digicert

DigiCert PKI Platform (MPKI 8.x) Service Description/Services Agreement

SERVICE DESCRIPTION

Use of the DigiCert PKI Platform (MPKI 8.x) and any Certificates requested or issued thereunder will be governed by thefollowing Certificate Terms of Use:

DIGITAL CERTIFICATES BY DIGICERT – TERMS OF USE

These Digital Certificates Terms of Use ("**Certificate Terms of Use**") apply to each digital certificate ("**Certificate**"), whether publicly-trusted TLS/SSL Certificates, Client Certificates (as defined in Section 9), Qualified Certificates (as defined in Section 10), or otherwise, issued by DigiCert, Inc., a Utah corporation or any of its affiliates, including its Qualified Trust Service Providers (collectively, "**DigiCert**") to an entity or person ("**Customer**"), as identified in the DigiCert services management portal and/or related API made available to Customer ("**Portal**") or issued Certificate. The account to access and use the Portal on Customer's behalf is referred to herein as the "**Portal Account**."

By accepting or signing an agreement that incorporates these Certificate Terms of Use by reference (such agreement, together with these terms, collectively, the "**Agreement**"), the accepter or signer (the "**Signer**") represents and warrants that he/she (i) is acting as an authorized representative of the Customer on whose behalf the Signer is accepting this Agreement, and is expressly authorized to sign the Agreement and bind Customer to the Agreement, (ii) has the authority to obtain the digital equivalent of a company stamp, seal, or officer's signature to establish (x) the authenticity of Customer's website, and (y) that Customer is responsible for all uses of the Certificate, (iii) is expressly authorized by Customer to approve Certificate requests on Customer's behalf, and (iv) has or will confirm Customer's exclusive right to use the domain(s) to be included in any issued Certificates.

Customer and DigiCert hereby agree as follows:

1. **Account Users.**

Customer authorizes each individual listed as an administrator in the Portal Account to act as a Certificate Requester, Certificate Approver, and Contract Signer (as defined in the EV Guidelines) and to communicate with DigiCert regarding the management of Certificates and key sets. "**EV Guidelines**" means the Extended Validation Guidelines published by the CA/Browser Forum ("**CAB Forum**") and made publicly available at www.cabforum.org. Customer may revoke this authority by sending notice to DigiCert. Customer is responsible for periodically reviewing and reconfirming which individuals have authority to request and approve Certificates. If Customer wishes to remove a Portal Account user, Customer will take the steps necessary to prevent such user's access to the Portal, including changing its password and other authentication mechanisms for its Portal Account. Customer must notify DigiCert immediately if any unauthorized use of the Portal or Portal Account is detected. Customer affirms that: (i) Customer authorizes DigiCert to scan, gather, and collect data pertinent to DigiCert's services and to automate Certificate renewal and upgrade; (ii) Customer will use the services to scan and automate only the domains, IP addresses, or assets that Customer owns or controls; (iii) Customer will use the services only for its intended purpose as described and marketed by DigiCert and in accordance with the DigiCert Acceptable Use Policy located at https://www.digicert.com/legal-repository.

2. **Requests.**

Customer may request Certificates only for domain names registered to Customer, an affiliate of Customer, or other 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 DigiCert's sole discretion.

3. **Verification.**

After receiving a request for a Certificate from Customer, DigiCert will review the request and attempt to verify the relevant information in accordance with the DigiCert Certification Practices Statement and applicable industry standards, guidelines and requirements, including laws and regulations related to the issuance of Certificates ("**Industry Standards**"). Verification of such requests is subject to DigiCert's sole discretion, and DigiCert may refuse to issue a Certificate for any reason or no reason. DigiCert will notify Customer if a Certificate request is refused but DigiCert is not required to provide a reason for the refusal. **"Certificate Practices Statement"** or **"CPS"** means the applicable written statements of the policies

and practices used by DigiCert to operate its public key infrastructure ("**PKI**"), including applicable Time-Stamp Policies and Statements. DigiCert's CPSs are available at https://www.digicert.com/legal-repository. CPSs for services issued from a QTSP (whether acting in its capacity as a QTSP or otherwise) or an affiliate entity are available at https://www.quovadisglobal.com/repository.

4. 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) the Agreement; (ii) Industry Standards; (iii) DigiCert's auditors; or (iv) an Application Software Vendor. "**Application Software Vendor**" means an entity that displays or uses Certificates in connection with a distributed root store in which DigiCert participates or will participate. Customer agrees to cease using a Certificate and its related Private Key (defined below) after the Certificate's expiration date or after DigiCert revokes a Certificate as permitted in the Agreement.

5. Issuance.

If verification of a Certificate is completed to DigiCert's satisfaction, DigiCert will issue and deliver the requested Certificate to Customer 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 Portal or in response to an API call made by Customer via the Portal. Publicly-trusted Certificates are issued from a 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. Customer will abide by all applicable laws, regulations and Industry Standards when ordering and using Certificates, including United States export control and economic sanctions laws and regulations. Customer acknowledges that the Certificates are not available in countries or regions restricted by the United States Treasury Department's Office of Foreign Assets Control, the United States Commerce Department, the European Commission, the United Kingdom HM Treasury's Office of Financial Sanctions Implementation, or other applicable governmental agencies having jurisdiction over DigiCert.

6. Certificate License.

Effective immediately after delivery and continuing until the Certificate expires or is revoked, Customer may only use, for the benefit of the Certificate's subject, each issued Certificate and corresponding Key Set for the purposes described in the CPS, in accordance with all applicable laws, regulations, Industry Standards, and with the terms herein. Any Certificates trusted by Application Software Vendors are subject to all applicable Industry Standards requirements, including those found in applicable Application Software Vendor root store policies and the CPS, regardless of how the Certificates are used. Any use that is not allowed by applicable Industry Standards or the CPS is not permitted. DigiCert strongly discourages certificate or key pinning, using Certificates trusted for the web with non-web PKI, or any other use of Certificates that would make it difficult for Customer to meet the revocation timelines or other requirements of the CPS, and any such use will not be considered a sufficient reason to delay revocation. "**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, wherein (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). Customer will promptly inform DigiCert if it becomes aware of any misuse of a Certificate, Private Key, or the Portal. Customer is responsible for obtaining and maintaining any authorization or license necessary to order, use, and distribute a Certificate to end users and systems, including any license required under United States' export laws. SSL Certificates may be used on one or more physical server or device at a time; however, DigiCert may charge a fee for use of Certificates on additional servers or devices.

7. Key Sets.

A "**Private Key**" means the key that is kept secret by Customer that is used to create digital signatures and/or decrypt electronic records or files that were encrypted with the corresponding Public Key. A "**Public Key**" means Customer's publicly-disclosed key that is contained in Customer's Certificate and corresponds to the secret Private Key that Customer uses. Customer must (i) generate Key Sets using trustworthy systems, (ii) use Key Sets that are at least the equivalent of RSA 2048 bit keys, and (iii) keep all Private Keys confidential. Customer is solely responsible for any failure to protect its Private Keys. Customer represents that it will only generate and store Key Sets for Adobe Signing Certificates and EV Code Signing Certificates on a FIPS 140-2 Level 2 device. All other Certificate types may be stored on secure software or hardware systems. Customer is responsible for ensuring that Customer's acquisition, use, or acceptance of Key Sets generated by

DigiCert in accordance with the Agreement complies with applicable local laws, rules and regulations – including but not limited to export and import laws, rules, and regulations – in the jurisdiction in which Customer acquires, uses, accepts or otherwise receives such Key Sets. If Customer is permitted to import or export Private Keys (including copies) in connection with its use of specific DigiCert services, DigiCert will not be liable to Customer for Customer's use or storage of Private Keys (including copies) that are not created in the applicable Portal or service or that are used outside such Portal or service, including after they are exported from the applicable Portal or service.

8. Certificate Transparency.

To ensure Certificates function properly throughout their lifecycle, DigiCert may log Certificates with a public certificate transparency database. Log server information is publicly accessible. Once submitted, information cannot be removed from a log server.

9. Client Certificates.

"**Client Certificate**" means a Certificate that contains any extendedKeyUsage other than codeSigning, timestamping or serverAuthentication. The Client Certificate uses are varied and are defined by the Client Certificate profile. Some of the possible uses defined in a Client Certificate profile may include, digital signature, email encryption, and cryptographic authentication. If Customer wishes to request Client Certificates, Customer must (i) confirm the identity and affiliation of the requester using appropriate internal documentation as prescribed the CPS, and (ii) confirm that the information provided and representations related to or incorporated in any Client Certificate are true, complete, and accurate in all material respects.

10. Qualified Certificates.

"**Qualified Certificate**" means a Certificate (i) that is issued by a Qualified Trust Service Provider pursuant to the requirements of applicable EU or Swiss certification and electronic signature laws, and (ii) that carries the highest assurance level of "qualified" pursuant to such requirements.

"**Qualified Trust Service Provider**" or "**QTSP**" means an affiliate entity of DigiCert that is certified by governmental authorities to issue Qualified Certificates. DigiCert's QTSP's are as follows:

QTSP Entity	Trusted List	Jurisdiction of Supervisory Body
QuoVadis Trustlink B.V.	Netherlands Trusted List	Netherlands
DigiCert Europe Belgium B.V.	Belgium Trusted List	Belgium
QuoVadis Trustlink Schweiz AG	Swiss Trusted List	Switzerland

With respect to Qualified Certificates, Customer will (i) where use of a Qualified Signature Creation Device (QSCD) is required by Industry Standards, only use its Qualified Certificates for electronic signatures generated using the QSCD storing the Qualified Certificates, (ii) if Customer is a natural person, maintain and use their Private Keys only under their sole control; and (iii) if Customer is a legal entity or organization, maintain and use its Private Keys only under its control and direction.

11. Management.

DigiCert will generally issue, manage, renew, and revoke a Certificate in accordance with any instructions submitted by Customer through the Portal and may rely on such instructions as accurate. Customer will provide accurate and complete information when communicating with DigiCert and will notify DigiCert within 5 Business Days if any information relating to its account on the Portal changes. Customer will respond to any inquiries from DigiCert regarding the validity of information provided by Customer within 5 Business Days after Customer receives notice of the inquiry. Customer will review and verify the Certificate data prior to using the Certificate for accuracy. Certificates are considered accepted by Customer thirty (30) days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Customer used the Certificate. 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. "**Business Day**" means Monday through Friday, excluding U.S. Federal Holidays, which are set forth in 5 U.S.C. § 6103.

12. Registration Authority.

Except for publicly-trusted TLS/SSL Certificates and Qualified Certificates, Customer is appointed as a Registration Authority (and Customer hereby accepts such appointment) pursuant to the terms of the applicable CPS. To the extent that Customer performs any functions of a Registration Authority, it will do so in compliance with the applicable CPS, and DigiCert may rely on Customer's actions when acting as a Registration Authority. To the extent any third-party claim, suit, proceeding or judgment arises from Customer's failure to strictly comply with the obligations of a Registration Authority, Customer must defend, hold harmless, and indemnify DigiCert and its directors, officers, agents, employees, successors and assigns from such claim. If operating as a Registration Authority, Customer will cause its subscribers receiving Certificates hereunder to abide by the terms of the DigiCert Subscriber Agreement, found at https://www.digicert.com/subscriber-agreement. Subscribers of Customer must accept the Subscriber Agreement before receiving Certificates.

13. Security and Use of Key Sets.

Customer will securely generate and protect the Key Sets associated with a Certificate and take all steps necessary to prevent the compromise, loss, or unauthorized use of a Private Key associated with a Certificate. Customer will use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport Private Keys. Customer will only allow Customer's 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 will notify DigiCert, request revocation of a Certificate and its associated Private Key, cease using such Certificate and its associated Private Key, and remove the Certificate from all devices where it is installed if: (i) any information in the Certificate is or becomes incorrect or inaccurate, or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate. For code signing Certificates, Customer will promptly cease using a Certificate and its associated Private Key and promptly request revocation of the Certificate if Customer believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect Code. "**Suspect Code**" means code that contains harmful or malicious functionality of any kind or that contains serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes. Customer will respond to DigiCert's instructions concerning Key Set compromise or Certificate misuse within 24 hours. Customer will promptly cease 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. After revocation, Customer must cease using the Certificate.

14. Defective Certificates.

Customer's sole remedy for a defect in a Certificate ("**Defect**") is to require DigiCert to use commercially reasonable efforts to cure the defect after receiving notice of such Defect 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 provision of the Agreement.

15. Relying Party Warranty.

Customer acknowledges that the Relying Party Warranty is only for the benefit of Relying Parties. "**Relying Party Warranty**" means a warranty offered to a Relying Party that meets the conditions found in the Relying Party Agreement and Limited Warranty posted on DigiCert's website at https://www.digicert.com/legal-repository. The Relying Party Warranty for Certificates issued from a QTSP or a DigiCert affiliate is posted at https://www.quovadisglobal.com/repository. Customer does not have rights under the Relying Party Warranty, including any right to enforce the terms of the Relying Party Warranty or make a claim under the Relying Party Warranty. "**Relying Party**" has the meaning set forth in the Relying Party Warranty. 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.

16. Representations.

For each requested Certificate, Customer represents and warrants 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 common name or organization name specified in the Certificate;

b. Customer will use the Certificate only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and will use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Certificate purpose, the CPS, any applicable certificate policy, and the Agreement;

c. Customer has read, understands, and agrees to the CPS;

d. Customer will immediately report in writing to DigiCert any non-compliance with the CPS or Baseline Requirements; and

e. the organization included in the Certificate and the registered domain name holder is aware of and approves of each Certificate request.

17. Restrictions.

Customer will only use a TLS/SSL Certificate on the servers accessible at the domain names listed in the issued Certificate. Additionally, Customer will not:

a. modify, sublicense, or create a derivative work of any TLS/SSL Certificate (except as required to use the Certificate for its intended purpose) or Private Key;

b. upload or distribute any files or software that may damage the operation of another's computer;

c. make representations about or use a TLS/SSL Certificate except as allowed in the CPS;

d. impersonate or misrepresent Customer's affiliation with any entity;

e. use a Certificate or any related software or service (such as the Portal) in a manner that could reasonably result in a civil or criminal action being taken against Customer or DigiCert;

f. use a Certificate or any related software to breach the confidence of a third party or to send or receive unsolicited bulk correspondence;

g. use code signing Certificates to sign Suspect Code;

h. apply for a code signing Certificate if the Public Key in the Certificate is or will be used with a non-code signing Certificate;

i. interfere with the proper functioning of the DigiCert website or with any transactions conducted through the DigiCert website;

j. attempt to use a Certificate to issue other Certificates;

k. monitor, interfere with or reverse engineer the technical implementation of the DigiCert systems or software or otherwise knowingly compromise the security of the DigiCert systems or software;

l. submit Certificate information to DigiCert that infringes the intellectual property rights of any third party; or

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

18. Certificate Revocation.

DigiCert may revoke a Certificate without notice 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 the Agreement or an obligation it has under the CPS;

c. any provision of an agreement with Customer 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 without authorization, outside of its intended purpose or used to sign Suspect Code;

g. the Private Key associated with the Certificate was disclosed or compromised;

h. the Certificate was (i) misused, (ii) used or issued contrary to law, the CPS, or Industry Standards, or (iii) used, directly or indirectly, for illegal or fraudulent purposes, such as phishing attacks, fraud, or the distribution of malware, other illegal or fraudulent purposes, or any other violations as outlined in the DigiCert Acceptable Use Policy; or

i. Industry Standards or DigiCert's CPS require Certificate revocation, or revocation is necessary to protect the rights, confidential information, operations, or reputation of DigiCert or a third party.

19. Sharing of Information.

Customer acknowledges and accepts that if (i) the Certificate or Customer is identified as a source of Suspect Code, (ii) the authority to request the Certificate cannot be verified, or (iii) the Certificate is revoked for reasons other than Customer request (e.g. as a result of private key compromise, discovery of malware, etc.), DigiCert is authorized to share information about Customer, any application or object signed with the Certificate, the Certificate, and the surrounding circumstances with other certification authorities or industry groups, including the CAB Forum.

20. Industry Standards.

Both parties will comply with all Industry Standards and laws that apply to the Certificates; if such an applicable law or Industry Standard changes and that change affects the Certificates or other services provided under the Agreement, then DigiCert may alter the services or amend or terminate the Agreement to the extent necessary to comply with the change.

21. 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 Certificates and related DigiCert software or services; and (ii) Customer's conduct and its website maintenance, operation, development, and content.

22. Certificate Beneficiaries.

Relying Parties and Application Software Vendors are express third-party beneficiaries of Customer's obligations and representations related to the use or issuance of a Certificate. The Relying Parties and Application Software Vendors are not express third party beneficiaries with respect to any DigiCert software.

23. Intermediate Certificates.

This Section 23 only applies if Customer purchases a dedicated Private Root Certificate and/or Intermediate Certificate for the issuance of Private Certificates or publicly-trusted Certificates as specified in an Order Form.

a. Creation. Within 60 days after receiving applicable payment pursuant to the Agreement and the information required by DigiCert to create the Root Certificate and/or Intermediate Certificate as described in subsection (b) below, DigiCert will create a Root Certificate and/or an Intermediate Certificate for issuing (i) non-publicly trusted Certificates through the Portal or (ii) publicly-trusted Certificates as specified in an Order Form. A "**Private Certificate**" means a Certificate that is not embedded in any trust store. A "**Root Certificate**" means a self-signed Certificate that is stored in a secure off-line state and used to issue other Certificates. "**Intermediate Certificate**" means a Certificate that is signed by a Private Key corresponding to a Root Certificate and that is used to issue Certificates for use by Customer.

b. Contents. DigiCert and Customer will work together in good-faith to determine the appropriate contents of the Root Certificate and/or Intermediate Certificate. Customer must provide DigiCert with all information required by DigiCert for the creation of the Root Certificate and/or Intermediate Certificate within twelve (12) months of concluding an agreement for the creation of that Root Certificate and/or Intermediate Certificate. If Customer

fails to provide all required information within that time frame, Customer will forfeit the right to request the Root Certificate and/or Intermediate Certificate and DigiCert will retain any fees paid for the creation of the Root Certificate and/or Intermediate Certificate. After an Intermediate Certificate is created, Customer may not modify the contents of such Intermediate Certificate but may create as many identical copies of the Intermediate Certificate as needed. Intermediate Certificates have a set ten-year lifecycle, after which they expire without renewal. Customer is responsible for ensuring that all Certificates issued from an Intermediate Certificate expire at least two years prior to the expiration of the Intermediate Certificate. DigiCert has the right to revoke any Certificates issued from the Intermediate Certificates that are still valid within two years of the expiration of the Intermediate Certificate.

c. Ownership. DigiCert retains sole ownership of the Intermediate Certificate but, except as otherwise provided herein, will use the Intermediate Certificate issued in connection with this Agreement solely in accordance with the instructions provided by Customer through the Portal. Customer may generate copies of the Intermediate Certificate and distribute copies of the Intermediate Certificate to its own end users and customers.

d. Hosting. DigiCert will host the Intermediate Certificate's Private Key in DigiCert's secure PKI systems. Customer may not remove or have a third party remove the Intermediate Certificate's Private Key from DigiCert's PKI systems for any reason. DigiCert will provide and host CRL/OCSP services for Customer. DigiCert will continue to provide the CRL/OCSP services after the Agreement's termination until all Certificates issued thereunder expire or are revoked. For an Intermediate Certificate that issues publicly-trusted Certificates, because the Intermediate Certificate issues publicly-trusted Certificates, is hosted in DigiCert's PKI, and is managed by DigiCert's personnel, the Intermediate Certificate will be covered by DigiCert's WebTrust audit. If Industry Standards or the policies of an Application Software Vendor change in a manner that requires a separate audit of the Intermediate Certificate, then DigiCert and Customer will work together in good faith to obtain the required audit.

e. Revocation. DigiCert will have the right to revoke the Intermediate Certificate if: (i) Customer requests revocation in writing to DigiCert, citing a specific violation of industry standards; (ii) DigiCert has reasonable grounds to believe the Intermediate Certificate has been compromised; (iii) Customer materially breaches the Agreement and fails to remedy the breach within 30 days after receiving notice of the breach; (iv) Customer continues to use the Intermediate Certificate after Customer's right to use the Intermediate Certificate terminates, or (v) DigiCert reasonably believes the revocation is required by Industry Standards.

f. Restrictions. Customer will not: (i) create or attempt to create additional intermediate certificates from the Intermediate Certificate; (ii) sell, distribute, rent, lease, license, assign, or otherwise transfer the Intermediate Certificate to any third party; (iii) use an Intermediate Certificate provided by DigiCert after its expiration, its revocation, or the termination of this Agreement; (iv) alter, modify or revise an Intermediate Certificate provided by DigiCert; or (v) use the Intermediate Certificate if Customer has reason to believe that the Intermediate Certificate's Private Key was compromised.

24. EULA & Third-Party Terms.

a. Customer's use of any DigiCert service (or component thereof) that is in the form of software ("**Licensed Software**") meant to be installed on equipment or devices by or on behalf of Customer will be governed by the license agreement accompanying the Licensed Software; provided that if no license agreement accompanies the Licensed Software, the use of such Licensed Software will be governed by the Software End User License Agreement ("**EULA**") set forth in https://www.digicert.com/eula.

b. Customer acknowledges and agrees that if Customer's Certificate includes a legal entity identifier ("**LEI**") provided by Ubisecure Oy, then the Ubisecure Oy – RapidLEI Terms of Service available at https://rapidlei.com/documents/global-lei-system-terms/ will apply to Customer's LEI and use of the RapidLEI Legal Entity Identifier Management System or successor service.

c. Customer acknowledges and agrees that Customer's use of DigiCert's post-quantum cryptographic (PQC) toolkit (the "**PQC Toolkit**") will be governed by the following terms, in addition to the terms of any other applicable license agreement: (i) the license granted to Customer in relation to the PQC Toolkit is a non-exclusive, terminable license to be used only in connection with a DigiCert certificate that includes a signature and public key generated by or with the PQC Toolkit or related testing and configuration activities; (ii) Customer acquires no intellectual property or other proprietary rights in the PQC Toolkit or intellectual

property related to it; (iii) Customer will not reverse engineer, translate, disassemble, decompile, decrypt or deconstruct the PQC Toolkit; (iv) Customer will cease use of the PQC Toolkit upon termination of the related services from DigiCert; (v) ISARA Corporation will not be liable to Customer for any damages whatsoever; (vi) Customer will import, export and re-use the PQC Toolkit only in accordance with applicable laws of the countries or territories in which the PQC Toolkit is used or imported or from which it is exported or re-exported; (vii) DigiCert makes no warranties, express or implied, related to the PQC Toolkit on behalf of ISARA Corporation; and (viii) Customer will not alter any copyright, trademark or patent notice included in or with the PQC Toolkit or any related materials.

25. Flow-Down Requirements. Customer must not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any DigiCert system or software, and must impose the same restriction on its appointed manufacturers, if any.

26. Microsoft-Required Supplemental Obligations.

a. If Customer uses the Microsoft Auto Enrollment component, then the following MICROSOFT REQUIRED SUPPLEMENTAL OBLIGATIONS will apply:

b. Disclaimer of Warranties. MICROSOFT AND ITS AFFILIATES MAKE NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY AS TO THE SERVER SOFTWARE PROVIDED HEREUNDER ("**SERVER SOFTWARE**"), AND HAVE NO RESPONSIBILITY FOR ITS PERFORMANCE OR FAILURE TO PERFORM. AS TO MICROSOFT, THE SERVER SOFTWARE IS PROVIDED AS IS AND WITH ALL FAULTS, AND MICROSOFT AND ITS AFFILIATES HEREBY DISCLAIM ALL OTHER WARRANTIES, DUTIES AND CONDITIONS, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY (IF ANY) IMPLIED WARRANTIES, CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF RELIABILITY OR AVAILABILITY, ALL WITH REGARD TO THE SERVER SOFTWARE. ALSO, MICROSOFT AND ITS AFFILIATES MAKE NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SERVER SOFTWARE.

c. Exclusion of Certain Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL MICROSOFT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SERVER SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SERVER SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SERVER SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY OF THESE SERVICE DESCRIPTION TERMS AND CONDITIONS, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF MICROSOFT, AND EVEN IF MICROSOFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

d. Server Software Requirements. Customer may use only one (1) copy (unless otherwise specified in the applicable Order) of the Server Software provided hereunder as specified in the documentation accompanying this software, and only to interoperate or communicate with native Microsoft Windows 2000 Professional , Windows XP Home or Professional, or Vista client operating systems (or any successors thereto). Customer may not use the Server Software on a Personal Computer under any circumstances. For purposes of the foregoing, a "**Personal Computer**" means any computer configured so that its primary purpose is for use by one person at a time and that uses a video display and keyboard.

e. Third Party Beneficiary. Notwithstanding any inconsistent terms of the Agreement, Customer hereby agrees that Microsoft Corporation, as a licensor of intellectual property included in the Server Software, is intended to be a third party beneficiary of the terms and conditions of this Section 26 with rights to enforce any terms herein that affect any included Microsoft intellectual property or other Microsoft interest related to the terms hereof.

f. Server Class 2. If Customer has elected the Server Class 2, Customer may use the Server Software on a server that (a) contains not more than four (4) processors, where each such processor has a maximum of thirty-two (32) bits and four (4) gigabytes of RAM, and (b) is not capable of having memory added, changed or removed without the requirement that the server on which it is running be rebooted ("**Hot Swapping Capabilities**"). Customer may not use the Server Software in conjunction with any software that supports Hot Swapping Capabilities or Clustering Capabilities, where "**Clustering Capabilities**" means the ability to allow a group of servers to function as a single high-availability platform for running applications using application failover between Server nodes in the group.

g. Audit Rights. DigiCert may audit Customer and inspect Customer's facilities and procedures during regular business hours at Customer premises upon not less than fourteen (14) days' notice to verify Customer's compliance with all terms and conditions hereof. Notwithstanding any inconsistent terms of the Agreement (including without limitation any confidentiality provisions), should Customer refuse to undergo such audit and DigiCert has reason to believe Customer may not be in compliance with the Service Description terms and conditions, Customer agrees that DigiCert may disclose (i) Customer's identity to Relying Parties and Application Software Vendors and (ii) the basis for DigiCert's belief of noncompliance.

h. Multiplexing Devices. Hardware or software that reduces the number of users directly accessing or using services provided by the Server Software does not reduce the number of users deemed to be accessing or using services provided by the Server Software. The number of users accessing or using the Server Software is equal to the number of users who access or use, either directly or through a Multiplexing Device, services provided by (a) the Server Software or (b) any other software or system where the authentication or authorization for such software or system is provided by the Server Software (an "**Other Authenticated System**"). As used here, a "**Multiplexing Device**" means any hardware or software that provides or obtains access, directly or indirectly, to services provided by the Server Software or any Other Authenticated System to or on behalf of multiple other users through a reduced number of connections.

i. Windows CAL Requirement. Customer must acquire and dedicate a separate Windows CAL for each user that is accessing or using, either directly or through or from a Multiplexing Device, services provided by the Server Software or any Other Authenticated System. A "**Windows CAL**" means (a) a Windows Device Client Access License ("**CAL**"), or a Windows User CAL, in either case for a Microsoft Windows Server 2003 (Standard Edition, Enterprise Edition, or Datacenter Edition) server operating system product (or any successors thereto) ("**Windows Server**"); or (b) a Microsoft Core CAL that provides an individual person or electronic device with rights to access and use Windows Server, in either of (a) or (b) above that Customer has acquired for use with one or more such Microsoft Windows Server operating system products or electronic device and that is used on a per user or per device basis.

27. Adobe-Required Supplemental Obligations

If Customer is issued Adobe Signing Certificates, Customer agrees to:

a. Adhere to the Adobe Systems Inc. AATL Certificate Policy 2.0 currently available at https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf which includes, but is not limited to: (1) only generating and storing Key Sets for Adobe Signing Certificates on a FIPS 140-2 Level 2 device; and (2) upon enrollment of a new account, or at any time a new AATL Certificate enrollment is initiated for a subscriber, providing accurate and true information to DigiCert which requires (A) an account administrator to carry out strong identity proofing based on a face to face meeting with DigiCert or on a procedure that provides an equivalent assurance (e.g. by means of a secure video communication), (B) an account administrator to carry out strong identity proofing based on a face to face meeting with its subscribers (i.e. end-users), and store the recording locally to support audits, until DigiCert provides an online mechanism for administrator to upload attestations and recordings; and (C) the identity proofing process, regardless of an administrator or a subscriber, must include recording of the subscriber showing themselves and a valid government ID (e.g. driving license, passport, national ID card, etc.) displaying a matching photo of the subscriber; and

b. the terms of the applicable CPS.

28. **Additional Restrictions for Code Signing Certificates**. Customer must not use a code signing Certificate: (i) for or on behalf of any organization other than Customer's organization; (ii) to perform Private Key or Public Key operations in connection with any domain and/or organization name other than the one Customer submitted on the Certificate application; (iii) to distribute Suspect Code; or (iv) in a manner that transfers control or permits access for the Private Key corresponding to the Public Key of the Certificate to anyone other than an employee that Customer has authorized (any such transfer to be in a secure manner so as to protect the Private Key).

29. **Additional Restrictions for non-public TLS/SSL Certificates**. TLS/SSL Certificates that are chained to a Private Root Certificate must be used only with intranet domains and may not be assigned to devices that are publicly accessible from the Internet. DigiCert reserves the right to monitor publicly-facing Internet servers and/or devices to ensure that private TLS/SSL Certificates comply with this clause. If DigiCert discovers any use of private TLS/SSL Certificate(s) not in compliance with this clause, then DigiCert will immediately notify Customer of non-compliance. Customer must, within twenty (24) hours, either (i) immediately move the private TLS/SSL Certificate to an intranet domain; or (ii) remove and revoke the private TLS/SSL Certificate from Customer's servers. If the Customer does not revoke or remove the non-compliant Certificate, then DigiCert may revoke the Certificate.

[End of Service Description]

digicert

MASTER SERVICES AGREEMENT

Thank you for your interest in the products and services of DigiCert, Inc., a Utah corporation ("**DigiCert**"). This Master Services Agreement, together with any appendices, addenda, Order Forms, schedules, and other terms referenced herein (collectively, the "**Agreement**"), governs your use of DigiCert's products and services presented in connection with this Agreement. The Certificate Terms of Use, the applicable Certification Practices Statement(s) ("**CPS**"), and the Privacy Policy, each available at https://www.digicert.com/legal-repository/ (as updated from time to time, the "**Legal Repository**") are incorporated by reference into this Agreement.

If you are accessing or using the Services on behalf of a business, entity, or individual, then: (a) you represent and warrant that you are an authorized representative of such business, entity, or with the authority to bind the entity or individual to this Agreement; and (b) such business, entity, or individual is legally and financially responsible for your access to and use of the Services as well as for the use of your account by others affiliated with you, including any employees, agents or contractors. "**Customer**" means you and any entity, business, or individual on whose behalf you are accessing or using Services.

By accessing or using DigiCert's Services, by electronically accepting this Agreement via DigiCert's online services, or by mutually agreeing to an Order Form with DigiCert in the manner specified in Section 1.1 below and which Order Form references this Agreement, Customer hereby accepts this Agreement as it relates to Customer's use of the Services. If Customer does not agree to the terms of this Agreement (or you do not have authority to enter into this Agreement on behalf of Customer), then Customer may not purchase or use any DigiCert Service. This Agreement is effective as of the date Customer first accepted this Agreement (the "**Effective Date**").

WHEREBY, DigiCert is a trusted third-party certification authority and experienced provider of digital certificates ("**Certificates**") and other related products, software, and services (collectively with the Certificates, the "**Services**");

WHEREBY, as part of the Services, DigiCert operates account management interfaces, portals and related APIs to facilitate the management of Certificates and other Services provided by DigiCert (each, a "**Portal**"); and

WHEREBY, Customer wishes to purchase, and DigiCert wishes to provide, one or more Services pursuant to the terms of this Agreement.

NOW THEREFORE, in consideration of the mutual covenants contained herein and good and valuable consideration which is hereby acknowledged, DigiCert and Customer hereby agree as follows:

1. Order Forms; Certificates.

1.1. Order Forms. Customer may purchase specific Services from DigiCert by entering into one or more mutually agreed upon quotes, purchase schedules, purchase orders, or order forms (whether online or electronic) that set forth the specific Services being procured by Customer under this Agreement, the term when each such Service is to be provided by DigiCert (the "**Service Term**") and the related payment terms for such Service (each, an "**Order Form**"). Order Forms are considered "mutually agreed upon" either (i) when executed by both parties in writing, (ii) when Customer affirms its electronic acceptance of an Order Form that DigiCert has presented to Customer via electronic means (e.g., at https://www.digicert.com/order), or (iii) when DigiCert presents Customer with an Order Form and Customer affirms its acceptance by issuing a purchase order. Customer and DigiCert acknowledge and agree that each Order Form will be governed by and incorporated by reference into the terms of this Agreement.

1.2. Portal; Portal API. Subject to Customer's compliance with the terms and conditions of this Agreement, DigiCert hereby grants Customer permission, during the term of this Agreement, to use the Portal (in the form made available by DigiCert to Customer) to manage Certificates (or to manage any other Services to the extent permitted in the Portal). Further, subject to Customer's compliance with this Agreement, if Customer has been granted access to the Portal API by DigiCert, then DigiCert hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable, revocable, limited license during the term of this Agreement to install, use and make calls to

and from such Portal API solely for the purpose of facilitating Customer's use of the Portal (and its tools and functionalities) directly from Customer's internal systems. "**Portal API**" means the portion of the Portal that constitutes an application programming interface and that facilitates the integration of the Portal with Customer's internal systems, as such application programming interface may be made available by DigiCert under this Agreement.

1.3. Applicable Certificates. This Agreement applies to each Certificate issued to Customer by DigiCert, regardless of: (i) the Certificate type (client, code signing, or TLS/SSL), (ii) when Customer requested the Certificate, or (iii) when the Certificate is issued. With respect to any Certificates issued by DigiCert to Customer hereunder, the parties acknowledge and agree that this Agreement constitutes the subscriber agreement, as required under the applicable industry standards, guidelines and requirements related to the issuance of Certificates (including the EV Guidelines, as defined in the Certificate Terms of Use).

1.4. Portal Accounts. In connection with the Services, DigiCert will provide the Customer with accounts to access and use the Portal (the "**Portal Accounts**"). Customer must maintain security over its Portal Accounts. Customer assumes liability for any use of its Portal Accounts by individuals obtaining access credentials from Customer.

1.5. IP Address Scanning. Customer will not scan a DigiCert IP address (including through automated means) without obtaining DigiCert's prior written consent. DigiCert reserves the right to block an IP address that has been used to initiate connections that are not related to normal use of services without DigiCert's prior written consent. Examples of non-normal use connections include, but are not limited to, vulnerability or load/performance scans. DigiCert may throttle any access to the Portal or Portal API if DigiCert believes a system has initiated excessive connections to DigiCert's Portals or Portal API. For the Portal API, excessive connections are defined as greater than 1,000 requests/5 minutes per API key.

1.6. Certificates. Customer will order, manage, and use, and DigiCert will provide and manage Certificates in accordance with DigiCert's Certificate Terms of Use, available at https://www.digicert.com/certificate-terms (as updated from time to time, the "**Certificate Terms of Use**").

1.7. QTSP Services. Notwithstanding anything to the contrary in this Agreement, if Customer purchases certain Services issued by DigiCert's QTSP (as defined below) (whether acting in its capacity as QTSP or otherwise) or its Affiliates ("**QTSP Services**"), then the applicable CPS for certain such QTSP Services is located at https://www.quovadisglobal.com/repository/ (as updated from time to time and where such repository is applicable, also the "**Legal Repository**").

1.8. DigiCert Vendor Entities. DigiCert's Vendor Entities may exercise any right or perform any obligation under this Agreement. For clarity, a Vendor Entity may (i) exercise DigiCert's billing rights and obligations, and (ii) execute Order Forms with Customer. If Customer purchases Qualified Certificates, then Customer acknowledges that the applicable Qualified Trust Service Provider is the provider of such Services. "**Vendor Entity**" means the QTSPs and any Affiliate of DigiCert. "**Qualified Certificates**" means a Certificate (i) that is issued by a Qualified Trust Service Provider pursuant to the requirements of applicable EU or Swiss certification and electronic signature laws, and (ii) that carries the highest assurance level of "qualified" pursuant to such requirements. "**Qualified Trust Service Provider**" or "**QTSP**" means the following entities that are authorized by governmental authorities to issue Qualified Certificates:

Qualified Trust Service Provider	**Trusted List**	**Jurisdiction of Supervisory Body**
QuoVadis Trustlink B.V.	Netherlands Trusted List	Netherlands
DigiCert Europe Belgium B.V.	Belgium Trusted List	Belgium
QuoVadis Trustlink Schweiz AG	Swiss Trusted List	Switzerland

1.9. Purchases for Resale. If Customer purchases Services on behalf, or for the use of, anyone other than Customer or an Affiliate of Customer (including employees or contractors of Customer or an Affiliate of Customer), then Customer agrees that such purchases will be governed by the terms of the Master Reseller Agreement, available at https://www.digicert.com/master-reseller-agreement (as updated from time to time), which terms are incorporated herein by reference. For purposes of this Agreement, "**Affiliate**" means any entity that directly or

indirectly controls, is controlled by, or is under common control with a party to this Agreement.

2. Fees.

2.1. Fees. Customer will pay DigiCert the fees for Services provided hereunder as posted in the Portal or as set forth in an Order Form. Prices of Certificates available for purchase on a per-Certificate basis are subject to change; updates to pricing will be posted in the Portal. All payments are due and payable either within 30 days of the date of purchase or such other period, if any, stated in an Order Form. Fees payable hereunder are in exchange for the provision of Services by DigiCert and are not a royalty or license fee. If Customer submits funds to its Portal Account that are not connected to an Order Form (i.e., funds not connected to the purchase of Services with a definite term length), Customer may use such funds to purchase Services within 12 months. If Customer fails to use all such funds, any remaining funds will be deemed fees earned by DigiCert for Services provided, and Customer may not use them in connection with any other purchase. If any undisputed invoiced amount is not received by DigiCert by the due date, then without limiting DigiCert's rights or remedies, (a) those charges will accrue late interest at the rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower, (b) DigiCert may accelerate Customer's unpaid fee obligations so that they become immediately due and payable, and (c) DigiCert may suspend or limit Customer's access to the Portal or Services without notice until full payment is made. Customer must notify DigiCert of any fee disputes within 30 days of the applicable invoice date or such invoice will be deemed accepted.

2.2. Taxes. DigiCert may charge, and Customer will pay, all applicable federal, state, or local sales or use taxes, value added taxes ("**VAT**"), goods and services taxes ("**GST**"), and consumption taxes that DigiCert is legally obligated to charge ("**Taxes**"). All fees charged by DigiCert are exclusive of any Taxes however imposed, e.g., VAT, GST, or consumption taxes, unless such Taxes are stated on the invoice DigiCert provides to Customer. Customer may provide DigiCert an exemption certificate or equivalent information acceptable to the relevant taxing authority. In such case, DigiCert will not charge or collect the Taxes covered by such exemption certificate. During the term of this Agreement, DigiCert will provide Customer with forms, documents, or certifications as may be required for Customer to satisfy information reporting or withholding tax obligations with respect to payments under this Agreement. Upon DigiCert's receipt of Customer's proof of withholding (which proof must be acceptable in DigiCert's sole discretion), Customer may deduct or withhold any taxes that Customer determines it is obligated to withhold from any amounts payable to DigiCert under this Agreement. Except as stated in this Section 2.2, Customer may not withhold or offset any amount owed to DigiCert for any reason.

3. Intellectual Property Rights; Restrictions.

3.1. DigiCert Intellectual Property Rights. DigiCert retains, and Customer will not obtain or claim, any title, interest, or ownership rights in any of DigiCert's products or services (including the Services), including all software associated with the Portal, the Services, or techniques and ideas embedded therein; all copies or derivative works of such products or services or software provided by DigiCert, regardless of who produced, requested, or suggested the copy or derivative work; all documentation and marketing material provided by DigiCert to Customer; and all of DigiCert's copyrights, patent rights, trade secret rights and other proprietary rights.

3.2. Restrictions. Customer will protect DigiCert's intellectual property, and the value, good will, and reputation associated therewith when accessing or using the Services. Customer will not: (i) attempt to interfere with, or disrupt the operations of, the Services or attempt to gain access to any systems or networks that connect thereto, except as required to access and use the Portal (including the Portal API) as permitted hereunder, (ii) re-engineer, reverse engineer, decompile or disassemble any portion of the Services; (iii) use, copy or modify the Services for any purpose other than as expressly permitted herein; (iv) transfer, sublicense, rent, lease, lend, distribute or otherwise make available the Services to any third party other than as expressly permitted herein; (v) replicate, frame or mirror the Services; (vi) remove, erase or tamper with any copyright or other proprietary notice encoded or recorded in the Services; (vii) introduce into the Services any computer virus, malware, software lock or other such harmful program or data which destroys, erases, damages or otherwise disrupts the normal operation of the Services or allows for unauthorized access to the Services, (viii) access, or allow another party to access or use, the Services for any benchmarking purposes or to develop or improve a product or service that competes with DigiCert, (ix) impersonate or misrepresent Customer's affiliation with any entity, or (x) encourage or authorize a third party to do any of the foregoing. DigiCert may terminate this Agreement or Customer's Portal Accounts,

restrict Customer's access to the Services, or revoke the Certificates if DigiCert reasonably believes that Customer is using the Services, to post or make accessible any material that infringes DigiCert's or any third party's rights or is in breach of this Agreement. Customer will not use any marketing material or documentation that refers to DigiCert or its products or services without receiving written prior approval from DigiCert, except as outlined in Section 3.4 (Mark License).

3.3. Trademark Usage. Customer agrees that DigiCert may use Customer's name and trademark to perform its obligations under this Agreement and to indicate that Customer is receiving DigiCert's Service, provided that such use would not foreseeably diminish or damage Customer's rights in any of its trademarks, create a misrepresentation of the parties' relationship, or diminish or damage a party's reputation. Neither party may register or claim any right in the other party's trademarks. Customer grants DigiCert a right to use any trademark of Customer included in the Certificate to the extent necessary to operate such Certificate.

3.4. Mark License. DigiCert may make certain marks available for Customer to display to indicate that a particular Certificate has been issued for a particular Customer property (each, a "**Mark**"). Effective upon issuance of the applicable Certificate, and only for so long as such Certificate remains valid, and Customer is in full compliance with all applicable terms related thereto, DigiCert grants to Customer a limited, revocable license during the validity period of the applicable Certificate to display the applicable Mark (in the form provided by DigiCert to Customer) to accurately and not misleadingly indicate the applicable Certificate on Customer's products, domain names or services. Customer agrees to not modify Marks in any manner or use or display Marks for any inappropriate purpose or in any way that could misrepresent the parties' relationship or diminish or damage DigiCert's reputation or the goodwill associated with any Mark or other DigiCert trademarks or service marks, including using a Mark or Certificate with a website that could be considered associated with crime, fraud, deception, defamation, libel, obscenity, misappropriation or infringement or that is otherwise reasonably objectionable to DigiCert. All goodwill arising in connection with the use of Marks will inure to the benefit of DigiCert and if Customer obtains any right, title or interest in or to any Mark as a result of the use of such Mark, then Customer hereby irrevocably assigns to DigiCert all such right, title and interest therein and thereto.

4. Evaluation License.

The terms in this Section 4 apply if Customer is granted the right to access or use any Services free-of-charge for evaluation purposes, including trials, proofs of concept, or other demonstrations or tests ("**Trial Basis**").

4.1. Use Rights. Customer agrees that it may only access or use any Services provided under this Agreement on a Trial Basis solely for the purpose of Customer's internal, non-production, non-commercial evaluation and interoperability testing of the applicable Services, and Customer may not use the Services provided on a Trial Basis for any other purpose.

4.2. Evaluation Period. Customer's right to use the Services on a Trial Basis are time-limited and will terminate immediately upon the earlier of (i) the trial end date as specified in an Order Form or other document executed by the parties regarding such trial, or (ii) the start date of when Customer purchases a right to use such Services on a non-Trial Basis, or (iii) the date when DigiCert terminates Customer's right to use the Services on a Trial Basis (which DigiCert may do at any time in its sole discretion). Customer must cease using the Services on a Trial Basis upon any such termination.

4.3. Trial Data. Customer agrees that any data or information that Customer enters into the Services used on a Trial Basis, and any customizations made to such Services by or for Customer, during the Trial Basis period may be permanently lost unless Customer purchases the same Services on a non-Trial Basis before the termination date set forth in Section 4.2 above.

4.4. Limitation of Liability. IN NO EVENT WILL DIGICERT BE LIABLE FOR ANY DAMAGES UNDER THE AGREEMENT, INCLUDING, WITHOUT LIMITATION, ANY LOST REVENUE, LOST PROFITS, OR CONSEQUENTIAL DAMAGES EVEN IF DIGICERT IS ADVISED OF THEIR POSSIBILITY.

4.5. Warranty Disclaimer. CUSTOMER ACKNOWLEDGES THAT NO WARRANTIES, SERVICE LEVELS, OR SPECIFICATIONS SET FORTH IN THIS AGREEMENT WITH RESPECT TO THE SERVICES WILL APPLY TO ANY

SERVICES PROVIDED ON A TRIAL BASIS. THE PARTIES ACKNOWLEDGE THAT THE SERVICE PROVIDED ON A TRIAL BASIS ARE PROVIDED "AS IS" AND WITHOUT ANY WARRANTY WHATSOEVER. DIGICERT DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD-PARTY RIGHTS.

4.6. Order of Precedence. In the event of a conflict between this Section 4 and any provision of the Agreement, this Section 4 will prevail and supersede the conflicting provisions in the Agreement with respect to the Services provided by DigiCert to Customer on a Trial Basis.

5. Confidentiality.

5.1. Definition. **"Confidential Information"** means any information, documentation, system, or process disclosed by a party or a party's Affiliate that is: (i) designated as confidential (or a similar designation) at the time of disclosure; (ii) disclosed in circumstances of confidence; or (iii) understood by the parties, exercising reasonable business judgment, to be confidential.

5.2. Exclusions. Confidential Information does not include information that: (i) was lawfully known or received by the receiving party prior to disclosure; (ii) is or becomes part of the public domain other than as a result of a breach of this Agreement; (iii) 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 to such information; or (iv) is independently developed by the receiving party as evidenced by independent written materials.

5.3. Obligations. Each party will keep confidential all Confidential Information it receives from the other party or its Affiliates. Each party will use disclosed Confidential Information only for the purpose of exercising its rights and fulfilling its obligations under this Agreement and will protect all Confidential Information against disclosure using a reasonable degree of care. Each party may disclose 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 may disclose such Confidential Information that it is advised by its legal counsel is legally required, but only after using 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 and reasonably cooperates with such attempts by the other party.

5.4. Privacy. Customer consents, for itself, its users and contacts, to provide certain required information relating to an identified or identifiable natural person ("**Personal Data**"), which is necessary for use of the Services (including the Certificates), and which will be processed and used in accordance with DigiCert's Privacy Policy available as at https://www.digicert.com/digicert-privacy-policy (as updated from time to time, the "**Privacy Policy**"). The Privacy Policies applicable to QTSP Services are available at https://www.quovadisglobal.com/privacy/ (as updated from time to time).

5.5. Publication of Certificate Information. Notwithstanding anything in this Agreement to the contrary, Customer consents to: (i) DigiCert's public disclosure of information (such as Customer's domain name, jurisdiction of incorporation, or contact information), embedded in an issued Certificate; and (ii) Customer's Certificates and information embedded therein being logged by or on behalf of DigiCert in publicly-accessible Certificate transparency databases for purposes of detecting and preventing phishing attacks and other forms of fraud, and Customer agrees that such information when logged may not be removed. This consent survives termination of this Agreement. DigiCert may rely on and use information provided by Customer for any purposes connected to the Services, but only if such use is in compliance with DigiCert's Privacy Policy and complies with the confidentiality obligations in this Section 5.

6. Term and Termination.

6.1. Term. This Agreement is effective upon the Effective Date and will remain in effect unless earlier terminated in accordance with this Agreement.

6.2. Termination. Either party may terminate this Agreement immediately if the other party: (i) materially breaches this Agreement (including any appendices, addenda, Order Forms, schedules and other terms referenced herein) and fails to remedy the material breach within thirty (30) days after receiving notice of the material breach (except that any breach by Customer of the Certificate Terms of Use will be deemed a material breach of this Agreement for which DigiCert can immediately terminate this Agreement without a remedy period); (ii) engages in illegal or fraudulent activity in connection with this Agreement (or in the case of termination by DigiCert, Customer engages in an activity that could otherwise materially harm DigiCert's business in connection with this Agreement); (iii) has a receiver, trustee, or liquidator appointed over substantially all of its assets; (iv) has an involuntary bankruptcy proceeding filed against it that is not dismissed within 30 days of filing; or (v) files a voluntary petition of bankruptcy or reorganization.

6.3. Restrictions on Further Use. Upon expiration or termination of the Agreement: (i) except as otherwise specified, all other rights and licenses granted herein terminate; (ii) each party will immediately discontinue all representations or statements that could imply that a relationship exists between DigiCert and Customer; (iii) each party will continue to comply with the confidentiality requirements in this Agreement; and (iv) Customer will, within 30 days of the date of termination, pay to DigiCert any fees, or part thereof, still owed as of the date of termination and destroy or deliver to DigiCert all sales manuals, price lists, literature and other materials relating to DigiCert.

6.4. Survival**.** The CPS, the Certificate Terms of Use, and any applicable sections herein or appendices that specifically state they survive termination of this Agreement, will survive expiration or termination of this Agreement until all Certificates issued or other Services provided by DigiCert expire or are revoked. In addition, the obligations and representations of the parties under Section 3.1, Section 3.2, Section 5 (Confidentiality), Section 6 (Termination), Section 7 (Disclaimers of Warranties, Limitation of Liability, and Indemnification), and Section 8 (Miscellaneous) survive expiration or termination of this Agreement. Customer's obligation to pay all amounts owed by Customer to DigiCert survive termination of this Agreement.

7. Disclaimer of Warranties, Limitation of Liability, and Indemnification.

7.1. Warranties. DigiCert warrants the Certificates offered under this Agreement will comply in all material respects to the requirements in the CPS and with applicable law.

7.2. DISCLAIMERS. OTHER THAN AS PROVIDED IN SECTION 7.1, THE SERVICES, AND ANY RELATED SOFTWARE (INCLUDING THE PORTAL) ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND 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 SERVICES WILL BE TIMELY OR ERROR-FREE. DigiCert does not guarantee the accessibility of any products or services and may modify or discontinue offering any product or service offering at any time. Customer's sole remedy for a defect in the Services is for DigiCert to use commercially reasonable efforts, upon notice of such defect from Customer, to correct the defect, except that DigiCert has no obligation to correct defects that arise from (i) misuse, damage, modification or damage of the Services or combination of the Services with other products and services by parties other than DigiCert, or (ii) Customer's breach of any provision of this Agreement.

7.3. Limitation of Liability. This Agreement does not limit a party's liability for: (i) death or personal injury resulting from the negligence of a party; (ii) gross negligence, willful misconduct or violations of applicable law, or (iii) fraud or fraudulent statements made by a party to the other party in connection with this Agreement. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (A) DIGICERT AND ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS (THE "**DIGICERT ENTITIES**") WILL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES (INCLUDING ANY DAMAGES ARISING FROM LOSS OF USE, LOSS OF DATA, LOST PROFITS, BUSINESS INTERRUPTION, OR COSTS OF PROCURING SUBSTITUTE SOFTWARE OR SERVICES) ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE SUBJECT MATTER HEREOF; AND (B) THE DIGICERT ENTITIES' TOTAL

CUMULATIVE LIABILITY ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE SUBJECT MATTER HEREOF WILL NOT EXCEED THE AMOUNTS PAID BY CUSTOMER TO DIGICERT IN THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY, REGARDLESS OF WHETHER SUCH LIABILITY ARISES FROM CONTRACT, INDEMNIFICATION, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND REGARDLESS OF WHETHER DIGICERT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. NO CLAIM, REGARDLESS OF FORM, WHICH IN ANY WAY ARISES OUT OF THIS AGREEMENT, MAY BE MADE OR BROUGHT BY CUSTOMER OR CUSTOMER'S REPRESENTATIVES MORE THAN ONE (1) YEAR AFTER THE BASIS FOR THE CLAIM BECOMES KNOWN TO CUSTOMER.

7.4. Indemnity. Customer will indemnify, defend and hold harmless DigiCert and DigiCert's employees, officers, directors, shareholders, Affiliates, and assigns (each an "**Indemnified Party**") against all third party claims and all related liabilities, damages, and costs, including reasonable attorneys' fees, arising from (i) Customer's breach of this Agreement; (ii) Customer's online properties for which DigiCert provides Services hereunder, or the technology or content embodied therein or made available through such properties; (iii) DigiCert's access or use in compliance with this Agreement of any information, systems, data or materials provided by or on behalf of Customer to DigiCert hereunder, (iv) Customer's failure to protect the authentication mechanisms used to secure the Portal or a Portal Account; (v) Customer's modification of a DigiCert product or service or combination of a DigiCert product or service with any product or service not provided by DigiCert; (vi) an allegation that personal injury or property damage was caused by the fault or negligence of Customer; (vii) Customer's failure to disclose a material fact related to the use or issuance of the Services; or (viii) an allegation that the Customer, or an agent of Customer, used DigiCert's Services to infringe on the rights of a third party.

7.5. Indemnity Obligations. An Indemnified Party seeking indemnification under this Agreement must notify the 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 the defense of any proceeding requiring indemnification unless assuming the defense would result in potential conflicting interests as determined by the Indemnified Party in good faith. An Indemnified Party may, at the indemnifying party's expense, defend itself until the indemnifying party's counsel has initiated a defense of the Indemnified Party. Even after the indemnifying party assumes the defense, the Indemnified Party may participate in any proceeding using counsel of its own choice and at its own 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. The indemnifying party's indemnification obligations hereunder are not an Indemnified Party's sole remedy for events giving rise to indemnity by the indemnifying party hereunder, and are in addition to any other remedies an Indemnified Party may have against the indemnifying party under this Agreement.

7.6. Injunctive Relief. Customer acknowledges that its breach of this Agreement may result in irreparable harm to DigiCert that cannot adequately be redressed by damages. Accordingly, in addition to any other legal remedies which may be available, DigiCert may seek and obtain an injunctive order against a breach or threatened breach of this Agreement by Customer, and without a need to post a bond or similar action.

7.7. Extent. The limitations and obligations 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.

8. Miscellaneous.

8.1. Force Majeure. Except for Customer's payment obligations, 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 Services (including the Portal 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.

8.2. Entire Agreement. This Agreement, along with all documents referred to herein, including any applicable Order Form, constitutes the entire agreement between the parties with respect to the subject matter, superseding all

other prior agreements that might exist. All DigiCert products and services are provided only upon the terms and conditions of this Agreement, and this Agreement prevails over any conflicting, additional, or different terms and conditions proposed by Customer. Except as otherwise allowed herein, neither party may amend this Agreement unless the amendment is both in writing and signed by the parties. Any terms in a purchase order or similar ordering document provided by Customer and not executed by DigiCert that conflict with the terms of this Agreement or materially alter the rights or obligations of the parties are expressly rejected and will be of no effect. In the event of an inconsistency between documents, the following order of precedence will apply: (1) Master Services Agreement, (2) Certificate Terms of Use; (3) other applicable appendices, addenda, and schedules, and (4) Order Forms, unless the Order Form expressly states that it will take precedence.

8.3. Amendment. DigiCert may amend: (i) this Agreement; (ii) the CPS; (iii) the Privacy Policy; (iv) the Certificate Terms of Use; and (v) any other applicable appendices, addenda and schedules (but for clarity not an Order Form) at any time and will give notice of any material changes via the Portal, by posting the amended version to the Legal Repository, or by a means set forth in Section 8.7. If such an amendment materially and adversely affects Customer's rights herein, Customer will have the right, as its sole and exclusive remedy in connection with such amendment, to terminate this Agreement during the 30-day period after DigiCert's notice of such amendment, by providing written notice of termination to DigiCert. Customer's continued use of the Services after 30 days of DigiCert's notice of the amendment constitutes Customer's acceptance of the amendment.

8.4. Waiver. A party's failure to enforce or delay in enforcing a provision of this Agreement does not waive the party's right to enforce the same provision later or the party's right to enforce any other provision of this Agreement. A waiver is only effective if in writing and signed by both parties.

8.5. Assignment. Customer may not assign or delegate any of its rights or obligations under this Agreement without the prior written consent of DigiCert. DigiCert may assign or delegate any of its rights and obligations under this Agreement without Customer's consent. Any purported assignment or delegation in violation of this Agreement is null and void.

8.6. Relationship. 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 or to make any statements, representations, warranties or commitments on behalf of the other party. Each party is responsible for its own expenses and employees. All persons employed by a party will be employees of such party and not of the other party and all costs and obligations incurred by reason of any such employment will be for the account and expense of such party.

8.7. Notices. DigiCert will send notices of early termination or breach of this Agreement to Customer by first class mail to the address listed in the Portal Account, which notices are effective upon receipt. DigiCert will send all other notices (or if no physical address is provided by Customer, then DigiCert will send all notices hereunder including notices of early termination or breach of this Agreement) by posting the notice in the Portal Account or by email via the email address of Customer's administrator Portal Account (or other alternate email address associated with the Portal Account if provided), or by regular mail. All such notices are effective when posted in the Portal or when sent to the Portal Account. It is Customer's responsibility to keep its email address current. Customer will be deemed to have received any email sent to the email address then associated with the Portal Account when DigiCert sends the email, regardless of whether Customer receives the email. Customer will send DigiCert notices in writing by postal mail that is addressed to DigiCert, Inc., Attn: General Counsel, 2801 North Thanksgiving Way, Suite 500, Lehi, Utah 84043. Notices from Customer are effective upon receipt. DigiCert may change its address for notice either by providing written (including email) notice to Customer or by publishing a new address for notice through the Portal.

8.8. Governing Law and Jurisdiction. The (i) laws that govern the interpretation, construction, and enforcement of this Agreement and all matters, claims or disputes related to it, including tort claims, and (ii) the courts or arbitration bodies that have exclusive jurisdiction over any of the matters, claims or disputes contemplated in sub-section (i) above, will each depend on where Customer is domiciled, as set forth in the table below. In instances where the International Chamber of Commerce is designated below as the court or arbitration body with exclusive jurisdiction of such matters, claims or disputes, then the parties hereby agree that (x) all matters, claims or disputes arising out of or in connection with this Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce ("**Rules**") by one or more arbitrators appointed in accordance with the Rules,

(y) judgment on the award rendered by such arbitration may be entered in any court having jurisdiction, and (z) this arbitration clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

Customer is Domiciled in:	**Governing Law is laws of:**	**Court or arbitration body with exclusive jurisdiction:**
The United States of America, Canada, Mexico, Central America, South America, the Caribbean, or any other country not otherwise included in the rest of the table below	Utah state law and United States federal law	State and Federal courts located in Salt Lake County, Utah
Europe, the United Kingdom, Switzerland, Russia, the Middle East or Africa	England	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in London
Japan	Japan	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Tokyo
Australia or New Zealand	Australia	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Melbourne
A Country in Asia or the Pacific region, other than Japan, Australia or New Zealand	Singapore	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Singapore

8.9. Dispute Resolution. To the extent permitted by law, before Customer files suit or initiates an arbitration claim with respect to a dispute involving any aspect of this Agreement, Customer shall notify DigiCert, and any other party to the dispute for the purpose of seeking business resolution. Both Customer and DigiCert shall make good faith efforts to resolve such dispute via business discussions. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may proceed as permitted under applicable law and as specified under this Agreement.

(i) Arbitration. In the event a dispute is allowed or required under this agreement to be resolved through arbitration, the parties will maintain the confidential nature of the existence, content, or results of any arbitration hereunder, except as may be necessary to prepare for or conduct the arbitration hearing on the merits, or except as may be necessary in connection with a court application for a preliminary remedy, a judicial confirmation or challenge to an arbitration award or its enforcement, or unless otherwise required by law or judicial decision.

(ii) Class Action and Jury Trial Waiver. THE PARTIES EXPRESSLY WAIVE THEIR RESPECTIVE RIGHTS TO A JURY TRIAL FOR THE PURPOSES OF LITIGATING DISPUTES HEREUNDER. Each party agrees that any dispute must be brought in the respective party's individual capacity, and not as a plaintiff or class member in any purported class, collective, representative, multiple plaintiff, or similar proceeding ("**Class Action**"). The parties expressly waive any ability to maintain any Class Action in any forum in connection with any dispute. If the dispute is subject to arbitration, the arbitrator will not have authority to combine or aggregate similar claims or conduct any Class Action nor make an award to any person or entity not a party to the arbitration. Any claim that all or part of this Class Action waiver is unenforceable, unconscionable, void, or voidable may be determined only by a court of competent jurisdiction and not by an arbitrator.

8.10. Compliance with Law. Each party will comply with all applicable laws, including federal, state and local laws and regulations in connection with its performance under this Agreement. Customer acknowledges that Services provided or offered under this Agreement may be subject to, and Customer agrees to comply with all applicable laws in connection with is use of the Services, including all applicable export controls, trade sanctions, and

physical or electronic import laws, advertising laws, privacy laws, regulations, and rules. DigiCert may suspend performance of any of its obligations under the Agreement, without any prior notice or cure period and without any liability, if Customer fails to comply with this provision.

8.11. Severability. The invalidity or unenforceability of any provision of this Agreement, as determined by a court or administrative body of competent jurisdiction, will not affect the validity or enforceability of the remainder of this Agreement, and the provision affected will be construed so as to be enforceable to the maximum extent permissible by law.

8.12. Rights of Third Parties. Except as stated in the Certificate Terms of Use or Section 1.8, no third parties have any rights or remedies under this Agreement.

8.13. 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.