreement* posted on DigiCert's website at http://www.digicert.com/docs/agreements/DigiCert_RPA.pdf.

1.21. **"Revoke"** means to make a Certificate ineffective from a specified time forward. DigiCert Revokes a Certificate by issuing an OCSP response. The term does not imply that a revoked Certificate is destroyed or made illegible.

1.22. **"Site Seal"** means a logo or trademark provided by DigiCert for use on a website that is associated with a domain using a Certificate to encrypt TLS/SSL communication.

1.23. **"SSL Certificate"** means a Certificate used to encrypt TLS/SSL communication.

1.24. **"Subscriber"** means a person, entity, or organization that is the system or device owner identified in, the subject named in, or otherwise identified in a Certificate.

2. Account License.

2.1. Qualifications. Prior to providing access to the Account, DigiCert may verify Customer's existence and operations in accordance with the CPS. DigiCert may terminate this Agreement, without liability other than a refund of the fees paid by Customer, if DigiCert is unable to verify Customer to DigiCert's reasonable satisfaction, within thirty (30) days after the Effective Date.

2.2. License. DigiCert grants Customer a limited, non-exclusive, non-transferable, and non-sublicenseable license to use the Account, through either the API or DigiCert's provided web interface and using approved Authentication Mechanisms, to order and approve Certificates for use by Customer, an Affiliate of Customer, or a third party designated by Customer who is hosting systems on behalf of Customer and for conducting Customer's business.

2.3. Maintain Account Security. Customer shall ensure that each Account User maintains the confidentiality of its Authentication Mechanisms and is solely responsible for ensuring that the individuals and systems accessing the Account and requesting Certificates are authorized to do so. DigiCert is not liable for any loss incurred as a result of Customer's disclosure of its Authentication Mechanisms, either with or without Customer's knowledge or authorization. Customer is responsible for all activity in its Account, including any liability incurred by DigiCert or a third party resulting from someone else's use of the Account, unless any unauthorized access is due to an act or omission of DigiCert. Each Party shall notify the other Party immediately if it becomes aware that there is any unauthorized use of or any other breach in the security of Customer's Account.

2.4. Reporting of Errors. Customer shall document and promptly report to DigiCert any errors or malfunctions associated with the Certificates or Account. Customer shall promptly assist DigiCert in rectifying any errors or malfunctions in the Certificates or Account upon DigiCert's reasonable request.

3. Certificate Issuance.

3.1. Applicability. This Agreement applies to each Certificate issued by DigiCert to Customer, regardless of (i) the Certificate type (email, code signing, or TLS/SSL), (ii) when the Customer requested the Certificate, or (iii) when the Certificate issues. This Agreement constitutes the subscriber agreement, as required under industry standards, for all Certificates issued through the Account.

3.2. Requests. Customer may request SSL Certificates only for domain names registered to Customer, an Affiliate of Customer, or an entity that expressly authorizes DigiCert to allow Customer to obtain and manage Certificates for the domain name. DigiCert may limit the number of domain names that Customer may include in a single Certificate in its sole discretion.

3.3. Administrators. Customer authorizes each Administrator in the Account to act as a Certificate Requester, Certificate Approver, and Contractor Signer (as defined in the EV Guidelines) and to communicate with DigiCert regarding the management of Key Sets and Certificates. Customer may revoke this authority by sending notice to DigiCert. Customer is responsible for all Certificates requested by an Administrator until the Administrator's authority is revoked. Customer is responsible for periodically reviewing and reconfirming which individuals have Certificate authority. If Customer wishes to remove an Administrator or other user from the Account, then Customer shall take the steps necessary to prevent the user's access to the Account, including changing the Authentication Mechanisms.

3.4. Verification. After receiving a Certificate request through the Account, DigiCert will review the request and attempt to verify the relevant information in accordance with the DigiCert CPS and industry guidelines. Verification is subject to DigiCert's sole satisfaction, and DigiCert may refuse to issue a Certificate for any reason. DigiCert shall notify Customer if a certificate request is refused; however, DigiCert is not required to provide a reason for the refusal.

3.5. Certificate Life Cycle. The lifecycle of an issued Certificate depends on the selection made by Customer when ordering the Certificate, the requirements in the CPS, and the intended use of the Certificate. DigiCert may modify Certificate lifecycles for unissued Certificates as necessary to comply with requirements of (i) this Agreement, (ii) industry standards, (iii) DigiCert's auditors, or (iv) an Application Software Vendor. Customer shall not use Certificates after their expiration date. Certificates containing internal server names or private IP addresses must expire on or before Nov 1, 2015.

3.6. Certificate Issuance. If verification is completed to DigiCert's satisfaction, DigiCert will issue the requested Certificate and deliver the Certificate to Customer. DigiCert may deliver the Certificate using any reasonable means of delivery. Typically, DigiCert will deliver Certificates via email to an address specified by Customer, as an electronic download in the Account, or in response to an API call made by Customer. 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. The terms in Schedule 1 apply to the issuance and use of each Certificate.

3.7. Client Certificates. If Client Certificates are included as part of this Agreement, then the following applies:

(i) Prior to confirming a Client Certificate request, Customer shall (i) confirm the identity and affiliation of the requester using appropriate internal documentation, such as human resources and network schematics, (ii) confirm that the Certificate meets the minimum issuance requirements set forth in the CPS, and (iii) confirm that the information provided and representations related to or incorporated in any Certificate are true, complete, and accurate in all material respects.

(ii) Prior to providing a Client Certificate, the Subject of the Certificate must accept a Client Agreement, which acceptance may occur electronically. DigiCert may present the Client Agreement automatically to users through the Account and may amend the Client Agreement without notice.

(iii) Each Administrator is appointed as a trusted agent for the sole purpose of requesting, issuing, managing, and requesting revocation of Client Certificates. Customer shall retain documentation showing Customer's affiliation with each individual who receives a Client Certificate under this Agreement from the time of issuance until at least one year after the Client Certificate's expiration date. Customer shall provide this documentation to DigiCert within two days after receiving a request for such information. If Customer fails to provide this documentation upon request, DigiCert may, in addition to any other remedies available to DigiCert, revoke all Client Certificates issued under this Agreement and terminate this Agreement.

(iv) DigiCert may revoke an Administrator's appointment as a trusted agent at any time. If this appointment is revoked, DigiCert shall validate any additional Client Certificates ordered under this Agreement.

3.8. EV Certificates. To the extent permitted under section 12.2.2 of the EV Guidelines, DigiCert may allow Customer to act as an "Enterprise Registration Authority" (Enterprise RA) and assist in the issuance of EV Certificates that list the Customer or an Affiliate as the subject. When acting as an Enterprise RA, Customer shall, at all times, follow the EV Guidelines. If DigiCert allows Customer to act as an Enterprise RA then:

(i) DigiCert shall perform all validation procedures required to issue EV Certificates to Customer's top level domains.

(ii) Customer may request the issuance of EV Certificates for subdomain levels that are contained within the top level domain that DigiCert has verified in accordance with the EV Guidelines. Customer shall follow the EV Guidelines and the CPS when requesting and using EV Certificates.

(iii) Customer may authorize at least one of its employees having the training and skill required by the EV Guidelines to perform the final cross-correlation and due diligence required by section 10.12 of the EV Guidelines. In all cases, the subject of each EV Certificate issued must be Customer or an Affiliate of Customer verified by DigiCert in accordance with the EV Guidelines.

(iv) Customer shall retain sufficient documentation to show its compliance with the EV Guidelines in approving the issuance of each EV Certificate and make this documentation available to DigiCert upon request

4. Site Seals.

4.1. Site Seal Licenses. Customer may display a Site Seal on any website used on a domain name secured by a DigiCert Certificate. If a Certificate securing a domain displaying a Site Seal is revoked or expires, Customer's license to display the Site Seal is also revoked unless a replacement Certificate is issued by DigiCert. Customer may not alter the Site Seal in any way, including any change to the Site Seal's size.

4.2. Limitations on Use. Customer may use only the latest version of the Site Seal and only to indicate that Customer is a recipient of DigiCert's services. Customer may not display a Site Seal on any website if (i) the display would lead a reasonable person to believe that DigiCert guarantees a non-DigiCert product or service, (ii) the site contains content that is misleading, illegal, libelous, or otherwise objectionable to DigiCert, or (iii) the display could harm or limit DigiCert's rights in the Site Seal or DigiCert's business reputation.

5. Fees.

5.1. Certificate Fees. Customer shall pay DigiCert a service fee for each ordered Certificate in accordance with the Fee Schedule attached as Schedule 2 to this Agreement. If Customer is paying for the Certificate on a cash basis, then Customer shall pay DigiCert when the request is made through the Account. If Customer is paying for the Certificate with a purchase order, then Customer shall pay DigiCert the fees within thirty (30) days after receiving an accurate invoice from DigiCert. DigiCert may amend the fees listed on Schedule 2 at any time by providing Customer 30-days prior notice of the amendment, provided that any such increases will not go into effect until the renewal of any Certificates.

5.2. Late Payments. Intentionally omitted.

5.3. Taxes. This Agreement is entered into, and all of the services are performed and provided, entirely within the United States of America. All fees for services are exclusive of any taxes however imposed, e.g. sales tax, income tax, GST, or VAT. Customer will pay all tax obligations resulting from Customer's acceptance of this Agreement, including sales tax, Customer's income tax, GST, or VAT, if such taxes are separately itemized on an invoice to Customer. Customer may not withhold or offset any amount owed to DigiCert for any reason. If a withholding or deduction is required by law, then Customer shall pay an additional fee that is equal to the amount withheld, causing DigiCert to receive a net amount from Customer that is equal to the amount DigiCert would receive if a withholding or deduction was not required.

6. **Intellectual Property Rights.**

6.1. DigiCert Intellectual Property Rights. DigiCert retains, and Customer shall not obtain or claim, any title, interest, and ownership rights in:

(i) the Certificates, API, and Account, including all software associated with the Account and API and any techniques and ideas embedded therein,

(ii) all copies or derivative works of the Certificates or software provided by DigiCert, regardless of who produced, requested, or suggested the copy or derivative work,

(iii) all documentation and marketing material provided by DigiCert to Customer (excluding any documentation or marketing material originally provided by Customer), and

(iv) all of DigiCert's copyrights, patent rights, trade secret rights and other proprietary rights.

6.2. Restrictions. Each party shall protect the other party's intellectual property, good will, and reputation when accessing or using the other party's services or products. Customer may not decompile or create derivative works of the Certificates or Account without the prior written consent of DigiCert. DigiCert may terminate this Agreement or restrict access to the Account if DigiCert reasonably believes that Customer is using the Account or Certificates to post or make accessible any material that infringes DigiCert's or any third party's rights. Customer shall not use any marketing material or documentation that refers to DigiCert, the Site Seals, or the Certificates without receiving written prior approval from DigiCert. Customer shall use only facts that DigiCert itself uses in its non-confidential written materials when referring to the Account or Certificates.

6.3. Use of Trademarks. Customer shall not register a DigiCert trademark or any confusingly similar mark. Customer shall not use any DigiCert trademark as part of Customer's trade names or domain names. Customer shall not use the Account or Certificates in a way intended to diminish or damage DigiCert's reputation, including using a Certificate with a website that could be considered associated with crime, defamation, or copyright infringement.

7. **Confidentiality.**

7.1. Obligations. 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. Customer consents to (i) DigiCert's public disclosure of information embedded in an issued Certificates and (ii) DigiCert's transfer of Customer's information to servers located inside the United States. This consent survives termination of this Agreement.

7.3. Storage and Use of Information. DigiCert shall comply with this Agreement when receiving and using information from the Customer. Customer authorizes communication from DigiCert about ordered products and similar services unless Customer unsubscribes.

8. **Termination.**

8.1. Termination for Breach. (A) DigiCert may terminate the Agreement immediately if (i) Customer materially breaches this Agreement and fails to remedy the material breach within twenty Business Days after receiving notice of the material breach, (ii) Customer has engaged in illegal or fraudulent activity, (iii) DigiCert cannot verify Customer to its reasonable satisfaction within thirty (30) days after the Effective Date, or (iv) if Customer (a) has a receiver, trustee, or liquidator appointed over substantially all of its assets, (b) has an involuntary bankruptcy proceeding filed against it that is not dismissed within 90 days of filing, or (c) files a voluntary petition of bankruptcy or reorganization. (B) Customer may terminate the Agreement immediately if DigiCert materially breaches this Agreement and fails to remedy the material breach within twenty Business Days after receiving notice of the material breach, and for clarity, any Certificates and Site Seals issued prior to such termination will survive and remain in effect until the natural expiration of such Certificates and Site Seals.

8.2. Events Upon Termination. If this Agreement is terminated under Section 8.1(A), then DigiCert may revoke the Certificates and Site Seals issued under the Agreement. Otherwise, all Certificates and Site Seals issued prior to termination will remain valid until the earlier of the Certificate's validity period and the Certificate is revoked as allowed herein, and Customer may continue to use those Certificates in accordance with Schedule 1. All other rights and licenses granted to Customer terminate immediately upon termination of this Agreement. Upon termination, Customer shall:

(i) immediately discontinue all representations or statements that could infer that a relationship exists between DigiCert and Customer,

(ii) immediately cease using DigiCert's trademarks and make any transfers requested by DigiCert to ensure that all rights in the trademarks remain with DigiCert,

(iii) within thirty days pay to DigiCert any fees, or part thereof, still owed as of the date of termination,

(iv) within ten days, destroy or deliver to DigiCert all sales manuals, price lists, literature and other materials relating to DigiCert, and

(v) continue to comply with the confidentiality requirements in this agreement.

Upon termination, DigiCert will provide a refund for Certificates that are prepaid but will not issue under the Agreement, but is not required to provide a refund for any issued certificates.

8.3. Survival. The conditions in Schedule 1 survive termination of this Agreement until all Certificates issued expire or are revoked. In addition, the obligations and representations of the parties under Sections 7 (Confidentiality), 9 (Limitation of Liability), 10 (Indemnity), and 11 (Miscellaneous) survive termination of this Agreement. All amounts owed by Customer for services and products ordered prior to termination remain owed after termination of this Agreement.

9. Disclaimer of Warranties and Limitation of Liability.

9.1. Relying Party Warranties. Customer acknowledges that the Relying Party Warranty is only for the benefit of Relying Parties. Customer 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. Warranty Disclaimers. THE ACCOUNT, CERTIFICATES, AND ANY RELATED SOFTWARE ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET CUSTOMER'S EXPECTATIONS OR THAT ACCESS TO THE ACCOUNT WILL BE TIMELY OR ERROR-FREE. DigiCert does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

9.3. Limitation on Liability. This Agreement does not limit a party's liability for (i) death or personal injury resulting from the negligence of a party or (ii) fraud or fraudulent statements made by a party. EXCEPT AS STATED ABOVE AND EXCLUDING EACH PARTY'S INDEMNIFICATION OBLIGATIONS, EACH PARTY'S MAXIMUM LIABILITY RESULTING FROM THIS AGREEMENT IS LIMITED TO THE AMOUNT PAID BY CUSTOMER TO DIGICERT DURING THE 12 MONTHS PRIOR TO WHEN THE LIABILITY OCCURRED. NEITHER PARTY IS LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OR ANY LOSS OF

PROFIT, REVENUE, DATA, OR OPPORTUNITY, EVEN IF SUCH PARTY IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES.

9.4. Extent. The limitations in this section apply 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 claims of liability, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this Agreement were breached or proven ineffective.

10. Indemnity.

10.1. Obligation. Customer shall indemnify and defend DigiCert and its employees, officers, directors, shareholders, Affiliates, and assigns against all third party claims and all resulting liabilities, damages, and costs, including reasonable attorneys' fees, payable to a third party and arising from (i) Customer's failure to protect the Authentication Mechanisms used to secure the Account, (ii) an allegation that personal injury or property damage caused by the fault or negligence of Customer, (iii) Customer's failure to disclose a material fact related to the use or issuance of the Account or Certificate, or (iv) an allegation that the Customer, or an agent of Customer, used DigiCert's products or services to infringe on the rights of a third party. Customer's indemnification obligations under this section are limited to direct damages only, provided that any amount that DigiCert is required to pay to a third party is deemed a direct damage. DigiCert shall indemnify and defend Customer and its employees, officers, directors, shareholders, Affiliates, and assigns against all third party claims and all resulting liabilities, damages, and costs, including reasonable attorneys' fees, payable to a third party and arising from (i) DigiCert's failure to protect the Authentication Mechanisms used to secure the Account, (ii) an allegation that personal injury or property damage caused by the fault or negligence of DigiCert, (iii) an allegation that DigiCert's trademarks, products or services infringe on the rights of a third party, provided that such allegation is based on Customer's use of the products or services in accordance with the CPS.

10.2. Indemnification Procedure. An entity seeking indemnification under this Agreement ("**Indemnified Party**") must notify the other party ("**Indemnifying Party**") promptly of any event requiring indemnification. However, an Indemnified Party's failure to notify will not relieve the Indemnifying Party from its indemnification obligations, except to the extent that the failure to notify materially prejudices the Indemnifying Party. The Indemnifying Party may assume sole control of the defense of any proceeding requiring indemnification. The Indemnified Party will reasonably cooperate in the defense and settlement of any such claim at the Indemnifying Party's expense. The Indemnifying Party may not settle any proceeding related to this Agreement unless the settlement also includes an unconditional release of liability for all Indemnified Parties.

10.3. Additional Liability. The Indemnifying Party's indemnification obligations are not the Indemnified Party's sole remedy for the other party's breach of this Agreement and are in addition to any other remedies that the Indemnified Party may have against the Indemnifying Party under this Agreement.

11. Miscellaneous.

11.1. Independent Contractors. DigiCert and Customer 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.

11.2. Force Majeure. 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. Customer acknowledges that the Account and Certificates are subject to the operation and telecommunication infrastructures of the Internet and the operation of Customer's Internet connection services, all of which are beyond DigiCert's control.

11.3. Entire Agreement. This Agreement, along with all documents referred to herein, constitute the entire agreement between the parties with respect to the subject matter, superseding all other prior agreements that might exist.

11.4. Amendments. Except as otherwise allowed herein, neither party may amend this Agreement unless the amendment is both in writing and signed by the parties. DigiCert may amend any of its (i) website and any documents listed thereon, (ii) CPS, or (iii) privacy policy. Amendments to the foregoing (i) through (iii) are effective upon Customer's receipt of the amendment by DigiCert posting notice in the Account. If an amendment materially affects Customer's rights herein, Customer may terminate the Agreement within 30 days of the effective date of the amendment after providing DigiCert notice of termination, and DigitCert will (within thirty days after termination) provide a pro-rata refund of any pre-paid fees for Certificates that will not issue under the Agreement.

11.5. 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.

11.6. Notices. DigiCert shall send notices of termination or breach of this Agreement to Customer by first class mail at the address listed on the first page of the Agreement, which notices are effective upon receipt. DigiCert shall send all other notices by posting the notice in the Account. All such notices are effective when posted. Customer shall send DigiCert notices in writing by postal mail that is addressed to DigiCert, Inc., Attn: Legal Department, 2600 West Executive Parkway, Suite 500, Lehi, Utah 84043. Notices from each Party are effective upon receipt.

11.7. Assignment. Customer shall not assign any of its rights or obligations under this Agreement without the prior written consent of DigiCert, provided that Customer may assign this Agreement without consent to a successor to all or substantially all of its assets or business. Any other transfer without consent is void and a material breach of this Agreement. DigiCert may assign its rights and obligations without Customer's consent by providing written notice to Customer.

11.8. Governing Law and Jurisdiction. The laws of the state of Delaware 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.

11.9. 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.

11.10. Rights of Third Parties. Except as stated in Schedule 1, no third parties have any rights or remedies under the agreement.

11.11. 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. This Agreement expressly supersedes any click-through agreement on DigiCert's website. Section headings in this Agreement are for reference and convenience only and are not part of the interpretation of the Agreement.

These terms and conditions were last updated on 2 August 2013.

SCHEDULE 1

Certificate Terms of Use

For each issued Certificate, Customer and DigiCert agree as follows:

1. Certificate License. Effective immediately after delivery and continuing until the Certificate expires or is Revoked, DigiCert grants Customer a revocable, non-exclusive, non-transferable license to use, for the benefit of the Certificate's subject, each issued Certificate for the purposes described in the CPS and in accordance with the Certificate Terms of Use set forth in this Agreement. Customer shall not install or use a Certificate until after Customer has reviewed and verified the accuracy of the data included in the Certificate. Customer may install and use each Certificate and its corresponding Key Set (i) in compliance with law, (ii) for authorized company business, and (iii) in accordance with DigiCert's CPS. Each Party shall promptly inform the other Party if it becomes aware of any misuse of a Certificate, Private Key, or the Account. Customer is responsible for obtaining and maintaining any authorization or license necessary to use a Certificate, including any license required under United States' export laws.

2. Management. DigiCert will generally issue, manage, renew, and/or Revoke a Certificate in accordance with any instructions submitted by Customer through the Account or API and may rely on such instructions as accurate. 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 prior to expiration.

3. Security and Use of Key Sets. Customer shall protect the Key Sets associated with a Certificate and take commercially reasonable steps designed to prevent the Compromise, loss or unauthorized use of a Private Key associated with a Certificate. To minimize internal risk of Private Key Compromise, Customer shall only allow employees, agents, and contractors to access or use Private Keys if the employee, agent, or contractor has undergone a background check by Customer (to the extent allowed by law) and has training or experience in PKI and other information security fields. Customer shall request revocation of any Certificate if Customer has reason to believe that the integrity or reliability of a Certificate is compromised. If Customer suspects misuse or Compromise of a Private Key, Customer shall promptly notify DigiCert, cease using the Certificate, and request revocation of the Certificate. Customer shall promptly cease all using the Key Set corresponding to a Certificate upon the earlier of (i) revocation of the Certificate and (ii) the date when the allowed usage period for the Key Set expires.

4. Defective Certificates. If a Certificate contains a defect, DigiCert shall cure the defect promptly after receiving notice from Customer. DigiCert is not obligated to correct a defect if (i) Customer misused, damaged, or modified the Certificate, (ii) Customer did not promptly report the defect to DigiCert, or (iii) Customer has breached any material provision of this Agreement

5. Accurate Information. Customer shall notify DigiCert within ten Business Days if any information included in a Certificate or provided to DigiCert by Customer changes. Customer shall respond to any inquiries from DigiCert regarding the validity of information provided by Customer within ten Business Days after Customer receives notice of the inquiry. Customer's failure to respond to a request from DigiCert within twenty Business Days constitutes a material breach of this Agreement. DigiCert may rely on and use any information provided by Customer for any purposes connected to the services, provided that such use is in compliance with this Agreement. If any information provided by Customer is false or misleading, DigiCert may terminate this Agreement in accordance with Section 8.1(i) of the Agreement, Revoke any Certificates issued to Customer, and close the Account.

6. Representations. For each requested Certificate, Customer represents to DigiCert that:

   (a) Customer has the right to use or is the lawful owner of (i) any domain name(s) specified in the Certificate and (ii) any organization name specified in the Certificate,

   (b) the individual accepting this Agreement is expressly authorized by the Customer to sign this Agreement for the Customer,

   (c) Customer has read, understands, and agrees to the CPS, and

   (d) the organization included in the certificate and the registered domain name holder is aware of and approves of each Certificate request.

By accepting this Agreement, the signer is entering into a legally valid and enforceable agreement to obtain a form of digital identity for the Customer. The signer acknowledges that he/she has the authority to obtain the digital equivalent of a company stamp, seal, or officer's signature to establish the authenticity of the Customer's website, and that the Customer is responsible for all uses of an Certificate. By accepting this Agreement on behalf of the Customer, the signer represents that he/she (i) is acting as an authorized representative of the Customer, (ii) is expressly authorized by Customer to sign Agreements and approve Certificate requests on Customer's behalf, and (iii) has or will confirm Customer's exclusive right to use the domain(s) to be included in any issued Certificates.

7. Restrictions. Customer shall only use a TLS/SSL Certificate on the servers accessible at the domain names listed in the issued Certificate. Customer shall not:

(a) modify, sub license, or create a derivative work of any Certificate (except as required to use the Certificate for its intended purpose) or Private Key,

(b) upload or distribute any files or software that are intended to damage the operation of another's computer,

(c) make representations about or use a Certificate except as allowed in the CPS,

(d) impersonate or misrepresent Customer's affiliation with any entity,

(e) use the Account or Certificates in a manner that could reasonably result in a civil or criminal action being taken against Customer or DigiCert,

(f) use a Certificate or Account to breach the confidence of a third party or to send or receive unsolicited bulk correspondence,

(g) intentionally interfere with the proper functioning of the DigiCert website or with any transactions conducted through the DigiCert website,

(h) attempt to use a Certificate to issue other Certificates, or

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

8. Certificate Revocation. DigiCert may Revoke a Certificate with notice sent through the email address listed in the Account for the reasons stated in the CPS, including if DigiCert reasonably believes that:

(a) Customer requested revocation of the Certificate or did not authorize the issuance of the Certificate,

(b) Customer has breached this Agreement or an obligation it has under the CPS,

(c) any provision of this Agreement containing a representation or obligation related to the issuance, use, management, or revocation of the Certificate terminates or is held invalid,

(d) Customer is added to a government prohibited person or entity list or is operating from a prohibited destination under the laws of the United States,

(e) the Certificate contains inaccurate or misleading information,

(f) the Certificate was used outside of its intended purpose or used to sign malicious software,

(g) the Private Key associated with a Certificate was disclosed or Compromised,

(h) the Certificate was (a) used or issued contrary to law, the CPS, or industry standards, or (c) used, directly or indirectly, for illegal or fraudulent purposes,

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

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

After revocation, Customer shall cease using the Certificate and remove the Certificate from all devices where it is installed and cease using the Certificate. If any such revocation without providing Customer with an opportunity to cure the applicable breach in accordance with Section 8.1(i), then DigiCert shall , at its election, either provide a free replacement certificate, if permitted under industry standard and its agreement with the Application Vendors, or provide a pro-rata refund of any pre-paid fees with respect to the remainder of the effective period of such Certificate.

9. Industry Standards. Both parties shall comply with all industry and privacy standards that apply 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.

10. Equipment. Customer is responsible, at Customer's expense, for (i) all computers, telecommunication equipment, software, access to the Internet, and communications networks (if any) required to use the Account or Certificates, and (ii) Customer's conduct and its website maintenance, operation, development, and content.

11. Certificate Beneficiaries. The Certificate Beneficiaries are express third party beneficiaries of Customer's obligations and representations related to the use or issuance of a Certificate. The Certificate Beneficiaries are not express third party beneficiaries with respect to the Account or any DigiCert Software.

SCHEDULE 2

Fees

Customer shall pay the service fee listed below for each Certificate ordered.

Certificate Type	Term		
	1-year	2-year	3-year
SSL Plus Certificate	$175.00	$314.00	$422.00
SSL Wildcard Certificate	$595.00	$1070.00	$1425.00
EV Certificate	$295.00	$469.00	N/A
UC Certificate (up to 4 domains)	$299.00	$539.00	$719.00
Additional UC Domains (per domain)	$39.00	$69.00	$89.00
EV UC Certificate (up to 4 domains)	$488.00	$780.00	N/A

DigiCert will discount the price listed above based on the number of Certificates previously ordered by Customer through the Account. Discount tiers may be modified by DigiCert at any time and are reset if the Agreement terminates without renewal.

Number of Certificates Previously Ordered	Discount
1-15	0%
16-30	5%
31-50	10%
51-100	15%
101+	20%

Customer shall pay all fees listed in this schedule in accordance with Section 5.1.