THE INFORMATION IN THIS BOX IS NOT A PART OF THE CONTRACT AND IS FOR COUNTY USE ONLY

SAN BERNARDINO COUNTY

Contract Number 20-81

SAP Number

Information Services Department

Department Contract Representative	Jennifer Mancebo
Telephone Number	909-388-5579
Contractor	DigiCert, Inc.
Contractor Representative	John Frye
Telephone Number	801-770-1722
Contract Term	2/11/2020-2/10/2025
Original Contract Amount	Non-financial
Amendment Amount	N/A
Total Contract Amount	Non-financial
Cost Center	1200604048

Briefly describe the general nature of the contract: *Master Services Agreement with DigiCert, Inc. for high-assurance digital Secure Sockets Layer (SSL) certificates for the County's websites.*

FOR COUNTY USE ONLY

Approved as to Legal Form	Reviewed for Contract Compliance	Reviewed/Approved by Department
► Bonnie Ogilvie, County Counsel	►	►
Date 1-29-20	Date	Date

MASTER SERVICES AGREEMENT

This Master Services Agreement, together with any appendices, addenda, Order Forms, schedules, and other terms referenced herein (collectively, the "**Agreement**") is dated February 11, 2020 ("**Effective Date**"), and is between DigiCert, Inc., a Utah corporation ("**DigiCert**") and the County of San Bernardino, ("**Customer**"). This Agreement governs Customer's use of DigiCert's products and services presented in connection with this Agreement. The Certificate Terms of Use ("**Certificate Terms of Use**"), the applicable Certification Practices Statement(s) ("**CPS**"), the End User License Agreement ("**EULA**"), and the Privacy Policy, each as attached hereto as Exhibits A-D for reference purposes only, and as available at https://www.digicert.com/legal-repository/ (as updated from time to time), are incorporated by reference into this Agreement.

If Customer is accessing or using the Services on behalf of a business, entity, or individual, then: (a) Customer represents and warrants that it is 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 Customer's access to and use of the Services as well as for the use of Customer's account by others affiliated with Customer, including any employees, agents or contractors.

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 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, or (ii) when Customer affirms its electronic acceptance to an Order Form that DigiCert has presented to Customer via electronic means (e.g., at https://www.digicert.com/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/hour 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.

1.7. 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 60 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, DigiCert may suspend or limit Customer's access to the Portal or Services, including revocation of Certificates, upon written 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 for restricted use in a non-production, test environment, and solely for the purpose of Customer's internal, 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 FOR ANY SERVICES PROVIDED ON A TRIAL BASIS, 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 will, to the extent legally permissible, promptly notify the disclosing party and if requested by the disclosing party, tender to the disclosing party the defense of the subpoena or process. Unless the subpoena or process is timely limited, quashed or extended, the receiving party will then be entitled to comply with the request to the extent permitted by law.

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 at https://www.digicert.com/digicert-privacy-policy (as updated from time to time, the "**Privacy Policy**").

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 for a period of five (5) years 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. This Agreement may be terminated by Customer upon thirty (30) days' prior written notice if Customer does not approve or otherwise receive funds sufficient to continue payments set forth in this Agreement. If Customer terminates the Agreement pursuant to this Section 6.2, Customer may be entitled to receive a pro-rated refund based on its unused prepaid Certificates, or the number of days remaining under the applicable Order Form, whichever is less.

6.3. Restrictions on Further Use. Upon expiration or termination of the Agreement: (i) DigiCert will have the right to revoke all Certificates issued under this Agreement and cease providing all other Services; (ii) except as otherwise specified, all other rights and licenses granted herein terminate,

(iii) each party will immediately discontinue all representations or statements that could imply that a relationship exists between DigiCert and Customer; (iv) each party will continue to comply with the confidentiality requirements in this Agreement; and (v) 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, 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. Third-Party Claims. In the event of any third-party claim against DigiCert, its employees, officers,

directors, shareholders, affiliates, or assigns, arising from (i) Customer's breach of the Agreement, (ii) Customer's failure to protect the authentication mechanisms used to secure the Account, (iii) an allegation of personal injury or property damage caused by the fault or negligence of Customer, (iv) Customer's failure to disclose a material fact related to the use or issuance of the Account or Certificate, or (v) an allegation that the Customer, or an agent of Customer, used DigiCert's product or services to infringe on the rights of a third party (collectively, "**Third-Party Claims**"), DigiCert shall have the right, in its sole discretion, to take any Corrective Measure without liability. For the purposes of this section, a "**Corrective Measure**" includes: (a) immediate termination of the Agreement upon written notice to Customer, (b) restriction to or termination of Customer's access to the Account, (c) removal of allegedly infringing items from DigiCert's products or services, and (d) any other action DigiCert deems, in its reasonable discretion, likely to limit its liability with respect to Third-Party Claims. DigiCert's right to take Corrective Measures is in addition to and does not limit any other remedies available to DigiCert.

7.5. Indemnity. DigiCert agrees, at its own expense, to defend or at its option to settle, any claim, suit or proceeding brought against Customer by any third party for infringement or misappropriation of a valid U.S. patent, copyright or trade secret by the DigiCert Services ("Claim"), except that DigiCert shall have no liability for any Claim resulting from: (i) use or combination of the DigiCert Services with any other goods or services not supplied by DigiCert; (ii) any modification or alteration of any part of the DigiCert Services not provided or authorized by DigiCert, where such Claim would not have arisen except for such use, combination, modification or alteration; (iii) any use of the DigiCert Services by or on behalf of Customer in a manner not permitted under this Agreement, or (iv) continued use of the DigiCert Services by the Customer after being requested to return the infringing DigiCert Services. Should the DigiCert Service become or, in DigiCert's reasonable opinion is likely to become, the subject of any Claim, DigiCert may, at its option and expense, either: (i) procure for Customer the right to continue to use the DigiCert Services as contemplated by this Agreement, (ii) replace or modify the DigiCert Service to make its use in accordance with this Agreement non-infringing, without incurring a material diminution in performance or function, or (iii) with thirty (30) days' notice to Customer, terminate this Agreement and refund to Customer any prepaid fees covering the remainder of the Term after the effective date of termination.

7.6. Indemnity Obligations. Customer must notify DigiCert promptly upon learning of any Claim for which Customer is seeking indemnification pursuant to this Section 7.6, and Customer must provide DigiCert with sole control and authority over the defense and/or settlement of the Claim, subject to Customer's provision of reasonable assistance at the request of DigiCert and at DigiCert's expense; provided that DigiCert may not settle the claim or suit absent the written consent of Customer unless such settlement (a) includes a release of all claims pending against Customer, (b) contains no admission of liability or wrongdoing by Customer, and (c) imposes no obligations upon Customer other than an obligation to stop using the DigiCert Services that are the subject of the claim. DigiCert agrees to pay, subject to the limitations set forth herein, any final judgment entered against Customer or settlement of any such Claim. Customer agrees that DigiCert, at its sole option, shall be relieved of the foregoing obligations unless Customer (i) gives prompt, written notice to DigiCert of any Claims, (ii) cooperates reasonably with DigiCert, and (iii) allows DigiCert the sole right to defend, or at DigiCert's option settle, any such Claim. Section 7.5 states DigiCert's sole liability to the Customer, and the Customer's exclusive remedy against the DigiCert, for any type of Claim described in Section 7.5.

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) the CPS; (ii) the Privacy Policy; (iii) the Certificate Terms of Use; and (iv) 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 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. Neither party may assign any of its rights or obligations under this Agreement without the prior written consent of the other party; however, DigiCert may assign without Customer's prior written consent in the event of a merger, acquisition, change in control, or sale of all or of substantially all of its assets, provided that such assignment does not create a conflict of interest for Customer or is suspended by the Federal government. Otherwise DigiCert will provide Customer with ten (10) days' prior written notice of such assignment and Customer has the right to terminate this Agreement, if required by applicable law.

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 or 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	California state law and United States federal law	Santa Clara County, California
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 either party files suit or initiates an arbitration claim with respect to a dispute involving any aspect of this Agreement, the party shall notify the other party, 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. 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, 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.

DIGICERT, INC.

By: _____

Name: Eric Porter

Title: VP of Finance

CUSTOMER

By: _____

Name: Curt Hagman

Title: Chairman, Board of Supervisors

SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIRMAN OF THE BOARD
LYNNA MONELL
Clerk of the Board of Supervisors
of the County of San Bernardino

By _____ Deputy

Exhibit A

Certification Practices Statement

[Begins on the following page]

DigiCert

Certification Practices Statement

DigiCert, Inc.
Version 4.20
November 22, 2019

2801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This document is the DigiCert, Inc. ("DigiCert") Certification Practices Statement (CPS) that outlines the principles and practices related to DigiCert's certification and time-stamping services. This CPS applies to all entities participating in or using DigiCert's certificate and time-stamping services, excluding participants in DigiCert's Private PKI services, which are not cross-certified or publicly trusted. This CPS only addresses the actions of DigiCert and not those of third parties operating with cross certificates issued by DigiCert. Specific requirements regarding those Certificates are set forth in the individual agreements with the appropriate DigiCert customer and in that third party's own CPS.

This CPS describes the practices used to comply with the current versions of the following policies, guidelines, and requirements:

- the DigiCert Certificate Policy (the "CP"),
- the Adobe Systems Inc. ("Adobe") AATL Certificate Policy,
- Mozilla Root Store Policy,
- the Federal Bridge Certification Authority ("FBCA") Certificate Policy,
- the Certification Authority/Browser Forum ("CAB Forum") Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") located at https://cabforum.org/baseline-requirements-documents,
- the CAB Forum Guidelines for the Issuance and Management of Extended Validation Certificates ("EV Guidelines") located at https://cabforum.org/extended-validation,
- the CAB Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates,
- the CAB Forum Network and Certificate System Security Requirements,
- the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ("Minimum Requirements for Code Signing") located at https://aka.ms/csbr,
- the Direct Trust Community X.509 Certificate Policy, and
- the Wi-Fi Alliance Hotspot 2.0 Specification.

If any inconsistency exists between this CPS and the normative provisions of the foregoing policies, guidelines, and requirements ("Applicable Requirements"), then the Applicable Requirements take precedence over this CPS. Time-stamping services are provided according to IETF RFC 3161 and other technical standards.

This CPS is only one of several documents that control DigiCert's certification services. Other important documents include both private and public documents, such as the CP, DigiCert's agreements with its customers, Relying Party agreements, and DigiCert's privacy policy. DigiCert may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CPS is divided into nine parts that cover the security controls and practices and procedures for certificate and time-stamping services within the DigiCert PKI. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation."

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the DigiCert Certification Practices Statement and was first approved for publication on 9 August 2010 by the DigiCert Policy Authority (DCPA). The following revisions have been made to the original document:

Date	Changes	Version
21-November-2019	Minor editorial changes throughout the document for consistency and accuracy.	4.20
25-July-2019	Added reference to AATL 2.0 to section 1.6.3 for continuity. Modifications added to sections 3.2.2 and 7.1.4 to include details about information source review. Added security policy reference to section 6.4.2.	4.19
17-April-2019	Edited sections 3.1.6, 3.2.1, 6.1.3, and 7.1.4 to clarify naming and proof-of-possession practices.	4.18
01-March-2019	Added Class 2 Authentication-Only OID, clarified Legacy OIDs, updated validation practices for compliance with Baseline Requirements, clarified physical security control areas, modified archive procedures, and updated certificate validity table in section 6.3.2.	4.17
09-October-2018	Clarification to email validation methods and Mozilla CA Root Policy 2.6.1 updates made throughout the document. Removed frequent password changing practice from section 6.4.1 to comply with NIST Special Publication 800-63-3: Digital Authentication Guidelines. Changes made to section 3.2.2 to clarify differences between Levels 1-4 and Class 1-3 Certificate issuance practices. Added sections 1.5.2.1 for Revocation Reporting Contact Person and additions/revisions to section 4.9 to meet the revocation requirements for CABF ballot SC6.	4.16
24-August-2018	Updates throughout for Adobe AATL 2.0, added Class 1-3 OIDs, removed unused definitions and references to EU Qualified Certificates, updated sections 3.2.2 and 3.2.3 regarding email validation, added language in section 6.1.1 to specify that DigiCert does not create key pairs for publicly trusted end- entity TLS Certificates, amended limitation of liability in section 9.8 to address Netsure Extended Warranty and Relying Party Agreement, and removed line 9 in Appendix A	4.15
25-January-2018	Added language based on the CAB Forum's Baseline Requirements, as indicated by Mozilla's Self-Assessment process	4.14
8-November-2017	Added Symantec CAA identifying domains	4.13
8-September-2017	Added CAA processing provisions, removed references to PIV-I, revised descriptions of processes used for validating identity, updated description of physical access and security, added trusted role of RA Administrator, and removed "conflict-of-interest" prohibition from trusted roles.	4.12
23-February-2017	Updated address, made revisions related to the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, and made other changes to update the CPS.	4.11
9-September-2016	Updated to: include Cybertrust CAs acquired from Verizon, clarify identity verification process, update document in accordance with FBCA CP v. 2.29 and sec. 9.6.3 of Baseline Requirements.	4.10
1-June-2015	Updated CPS to conform to practices for backup, archival, CA key generation, and certificate acceptance.	4.09
1-April-2015	Minor changes made to update with CA/Browser Forum guidelines and for consistency with DigiCert CP v. 4.08	4.08
7-October-2014	Updated for consistency with DigiCert CP v. 4.07	4.07

Date	Changes	Version
21-November-2019	Minor editorial changes throughout the document for consistency and accuracy.	4.20
25-July-2019	Added reference to AATL 2.0 to section 1.6.3 for continuity. Modifications added to sections 3.2.2 and 7.1.4 to include details about information source review. Added security policy reference to section 6.4.2.	4.19
17-April-2019	Edited sections 3.1.6, 3.2.1, 6.1.3, and 7.1.4 to clarify naming and proof-of-possession practices.	4.18
14-May-2014	Updated practices to comply with new policy requirements and changes to the DirectTrust CP, Baseline Requirements, EV Guidelines, and EV Code Signing Guidelines.	4.06
2-May-2013	Updated mailing address. Also updated practices to comply with new policy requirements, the DirectTrust CP, changes to the Adobe program, and CAB Forum guidelines.	4.05
10-May-2012	Updated to include practices set forth in the Baseline Requirements, the current Mozilla CA Policy, EV Code Signing, the IGTF, and other policy bodies.	4.04
3-May-2011	IGTF Certificates added and minor updates made to several sections.	4.03
29-October-2010	Changes made in response to comments from the FPKI CPWG regarding certificate status services, trusted roles, and off-site backup of archive.	4.02
26-August-2010	Updated the process used to authenticate the certificate requester's authority under section 3.2.5 for code signing Certificates issued to organizations	4.01
9-August-2010	This version 4.0 replaces the DigiCert Certificate Policy and Certification Practices Statement, Version 3.08, dated May 29, 2009, and the DigiCert Certification Practice Statement for Extended Validation Certificates, Version 1.0.4, May 29, 2009.	4.0

The OID for DigiCert is joint-iso-ccitt (2) country (16) USA (840) US-company (1) DigiCert (114412). The OID-arc for this version 4 of the CPS is 2.16.840.1.114412.0.2.4. Subsequent revisions to this CPS might have new OID assignments. DigiCert issues Certificates and time-stamp tokens containing the following OIDs / OID arcs:

Digitally Signed Object	Object Identifier (OID)
Domain Vetted (DV) SSL/TLS Server Certificates per the Baseline Requirements	2.16.840.1.114412.1.2 and/or 2.23.140.1.2.1 (CAB Forum Baseline Reqs.)
Organization Vetted (OV) SSL/TLS Server Certificates per the Baseline Requirements	2.16.840.1.114412.1.1 and/or 2.23.140.1.2.2 (CAB Forum Baseline Reqs.)
Individual Vetted (IV) SSL/TLS Server Certificates per the Baseline Requirements	2.16.840.1.114412.1.1 and/or 2.23.140.1.2.3 (CAB Forum Baseline Reqs.)
Hotspot 2.0 OSU Server Certificates	2.16.840.1.114412.1.5
Federated Device Certificate	2.16.840.1.114412.1.11
Federated Device Hardware Certificate	2.16.840.1.114412.1.12
Issuer CA (where allowed by policy)	2.5.29.32.0 (anyPolicy)
Extended Validation (EV) SSL/TLS Server Certificates	2.16.840.1.114412.2.1, 2.23.140.1.1(CAB Forum EV Guidelines), 1.3.6.1.4.1.6334.1.100.1 (originally registered by beTRUSTed), and/or 2.16.840.1.113733.1.7.23.6 (originally registered by Verisign)

Digitally Signed Object	Object Identifier (OID)
Object Signing Certificates	2.16.840.1.114412.3
Code Signing Certificates	2.16.840.1.114412.3.1
Minimum Requirements for Code Signing	2.16.840.1.114412.3.1.1 and/or 2.23.140.1.4.1
Extended Validation Code Signing	2.16.840.1.114412.3.2 and/or 2.23.140.1.3
Windows Kernel Driver Signing	2.16.840.1.114412.3.11
Adobe Signing Certificate	2.16.840.1.114412.3.21
Client Certificate OID Arc	2.16.840.1.114412.4
Level 1 Certificates - Personal	2.16.840.1.114412.4.1.1
Level 1 Certificates - Enterprise	2.16.840.1.114412.4.1.2
Level 2 Certificates	2.16.840.1.114412.4.2
Level 3 Certificates - US	2.16.840.1.114412.4.3.1
Level 3 Certificates - CBP	2.16.840.1.114412.4.3.2
Level 4 Certificates - US	2.16.840.1.114412.4.4.1
Level 4 Certificates - CBP	2.16.840.1.114412.4.4.2
Class 1-3 Certificates	2.16.840.1.114412.5
Class 1 Certificates	2.16.840.1.113733.1.7.23.1 and/or 2.16.840.1.114412.5.1
Class 2 Certificates	2.16.840.1.113733.1.7.23.2 and/or 2.16.840.1.114412.5.2
Class 3 Certificates	2.16.840.1.113733.1.7.23.3.2 (private hierarchy) and/or 2.16.840.1.114412.5.3
Grid Certificate OID Arcs	2.16.840.1.114412.4.31 or 2.16.840.1.114412.31 (Grid-only arc)
IGTF Classic X.509 Authorities with secured infrastructure	2.16.840.1.114412.4.31.1 (Client w/ Public), 2.16.840.1.114412.31.4.1.1 (Client Grid Only), and/or 1.2.840.113612.5.2.2.1.x (IGTF)
IGTF Member Integrated X.509 Credential Services with Secured Infrastructure Certificates	2.16.840.1.114412.4.31.5 and/or 1.2.840.113612.5.2.2.5.x (IGTF)
IGTF Grid Host - Public Trust	2.16.840.1.114412.1.31.1
IGTF Grid-Only Host Certificate	2.16.840.1.114412.31.1.1.1, 1.2.840.113612.5.2.2.1.x (IGTF), and/or 1.2.840.113612.5.2.2.5.x (IGTF)
Authentication-Only Certificates	2.16.840.1.114412.6
Class 2 Authentication-Only Certificates	2.16.840.1.114412.6.2
Trusted Time-stamping	2.16.840.1.114412.7.1
Legacy arc	2.16.840.1.114412.81
Test arc	2.16.840.1.114412.99

All OIDs mentioned above belong to their respective owners. The specific OIDs used when objects are signed pursuant to this CPS are indicated in the object's respective Certificate Policies extension. For instance, when DigiCert issues a Certificate containing one of the above-specified policy identifiers for "Baseline Requirements," "Minimum Requirements," or "Extended Validation," it asserts that the Certificate was issued and is managed in accordance with those applicable requirements. Commercial Best Practices ("CBP") differs from "US" in that there are no trusted role citizenship requirements for an Issuer CA issuing under a CBP policy, whereas policies designated "US" must follow the citizenship practices set forth in Section 5.3.1.

The Legacy arc exists to identify Certificates issued to achieve compatibility with legacy systems (e.g. systems that are incapable of processing newer algorithms that might be required by industry best practices, systems that due to pinning still require CA certificates that are no longer publicly trusted, etc.).

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

DigiCert operates certification authorities (CAs) that issue digital certificates. As the operator of several CAs, DigiCert performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital Certificate, and maintaining, issuing, and publishing CRLs and OCSP responses. General information about DigiCert's products and services are available at www.digicert.com.

DigiCert owns and operates the GTE Cybertrust Global Root, the Baltimore Cybertrust Root, the Cybertrust Global Root CA, and the Verizon Global Root CA. In limited circumstances, these root CAs are used to issue cross Certificates to external third parties operating their own PKIs. An "external subordinate CA" is an unaffiliated third party that is issued a subordinate CA Certificate by DigiCert where the Private Key associated with that CA Certificate is not maintained under the physical control of DigiCert. In accordance with requirements of the U.S. Federal PKI Policy Authority (FPKIPA), DigiCert notifies the FPKIPA prior to issuing a CA Certificate chaining to the Federal Bridge CA to an external subordinate CA. All external subordinate CAs are prohibited, either technically or contractually, from issuing Certificates to domain names or IP addresses that a Subscriber does not legitimately own or control (i.e. issuance for purposes of "traffic management" is prohibited), and external subordinate CAs are required to implement procedures that are at least as restrictive as those found herein. DigiCert ensures that no CA chaining to the Federal Bridge CA has more than one trust path to the Federal Bridge CA (regardless of path validation results).

DigiCert is also a time stamping authority (TSA) and provides proof-of-existence for data at an instant in time as described herein.

1.3.2. Registration Authorities and Other Delegated Third Parties

Except for the authentication of domain control or IP address verification performed solely by DigiCert in accordance with Section 3.2.2, DigiCert may delegate the performance of certain functions to third party Registration Authorities (RA). The specific role of an RA or Delegated Third Party varies greatly between entities, ranging from simple translation services to actual assistance in gathering and verifying Applicant information. Some RAs operate identity management systems (IdMs) and may manage the certificate lifecycle for end-users. For IGTF Certificates, designated RAs are responsible for vetting the identity of each certificate applicant. DigiCert contractually obligates each Delegated Third Party to abide by the policies and industry standards that are applicable to that Delegated Third Party's delegated responsibilities. RA personnel involved in the issuance of publicly-trusted SSL/TLS Server Certificates must undergo the skills and training required under Section 5.3.

1.3.3. Subscribers

Subscribers use DigiCert's services and PKI to support transactions and communications. Subscribers are not always the party identified in a Certificate, such as when Certificates are issued to an organization's employees. The *Subject* of a Certificate is the party named in the Certificate. A *Subscriber*, as used herein, may refer to the Subject of the Certificate and the entity that contracted with DigiCert for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

1.3.4. Relying Parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature issued by DigiCert. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the CRL distribution point is detailed within the Certificate.

1.3.5. Other Participants

Other participants include Accreditation Authorities (such as Policy Management Authorities, Federation Operators, Application Software Vendors, and applicable Community-of-Interest sponsors); Bridge CAs and CAs cross-certified with DigiCert's CAs that serve as trust anchors in other PKI communities; and Time Source Entities, Time Stamp Token Requesters, and Time Stamp Verifiers involved in trusted time stamping.

Accreditation Authorities are granted an unlimited right to re-distribute DigiCert's root Certificates and related information in connection with the accreditation.

1.4. CERTIFICATE USAGE

A *digital Certificate* (or *Certificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card. A *time-stamp token* (*TST*) cryptographically binds a representation of data to a particular time stamp, thus establishing evidence that the data existed at a certain point in time.

1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CPS.

This CPS covers several different types of end entity Certificates/tokens with varying levels of assurance. The following table provides a brief description of the appropriate uses of each. The descriptions are for guidance only and are not binding.

Certificate	Appropriate Use
DV SSL/TLS Server Certificates	Used to secure online communication where the risks and consequences of data compromise are low, including non-monetary transactions or transactions with little risk of fraud or malicious access.
OV SSL/TLS Server Certificates	Used to secure online communication where the risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.
EV SSL/TLS Server Certificates	Used to secure online communication where risks and consequences of data compromise are high, including transactions having high monetary value, risk of fraud, or where involving access to private information where the likelihood of malicious access is high.
Hotspot 2.0 OSU Server Certificates	Used to authenticate OSU Servers pursuant to the Wi-Fi Alliance's Hotspot 2.0 specification.
Federated Device Certificates	Similar to SSL/TLS Server Certificates above but for use as necessary in connection with specific cross-certified PKIs
Code Signing Certificates, including EV Code Signing	Establishes the identity of the Subscriber named in the Certificate and that the signed code has not been modified since signing.
Rudimentary Level 1 Client Certificates - Personal	Provides the lowest degree of assurance concerning identity of the individual and is generally used only to provide data integrity to the information being signed. These Certificates should only be used where the risk of malicious activity is low and if an authenticated transaction is not required.

Certificate	Appropriate Use
Level 1 Client Certificates - Enterprise and Class 1 and 2 Certificates	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 2 Client Certificates (FBCA basic assurance certificates)	Issued to identity-vetted individuals. Certificates specify if the name is a pseudonym. Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 3 Client Certificates (FBCA medium certificates) and Class 3 Certificates	Used in environments where risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.
Level 4 Client Certificates (FBCA medium hardware Certificates)	Used in environments where risks and consequences of data compromise are high, including transactions having high monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is high.
Direct Certificates	Used to transfer health care information in accordance with the Direct Protocol adopted by the ONC. Direct Certificates are issued as Level 2 or Level 3 Certificates.
Authentication Only	Used where the identity of the certificate holder is irrelevant and where the risk of unauthorized access to a secure site is low.
IGTF and Grid-only Certificates	Support identity assertions and system authentication amongst participants in the International Grid Trust Federation. IGTF Certificates include those issued as publicly-trusted client Certificates and those issued under the Grid-only arc.
Adobe Signing Certificates	Used to sign Adobe documents and show that the portion of the document signed by the author has not been modified since signing.
Time Stamp Token	Used to identify the existence of data at a set period of time.

1.4.2. Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified in accordance with this CPS when the Certificate issued. Code signing Certificates do not indicate that the signed code is safe to install or free from malware, bugs, or vulnerabilities.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

This CPS and the documents referenced herein are maintained by the DCPA, which can be contacted at:

DigiCert Policy Authority Suite 500
2801 N. Thanksgiving Way Lehi,
UT 84043 USA
Tel: 1-801-701-9600
Fax: 1-801-705-0481
www.digicert.com
support@digicert.com

1.5.2. Contact Person Attn:

Legal Counsel DigiCert
Policy Authority Suite 500

2801 N. Thanksgiving Way Lehi,
UT 84043 USA
www.digicert.com
support@digicert.com

1.5.2.1. Revocation Reporting Contact Person

Attn: Support
DigiCert Technical Support Suite
500
2801 N. Thanksgiving Way Lehi,
UT 84043 USA
https://www.digicert.com/certificate-revocation.htm

To request that a Certificate be revoked, please email revoke@digicert.com.

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. DigiCert or an RA will authenticate and log each revocation request according to Section 4.9 of the DigiCert CP and this CPS. DigiCert will always revoke a Certificate if the request is authenticated as originating from the Subscriber or the Affiliated Organization listed in the Certificate. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, DigiCert or an RA will investigate the alleged basis for the revocation request prior to taking action in accordance with Section 4.9.1 and 4.9.3.

1.5.3. Person Determining CPS Suitability for the Policy

The DCPA determines the suitability and applicability of this CPS based on the results and recommendations received from an independent auditor (see Section 8). The DCPA is also responsible for evaluating and acting upon the results of compliance audits.

1.5.4. CPS Approval Procedures

The DCPA approves the CPS and any amendments. Amendments are made after the DCPA has reviewed the amendments' consistency with the CP, by either updating the entire CPS or by publishing an addendum. The DCPA determines whether an amendment to this CPS is consistent with the CP, requires notice, or an OID change. *See also* Section 9.10 and Section 9.12 below.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

"Applicant" means an entity applying for a Certificate.

"Application Software Vendor" means a software developer whose software displays or uses DigiCert Certificates and distributes DigiCert's root Certificates.

"CAB Forum" is defined in section 1.1.

"Certificate" means an electronic document that uses a digital signature to bind a Public Key and an identity.

"Certificate Approver" is defined in the EV Guidelines.

"Certificate Requester" is defined in the EV Guidelines. **"Contract**

Signer" is defined in the EV Guidelines.

"Direct Address" means an email address conforming to the Applicability Statement for Secure Health Transport.

"Direct Address Certificate" means a Certificate containing an entire Direct Address.

"Direct Organizational Certificate" means a Certificate containing only the domain name portion of a Direct Address.

"Domain Name" is as defined in the Baseline Requirements.

"EV Guidelines" is defined in section 1.1.

"Key Pair" means a Private Key and associated Public Key.

"OCSP Responder" means an online software application operated under the authority of DigiCert and connected to its repository for processing certificate status requests.

"Private Key" means the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

"Public Key" means the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

"Qualified Certificate" means a Certificate that meets the requirements of EU law and is provided by an Issuer CA meeting the requirements of EU law.

"Relying Party" means an entity that relies upon either the information contained within a Certificate or a time-stamp token.

"Relying Party Agreement" means an agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using DigiCert's Repository. The Relying Party Agreement is available for reference through a DigiCert online repository.

"Subscriber" means either the entity identified as the subject in the Certificate or the entity that is receiving DigiCert's time-stamping services.

"Subscriber Agreement" means an agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

"WebTrust" means the current version of CPA Canada's WebTrust Program for Certification Authorities.

"WHOIS" Information retrieved directly from the Domain Name Registrar or registry operator via the protocol, the Registry Data Access Protocol, or an HTTPS website.

1.6.2. Acronyms

AATL	Adobe Approved Trust List
CA	Certificate Authority or Certification Authority
CAA	Certification Authority Authorization
CAB	"CA/Browser" as in "CAB Forum"
CMS	Card Management System

CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As (also known as "Trading As") DCPA DigiCert Policy Authority
DNS	Domain Name Service
DV	Domain Validated
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard FQDN Fully Qualified Domain Name
FTP	File Transfer Protocol
GLEIF	Global Legal Entity Identifier Foundation HISP Health Information Service Provider
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers IdM Identity Management System
IDN	Internationalized Domain Name
ISSO	Information System Security Officer
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
ITU	International Telecommunication Union
IV	Individual Validated
LEI	Legal Entity Identifier
MICS	Member-Integrated Credential Service (IGTF) NIST National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ONC	Office of the National Coordinator for Healthcare (U.S.) OSU Online Sign-Up (Wi-Fi Alliance Hotspot 2.0)
OV	Organization Validated
PIN	Personal Identification Number (e.g. a secret access code)
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure RA Registration Authority
RFC	Request for Comments (at IETF.org)
SAN	Subject Alternative Name
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TSA	Time Stamping Authority
TST	Time-Stamp Token
TTL	Time To Live
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3. References

Adobe Approved Trust List Technical Requirements, v.2.0

CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")

CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates ("EV Guidelines")

DirectTrust Community X.509 Certificate Policy, v.1.3 FBCA

Supplementary Antecedent, In-Person Definition

Wi-Fi Alliance Hotspot 2.0 Release 2 Online Signup Certificate Policy Specification (Hotspot 2.0 CP)

X.509 Certificate Policy for the Federal Bridge Certification Authority, v. 2.32 Mozilla

Root Store Policy v.2.6.1

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

DigiCert makes its root Certificates, revocation data for issued digital Certificates, CPs, CPSs, Relying Party Agreements, and standard Subscriber Agreements available in public repositories. DigiCert develops, implements, enforces, and annually updates this CPS to meet the compliance standards of the documents listed in Section 1.6.3. These updates also describe how the latest version of the Baseline Requirements are implemented. As Baseline Requirements are updated, DigiCert reviews the changes to determine their impact on these practices. Each section impacted by the Baseline Requirements will be updated and provided to the DCPA for approval and implementation. If an SSL/TLS Server Certificate is intended to be trusted in Chrome, it is published by posting it in a Certificate Transparency log.

DigiCert's legal repository for most services is located at https://www.digicert.com/legal-repository/. DigiCert's publicly trusted root Certificates and its CRLs and OCSP responses are available through online resources 24 hours a day, 7 days a week with systems described in Section 5 to minimize downtime.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The DigiCert certificate services and the repository are accessible through several means of communication:

1. On the web: https://www.digicert.com (and via URIs included in the certificates themselves)
2. By email to admin@digicert.com
3. By mail addressed to: DigiCert, Inc., Suite 500, 2801 N. Thanksgiving Way, Lehi, Utah 84043 4. By telephone Tel: 1-801-877-2100

5. By fax: 1-801-705-0481

2.3. TIME OR FREQUENCY OF PUBLICATION

CA Certificates are published in a repository as soon as possible after issuance. CRLs for end-user Certificates are issued at least once per day. CRLs for CA Certificates are issued at least every 6 months (every 31 days for offline CAs chaining to the Federal Bridge CA), and also within 18 hours if a CA Certificate is revoked. Under special circumstances, DigiCert may publish new CRLs prior to the scheduled issuance of the next CRL. (See Section 4.9 for additional details.)

New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

2.4. ACCESS CONTROLS ON REPOSITORIES

Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards except that DigiCert may issue a Level 1 Certificate with a null subject DN if it includes at least one alternative name form that is marked critical. When DNs are used, common names must respect namespace uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous Certificates, except where stated otherwise under Section 3.1.3.

DigiCert issues EV SSL/TLS Certificates to .onion domains in accordance with Appendix F of the EV Guidelines.

DigiCert issues OSU Server Certificates with subject alternative names that contain: (1) OSU Server FQDN(s) and (2) Friendly Name(s) that identify the wifi service provider, in accordance with section 3.4 of the Hotspot 2.0 CP.

3.1.2. Need for Names to be Meaningful

DigiCert uses distinguished names that identify both the entity (i.e. person, organization, device, or object) that is the subject of the Certificate and the entity that is the issuer of the Certificate. DigiCert only allows directory information trees that accurately reflect organization structures.

3.1.3. Anonymity or Pseudonymity of Subscribers

Generally, DigiCert does not issue anonymous or pseudonymous Certificates; however, for IDNs, DigiCert may include the Punycode version of the IDN as a subject name. DigiCert may also issue other pseudonymous end-entity Certificates if they are not prohibited by policy and any applicable name space uniqueness requirements are met.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5. Uniqueness of Names

The uniqueness of each subject name in a Certificate is enforced as follows:

SSL/TLS Server Server Certificates	Inclusion of the domain name in the Certificate. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).
Client Certificates	Requiring a unique email address or a unique organization name combined/associated with a unique serial integer.
IGTF and Grid-only Device Certificates	For device Certificates, an FQDN is included in the appropriate fields. For other Certificates, DigiCert may append a unique ID to a name listed in the Certificate.
Code Signing Certificates (including CDS Certificates)	Requiring a unique organization name and address or a unique organization name combined/associated with a unique serial integer.
Time Stamping	Requiring a unique hash and time or unique serial integer assigned to the time stamp

3.1.6. Recognition, Authentication, and Role of Trademarks

For OSU Server Certificates, DigiCert conducts a trademark search of logos and Friendly Names in relevant mark registration databases, such as the U.S. Patent and Trademark Office or WIPO, to confirm an applicant's

right to use a particular trademark. Based on the results of such search(es), DigiCert issues an OSU Server Certificate with one or more logotype extensions containing the hash algorithm and hash value of logos associated with the service provider. If an applicant does not have a friendly name or logo available, DigiCert may include a logo and friendly name specified by the Wi-Fi Alliance.

For EV SSL Certificates, DigiCert implements a process that prevents EV Certificates from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless DigiCert has verified this information in accordance with the EV Guidelines and section 3.2.

For all other Certificates, unless otherwise specifically stated in this CPS, DigiCert does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. DigiCert may reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2. INITIAL IDENTITY VALIDATION

DigiCert may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. DigiCert may refuse to issue a Certificate in its sole discretion.

3.2.1. Method to Prove Possession of Private Key

DigiCert establishes that the Applicant for FBCA Certificates (where the party named in a certificate generates its own keys) holds or controls the Private Key corresponding to the Public Key by performing signature verification or decryption on data purported to have been digitally signed or encrypted with the Private Key by using the Public Key associated with the certificate request.

3.2.2. Authentication of Organization and Domain/Email Control

DV SSL/TLS Server Certificates	DigiCert validates the Applicant's right to use or control each domain name that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the following procedures from section 3.2.2.4 of the Baseline Requirements: 1. This method (BR Section 3.2.2.4.1) is no longer used because it was deprecated as of 1-August-2018; 2. Email, Fax, SMS, or Postal Mail to the Domain Contact by sending a unique Random Value (valid for no more than 30 days from its creation) through email, fax, SMS, or postal mail, to the Domain Contact and receiving confirmation by their use of the Random Value, performed in accordance with BR Section 3.2.2.4.2; 3. (BR Section 3.2.2.4.3) is no longer used because it was deprecated as of 31-May-2019; 4. Constructed Email to Domain Contact establishing the Applicant's control over the FQDN by sending an email created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, including a Random Value in the email, and receiving a response using the Random Value, performed in accordance with BR Section 3.2.2.4.4; 5. (BR Section 3.2.2.4.5) is no longer used because it was deprecated as of 1-August-2018; 6. An Agreed-Upon Change to the Website by the Applicant placing an agreed-upon Request Token or Random Value in the "/.well-known/pki-validation" directory, performed in accordance with BR Section 3.2.2.4.6;

	7. Domain Name Service (DNS) Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance BR Section 3.2.2.4.7; 8. IP Address - by confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Sections 3.2.2.5 and 3.2.2.4.8; 9. (BR Section 3.2.2.4.9) is no longer used because it was deprecated upon publication of v.4.16 of this CPS; 10. (BR Section 3.2.2.4.10) is no longer used because it was deprecated upon publication of v.4.16 of this CPS; 11. (BR Section 3.2.2.4.11) is no longer used because it was deprecated as of 5-February-2018; 12. Confirming that the Applicant is the Domain Contact for the Base Domain Name (provided that the CA or RA is also the Domain Name Registrar or an Affiliate of the Registrar), performed in accordance with BR Section 3.2.2.4.12; 13. Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 performed in accordance with BR Section 3.2.2.4.13; 14. Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.4.14; 15. Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.15; and 16. Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.16.

	All of the above methods for validation, except IP Address (BR Section 3.2.2.4.8) may be used for Wildcard Certificate Domain Name validation along with current best practice of consulting a public suffix list. DigiCert verifies an included country code using (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; or (c) information provided by the Domain Name Registrar.
IV and OV SSL/TLS Server, OSU Server, Object Signing, and Device Certificates (excluding device Certificates issued under the Grid-only arc)	DigiCert validates the Applicant's right to use or control the Domain Name(s) and the country code that will be listed in the Certificate using the DV SSL/TLS Server Certificate validation procedures above. DigiCert also verifies the identity and address of the Applicant using the procedures found in section 3.2.2.1 or section 3.2.3 of the Baseline Requirements. DigiCert verifies any DBA included in a Certificate using a third party or government source, attestation letter, or reliable form of identification in accordance with section 3.2.2 of the Baseline Requirements.
Device Certificates issued under the Grid-only arc	An RA or Trusted Agent validates the applicant's information in accordance with an RPS (or similar document) applicable to the community of interest.
EV SSL/TLS Server and EV Code Signing Certificates	Information concerning organization identity related to the issuance of EV SSL/TLS Server Certificates is validated in accordance with the EV Guidelines.
S/MIME Certificates issued as Level 1-4 Client Certificates using the native DigiCert infrastructure. [1]	DigiCert verifies an individual's or organization's right to use or control an email address to be contained in a Certificate that will have the "Secure Email" EKU by doing one of the following: 1. By verifying domain control over the email domain using one of the procedures listed above in this table under the heading "DV SSL/TLS Server Certificates"; or 2. by sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response through use of the Random Value to indicate that the Applicant and/or Organization owns or controls that same email address.
S/MIME Certificates issued as Class 1-2 Certificates using the acquired Symantec infrastructure[2]	An RA may have an Applicant associated with the Organization connect through a browser to complete one of the following three types of authentication: 1. Manual Authentication: The Applicant submits enrollment information and a Public Key/CSR. An RA reviews the enrollment information received from the Applicant in a customized interface. If approved, the system automatically

[1] Level 1 through Level 4 Certificates are distinct and different from Class 1 through 3 certificates listed in the next row because they are issued with different policy OIDs, as referenced in section 1.2, and issued by a separate system.

[2] Class 1 through Class 3 Certificates are distinct and different from Level 1 through 4 Certificates listed in the previous row and they are issued with different policy OIDs, as referenced in section 1.2, and issued by a separate system.

	sends a PIN to the enrolled email address for the Applicant to use to retrieve the Certificate at a specified URL. If the Applicant's Private Key matches, the Certificate is installed. 2. Manual Passcode Authentication: The system is pre- populated with the Applicant's information, including an email address, that the RA has reviewed that comes from existing business relations or an employee data base. The system sends a randomly generated passcode to the enrolled email address for the Applicant to use to retrieve the Certificate at a specified URL. The Applicant's key pair and certificate are generated and installed on the Applicant's system; or Automated Enrollment Code/Passcode Authentication: The system is pre-populated with the Applicant's information, including an email address, and an Enrollment Code/Passcode. The Enrollment Code/Passcode is sent to the Applicant's email address. The Enrollment Code/Passcode is checked for validity in the system and if verified, the system will generate the Certificate based on the Public Key matching the Private Key 3. Automated Administrative or Web Service API Authentication: Provided that the email address or domain has been verified pursuant to one of the methods used for Levels 1-4 as described above in this table, the Applicant submits enrollment information and a Public Key/CSR. Applicant data received through the portal is compared with a trusted source of verified email addresses (e.g., an active directory). Upon approval, the status of the request is set to "approved" and the Certificate is sent back through an API. If the Applicant's Private Key matches, the Certificate is installed.
Class 3 Certificates using the acquired Symantec infrastructure	An RA may connect through a customized interface to complete one of the following two types of authentication: 1. Manual Authentication: The Applicant submits enrollment information and a Public Key/CSR. An RA reviews the enrollment information received from the Applicant associated with the Organization in a customized interface. If approved, the system automatically sends the Certificate to the enrolled email for the Applicant which the Applicant must be able to access in order to install the certificate. 2. Automated Administrative or Web Service API Authentication: The Applicant submits enrollment information and a Public Key/CSR. Applicant data received through the portal is compared with a trusted source (e.g., an active directory) that contains the email address or domain that has been verified pursuant to methods used for Levels 1- 4 as described above in this table. Upon approval, the status of the request is set to "approved" and the Certificate is sent back through an API. If the Applicant's Private Key matches, the Certificate is installed.

DigiCert maintains and utilizes a scoring system to flag certificate requests that potentially present a higher risk of fraud. Those certificate requests that are flagged "high risk" receive additional scrutiny or verification

prior to issuance, which may include obtaining additional documentation from or additional communication with the Applicant.

Before issuing an SSL/TLS Server Certificate with a domain name that has not been previously verified as within the scope of an RA's or other Delegated Third Party's allowed domain names, DigiCert establishes that the RA or Delegated Third Party has the right to use the Domain Name by independently verifying the authorization with the domain owner, as described and allowed by the above.

For each IP Address listed in a Certificate, DigiCert confirms that, as of the date the Certificate was issued, the Applicant controlled the IP Address by:

1. Having the Applicant demonstrate practical control over the IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1;
2. Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.5.2;
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3;
4. After July 31, 2019, DigiCert will not perform IP Address validations using the any-other-method method of BR Section 3.2.2.5.4;
5. Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address Registration Authority, and obtaining a response confirming the Applicant's request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5;
6. Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.6; or
7. Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.7.

DigiCert verifies the organization name, address, legal existence, and authorization for CA Certificates that cross-certify with the FBCA.

DigiCert uses a documented internal process to check the accuracy of information sources and databases to ensure the data is acceptable, including reviewing the database provider's terms of use.

DigiCert uses data from databases and information sources after DigiCert determines that the sources are:

- not self-reported; and
- the database or the information sources that demonstrate transparent efforts and reported methods to be accurate which can then be verified by DigiCert through analysis of the resource against other known reliable resources.

For Legal Entity Identifier (LEI) numbers listed in Certificates, DigiCert includes the value after verification, through the appropriate mechanism provided by Global Legal Entity Identifier Foundation (GLEIF), that the LEI is associated with entity information provided. LEI lookups are treated as an information from a source described above, but not currently relied upon as a primary source of information for verification. Instead, this information is treated as additional correlation of identity information found in the certificate and provided in the certificate for the convenience and use of data researchers and the legal entities operating the certificates.

3.2.3. Authentication of Individual Identity

If a Certificate will contain the identity of an individual, then DigiCert or an RA validates the identity of the individual using the following procedures:

Certificate	Validation
IV SSL/TLS Server Certificates and Object Signing Certificates (issued to an individual)	1. a. DigiCert or the RA obtains and reviews a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type). DigiCert or the RA inspects the copy for any indication of alteration or falsification. b. For Object Signing Certificates, a validation specialist also engages in a videoconference call with the Applicant, who must present their photo ID and sign a Declaration of Identity, witnessed by the validation specialist, which is recorded as evidence. 2. DigiCert may additionally cross-check the Applicant's name and address for consistency with available third-party data sources. 3. If further assurance is required, then the Applicant must provide an additional form of identification, such as recent utility bills, financial account statements, credit card, an additional ID credential, or equivalent document type. 4. DigiCert or the RA confirms that the Applicant is able to receive communication by telephone, postal mail/courier, or fax. If DigiCert cannot verify the Applicant's identity using the procedures described above, then the Applicant must submit a Declaration of Identity that is witnessed and signed by a Registration Authority, Trusted Agent, notary, lawyer, accountant, postal carrier, or any entity certified by a State or National Government as authorized to confirm identities.
Device Certificate Sponsors	See section 3.2.3.3
OSU Server Certificates	DigiCert verifies that the requester is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization.
EV Certificates issued to a business entity	As specified in section 11.2.1(3) of the EV Guidelines
Grid-only Certificates	Either the RA responsible for the grid community or a Trusted Agent obtains an identity document during a face-to-face meeting with the Applicant, or a Trusted Agent attests that the Applicant is personally known to the Trusted Agent. The RA must retain sufficient information about the applicant's identity to prove upon DigiCert's request that the applicant was properly identified.
Authentication-Only Certificates	The entity controlling the secure location must represent that the certificate holder is authorized to access the location.
Level 1 Client Certificates – Personal (email Certificates)	As specified in Section 3.2.2 (no identity verification other than control of the email address listed in the Certificate).

Certificate	Validation
Level 1 Client Certificates - Enterprise	Any one of the following: 1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent with presentment of an identity credential (e.g., driver's license or birth certificate). 2. Using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as: a. the ability to place or receive calls from a given number; or b. the ability to obtain mail sent to a known physical address. 3. Through information derived from an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, employer, or retail company). Acceptable information includes: a. the ability to obtain mail at the billing address used in the business relationship; b. verification of information established in previous transactions (e.g., previous order number); or c. the ability to place calls from or receive phone calls at a phone number used in previous business transactions. 4. Any method used to verify the identity of an Applicant for a Level 2, 3, or 4 Client Certificate.
Level 2 Client Certificates and IGTF Classic/MICS Certificates	The CA or an RA confirms that the following are consistent with the application and sufficient to identify a unique individual: (a) the name on the government-issued photo-ID referenced below; (b) date of birth; and (c) current address or personal telephone number. 1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent (or entity certified by a state, federal, or national entity as authorized to confirm identities) with presentment of a reliable form of current government-issued photo ID. 2. The Applicant must possess a valid, current, government-issued, photo ID. The Registration Authority or Trusted Agent performing identity proofing must obtain and review, which may be through remote verification, the following information about the Applicant: (i) name, date of birth, and current address or telephone number; (ii) serial number assigned to the primary, government-issued photo ID; and (iii) one additional form of ID such as another government-issued ID, an employee or student ID card number, telephone number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the applicant's residence. Identity proofing through remote verification may rely on database record checks

Certificate	Validation
	with an agent/institution or through credit bureaus or similar databases. DigiCert or an RA may confirm an address by issuing credentials in a manner that confirms the address of record or by verifying knowledge of recent account activity associated with the Applicant's address and may confirm a telephone number by sending a challenge-response SMS text message or by recording the applicant's voice during a communication after associating the telephone number with the applicant in records available to DigiCert or the RA. 3. Where DigiCert or an RA has a current and ongoing relationship with the Applicant, identity may be verified through the exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo-ID, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret. 4. Any of the methods used to verify the identity of an applicant for a DigiCert Level 3 or 4 Client Certificate.
Level 3 Client Certificates	In-person proofing before an RA, Trusted Agent, or an entity certified by a state, federal, or national entity that is authorized to confirm identities. The information must be collected and stored in a secure manner. Required identification consists of one unexpired Federal/National Government-issued Picture I.D. (e.g. a passport), a REAL ID, or two unexpired Non-Federal Government I.D.s, one of which must be a photo I.D. Acceptable forms of government ID include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See e.g. USCIS Form I-9. The person performing identity proofing examines the credentials and determines whether they are authentic and unexpired and checks the provided information (name, date of birth, and current address) to ensure legitimacy. The Applicant signs a Declaration of Identity, defined below, to which the person performing identity proofing attests. DigiCert or the RA reviews and keeps a record of the Declaration of Identity. DigiCert also employs the in-person antecedent process, defined in FBCA Supplementary Antecedent, In-Person Definition, to meet this in-person identity proofing requirement. Under this definition, historical in-person identity proofing is sufficient if (1) it meets the thoroughness and rigor of in-person proofing described above, (2) supporting ID proofing artifacts exist to substantiate the antecedent relationship, and (3) mechanisms are in place that bind the individual to the asserted identity. In one use case, the Applicant (e.g. an employee) has been identified previously by an employer using USCIS Form I-9 and is bound to the asserted identity remotely through the use of known attributes or shared secrets. In another use case,

Certificate	Validation
	DigiCert uses a third party Identity Verification Provider that constructs a real-time, five-question process, based on multiple historic antecedent databases, and the applicant is given two minutes to answer at least four of the five questions correctly. See FBCA Supplementary Antecedent, In-Person Definition. The identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance.
Level 4 Client Certificates (Biometric ID Certificates)	In-person proofing before an RA, Trusted Agent, or an entity certified by a state, federal, or national entity that is authorized to confirm identities. A certified entity must forward the collected information directly to an RA in a secure manner. The Applicant must supply one unexpired Federal/National Government-issued Picture I.D. (e.g. a passport), a REAL ID, or two unexpired Non-Federal Government I.D.s, one of which must be a photo I.D.. Acceptable forms of government ID include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See e.g. USCIS Form I-9. The entity collecting the credentials must also obtain at least one form of biometric data (e.g. photograph or fingerprints) to ensure that the Applicant cannot repudiate the application. The person performing identity verification for DigiCert or the RA examines the credentials for authenticity and validity. The Applicant signs a Declaration of Identity, defined below, to which the person performing identity proofing attests. DigiCert or the RA reviews and keeps a record of the Declaration of Identity. Use of an in-person antecedent is not allowed. The identity of the Applicant must be established by in-person proofing no earlier than 30 days prior to initial certificate issuance. Level 4 Client Certificates are issued in a manner that confirms the Applicant's address.

A Declaration of Identity consists of:

1. the identity of the person performing the verification;
2. a signed declaration by the verifying person stating that they verified the identity of the Subscriber as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law, the signature on the declaration may be either a handwritten or digital signature using a Certificate that is of equal or higher level of assurance as the credential being issued;
3. unique identifying number(s) from the Applicant's identification document(s), or a facsimile of the ID(s);
4. the date of the verification; and
5. a declaration of identity by the Applicant that is signed (in handwriting or using a digital signature that is of equivalent or higher assurance than the credential being issued) in the presence of the person performing the verification using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

If in-person identity verification is required and the Applicant cannot participate in face-to-face registration alone (e.g. because Applicant is a network device, minor, or person not legally competent), then the Applicant may be accompanied by a person already certified by the PKI or who has the required identity credentials for a Certificate of the same type applied for by the Applicant. The person accompanying the Applicant (i.e. the

"Sponsor") will present information sufficient for registration at the level of the Certificate being requested, for himself or herself, and for the Applicant.

For in-person identity proofing at Levels 3 and 4, DigiCert may rely on an entity certified by a state, federal, or national entity as authorized to confirm identities may perform the authentication on behalf of the RA. The certified entity should forward the information collected from the applicant directly to the RA in a secure manner.

3.2.3.1. Authentication for Role-based Client Certificates

DigiCert may issue Certificates that identify a specific role that the Subscriber holds, if the role identifies a specific individual within an organization (e.g., *Chief Information Officer* is a unique individual whereas *Program Analyst* is not). These role-based Certificates are used when non-repudiation is desired. DigiCert only issues role-based Certificates to Subscribers who first obtain an individual Subscriber Certificate that is at the same or higher assurance level as the requested role-based Certificate. DigiCert may issue Certificates with the same role to multiple Subscribers. However, DigiCert requires that each Certificate have a unique Key Pair. Individuals may not share their issued role-based Certificates and are required to protect the role-based Certificate in the same manner as individual Certificates.

DigiCert verifies the identity of the individual requesting a role-based Certificate (the sponsor) in accordance with Section 3.2.3 before issuing a role-based Certificate. The sponsor must hold a DigiCert-issued client individual Certificate at the same or higher assurance level as the role-based Certificate. If the Certificate is a pseudonymous Certificate cross-certified with the FBCA that identifies subjects by their organizational roles, then DigiCert or an RA validates that the individual either holds that role or has the authority to sign on behalf of the role.

Regarding the issuance of role-based Certificates, this CPS requires compliance with all provisions of DigiCert's CP regarding key generation, private key protection, and Subscriber obligations.

IGTF Certificates are not issued as role-based Certificates.

3.2.3.2. Authentication for Group Client Certificates

Group Certificates correspond to a Private Key that is shared by multiple Subscribers, and are issued for allowed programs (if several entities are acting in one capacity and if non-repudiation is not required). Direct Address Certificates and Direct Organizational Certificates are used as group Certificates consistent with applicable requirements of the Direct Program. DigiCert or the RA records the information identified in Section 3.2.3 for a sponsor before issuing a group Certificate. The sponsor must be at least an Information Systems Security Officer (ISSO) or of the equivalent rank or greater within the organization.

The sponsor is responsible for ensuring control of the Private Key. The sponsor must maintain and continuously update a list of Subscribers with access to the Private Key and account for the time period during which each Subscriber had control of the key. Group Certificates may list the identity of an individual in the subjectName DN provided that the subjectName DN field also includes a text string, such as "Direct Group Cert," so that the Certificate specifies the subject is a group and not a single individual. Client Certificates issued in this way to an organization are always considered group client Certificates.

3.2.3.3. Authentication of Devices with Human Sponsors

DigiCert issues Level/Class 1, 2, 3 or 4 Client and Federated Device Certificates for use on computing or network devices, provided that the entity owning the device is listed as the subject. In all cases, the device has a human sponsor who provides:

1. Equipment identification (e.g., serial number) or service name (e.g., DNS name),
2. Equipment Public Keys,
3. Equipment authorizations and attributes (if any are to be included in the Certificate), and
4. Contact information.

If the Certificate's sponsor changes, the new sponsor is required to review the status of each device to ensure it is still authorized to receive Certificates. Each sponsor is required to provide proof that the device is still under the sponsor's control or responsibility on request. Sponsors are contractually obligated to notify DigiCert if the equipment is no longer in use, no longer under their control or responsibility, or no longer requires a Certificate. All registration is verified commensurate with the requested certificate type.

3.2.4. Non-verified Subscriber Information

The common name of a Level/Class 1 - Personal Client Certificates is not verified as the legal name of the Subscriber. DV SSL/TLS Server Certificates do not include a verified organizational identity. Any other non- verified information included in a Certificate is designated as such in the Certificate. Unverified information is never included in a Level/Class 2, Level, 3, Level 4, Object Signing, EV SSL/TLS Server, or Federated Device Certificate.

3.2.5. Validation of Authority

The authorization of a certificate request is verified as follows:

Certificate	Verification
DV SSL/TLS Server Certificate	The authority of the requester is verified by using one or more of the procedures listed in section 3.2.2.4. of the Baseline Requirements.
OV SSL/TLS Server and Federated Device Certificates	The request is verified using a Reliable Method of Communication, in accordance with section 3.2.5 of the Baseline Requirements.
OSU Server Certificates	DigiCert verifies that the requester is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization.
EV Certificates	The request is verified in accordance with section 11.8.3 of the EV Guidelines.
Object Signing Certificates and Adobe Signing Certificates	If the Certificate names an organization, the requester's contact information is verified with an authoritative source within the applicant's organization using a Reliable Method of Communication. The contact information is then used to confirm the authenticity of the certificate request.
Level 1 Client Certificates Personal (email Certificates) and Enterprise (email Certificates) issued through the native DigiCert infrastructure	The authority of the request is verified through the email address listed in the Certificate or with a person who has technical or administrative control over the domain or the email address to be listed in the Certificate.
Client Certificates Levels 2, 3 and 4 Certificates issued through the native DigiCert infrastructure	The organization named in the Certificate confirms to DigiCert or an RA that the individual is authorized to obtain the Certificate. The organization is required to request revocation of the Certificate when that affiliation ends.
Class 1-3 Client Certificates issued through the acquired Symantec infrastructure	If the Certificate contains organization information, DigiCert obtains documentation from the organization sufficient to confirm that the individual has an affiliation with the organization named in the Certificate.
Direct Address and Direct Organization Certificates	The entity named in the Certificate authorizes a HISP to order the Certificate and use the related Private Key on the entity's behalf. The HISP ISSO is responsible for tracking access to and ensuring proper use of the Private Key.
IGTF Certificates	An authorized individual approves the certificate request. For device Certificates, the RA retains contact information for each device's registered owner. The device owner is required to notify

Certificate	Verification
	the RA and request revocation if the device sponsor is no longer authorized to use the device or the FQDN in the Certificate.

An organization may limit who is authorized to request Certificates by sending a request to DigiCert. A request to limit authorized individuals is not effective until approved by DigiCert. DigiCert will respond to an organization's verified request for DigiCert's list of its authorized requesters.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

Subscribers may request re-key of a Certificate prior to a Certificate's expiration. After receiving a request for re-key, DigiCert creates a new Certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, DigiCert may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

Subscribers re-establish their identity as follows:

Certificate	Routine Re-Key Authentication	Re-Verification Required
DV and OV SSL/TLS Server and Device Certificates	Username and password	According to the Baseline Requirements
EV SSL/TLS Certificates	Username and password	According to the EV Guidelines
Subscriber Code Signing Certificates (Minimum Requirements and EV)	Username and password	At least every 39 months
Signing Authority EV Code Signing Certificates	Username and password	At least every 123 months
Timestamp EV Code Signing Certificates	Username and password	At least every 123 months
Object Signing Certificates (including Adobe Signing Certificates)	Username and password	At least every six years
Level 1 Client Certificates issued through the native DigiCert infrastructure	Username and password	At least every nine years
Level 2 Client Certificates issued through the native DigiCert infrastructure	Current signature key or multi- factor authentication meeting NIST SP 800-63 Level 3	At least every nine years
Level 3 and 4 Client Certificates issued through the native DigiCert infrastructure	Current signature key or multi- factor authentication meeting NIST SP 800-63 Level 3	At least every nine years
Class 1-3 Client Certificates issued through the acquired Symantec infrastructure	Challenge phrase	At least every six years
Federated Device and Federated Device-hardware	Current signature key or multi- factor authentication meeting NIST- 800-63 Level 3	At least every nine years
IGTF Certificates	Username and password, RA attestation after comparison of identity documents, re-authenticate through an approved IdM, or through associated Private Key	At least every 13 months. However, Certificates associated with a Private Key restricted solely to a hardware token may be rekeyed or

Certificate	Routine Re-Key Authentication	Re-Verification Required
		renewed for a period of up to 5 years
Authentication-Only Certificates	Username and password or with associated Private Key	None

DigiCert does not re-key a Certificate without additional authentication if doing so would allow the Subscriber to use the Certificate beyond the limits described above.

3.3.2. Identification and Authentication for Re-key After Revocation

If a Certificate was revoked for any reason other than a renewal, update, or modification action, then the Subscriber must undergo the initial registration process prior to rekeying the Certificate.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

DigiCert or an RA authenticates all revocation requests. DigiCert may authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

Either the Applicant or an individual authorized to request Certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to DigiCert.

EV Certificate requests must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The certificate request must be accompanied by a signed (in writing or electronically) Subscriber Agreement from a Contract Signer.

DigiCert does not issue Certificates to entities on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business.

4.1.2. Enrollment Process and Responsibilities

In no particular order, the enrollment process includes:

1. Submitting a certificate application,
2. Generating a Key Pair,
3. Delivering the Public Key of the Key Pair to DigiCert,
4. Agreeing to the applicable Subscriber Agreement, and
5. Paying any applicable fees.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

After receiving a certificate application, DigiCert or an RA verifies the application information and other information in accordance with Section 3.2. Prior to issuing a publicly-trusted SSL/TLS Server Certificate, DigiCert checks the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure in RFC 6844. If the Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater. DigiCert processes the "issue" and "issuewild" property tags and may not dispatch reports of issuance requests to the contact(s) listed in an "iodef" property tag. CAA checking is optional for Certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5.

The Certification Authority CAA identifying domains for CAs within DigiCert's operational control are "digicert.com", "digicert.ne.jp", "cybertrust.ne.jp", "symantec.com", "thawte.com", "geotrust.com", "rapidssl.com", "digitalcertvalidation.com" (with reseller-specific licensed prefixes) and any domain containing those identifying domains as suffixes (e.g. example.digicert.com).

If an RA assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to DigiCert. After verification is complete, DigiCert evaluates the corpus of information and decides whether or not to issue the Certificate. As part of this evaluation, DigiCert checks the Certificate against an internal database of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests. If some or all of the documentation used to support an application is in a language other than English, a DigiCert employee, RA, or agent skilled in the language performs the final cross-correlation and due diligence.

DigiCert considers a source's availability, purpose, and reputation when determining whether a third party source is reasonably reliable. DigiCert does not consider a database, source, or form of identification reasonably reliable if DigiCert or the RA is the sole source of the information.

4.2.2. Approval or Rejection of Certificate Applications

DigiCert rejects any certificate application that DigiCert or an RA cannot verify. DigiCert does not issue Certificates containing a new gTLD under consideration by ICANN until the gTLD has been approved. DigiCert may also reject a certificate application if DigiCert believes that issuing the Certificate could damage or diminish DigiCert's reputation or business.

Except for Enterprise EV Certificates, EV Certificate issuance approval requires two separate DigiCert validation specialists. The second validation specialist cannot be the same individual who collected the documentation and originally approved the EV Certificate. The second validation specialist reviews the collected information and documents any discrepancies or details that require further explanation. The second validation specialist may require additional explanations and documents prior to authorizing the Certificate's issuance. Enterprise RAs may perform the final cross-correlation and due diligence described herein using a single person representing the Enterprise RA. If satisfactory explanations and/or additional documents are not received within a reasonable time, DigiCert will reject the EV Certificate request and notify the Applicant accordingly.

If the certificate application is not rejected and is successfully validated in accordance with this CPS, DigiCert will approve the certificate application and issue the Certificate. DigiCert is not liable for any rejected Certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply.
Subscribers are required to check the Certificate's contents for accuracy prior to using the certificate.

4.2.3. Time to Process Certificate Applications

Under normal circumstances, DigiCert verifies an Applicant's information and issues a digital Certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. For non-EV SSL/TLS Server Certificates, DigiCert will usually complete the validation process and issue or reject a certificate application within two working days after receiving all of the necessary details and documentation from the Applicant, although events outside of the control of DigiCert can delay the issuance process.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

DigiCert confirms the source of a certificate request before issuance. DigiCert does not issue end entity Certificates directly from its root Certificates. DigiCert logs those SSL/TLS Server Certificates intended to be trusted in Chrome in two or more Certificate Transparency databases. See RFC 6962. Certificate issuance by the Root CA requires an individual authorized by DigiCert (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate

signing operation. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the Certificate is stored in a database and sent to the Subscriber.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

DigiCert may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, DigiCert delivers Certificates via email to the email address designated by the Subscriber during the application process.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued Certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.4.2. Publication of the Certificate by the CA

DigiCert publishes all CA Certificates in its repository. DigiCert publishes end-entity Certificates by delivering them to the Subscriber.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's issuance if the RA was involved in the issuance process.

The FPKIPA will be notified at least two weeks prior to the issuance of a new CA certificate or issuance of new inter-organizational CA cross-certificates with FBCA. The notification shall assert that the new CA cross-certification does not introduce multiple paths to a CA already participating in the FPKI. In addition, all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the CA certificate issuance shall be provided to the FPKIPA within 24 hours following issuance.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. DigiCert does not warrant that any third party software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by DigiCert are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the DigiCert repository.

A Relying Party should rely on a digital signature or SSL/TLS handshake only if:

1. the digital signature or SSL/TLS session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
2. the Certificate is not revoked and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and
3. the Certificate is being used for its intended purpose and in accordance with this CPS.

Before relying on a time-stamp token, a Relying Party must:

1. verify that the time-stamp token has been correctly signed and that the Private Key used to sign the time-stamp token has not been compromised prior to the time of the verification,
2. take into account any limitations on the usage of the time-stamp token indicated by the time-stamp policy, and
3. take into account any other precautions prescribed in this CPS or elsewhere.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for Certificate Renewal

DigiCert may renew a Certificate if:

1. the associated Public Key has not reached the end of its validity period,
2. the Subscriber and attributes are consistent, and
3. the associated Private Key remains uncompromised.

DigiCert may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. DigiCert may notify Subscribers prior to a Certificate's expiration date. Certificate renewal requires payment of additional fees.

4.6.2. Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's Certificates. For Certificates cross-certified with the FBCA, renewal requests are only accepted from certificate subjects, PKI sponsors, or RAs. DigiCert may renew a Certificate without a corresponding request if the signing Certificate is re-keyed.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate's original issuance. DigiCert will refresh any information that is older than the periods specified in the Baseline Requirements or EV Guidelines. DigiCert may refuse to renew a Certificate if it cannot verify any rechecked information. If an individual is renewing a client Certificate and the relevant information has not changed, then DigiCert does not require any additional identity vetting. Some device platforms, e.g. Apache, allow renewed use of the Private Key. If the Private Key and domain information have not changed, the Subscriber may renew the SSL/TLS Server Certificate using a previously issued Certificate or provided CSR.

4.6.4. Notification of New Certificate Issuance to Subscriber

DigiCert may deliver the Certificate in any secure fashion, typically by email or by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and download the Certificate.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed Certificates are considered accepted 30 days after the Certificate's renewal, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.6.6. Publication of the Renewal Certificate by the CA

DigiCert publishes a renewed Certificate by delivering it to the Subscriber. All renewed CA Certificates are published in DigiCert's repository.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's renewal if the RA was involved in the issuance process.

4.7. CERTIFICATE RE-KEY

4.7.1. Circumstance for Certificate Rekey

Re-keying a Certificate consists of creating a new Certificate with a new Public Key and serial number while keeping the subject information the same. The new Certificate may have a different validity date, key identifiers, CRL and OCSP distribution points, and signing key. After re-keying a Certificate, DigiCert may revoke the old Certificate but may not further re-key, renew, or modify the previous Certificate.

Subscribers requesting re-key should identify and authenticate themselves as permitted by section 3.3.1.

4.7.2. Who May Request Certificate Rekey

DigiCert will only accept re-key requests from the subject of the Certificate or the PKI sponsor. DigiCert may initiate a certificate re-key at the request of the certificate subject or in DigiCert's own discretion.

4.7.3. Processing Certificate Rekey Requests

DigiCert will only accept re-key requests from the subject of the Certificate or the PKI sponsor. If the Private Key and any identity and domain information in a Certificate have not changed, then DigiCert can issue a replacement Certificate using a previously issued Certificate or previously provided CSR.

DigiCert re-uses existing verification information unless re-verification and authentication is required under section 3.3.1 or if DigiCert believes that the information has become inaccurate.

4.7.4. Notification of Certificate Rekey to Subscriber

DigiCert notifies the Subscriber within a reasonable time after the Certificate issues.

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

Issued Certificates are considered accepted 30 days after the Certificate is rekeyed, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.7.6. Publication of the Issued Certificate by the CA

DigiCert publishes rekeyed Certificates by delivering them to Subscribers.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's rekey if the RA was involved in the issuance process.

4.8. CERTIFICATE MODIFICATION

4.8.1. Circumstances for Certificate Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CPS. The new Certificate may have the same or a different subject Public Key. After modifying a Certificate that is cross-certified with the FBCA, DigiCert may revoke the old Certificate but will not further re-key, renew, or modify the old Certificate.

4.8.2. Who May Request Certificate Modification

DigiCert modifies Certificates at the request of certain certificate subjects or in its own discretion. DigiCert does not make certificate modification services available to all Subscribers.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, DigiCert verifies any information that will change in the modified Certificate. DigiCert will only issue the modified Certificate after completing the verification process on all modified information. DigiCert will not issue a modified Certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.4. Notification of Certificate Modification to Subscriber

DigiCert notifies the Subscriber within a reasonable time after the Certificate issues.

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

Modified Certificates are considered accepted 30 days after the Certificate is modified, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.8.6. Publication of the Modified Certificate by the CA

DigiCert publishes modified Certificates by delivering them to Subscribers.

4.8.7. Notification of Certificate Modification by the CA to Other Entities

RAs may receive notification of a Certificate's modification if the RA was involved in the issuance process.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, DigiCert verifies the identity and authority of the entity requesting revocation.

DigiCert will revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that DigiCert revoke the Certificate;
2. The Subscriber notifies DigiCert that the original Certificate request was not authorized and does not retroactively grant authorization;
3. DigiCert obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. DigiCert obtains evidence that the validation of domain authorization or control for any FDQN or IP address in the Certificate should not be relied upon.

DigiCert may revoke a certificate within 24 hours and will revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B forum baseline requirements;
2. DigiCert obtains evidence that the Certificate was misused;
3. The Subscriber or the cross-certified CA breached a material obligation under the CP, this CPS, or the relevant agreement;
4. DigiCert confirms any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);
5. DigiCert confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
6. DigiCert confirms a material change in the information contained in the Certificate;
7. DigiCert confirms that the Certificate was not issued in accordance with the CA/B forum requirements or the DigiCert CP or this CPS;
8. DigiCert determines or confirms that any of the information appearing in the Certificate is inaccurate;
9. DigiCert's right to issue Certificates under the CA/B forum requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by the DigiCert CP and/or this CPS; or
11. DigiCert confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such

as a debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

DigiCert may revoke any Certificate in its sole discretion, including if DigiCert believes that:

1. Either the Subscriber's or DigiCert's obligations under the CP or this CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
2. DigiCert received a lawful and binding order from a government or regulatory body to revoke the Certificate;
3. DigiCert ceased operations and did not arrange for another Certificate authority to provide revocation support for the Certificates;
4. The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;
5. The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;
6. For Adobe Signing Certificates, Adobe has requested revocation; or
7. For code-signing Certificates, the Certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

DigiCert always revokes a Certificate if the binding between the subject and the subject's Public Key in the certificate is no longer valid or if an associated Private Key is compromised.

DigiCert will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies DigiCert that the original Certificate request was not authorized and does not retroactively grant authorization;
3. DigiCert obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B forum baseline requirements;
4. DigiCert obtains evidence that the CA Certificate was misused;
5. DigiCert confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. DigiCert determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7. DigiCert or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;
8. DigiCert's or the Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by DigiCert's Certificate Policy and/or Certification Practice Statement; or
10. The technical content or format of the CA Certificate presents an unacceptable risk to application software suppliers or Relying Parties.

DigiCert will revoke a cross-Certificate if the cross-certified entity (including DigiCert) no longer meets the stipulations of the corresponding policies, as indicated by policy OIDs listed in the policy mapping extension of the cross-Certificate.

4.9.2. Who Can Request Revocation

Any appropriately authorized party, such as a recognized representative of a subscriber or cross-signed partner, may request revocation of a Certificate. DigiCert may revoke a Certificate without receiving a request and without reason. Third parties may request certificate revocation for problems related to fraud.

misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

4.9.3. Procedure for Revocation Request

DigiCert processes a revocation request as follows:

1. DigiCert logs the identity of entity making the request or problem report and the reason for requesting revocation based on the list in section 4.9.1. DigiCert may also include its own reasons for revocation in the log.
2. DigiCert may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, DigiCert revokes the Certificate based on the timeframes listed in 4.9.1 as listed for the reason for revocation.
4. For requests from third parties, DigiCert personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem,
    b. the number of reports received about a particular Certificate or website,
    c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
    d. relevant legislation.
5. If DigiCert determines that revocation is appropriate, DigiCert personnel revoke the Certificate and update the CRL.

If DigiCert deems appropriate, DigiCert may forward the revocation reports to law enforcement.

The FPKIPA shall be notified at least two weeks prior to the revocation of a CA certificate cross-certified with FBCA, whenever possible. For emergency revocation, CAs shall follow the notification procedures in Section 5.7.

DigiCert maintains a continuous 24/7 ability to internally respond to any high priority revocation requests.

4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. DigiCert may grant and extend revocation grace periods on a case-by-case basis. DigiCert reports the suspected compromise of its CA Private Key and requests revocation to both the policy authority and operating authority of the superior issuing CA within one hour of discovery.

4.9.5. Time within which CA Must Process the Revocation Request

DigiCert will revoke a CA Certificate within one hour after receiving clear instructions from the DCPA.

Within 24 hours after receiving a Certificate problem report, DigiCert investigates the facts and circumstances related to a Certificate problem report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

After reviewing the facts and circumstances, DigiCert works with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which DigiCert will revoke the certificate. The period from receipt of the Certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by DigiCert will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate problem reports received about a particular Certificate or Subscriber;

4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

Under normal operating circumstances, DigiCert will revoke Certificates as quickly as practical after validating the revocation request following the guidelines of this section and Section 4.9.1, generally within the following time frames:

1. Certificate revocation requests for publicly-trusted Certificates are processed within 18 hours after their receipt,
2. Revocation requests received two or more hours before CRL issuance are processed before the next CRL is published, and
3. Revocation requests received within two hours of CRL issuance are processed before the following CRL is published.

4.9.6. Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a Certificate, a Relying Party must confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checking for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain.

4.9.7. CRL Issuance Frequency

DigiCert uses its offline root CAs to publish CRLs for its intermediate CAs at least every 6 months. For an offline CA that has been cross-signed by the Federal Bridge CA and only issues CA Certificates, certificate- status-checking certificates, or internal administrative Certificates, DigiCert issues a CRL at least every 31 days. All other CRLs are published at least every 24 hours. If a Certificate is revoked for reason of key compromise, an interim CRL is published as soon as feasible, but no later than 18 hours after receipt of the notice of key compromise.

4.9.8. Maximum Latency for CRLs

CRLs for Certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Irregular, interim, or emergency CRLs and all CRLs for CAs chaining to the Federal Bridge are posted within four hours after generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9. On-line Revocation/Status Checking Availability

DigiCert makes certificate status information available via OCSP for SSL/TLS Server Certificates. OCSP may not be available for other kinds of Certificates. Where OCSP support is required by the applicable CP, OCSP responses are provided within a commercially reasonable time and no later than six seconds after the request is received, subject to transmission latencies over the Internet.

OCSP responses conform to RFC 5019 and/or RFC 6960. OCSP responses either:

1. Are signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

4.9.10. On-line Revocation Checking Requirements

A relying party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.

DigiCert supports an OCSP capability using the GET method for Certificates issued in accordance with the

Baseline Requirements. OCSP Responders under DigiCert's direct control will not respond with a "good" status for a certificate that has not been issued.

4.9.11. Other Forms of Revocation Advertisements Available

4.9.12. Not applicable. Special Requirements Related to Key Compromise

DigiCert uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. DigiCert will transition any revocation reason code in a CRL to "key compromise" upon discovery of such reason or as required by an applicable CP. If a Certificate is revoked because of compromise, DigiCert will issue a new CRL within 18 hours after receiving notice of the compromise.

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

Certificate status information is available via CRL and OCSP responder. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period, except for revoked Code Signing Certificates and EV Code Signing Certificates, which remain on the CRL for at least 10 years following the Certificate's validity period. OCSP information for subscriber Certificates is updated at least every four days. OCSP information for subordinate CA Certificates is updated at least every 12 months and within 24 hours after revoking the Certificate.

4.10.2. Service Availability

Certificate status services are available 24x7. This includes the online repository that application software can use to automatically check the current status of all unexpired Certificates issued by DigiCert. DigiCert operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

DigiCert also maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3. Optional Features

OCSP Responders may not be available for all certificate types.

4.11. END OF SUBSCRIPTION

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy Practices

DigiCert never escrows CA Private Keys under this CPS.

DigiCert may escrow Subscriber key management keys to provide key recovery services. DigiCert encrypts and protects escrowed Private Keys using the same or a higher level of security as used to generate and deliver the Private Key. For Certificates cross-certified with the FBCA, third parties are not permitted to hold the Subscriber signature keys in trust.

DigiCert allows Subscribers and other authorized entities to recover escrowed (decryption) Private Keys. DigiCert uses multi-person controls during key recovery to prevent unauthorized access to a Subscriber's escrowed Private Keys. DigiCert accepts key recovery requests:

1. From the Subscriber or Subscriber's organization, if the Subscriber has lost or damaged the private-key token;
2. From the Subscriber's organization, if the Subscriber is not available or is no longer part of the organization that contracted with DigiCert for Private Key escrow;
3. From an authorized investigator or auditor, if the Private Key is part of a required investigation or audit;
4. From a requester authorized by a competent legal authority to access the communication that is encrypted using the key;
5. From a requester authorized by law or governmental regulation; or
6. From an entity contracting with DigiCert for escrow of the Private Key when key recovery is mission critical or mission essential.

Entities using DigiCert's key escrow services are required to:

1. Notify Subscribers that their Private Keys are escrowed;
2. Protect escrowed keys from unauthorized disclosure;
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys;
4. Release an escrowed key only after making or receiving (as applicable) a properly authorized request for recovery; and
5. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key-related information, or the facts concerning any key recovery request or process.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

5.1.1. Site Location and Construction

DigiCert performs its CA and TSA operations from secure and geographically diverse commercial data centers. The data centers are equipped with logical and physical controls that make DigiCert's CA and TSA operations inaccessible to non-trusted personnel. DigiCert operates under a security policy designed to detect, deter, and prevent unauthorized access to DigiCert's operations.

5.1.2. Physical Access

5.1.2.1. Data Centers

Systems providing online certificate issuance (e.g. Issuer CAs) are located in commercial data centers. DigiCert protects such online equipment (including certificate status servers and CMS equipment) from

unauthorized access and implements physical controls to reduce the risk of equipment tampering. Access to the data centers housing the CA and TSA platforms requires two-factor authentication—the individual must have an authorized access card and pass biometric access control authenticators. These biometric authentication access systems log each use of the access card. DigiCert deactivates and securely stores its CA equipment when not in use in accordance with section 5.1.2.3. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module.

Activation data is never stored with the cryptographic module or removable hardware associated with equipment used to administer DigiCert's Private Keys. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

The DigiCert data centers are continuously attended. However, if DigiCert ever becomes aware that a data center is to be left unattended or has been left unattended for an extended period of time, DigiCert personnel will perform a security check of the data center to verify that:

1. DigiCert's equipment is in a state appropriate to the current mode of operation,
2. Any security containers are properly secured,
3. Physical security systems (e.g., door locks) are functioning properly, and
4. The area is secured against unauthorized access.

DigiCert's administrators are responsible for making these checks and must sign off that all necessary physical protection mechanisms are in place and activated. The identity of the individual making the check is logged.

5.1.2.2. RA Operations Areas

DigiCert's RA operations are protected using physical access controls making them accessible only to appropriately authorized individuals. Access to secure areas of buildings requires the use of an "access" or "pass" card. Access card use is logged by the building security system. The exterior and internal passageways of buildings are equipped with motion detecting sensors and video cameras. Similarly, the support and vetting rooms where DigiCert personnel perform identity vetting and other RA functions are equipped with motion-activated video surveillance cameras. Access card logs and video records are reviewed on a regular basis. DigiCert securely stores all removable media and paper containing sensitive plain-text information related to its CA or RA operations in secure containers.

5.1.2.3. Offline CA Key Storage Rooms

DigiCert securely stores the cryptomodules used to generate and store offline CA Private Keys. Access to the rooms used for key storage is controlled and logged by the building access card system. When not in use during a key ceremony, CA cryptomodules are locked in a safe that provides two-person physical access control. Activation data is protected in accordance with section 6.4. Cryptomodule activation keys (operator cards and PED keys) are either sealed in tamper-evident bags and placed in safe deposit boxes or stored in the two-person safe when not in use. Access to the safe is manually logged. Access card logs and the manual logs of access to the safe are reviewed on a regular basis.

5.1.2.4. CA Key Generation and Signing Rooms

CA key generation and signing occurs either in the secure storage room described in section 5.1.2.3 or in a room of commensurate security in close proximity thereto. DigiCert's CA Administrators retrieve cryptographic materials necessary to perform key generation and certificate signing. At no time are cryptographic materials left unattended by fewer than two persons serving in trusted roles.

5.1.3. Power and Air Conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and diesel generators provide redundant backup power. DigiCert monitors capacity demands and makes projections about future capacity requirements to ensure that adequate processing power and storage are available.

DigiCert's data center facilities use multiple load-balanced HVAC systems for heating, cooling, and air ventilation through perforated-tile raised flooring to prevent overheating and to maintain a suitable humidity level for sensitive computer systems.

5.1.4. Water Exposures

The cabinets housing DigiCert's CA and TSA systems are located on raised flooring, and the data centers are equipped with monitoring systems to detect excess moisture.

5.1.5. Fire Prevention and Protection

The data centers are equipped with fire suppression mechanisms.

5.1.6. Media Storage

DigiCert protects its media from accidental damage and unauthorized physical access. Backup files are created on a daily basis. DigiCert's backup files are maintained at locations separate from DigiCert's primary data operations facility.

5.1.7. Waste Disposal

All unnecessary copies of printed sensitive information are shredded on-site before disposal. All electronic media are physically destroyed or are overwritten multiple times to prevent the recovery of the data.

5.1.8. Off-site Backup

DigiCert maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure. ackup copies of CA Private Keys and activation data are stored for disaster recovery purposes off-site in safe deposit boxes located inside federally insured financial institutions and are accessible only by trusted personnel.

5.1.9. Certificate Status Hosting, CMS and External RA Systems

All physical control requirements under Section 5.1 apply equally to any Certificate Status Hosting, CMS, or external RA system.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Personnel acting in trusted roles include CA, TSA, and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually.

5.2.1.1. CA Administrators

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. Administrators do not issue Certificates to Subscribers.

5.2.1.2. Registration Officers – CMS, RA, Validation and Vetting Personnel The Registration Officer role is responsible for issuing and revoking Certificates, including enrollment, identity verification, and compliance with required issuance and revocation steps such as managing the certificate request queue and completing certificate approval checklists as identity vetting tasks are successfully completed.

5.2.1.3. System Administrators/ System Engineers (Operator)

The System Administrator / System Engineer installs and configures system hardware, including servers, routers, firewalls, and network configurations. The System Administrator / System Engineer also keeps CA,

CMS and RA systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.4. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if DigiCert, an Issuer CA, or RA is operating in accordance with this CPS or an RA's Registration Practices Statement.

5.2.1.5. RA Administrators

RA Administrators install, configure and manage the RA software, including the assignment of Issuer CAs and certificate profiles to customer accounts.

5.2.2. Number of Persons Required per Task

DigiCert requires that at least two people acting in a trusted role (one the CA Administrator and the other not an Internal Auditor) take action requiring a trusted role, such as activating DigiCert's Private Keys, generating a CA Key Pair, or backing up a DigiCert Private Key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system but not logical access.

5.2.3. Identification and Authentication for each Role

All personnel are required to authenticate themselves to CA, TSA, and RA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. Those performing backups, recording, and record keeping functions;
3. Those performing audit, review, oversight, or reconciliation functions; and
4. Those performing duties related to CA/TSA key management or CA/TSA administration.

To accomplish this separation of duties, DigiCert specifically designates individuals to the trusted roles defined in Section 5.2.1 above. DigiCert appoints individuals to only one of the Registration Officer, Administrator, Operator, or Internal Auditor roles. Individuals designated as Registration Officer or Administrator may perform Operator duties, but an Internal Auditor may not assume any other role. DigiCert's systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

The DCPA is responsible and accountable for DigiCert's PKI operations and ensures compliance with this CPS and the CP. DigiCert's personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties. All trusted roles for CAs issuing Federated Device Certificates, Client Certificates at Levels 3-US and 4-US (which are intended for interoperability through the Federal Bridge CA at id-fpki-certpcy-mediumAssurance and id- fpki-certpcy-mediumHardware) are held by citizens of the United States. An individual performing a trusted role for an RA may be a citizen of the country where the RA is located. There is no citizenship requirement for personnel performing trusted roles associated with the issuance of other kinds of Certificates.

Management and operational support personnel involved in time-stamp operations possess experience with information security and risk assessment and knowledge of time-stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures. The DCPA ensures that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CPS.

5.3.2. Background Check Procedures

DigiCert verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. DigiCert requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I-9, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified). Background checks include employment history, education, character references, social security number, previous residences, driving records, and criminal background. Checks of previous residences are over the past three years. All other checks are for the previous five years. The highest education degree obtained is verified regardless of the date awarded. Based upon the information obtained during the background check, the human resources department makes an adjudication decision, with the assistance of legal counsel when necessary, as to whether the individual is suitable for the position to which they will be assigned. Background checks are refreshed and re-adjudication occurs at least every five years.

These procedures are subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met by DigiCert due to a prohibition or limitation in local law, DigiCert utilizes a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency. These substitutions will not be allowed for any applicant for a trusted role performing duties or that has access to the FBCA related Certificate systems and information.

5.3.3. Training Requirements

DigiCert provides relevant skills training to all employees involved in DigiCert's PKI and TSA operations. The training relates to the person's job functions and covers:

1. basic Public Key Infrastructure (PKI) knowledge,
2. software versions used by DigiCert,
3. authentication and verification policies and procedures,
4. DigiCert security principles and mechanisms,
5. disaster recovery and business continuity procedures,
6. common threats to the validation process, including phishing and other social engineering tactics, and
7. CA/Browser Forum Guidelines and other applicable industry and government guidelines.

Training is provided via a mentoring process involving senior members of the team to which the employee belongs.

DigiCert maintains records of who received training and what level of training was completed. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges.All Registration Officers are required to pass an internal examination on the EV Guidelines and the Baseline Requirements prior to validating and approving the issuance of Certificates. Where competence is demonstrated in lieu of training, DigiCert maintains supporting documentation.

5.3.4. Retraining Frequency and Requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. DigiCert makes all employees acting in trusted roles aware of any changes to DigiCert's operations. If DigiCert's operations change, DigiCert will provide documented training, in accordance with an executed training plan, to all employees acting in trusted roles.

5.3.5. Job Rotation Frequency and Sequence

Not applicable.

5.3.6. Sanctions for Unauthorized Actions

DigiCert employees and agents failing to comply with this CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7. Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

5.3.8. Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of the CP, this CPS, EV Guidelines, and other technical and operational documentation needed to maintain the integrity of DigiCert's CA operations. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

DigiCert's systems require identification and authentication at system logon with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

DigiCert enables all essential event auditing capabilities of its CA and TSA applications in order to record the events listed below. If DigiCert's applications cannot automatically record an event, DigiCert implements manual procedures to satisfy the requirements. For each event, DigiCert records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. DigiCert records the precise time of any significant TSA events. All event records are available to auditors as proof of DigiCert's practices.

Auditable Event
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum number of authentication attempts occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION

Auditable Event
Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys)
CA KEY LIFECYCLE MANAGEMENT
Key generation, backup, storage, recovery, archival, and destruction
Cryptographic device lifecycle management events
CA AND SUBSCRIBER CERTIFICATE LIFECYCLE MANAGEMENT
All verification activities stipulated in the Baseline Requirements and this CPS
Date, time, phone number used, persons spoken to, and end results of verification telephone calls
Acceptance and rejection of certificate requests
Issuance of Certificates
Generation of Certificate Revocation Lists and OCSP entries.
PRIVATE KEY LOAD AND STORAGE
The loading of Component Private Keys
All access to certificate subject Private Keys retained within the CA for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE
SECRET KEY STORAGE
The manual entry of secret keys used for authentication
PRIVATE AND SECRET KEY EXPORT
The export of private and secret keys (keys used for a single session or message are excluded)
CERTIFICATE REGISTRATION
All certificate requests, including issuance, re-key, renewal, and revocation
Certificate issuance
Verification activities
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL AND REJECTION
CA CONFIGURATION
Any security-relevant changes to the configuration of a CA system component
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
Generation of CRLs and OCSP entries
TIME STAMPING
Clock synchronization
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of an Operating System, PKI Application, or Hardware Security Module
Removal or Destruction of HSMs
System Startup
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set or modify passwords
Backup or restoration of the internal CA database
File manipulation (e.g., creation, renaming, moving)

Auditable Event
Posting of any material to a repository
Access to the internal CA database
All certificate compromise notification requests
Loading HSMs with Certificates
Shipment of HSMs
Zeroizing HSMs
Re-key of the Component
CONFIGURATION CHANGES
Hardware
Software
Operating System
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Personnel access to secure area housing CA or TSA component
Access to a CA or TSA component
Known or suspected violations of physical security
Firewall and router activities
Entries to and exits from the CA facility, PKI and security system actions performed
ANOMALIES
System crashes and hardware failures
Software error conditions
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of a CPS
Resetting Operating System clock

5.4.2. Frequency of Processing Log

At least once every two months, a DigiCert administrator reviews the logs generated by DigiCert's systems, makes system and file integrity checks, and conducts a vulnerability assessment. The administrator may perform the checks using automated tools. During these checks, the administrator (1) checks whether anyone has tampered with the log, (2) scans for anomalies or specific conditions, including any evidence of malicious activity, and (3) prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to DigiCert's operations management committee and are made available to DigiCert's auditors upon request. DigiCert documents any actions taken as a result of a review.

5.4.3. Retention Period for Audit Log

Audit logs related to publicly trusted SSL/TLS Certificates are retained for at least seven (7) years. DigiCert retains audit logs on-site until after they are reviewed. The individuals who remove audit logs from DigiCert's CA systems are different than the individuals who control DigiCert's signature keys.

5.4.4. Protection of Audit Log

CA audit log information is retained on equipment until after it is copied by a system administrator. DigiCert's CA and TSA systems are configured to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until

transferred to a backup site. DigiCert's off-site storage location is a safe and secure location that is separate from the location where the data was generated.

DigiCert makes time-stamping records available when required to prove in a legal proceeding that DigiCert's time-stamping services are operating correctly. Audit logs are made available to auditors upon request.

5.4.5. Audit Log Backup Procedures

DigiCert makes regular backup copies of audit logs and audit log summaries and saves a copy of the audit log to a secure, off-site location on at least a monthly basis.

5.4.6. Audit Collection System (internal vs. external)

Automatic audit processes begin on system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, DigiCert's Administrators and the DCPA shall be notified and the DCPA will consider suspending the CA's or RA's operations until the problem is remedied.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

DigiCert performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. DigiCert also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that DigiCert has in place to control such risks. DigiCert's Internal Auditors review the security audit data checks for continuity. DigiCert's audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5. RECORDS ARCHIVAL

DigiCert complies with all record retention policies that apply by law. DigiCert includes sufficient detail in all archived records to show that a Certificate or time-stamp token was issued in accordance with this CPS.

5.5.1. Types of Records Archived

DigiCert retains the following information in its archives (as such information pertains to DigiCert's CA / TSA operations):

1. Accreditations of DigiCert,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA / TSA,
4. System and equipment configurations, modifications, and updates,
5. Rejection or acceptance of a certificate request,
6. Certificate issuance, rekey, renewal, and revocation requests,
7. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes,
8. Any documentation related to the receipt or acceptance of a Certificate or token,
9. Subscriber Agreements,
10. Issued Certificates,
11. A record of certificate re-keys,
12. CRLs for CAs cross-certified with the Federal Bridge CA,
13. Data or applications necessary to verify an archive's contents,
14. Compliance auditor reports,
15. Changes to DigiCert's audit parameters,
16. Any attempt to delete or modify audit logs,
17. CA Key generation and destruction,
18. Access to Private Keys for key recovery purposes,

19. Changes to trusted Public Keys,
20. Export of Private Keys,
21. Approval or rejection of a revocation request,
22. Appointment of an individual to a trusted role,
23. Destruction of a cryptographic module,
24. Certificate compromise notifications,
25. Remedial action taken as a result of violations of physical security, and
26. Violations of the CP or CPS.

5.5.2. Retention Period for Archive

DigiCert retains archived data associated with Level 3 or Level 4, and federated device Certificates for at least 10.5 years. DigiCert, or the RA supporting issuance, archives data for other certificate types for at least 7.5 years.

5.5.3. Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the DCPA or as required by law. DigiCert maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If DigiCert needs to transfer any media to a different archive site or equipment, DigiCert will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4. Archive Backup Procedures

On at least an annual basis, DigiCert creates an archive disk of the data listed in section 5.5.1. Each archive disk is stored separately and available for integrity verification at a later date. DigiCert stores the archive disk in a secure off-site location for the duration of the set retention period.

5.5.5. Requirements for Time-stamping of Records

DigiCert automatically time-stamps archived records with system time (non-cryptographic method) as they are created. DigiCert synchronizes its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

5.5.6. Archive Collection System (internal or external)

Archive information is collected internally by DigiCert.

5.5.7. Procedures to Obtain and Verify Archive Information

Details concerning the creation and storage of archive information are found in section 5.5.4. After receiving a request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction involving the DigiCert PKI, DigiCert may elect to retrieve the information from archival. The integrity of archive information is verified by comparing a hash of the archive disk with the hash originally stored for that disk, as described in Section 5.5.4. DigiCert may elect to transmit the relevant information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with the data.

5.6. KEY CHANGEOVER

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of a CA Private Key's lifetime, DigiCert ceases using the expiring CA Private Key to sign Certificates and uses the old Private Key only to sign CRLs and OCSP responder Certificates. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key Certificate is provided to subscribers and relying parties through the delivery methods detailed in Section

6.1.4. Where DigiCert has cross-certified another CA that is in the process of a key rollover, DigiCert obtains a new CA Public Key (PKCS#10) or new CA Certificate from the other CA and distributes a new CA cross Certificate following the procedures described above.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

DigiCert maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. DigiCert reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

For CAs that are cross-certified with the FBCA, DigiCert will notify the FPKIPA within 24 hours and provide preliminary remediation analysis of the following:

- suspected or detected compromise of the CA systems;
- physical or electronic attempts to penetrate CA systems;
- denial of service attacks on CA components; or
- any incident preventing the CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

Within 10 business days of incident resolution, DigiCert will post a notice on its public web page identifying the incident and provide notification to the FPKIPA. The public notice shall include the following:

1. Which CA components were affected by the incident
2. DigiCert's interpretation of the incident.
3. Who is impacted by the incident
4. When the incident was discovered
5. A complete list of all certificates that were either issued erroneously or not compliant with the CP/CPS as a result of the incident
6. A statement that the incident has been fully remediated

The notification provided directly to the FPKIPA shall also include detailed measures taken to remediate the incident.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

DigiCert makes regular system backups on at least a weekly basis and maintains backup copies of its Private Keys, which are stored in a secure, separate location. If DigiCert discovers that any of its computing resources, software, or data operations have been compromised, DigiCert assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If DigiCert determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, DigiCert suspends such operation until it determines that the risk is mitigated.

5.7.3. Entity Private Key Compromise Procedures

If DigiCert suspects that one of its Private Keys has been comprised or lost then an emergency response team will convene and assess the situation to determine the degree and scope of the incident and take appropriate action. Specifically, DigiCert will:

1. Collect information related to the incident;
2. Begin investigating the incident and determine the degree and scope of the compromise;
3. Have its incident response team determine and report on the course of action or strategy that should be taken to correct the problem and prevent reoccurrence;
4. If appropriate, contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures;
5. If the compromise involves a Private Key used to sign time-stamp tokens, provide a description of the compromise to Subscribers and Relying Parties;
6. Notify any cross-certified entities of the compromise so that they can revoke their cross-Certificates;
7. Make information available that can be used to identify which Certificates and time-stamp tokens are affected, unless doing so would breach the privacy of a DigiCert user or the security of DigiCert's services;

8. Monitor its system, continue its investigation, ensure that data is still being recorded as evidence, and make a forensic copy of data collected;
9. Isolate, contain, and stabilize its systems, applying any short-term fixes needed to return the system to a normal operating state;
10. Prepare and circulate an incident report that analyzes the cause of the incident and documents the lessons learned; and
11. Incorporate lessons learned into the implementation of long term solutions and the Incident Response Plan.

DigiCert may generate a new Key Pair and sign a new Certificate. If a disaster physically damages DigiCert's equipment and destroys all copies of DigiCert's signature keys then DigiCert will provide notice to affected parties at the earliest feasible time.

5.7.4. Business Continuity Capabilities after a Disaster

To maintain the integrity of its services, DigiCert implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that certificate status services be only minimally affected by any disaster involving DigiCert's primary facility and that DigiCert be capable of maintaining other services or resuming them as quickly as possible following a disaster. DigiCert reviews, tests, and updates the BCMP and supporting procedures at leastannually.

DigiCert's systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes DigiCert's primary CA or TSA operations to become inoperative, DigiCert will re-initiate its operations at its secondary location giving priority to the provision of certificate status information and time stamping capabilities, if affected.

5.8. CA OR RA TERMINATION

Before terminating its CA or TSA activities, DigiCert will:

1. Provide notice and information about the termination by sending notice by email to its customers, Application Software Vendors, and cross-certifying entities and by posting such information on DigiCert's web site; and
2. Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, DigiCert will:

1. transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
2. revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
3. destroy all Private Keys; and
4. make other necessary arrangements that are in accordance with this CPS.

DigiCert has made arrangements to cover the costs associated with fulfilling these requirements in case DigiCert becomes bankrupt or is unable to cover the costs. Any requirements of this section that are varied by contract apply only the contracting parties.

Whenever possible, the FPKIPA shall be notified at least two weeks prior to the termination of any CA cross-certified with the FBCA. For emergency termination, the CA shall follow the notification procedures in Section 5.7.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

All keys must be generated using a FIPS-approved method or equivalent international standard.

DigiCert's CA Key Pairs are generated by multiple trusted individuals acting in trusted roles and using a cryptographic hardware device as part of scripted key generation ceremony. The cryptographic hardware is evaluated to FIPS 140-2 Level 3. Activation of the hardware requires the use of two-factor authentication tokens. DigiCert creates auditable evidence during the key generation process to prove that the CPS was followed and role separation was enforced during the key generation process. DigiCert requires that an external auditor witness the generation of or review a recording of any CA keys to be used as publicly trusted root Certificates or to sign EV Certificates. For other CA key pair generation ceremonies, an Internal Auditor, external auditor, or independent third party attends the ceremony, or an external auditor examines the signed and documented record of the key generation ceremony, as allowed by applicable policy.

Subscribers must generate their keys in a manner that is appropriate for the certificate type. DigiCert never creates key pairs for publicly trusted SSL/TLS Server Certificates. Certificates issued at Level 3 Hardware or at Level 4 Biometric must be generated on validated hardware cryptographic modules using a FIPS-approved method. For Adobe Signing Certificates, Subscribers must generate their Key Pairs in a medium that prevents exportation or duplication and that meets or exceeds FIPS 140-2 Level 3 certification standards.

6.1.2. Private Key Delivery to Subscriber

If DigiCert, a CMS, or an RA generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. Keys may be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module. In all cases:

1. Except where escrow/backup services are authorized and permitted, the key generator must not retain access to the Subscriber's Private Key after delivery,
2. The key generator must protect the Private Key from activation, compromise, or modification during the delivery process,
3. The Subscriber must acknowledge receipt of the Private Key(s), typically by having the Subscriber use the related Certificate, and
4. The key generator must deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
    a. For hardware modules, the key generator maintaining accountability for the location and state of the module until the Subscriber accepts possession of it, and
    b. For electronic delivery of Private Keys, the key generator encrypting key material using a cryptographic algorithm and key size at least as strong as the Private Key. The key generator shall deliver activation data using a separate secure channel.

The entity assisting the Subscriber with key generation shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's Key Pair. A CMS or RA providing key delivery services is required to provide a copy of this record to DigiCert.

6.1.3. Public Key Delivery to Certificate Issuer

Subscribers generate Key Pairs and submit the Public Key to DigiCert in a CSR as part of the certificate request process. For FBCA Certificates, where the party named in a certificate generates its own keys, the Subscriber's signature on the request is authenticated prior to issuing the Certificate.

6.1.4. CA Public Key Delivery to Relying Parties

DigiCert's Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed

by other CAs. All accreditation authorities supporting DigiCert Certificates and all application software providers are permitted to redistribute DigiCert's root anchors.

DigiCert may also distribute Public Keys that are part of an updated signature Key Pair as a self-signed Certificate, as a new CA Certificate, or in a key roll-over Certificate. Relying Parties may obtain DigiCert's self- signed CA Certificates from DigiCert's web site or by email.

6.1.5. Key Sizes

DigiCert generally follows the NIST timelines in using and retiring signature algorithms and key sizes. Accordingly, DigiCert is phasing out its use of the SHA-1 hash algorithm. Currently, DigiCert generates and uses at least the following minimum key sizes, signature algorithms, and hash algorithms for signing Certificates, CRLs, and certificate status server responses for policy OID arcs of 2.16.840.1.114412.1, 2.16.840.1.114412.2, or 2.16.840.1.114412.4 (for FBCA Certificates):

- 2048-bit RSA Key;
- 384-bit ECDSA Key with Secure Hash Algorithm version 2 (SHA-256); or
- a hash algorithm that is equally or more resistant to a collision attack).

Certificates that do not assert these certificate policies (see other policies listed in Section 1.2) may also be signed using the SHA-1 hash algorithm, provided that its use otherwise complies with requirements of the CA/Browser Forum or the relevant CP. Signatures on CRLs, OCSP responses, and OCSP responder Certificates that provide status information for Certificates that were generated using SHA-1 may continue to be generated using the SHA-1 algorithm. All other signatures on CRLs, OCSP responses, and OCSP responder Certificates must use the SHA-256 hash algorithm or one that is equally or more resistant to collision attack.

DigiCert requires end-entity Certificates to contain a key size that is at least 2048 bits for RSA, DSA, or Diffie- Hellman and 224 bits for elliptic curve algorithms.

DigiCert may require higher bit keys in its sole discretion.

Any Root Certificates participating in the AATL program issued after July 1, 2017 must be at least 3072-bit for RSA and 256-bit for ECDSA.

DigiCert and Subscribers may fulfill the transmission security requirements under the CP and this CPS using TLS or another protocol that provides similar security, provided the protocol requires at least AES 128 bits or equivalent for the symmetric key and at least 2048-bit RSA or equivalent for the asymmetric keys.

6.1.6. Public Key Parameters Generation and Quality Checking

DigiCert uses a cryptomodule that conforms to FIPS 186-2 and provides random number generation and on-board generation of Public Keys and a wide range of ECC curves. The value of this public exponent equates to an odd number equal to three or more.

6.1.7. Key Usage Purposes (as per X.509 v3 key usage field)

DigiCert's Certificates include key usage extension fields that specify the intended use of the Certificate and technically limit the Certificate's functionality in X.509v3-compliant software.

The use of a specific key is determined by the key usage extension in the X.509 Certificate.

Private Keys corresponding to Root CA Certificates are not used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates; and

4. Certificates for OCSP Response verification

Subscriber Certificates assert key usages based on the intended application of the Key Pair. Key usage

bits and extended key usages are specified in the certificate profile for each type of CertificateDigiCert's CA Certificates have at least two key usage bits set: keyCertSign and cRLSign, and for signing OCSP responses, the digitalSignature bit is also set.

Except for legacy applications requiring a single key for dual use with both encryption and signature, DigiCert does not issue Certificates with key usage for both signing and encryption. Instead, DigiCert issues Subscribers two Key Pairs—one for key management and one for digital signature and authentication. For Certificates at Levels 1, 2 and 3 that are used for signing and encryption in support of legacy applications, they must:

1. be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CPS,
2. never assert the non-repudiation key usage bit, and
3. not be used for authenticating data that will be verified on the basis of the dual-use Certificate at a future time.

No Level 4 Certificates may have such dual-use Key Pairs.

6.2. *PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING* CONTROLS

6.2.1. Cryptographic Module Standards and Controls

DigiCert's cryptographic modules for all of its CA and OCSP responder Key Pairs are validated to the FIPS 140- 2 Level 3. IGTF Certificate Subscribers must protect their Private Keys in accordance with the applicable Guidelines on Private Key Protection, including the use of strong pass phrases to protect Private Keys.

Cryptographic module requirements for subscribers and registration authorities are shown in the table below.

Assurance Level	Subscriber	Registration Authority
EV Code Signing	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)
Adobe Signing	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)
Rudimentary	N/A	FIPS 140-2 Level 1 (Hardware or Software)
Basic, LOA2, and LOA3	FIPS 140-2 Level 1 (Hardware or Software)	FIPS 140-2 Level 1 (Hardware or Software)
Medium	FIPS 140-2 Level 1 (Software) FIPS 140 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)

Medium Hardware, Biometric /Hardware Authentication	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)

DigiCert ensures that the Private Key of an EV Code Signing Certificate is properly generated, used, and stored in a cryptomodule that meets or exceeds the requirements of FIPS 140-2 level 2 by (i) shipping conforming cryptomodules with preinstalled Key Pairs, (ii) communicating via PKCS#11 crypto APIs of cryptomodules that DigiCert has verified meet or exceed requirements, or (iii) obtaining a suitable IT audit from the Subscriber that indicates compliance with FIPS 140-2 level 2 or the equivalent.

6.2.2. Private Key (n out of m) Multi-person Control

DigiCert's authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons.

Backups of CA Private Keys are securely stored off-site and require two-person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations.

6.2.3. Private Key Escrow

DigiCert does not escrow its signature keys. Subscribers may not escrow their private signature keys. DigiCert may provide escrow services for other types of Certificates in order to provide key recovery as described in section 4.12.1.

6.2.4. Private Key Backup

DigiCert's Private Keys are generated and stored inside DigiCert's cryptographic module, which has been evaluated to at least FIPS 140-2 Level 3. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. DigiCert's CA Key Pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted and video-recorded key backup process.

DigiCert may provide backup services for Private Keys that are not required to be kept on a hardware device. Access to back up Certificates is protected in a manner that only the Subscriber can control the Private Key. Backed up keys are never stored in a plain text form outside of the cryptographic module.

6.2.5. Private Key Archival

DigiCert does not archive Private Keys.

6.2.6. Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, DigiCert encrypts the Private Key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require two- person access. If DigiCert becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then DigiCert will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7. Private Key Storage on Cryptographic Module

DigiCert's Private Keys are generated and stored inside DigiCert's cryptographic module, which has been evaluated to at least FIPS 140-2 Level 3. Root Private Keys are stored offline in cryptographic modules or backup tokens as described above in Sections 6.2.2, 6.2.4, and 6.2.6.

6.2.8. Method of Activating Private Keys

DigiCert's Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys. *See also* Section 6.4.

6.2.9. Method of Deactivating Private Keys

DigiCert's Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. DigiCert never leaves its HSM devices in an active unlocked or unattended state.

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10. Method of Destroying Private Keys

DigiCert personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed.

DigiCert may destroy a Private Key by deleting it from all known storage partitions. DigiCert also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, DigiCert will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

DigiCert archives copies of Public Keys in accordance with Section 5.5.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

DigiCert Certificates have maximum validity periods of:

Type	Private Key Use*	Certificate Term
Publicly Trusted Root CAs	No stipulation	25 years
Root CAs (U.S. Federal per FBCA CP § 6.3.2)	20 years	37 years
Root CAs Not Otherwise Restricted	No stipulation	100 years
Publicly Trusted Sub CAs / Issuer CAs	No stipulation	15 years
FBCA-Cross-certified Sub CAs	6 years (period of key use for signing Certificates)	10 years (key still signs CRLs, OCSP responses, and OCSP responder Certificates)
IGTF Cross-certified Sub CA†	6 years	15 years
CRL and OCSP responder signing	3 years	31 days
OV SSL/TLS Server	No stipulation	825 days
EV SSL/TLS Server	No stipulation	825 days
Time Stamping Authority	15 months	135 months
Object Signing Certificate and Document Signing	No stipulation‡	123 months
Code Signing Certificate issued to Subscriber under the Minimum Requirements for Code	No stipulation	39 months

Type	Private Key Use*	Certificate Term
Signing Certificates or the EV Code Signing Guidelines		
EV Code Signing Certificate issued to Signing Authority	123 months	123 months
Adobe Signing Certificate	39 months	5 years
FBCA and IGTF End Entity Client used for signatures	36 months	36 months
FBCA and IGTF Client used for key management.	36 months	36 months
End Entity Client for all other purposes (FBCA or IGTF compliant)	36 months	36 months
End Entity / Client for all other purposes (non-FBCA and non-IGTF certs)	No Stipulation	60 months
IGTF on hardware	60 months	13 months
Hotspot 2.0 OSU Server Certificates	No stipulation	2 years

* CA Private Keys may continue to be used to sign CRLs, OCSP responses, and OCSP responder certificates.

† IGTF signing Certificates have a lifetime that is at least twice the maximum lifetime of an end entity Certificate.

‡ Code and content signers cross-certified with FBCA may use their Private Keys for three years; the lifetime of the associated Public Keys shall not exceed eight years.

Relying parties may still validate signatures generated with these keys after expiration of the Certificate.

DigiCert may voluntarily retire its CA Private Keys before the periods listed above to accommodate key changeover processes. DigiCert does not issue Subscriber Certificates with an expiration date that exceeds the Issuer CA's public key term stated in the table above or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

DigiCert activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CPS. DigiCert will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

All DigiCert personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. If DigiCert uses passwords as activation data for a signing key, DigiCert will change the activation data change upon rekey of the CA Certificate.

6.4.2. Activation Data Protection

DigiCert protects data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All DigiCert personnel are instructed to memorize and not to write down their password or share it with another individual. DigiCert locks accounts used to access secure CA processes if a certain number of failed password attempts occur as specified in the internal security policies, procedures, and relevant requirements in references listed in Section 1.6.3.

6.4.3. Other Aspects of Activation Data

Not applicable.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

DigiCert secures its CA systems and authenticates and protects communications between its systems and trusted roles. DigiCert's CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses.

DigiCert's CA systems, including any remote workstations, are configured to:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage the privileges of users and limit users to their assigned roles,
3. generate and archive audit records for all transactions,
4. enforce domain integrity boundaries for security critical processes, and
5. support recovery from key or system failure.

All Certificate Status Servers:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage privileges to limit users to their assigned roles,
3. enforce domain integrity boundaries for security critical processes, and
4. support recovery from key or system failure.

DigiCert enforces multi-factor authentication on any account capable of directly causing Certificate issuance.

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

DigiCert has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. DigiCert only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by DigiCert are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to DigiCert's operations is scanned for malicious code on first use and periodically thereafter.

6.6.2. Security Management Controls

DigiCert has mechanisms in place to control and monitor the security-related configurations of its CA systems. When loading software onto a CA system, DigiCert verifies that the software is the correct version and is supplied by the vendor free of any modifications. DigiCert verifies the integrity of software used with its CA processes at least once a week.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

DigiCert documents and controls the configuration of its systems, including any upgrades or modifications made. DigiCert's CA system is connected to one internal network and is protected by firewalls and Network Address Translation for all internal IP addresses (e.g., 192.168.x.x). DigiCert's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign Certificate-issuing subordinate CAs, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

DigiCert's security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. DigiCert's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

6.8. TIME-STAMPING

The system time on DigiCert's computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). All times are traceable to a real time value distributed by a UTC(k) laboratory or National Measurement Institute and are updated when a leap second occurs as notified by the appropriate body. DigiCert maintains an internal NTP server that synchronizes with cellular telephone networks and maintains the accuracy of its clock within one second or less. However, Relying Parties should be aware that all times included in a time-stamp token are synchronized with UTC within the accuracy defined in the time-stamp token itself, if present.

DigiCert will not issue a time-stamp token using any clock that is detected as inaccurate. All clocks used for time-stamping are housed in the DigiCert's secure facilities and are protected against threats that could result in an unexpected change to the clock's time. DigiCert's facilities automatically detect and report any clock that drifts or jumps out of synchronization with UTC. Clock adjustments are auditable events.

Some aspects of RFC 3161 time stamps differ from Microsoft Authenticode time stamps. For RFC 3161-compliant timestamps, DigiCert includes a unique integer for each newly generated time-stamp token. DigiCert only time-stamps hash representations of data, not the data itself. Information can be hashed for time-stamping using SHA-1 or SHA-256 with RSA encryption and either 1024 or 2048 bit key size for signature creation. (SHA-1, SHA-256, SHA-384, SHA-512, MD5, MD4, and MD2 are supported for RFC 3161-based requests.) DigiCert does not examine the imprint being time-stamped other than to check the imprint's length. DigiCert also does not include any identification of the Time Stamp Token Requester (TST Requester) in the time-stamp token. All time-stamp tokens are signed using a key generated exclusively for that purposes and have the property of the key indicated in the Certificate.

TST Requesters request time-stamp tokens by sending a request to DigiCert. After the TST Requester receives a response from DigiCert, it must verify the status error returned in the response. If an error was not returned, the TST Requester must then verify the fields contained in the time-stamp token and the validity of the time-stamp token's digital signature. In particular, the TST Requester must verify that the time-stamped data corresponds to what was requested and that the time-stamp token contains the correct certificate identifier, the correct data imprint, and the correct hash algorithm OID. The TST Requester must also verify

the timeliness of the response by verifying the response against a local trusted time reference. The TST Requester is required to notify DigiCert immediately if any information cannot be verified.

Time Stamp Verifiers shall verify the digital signature on the time-stamp token and confirm that the data corresponds to the hash value in the time-stamp token.

7. CERTIFICATE, CRL, AND OCSP PROFILES

DigiCert uses the ITU X.509, version 3 standard to construct digital Certificates for use within the DigiCert PKI. DigiCert adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. DigiCert generates non-sequential Certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from a CSPRNG.

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)

All Certificates are X.509 version 3 Certificates.

7.1.2. Certificate Extensions

IGTF Certificates comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates, with the exception of cross-certificates that share a private key with a corresponding root certificate: will contain an EKU extension; and cannot include the anyExtendedKeyUsage KeyPurposeId; DigiCert no longer includes both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate.

DigiCert's Technically Constrained Subordinate CA Certificates include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId does not appear in the EKU extension of publicly trusted certificates.

7.1.3. Algorithm Object Identifiers

DigiCert Certificates are signed using one of the following algorithms:

sha-1WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5]
sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
ecdsa-with-sha384	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures (4) ecdsa-with-SHA2 (3) 3]

DigiCert does not currently sign Certificates using RSA with PSS padding. SSL/TLS Server Certificates and OCSP Certificates are not signed with sha-1WithRSAEncryption.

DigiCert and Subscribers may generate Key Pairs using the following:

id-dsa	[iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1]
RsaEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1]
Dhpublicnumber	[iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1]
id-keyExchangeAlgorithm	[joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22]
id-ecPublicKey	[iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1]

Elliptic curve Public Keys submitted to DigiCert for inclusion in end entity Certificates should all be based on NIST "Suite B" curves.

DigiCert does not issue publicly trusted SSL/TLS Certificates to a Reserved IP address or Internal Name.

7.1.4. Name Forms

Each Certificate includes a unique serial number that is never reused. Optional subfields in the subject of an SSL Certificate must either contain information verified by DigiCert or be left empty. SSL/TLS Server Certificates cannot contain metadata such as '.', '-' and ' ' characters or and/or any other indication that the value/field is absent, incomplete, or not applicable. DigiCert has a process to restrict OU fields from containing Subscriber information that has not been verified in accordance with Section 3.

DigiCert has a process for excluding tradenames and organizations that are not authorized.

For Certificates that include LEI in the OU field, entries are verified accordance with the standards and requirements listed in sections 1.6.3 and 3.2 prior to being included.

For CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.

The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuer CA to support name chaining as specified in RFC 5280, section 4.1.2.4.

The contents of the fields in EV Certificates must meet the requirements in Section 8.1 of the EV Guidelines.

7.1.5. Name Constraints

DigiCert may include name constraints in the nameConstraints field when appropriate.

7.1.5.1. Name-Constrained serverAuth CAs

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then a technically constrained Subordinate CA Certificate includes the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

(a) For each dNSName in permittedSubtrees, the DigiCert confirms that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Baseline Requirements section 3.2.2.4.
(b) For each iPAddress range in permittedSubtrees, DigiCert confirms that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.
(c) For each DirectoryName in permittedSubtrees the DigiCert confirms the Applicant's and/or Subsidiary's Organizational name(s) and location(s) such that end entity certificates issued from the subordinate CA Certificate will comply with section 7.1.2.4 and 7.1.2.5 of the Baseline Requirements. If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate specifies the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate includes within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate also includes within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate includes at least one iPAddress in permittedSubtrees.

If the Subordinate CA is not allowed to issue certificates with dNSNames, then the Subordinate CA Certificate includes a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate includes at least one dNSName in permittedSubtrees.

7.1.5.2. Name-Constrained emailProtection CAs

If the technically constrained Subordinate CA certificate includes the id-kp-emailProtection extended key usage, it also includes the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2.4 of the Baseline Requirements.

7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs used by DigiCert are listed in Section 1.2.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

DigiCert includes brief statements in Certificates about the limitations of liability and other terms associated with the use of a Certificate in the Policy Qualifier field of the Certificates Policy extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

7.2.1. Version number(s)

DigiCert issues version 2 CRLs that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha384 [1 2 840 10045 4 3 3]
Issuer Distinguished Name	DigiCert
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

7.2.2. CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation

7.3. OCSP PROFILE

7.3.1. Version Number(s)

DigiCert's OCSP responders conform to version 1 of RFC 6960.

7.3.2. OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the WebTrust Programs for Certification Authorities. For purposes of interoperation with the U.S. Government, compliance can be determined by reference to any current auditor letter of compliance meeting FPKIPA Audit Requirements. (Note: For business purposes, cross-signed CAs operated by third parties in Europe, who operate under their own CPSs, are audited in accordance with ETSI audit criteria.)

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

DigiCert receives an annual period in time audit by an independent external auditor to assess DigiCert's compliance with this CPS, referenced requirements, any applicable CPs, FPKIPA Audit Requirements, and the WebTrust for CA programs criteria. The audit covers DigiCert's RA systems, Sub CAs, and OCSP Responders.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

WebTrust auditors must meet the requirements of Section 8.2 of the Baseline Requirements.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

DigiCert's WebTrust / Federal PKI auditor does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against DigiCert.

8.4. TOPICS COVERED BY ASSESSMENT

The audit covers DigiCert's business practices disclosure, the integrity of DigiCert's PKI operations, and DigiCert's compliance with this CPS and referenced requirements. The audit verifies that DigiCert is compliant with the CP, this CPS, and any MOA between it and any other PKI.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, this CPS, the CP, or any other contractual obligations related to DigiCert's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify DigiCert, and (3) DigiCert will develop a plan to cure the noncompliance. DigiCert will submit the plan to the DCPA for approval and to any third party that DigiCert is legally obligated to satisfy. The DCPA may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates.

8.6. COMMUNICATION OF RESULTS

The results of each audit are reported to the DCPA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. Copies of DigiCert's WebTrust for CAs audit reports can be found at: https://www.digicert.com/webtrust-audits. On an annual basis and within three months of completion, DigiCert submits copies of relevant audit compliance reports to various parties, such as Mozilla, Adobe, the Federal PKI Policy Authority, CA licensing bodies, etc.

8.7. SELF-AUDITS

On at least a quarterly basis, DigiCert performs regular internal audits against a randomly selected sample of at least three percent of its SSL/TLS Server Certificates and EV Code Signing Certificates issued since the last internal audit. Self-audits on server and code signing Certificates are performed in accordance with Guidelines adopted by the CA / Browser Forum.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

DigiCert charges fees for certificate issuance and renewal. DigiCert may change its fees at any time in accordance with the applicable customer agreement.

9.1.2. Certificate Access Fees

DigiCert may charge a reasonable fee for access to its certificate databases.

9.1.3. Revocation or Status Information Access Fees

DigiCert does not charge a certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL. DigiCert may charge a fee for providing certificate status information via OCSP.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

Subscribers must request refunds, in writing, within 30 days after a Certificate issues. After receiving the refund request, DigiCert may revoke the Certificate and refund the amount paid by the Applicant, minus any applicable application processing fees.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

DigiCert maintains Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

DigiCert provides a warranty to Subscribers according to the terms of the Netsure Extended Warranty Protection Plan. DigiCert provides a limited warranty to Relying Parties in DigiCert's Relying Party Agreement.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability ofinformation;
5. Information held by DigiCert as private information in accordance with Section 9.4;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS).

9.3.2. Information Not Within the Scope of Confidential Information

Any information not listed as confidential is considered public information. Published Certificate and revocation data is considered public information.

9.3.3. Responsibility to Protect Confidential Information

DigiCert's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

DigiCert follows the privacy policy posted on its website when handling personal information. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information.

9.4.2. Information Treated as Private

DigiCert treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. DigiCert protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3. Information Not Deemed Private

Private information does not include Certificates, CRLs, or their contents.

9.4.4. Responsibility to Protect Private Information

DigiCert employees and contractors are expected to handle personal information in strict confidence and meet the requirements of US and European law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice and Consent to Use Private Information

Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. DigiCert will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

DigiCert may disclose private information, without notice, if DigiCert believes the disclosure is required by law or regulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

DigiCert and/or its business partners own the intellectual property rights in DigiCert's services, including the Certificates, trademarks used in providing the services, and this CPS. "DigiCert" is a registered trademark of DigiCert, Inc.

Certificate and revocation information are the property of DigiCert. DigiCert grants permission to reproduce and distribute Certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. DigiCert does not allow derivative works of its Certificates or products without prior written permission. Private and Public Keys remain the property of the Subscribers who rightfully hold them. All secret shares (distributed elements) of the DigiCert Private Keys are the property of DigiCert.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, DigiCert does not make any representations regarding its products or services. DigiCert represents, to the extent specified in this CPS, that:

1. DigiCert complies, in all material aspects, with the CP, this CPS, and all applicable laws and regulations,
2. DigiCert publishes and updates CRLs and OCSP responses on a regular basis,
3. All Certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein and in the Baseline Requirements,
4. DigiCert will maintain a repository of public information on its website, and
5. Information published on a qualified Certificate meets the requirements specified in EU law.

To the extent allowed under EU law, DigiCert:

1. Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information, including name verification for (1) Certificates intended for email and intranet use, (2) Multi-SAN Certificates, and (3) other Certificates issued to individuals and intranets.
2. Is not responsible for information contained in a Certificate except as stated in this CPS,
3. Does not warrant the quality, function, or performance of any software or hardware device, and
4. Is not responsible for failing to comply with this CPS because of circumstances outside of DigiCert's control.

For EV Certificates, DigiCert represents to Subscribers, Subjects, Application Software Vendors that distribute DigiCert's root Certificates, and Relying Parties that use a DigiCert Certificate while the Certificate is valid that DigiCert followed the EV Guidelines when verifying information and issuing EV Certificates.

This representation is limited solely to DigiCert's compliance with the EV Guidelines (e.g., DigiCert may rely on erroneous information provided in an attorney's opinion or accountant's letter that is checked in accordance with the Guidelines).

9.6.2. RA Representations and Warranties

RAs represent that:

1. The RA's certificate issuance and management services conform to the DigiCert CP and this CPS,
2. Information provided by the RA does not contain any false or misleading information,
3. Translations performed by the RA are an accurate translation of the original information, and
4. All Certificates requested by the RA meet the requirements of this CPS.

DigiCert's agreement with the RA may contain additional representations.

9.6.3. Subscriber Representations and Warranties

Prior to being issued and receiving a Certificate, subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify DigiCert and any applicable RA if a change occurs that could affect the status of the Certificate.

DigiCert requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of DigiCert and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, DigiCert will obtain, for the express benefit of DigiCert and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with DigiCert, or
2. The Applicant's acknowledgement of the Terms of Use.

Subscribers represent to DigiCert, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with DigiCert,
3. Confirm the accuracy of the certificate data prior to using the Certificate,
4. Promptly (i) request revocation of a Certificate, cease using it and its associated Private Key, and notify DigiCert if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the certificate, and (ii) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
5. Ensure that individuals using Certificates on behalf of an organization have received security training appropriate to the Certificate,
6. Use the Certificate only for authorized and legal purposes, consistent with the certificate purpose, this CPS, any applicable CP, and the relevant Subscriber Agreement, including only installing SSL/TLS Server Certificates on servers accessible at the domain listed in the Certificate and not using code

signing Certificates to sign malicious code or any code that is downloaded without a user's consent, and

7. Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

9.6.4. Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a DigiCert Certificate, it:

1. Obtained sufficient knowledge on the use of digital Certificates and PKI,
2. Studied the applicable limitations on the usage of Certificates and agrees to DigiCert's limitations on liability related to the use of Certificates,
3. Has read, understands, and agrees to the DigiCert Relying Party Agreement and this CPS,
4. Verified both the DigiCert Certificate and the Certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use a DigiCert Certificate if the Certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a DigiCert Certificate after considering:
    a) applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
    b) the intended use of the Certificate as listed in the certificate or this CPS,
    c) the data listed in the Certificate,
    d) the economic value of the transaction or communication,
    e) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
    f) the Relying Party's previous course of dealing with the Subscriber,
    g) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
    h) any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own risk.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES 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. A fiduciary duty is not created simply because an entity uses DigiCert's services.

9.8. LIMITATIONS OF LIABILITY

NOTHING HEREIN LIMITS LIABILTY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM DIGICERT'S NEGLIGENCE OR (II) FRAUD COMMITTED BY DIGICERT. EXCEPT AS STATED ABOVE, ANY ENTITY USING A DIGICERT CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF DIGICERT RELATED TO SUCH USE, PROVIDED THAT DIGICERT HAS MATERIALLY COMPLIED WITH THIS CPS IN PROVIDING THE CERTIFICATE OR SERVICE. DIGICERT'S LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS CPS IS LIMITED AS SET FORTH IN THE NETSURE EXTENDED WARRANTY PROTECTION PLAN AND THE DIGICERT RELYING PARTY AGREEMENT.

All liability is limited to actual and legally provable damages. DigiCert is not liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if DigiCert is aware of the possibility of such damages;

2. Liability related to fraud or willful misconduct of the Applicant;
3. Liability related to use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate or this CPS;
4. Liability related to the security, usability, or integrity of products not supplied by DigiCert, including the Subscriber's and Relying Party's hardware; or
5. Liability related to the compromise of a Subscriber's Private Key.

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, (iv) whether DigiCert failed to follow any provision of this CPS, or (v) whether any provision of this CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CPS are fundamental terms to the use of DigiCert's Certificates and services.

9.9. INDEMNITIES

9.9.1. Indemnification by DigiCert

DigiCert shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by an Application Software Vendor related to an EV Certificate issued by DigiCert, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (1) a valid and trustworthy EV Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) an EV Certificate that has expired or (ii) a revoked EV Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

9.9.2. Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify DigiCert, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3. Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify DigiCert, its partners, and any cross- signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10. TERM AND TERMINATION

9.10.1. Term

This CPS and any amendments to the CPS are effective when published to DigiCert's online repository and remain in effect until replaced with a newer version.

9.10.2. Termination

This CPS and any amendments remain in effect until replaced by a newer version.

9.10.3. Effect of Termination and Survival

DigiCert will communicate the conditions and effect of this CPS's termination via the DigiCert Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related

to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the Certificate is revoked or expired, even if this CPS terminates.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

DigiCert accepts notices related to this CPS at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from DigiCert. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. DigiCert may allow other forms of notice in its Subscriber Agreements.

DigiCert will notify the FPKIPA at least two weeks prior to implementation of any planned change to the infrastructure that has the potential to affect the FPKI operational environment, and all new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change will be provided to the FPKIPA within 24 hours following implementation.

DigiCert will notify Adobe a month in advance of any updates or changes with the potential to affect compliance with the AATL program, including:

1. Additions of Root CAs and Subordinate CAs
2. Additional CPs at the Root CA level
3. Changes in Certificate issuance procedures
4. Terminations or transition of ownership of Root CAs or Subordinate CAs.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

This CPS is reviewed annually. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the DCPA.

9.12.2. Notification Mechanism and Period

DigiCert posts CPS revisions to its website. DigiCert does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice and without changing the version number. Major changes affecting accredited Certificates are announced and approved by the accrediting agency prior to becoming effective. The DCPA is responsible for determining what constitutes a material change of the CPS.

9.12.3. Circumstances under which OID Must Be Changed

The DCPA is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13. DISPUTE RESOLUTION PROVISIONS

Parties are required to notify DigiCert and attempt to resolve disputes directly with DigiCert before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14. GOVERNING LAW

The national law of the relevant member state governs any dispute involving Qualified Certificates. Except for disputes involving Qualified Certificates, the laws of the state of Utah govern the interpretation, construction, and enforcement of this CPS and all proceedings related to DigiCert's products and services, including tort claims, without regard to any conflicts of law principles. The state of Utah has non-exclusive venue and jurisdiction over any proceedings related to the CPS or any DigiCert product or service.

9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products. Subject to section 9.4.5's Notice and Consent to Use Private Information

contained in Certificates. DigiCert meets the requirements of the European data protection laws and has established appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

DigiCert contractually obligates each RA to comply with this CPS and applicable industry guidelines. DigiCert also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2. Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of DigiCert. Unless specified otherwise in a contact with a party, DigiCert does not provide notice of assignment.

9.16.3. Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

DigiCert may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. DigiCert's failure to enforce a provision of this CPS does not waive DigiCert's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by DigiCert.

9.16.5. Force Majeure

DigiCert is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond DigiCert's reasonable control. The operation of the Internet is beyond DigiCert's reasonable control.

9.17. OTHER PROVISIONS

No stipulation.

APPENDIX A: SAMPLE OPINION LETTER

[*Date*]

To: DigiCert, Inc.
2801 N. Thanksgiving Way Suite
500
Lehi, UT 84043
Email: support@digicert.com
Fax: 801-705-0481

Re: Digital Certificate for *[Exact company name of client – see footnote 1]* ("**Client**")

This firm represents Client, who asked that I, as its [*accountant ,lawyer, solicitors, barrister, advocate, etc.*], attest to the following information solely as related to the Client's application for a digital certificate.

After reviewing the Client's records and based on my investigation, my professional opinion is that:

1. Client is a duly formed [*corporation, LLC, etc.*] under the laws of the [*state/province*] of [*name of governing jurisdiction where Client is incorporated or registered*]; is "active," "valid," "current," or the equivalent; and is not under any known legal disability.

2. [*If applicable*] The Romanized transliteration of Client's formal legal name is: [*Romanized name].*

3. [*If applicable*] Client conducts business under the [*assumed/DBA/trade*] name of *[assumed name of Client].* Client has a currently valid registration of the name with the government agency that has jurisdiction over the place of business listed below.

4. The address where [*Client, Client's parent, or Client's subsidiary – select one*] conducts business operations is:
[Insert place of business – this should match the address on the certificate application]

5. A main telephone number at Client's place of business is:
[Insert primary telephone number of business]

6. *[Name of Client's Representative – see footnote 2]* is an individual (or are individuals) with the authority to act on behalf of Client to:
   a) Provide information about the Client contained in the referenced application,
   b) Request one or more digital certificates and designate other persons to request digital certificates, and
   c) Agree to the contractual obligations contained in DigiCert's agreements.

7. *[Name and title of Client's Representative],* who is Client's *[Title of Client Representative],* can be contacted at:
Email: *[Email address of Client Representative]*
Phone: *[Phone number of Client Representative]*

8. Client has either operated as a business for three or more years or has an active deposit account held at a bank or other financial institution where funds deposited are payable on demand.

Although we did not find any exceptions to the above identification procedures, these procedures do not constitute an audit or opinion of Client's application for a digital certificate. We are not expressing an opinion

on Client's digital certificate application and have provided this letter solely for the benefit of DigiCert in connection with Client's application for a digital certificate. No other person or entity may rely on this letter without my express written consent. This letter shall not be quoted in whole or in part, used, published or otherwise referred to or relied upon in any manner, including, without limitation, in any financial statement or other document.

Signature: _____

Print Accountant/Attorney Name: _____ Phone Number: _____

Email: _____

Firm Name: _____ Licensed in: _____

License number, if any: _____

Contact information for licensing agency where this accountant's/attorney's license information may be verified: _____

Note 1: This must be the Client's exact corporate name as registered with the relevant Incorporating Agency in the Client's Jurisdiction of Incorporation.

Note 2: A Power of Attorney from an officer of the Client who has the power to delegate authority is sufficient to establish the Client Representative's actual authority. Multiple representatives may be listed.

Note 3: In-house counsel of the Client may submit this letter if permitted by the rules of your jurisdiction. Note 4: This letter may be submitted by mail, fax, or email.

Exhibit B

End User License Agreement
[Begins on the following page]

FINAL – DIGICERT EULA

DigiCert is willing to license the Licensed Software to Customer on the terms and conditions set forth in this Software End User License Agreement ("**EULA**"). By using the Licensed Software, Customer agrees to the terms and conditions set forth in this EULA. Capitalized terms used in this EULA but not defined herein have the meaning set forth in the DigiCert Master Services Agreement available at www.digicert.com/master-services-agreement.

1. License Rights. Subject to Customer's compliance with the terms and conditions of this License Agreement, DigiCert grants to Customer a non-exclusive, non-transferable license to use a reasonable number of copies of the Licensed Software solely in support of Customer's use of the specific Service that the Licensed Software is provided in connection with.
2. License Restrictions. Customer may not, without DigiCert's prior written consent, conduct, cause or permit the: (i) use, copying, modification, rental, lease, sublease, sublicense, or transfer of the Licensed Software except as expressly provided in this EULA; (ii) creation of any derivative works based on the Licensed Software, except as expressly provided in this EULA; (iii) reverse engineering, disassembly, or decompiling of the Licensed Software (except that Customer may decompile the Licensed Software for the purposes of interoperability only to the extent permitted by and subject to strict compliance under applicable law); (iv) use of the Licensed Software in connection with service bureau, facility management, timeshare, service provider or like activity whereby Customer operates or uses the Licensed Software for the benefit of a third party; or (v) use of the Licensed Software by any party other than Customer, except as expressly provided in this EULA.
3. Ownership/Title. The Licensed Software is the proprietary property of DigiCert or its licensors and is protected by copyright and patent laws. DigiCert and its licensors retain any and all rights, title and interest in and to the Licensed Software, including in all copies, improvements, enhancements, modifications and derivative works of the Licensed Software. Customer's rights to use the Licensed Software shall be limited to those expressly granted in this EULA. All rights not expressly granted to Customer are retained by DigiCert and/or its licensors.
4. Updates. Any updates to the Licensed Software provided by DigiCert at its sole discretion ("**Updates**") shall be subject to any terms and conditions provided with such Updates. If no terms and conditions are provided, then Updates are subject to this EULA. These updates may affect Customer's product and may require Customer to make changes to Customer's product in order to maintain interoperability.
5. Third Party Programs. This Licensed Software may contain third party software programs ("**Third Party Programs**") that are available under open source or free software licenses. This EULA does not alter any rights or obligations Customer may have under those open source or free software licenses. Notwithstanding anything to the contrary contained in such licenses, the disclaimer of warranties and the limitation of liability provisions in this EULA shall apply to such Third Party Programs.
6. Warranty and Limitation of Liability.
   - **6.1.** WARRANTY DISCLAIMER. THE LICENSED SOFTWARE IS PROVIDED "AS IS," EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ANY OTHER WARRANTY, WHETHER EXPRESSED OR IMPLIED.
   - **6.2.** LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL DIGICERT BE LIABLE TO YOU FOR ANY DIRECT, SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA, ARISING OUT OF THE USE OR INABILITY TO USE THE LICENSED SOFTWARE, EVEN IF DIGICERT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
   - **6.3.** SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.
7. Export Regulation. Customer acknowledges that it is not located in or a national of Cuba, North Korea, Iran, Syria or the Crimea Region of Ukraine or any other country or region subject to comprehensive

U.S. economic sanctions or on any United States Government list or other government list of prohibited or restricted parties for export control or economic sanctions purposes (including lists published by the U.S. Government, European Union or the United Nations). Customer acknowledges that the Licensed Software and related technical data and services (collectively "**Controlled Technology**") are subject to the import and export laws of the United States, specifically the U.S. Export Administration Regulations (EAR), and the laws of any country where Controlled Technology is imported or re-exported. The export or re-export of the Licensed Software in violation of the foregoing laws and regulations is strictly prohibited. Customer agrees that it will comply with all applicable export or import control laws and regulations and obtain appropriate U.S. and foreign governmental authorizations before exporting, re-exporting, importing, transferring or using the Licensed Software. The Licensed Software may be subject to import, distribution, transfer, or use restrictions for which Customer is solely responsible. The Licensed Software is prohibited for export or re-export to Cuba, North Korea, Iran, Syria, the Crimea Region of Ukraine and to any other country or region subject to

U.S. economic sanctions. Customer shall not, directly or indirectly, facilitate giving a country, entity or individual sanctioned under U.S. law access to the Licensed Software. Customer may not export the Licensed Software in connection with the use or development of missiles or chemical, biological, and nuclear weapons. Customer may not export the Licensed Software to any military entity, or to any other entity for a military purpose, unless subject to a valid license or license exception.

8. Term and Termination. This EULA will continue as long as Customer in compliance with its terms and are validly using the applicable Service. In the event Customer breaches this EULA or discontinues use of the applicable Service, this EULA will automatically terminate. Upon termination, Customer must immediately stop using and destroy all copies of the Licensed Software within Customer's possession or control. The Ownership/Title, Warranty and Limitation of Liability and General sections of this EULA will survive termination of theAgreement.

9. US Government Restricted Rights. The Licensed Software is provided with "Restricted Rights." Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the *Rights in Technical Data and Computer Software* clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the *Commercial Computer Software - Restricted Rights* at 48 CFR 52.227- 19, as applicable (and the successor clauses to any of the foregoing). The contractor/manufacturer is DigiCert, Inc. All Software provided to the U.S. Government, including its civilian and military agencies, is commercial computer software that was developed at private expense prior to its provision to any U.S. Government entity. Subject to any applicable regulations set out in the FAR or DFARS (and any superseding regulations), the Software is provided with the commercial license rights and restrictions described elsewhere in the Agreement. For Department of Defense agencies, the restrictions set forth in the *Technical Data - Commercial items* clause at DFARS 252.227-7015 (Nov 1995) shall alsoapply.

10. General. Customer may not assign the rights granted hereunder or this EULA, in whole or in part and whether by operation of contract, law or otherwise, without DigiCert's prior express written consent. DigiCert may audit Customer's use of the Licensed Software. If any provision of this EULA is found partly or wholly illegal or unenforceable, such provision shall be enforced to the maximum extent permissible, and remaining provisions of this EULA shall remain in full force and effect. A waiver of any breach or default under this EULA shall not constitute a waiver of any other subsequent breach or default. This EULA is the complete and exclusive agreement between Customer and DigiCert relating to the Licensed Software and supersedes any previous or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter.

Exhibit C

Digital Certificates by DigiCert – Terms of Use

[Begins on the following page]

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), or otherwise, issued by DigiCert, Inc., a Utah corporation ("**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.

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 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**"). DigiCert's CPSs are available at https://www.digicert.com/legal-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. Public 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 laws. Customer acknowledges that the Certificates are not available in countries restricted by the Office of Foreign Assets Control.

6. Certificate License.

Effective immediately after delivery and continuing until the Certificate expires or is revoked, Customer may 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. "**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.

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.

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. 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.

11. 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 http://www.digicert.com/subscriber-agreement. Subscribers of Customer must accept the Subscriber Agreement before receiving Certificates. For the purpose of this section, a "**Qualified Certificate**" is a Certificate (i) issued pursuant to the requirements of applicable EU or Swiss certification and electronic signature laws, and (ii) carries the highest assurance level of "qualified" pursuant to such requirements.

12. 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.

13. 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.

14. 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. 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.

15. 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.

16. 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.

17. 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 or other illegal or fraudulent purposes;

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.

18. 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.

19. 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 amend or terminate the Agreement to the extent necessary to comply with the change.

20. 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.

21. 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.

22. Intermediate Certificate for Private Certificates.

This Section 22 only applies if Customer purchases a dedicated Private Root Certificate and/or Intermediate Certificate for the issuance of Private Certificates 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 non-publicly trusted Certificates through the Portal. 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 non-publicly trusted 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 acknowledges and agrees that all Certificates issued from an Intermediate Certificate must expire at least two years prior to 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 hereunder expire or are revoked.

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; or (iv) Customer continues to use the Intermediate Certificate after Customer's right to use the Intermediate Certificate terminates.

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.

23. EULA & Third-Party Terms.

a. Customer's use of any 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.

24. 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.

25. 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 25 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.

26. Adobe-Required Supplemental Obligations

If Customer uses DigiCert PKI Platform to issue 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.

27. 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).

28. 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.

Exhibit D

Privacy Policy

[Begins on the following page]

DigiCert Public Privacy Notice

Effective Date

February 13, 2020
Privacy Notice Archive

Introduction

DigiCert, Inc. and its subsidiaries ("DigiCert", "DigiCert Group," "we" or "us") are committed to protecting the privacy of its Website visitors ("you") and Customers ("you" or "Customer") and employees or agents of Customers ("you" or "Individuals"). As a result, DigiCert has promulgated this privacy notice to inform its Website visitors, Customers and Individuals about how DigiCert will collect, use, share or otherwise process any personal data or usage information. This privacy notice applies to all sites owned and operated by DigiCert (collectively, "Websites," individually referred to as a "Website," meaning each and every Website owned and operated by DigiCert). This privacy notice also applies to DigiCert's provision of website and other certificate services and all dealings with natural-person representatives of our Customers (the "Validation Services" or "Certificates").

DigiCert is a company established in the United States with principal offices at 2801 North Thanksgiving Way, Suite 500, Lehi, Utah 84043 and for the purpose of the EU General Data Protection Regulation ("GDPR") and any other applicable data privacy laws, we are the data controller of personal information obtained through our Website. We are also a data controller in relation to the Individuals' personal information that we receive from Customers, either directly or through resellers.

If you have any concerns or questions regarding the personal data we process through our Website or through providing services to our Customers, you may contact DigiCert's Data Privacy Officer at dpo@digicert.com. If you are an EU or Switzerland resident, we have appointed a Data Protection Liaison for Europe at DigiCert Ireland Ltd. as our Europe Representative who you can contact (in addition to or instead of our Data Privacy Officer, located at our US headquarters) should you have any issues in connection with personal information processed through our Website. Contact details for the Data Privacy Officer and Europe Data Protection Liaison are provided below.

Information that DigiCert Receives

- **Through our Website**: DigiCert collects information such as the name, organization, and email address of Website visitors and Customers who voluntarily submit that information via our Website, email, instant chat, by creating an account or otherwise, in order to download software or to submit sales or technical support questions.

- **From Customers**: Customers request DigiCert Certificates through their account in DigiCert's Website (the "Account") or through other contact with DigiCert or its resellers. When submitting a request, Customers typically provide to DigiCert the following information about Individuals: name, email address, telephone number, address and government-issued identification (which may include additional information, depending on the identification used). Specific information about personal data required for particular DigiCert services and products may be found in DigiCert's Certification Practices Statement.

  Where Customers share personal information of Individuals with DigiCert, Customers represent that they have collected and processed such information in accordance with data privacy laws, and that they have duly informed the Individuals that their personal information was provided to DigiCert. DigiCert will process such information following Customer instructions as well as according to the industry standards that govern the issuance of digital Certificates ("Industry Standards"). More information on the Industry Standards may be found through consulting DigiCert's Certification Practices Statement.

- **From Candidates for Employment:** Interested persons submit personal information relevant to a job inquiry or application for employment. Candidates for employment can find specific information about how we use personal information provided to us in this context in our Candidate Portal Privacy Notice.

Use of Information

We will use your information to:

- **Provide products and services / live chat / sales & support**: As it is in our legitimate interest to market, sell and provide our products and services, send order confirmations, respond to Customer service requests, provide chat services with sales questions and technical support needs, and fulfill your order, including using the information to verify the identity of the Customer or to contact the Customer in order to discuss support, renewal, and the purchase of products and services.

- **Marketing**: We will use your information as it is in our legitimate interests to send out promotional emails (subject to seeking your consent where required by applicable law). These emails include beacons that communicate information about the email back to DigiCert, as further set out in Cookie Settings. Such tracking allows DigiCert to gauge the effectiveness of its advertising and marketing campaigns. Recipients can opt-out of receiving promotional communications from DigiCert by following the unsubscribe instructions provided in each email or by emailing privacy@digicert.com. DigiCert may use third parties, with which it has a confidentiality agreement, to send promotional emails on our behalf. However, DigiCert does not permit any third party to use Customer information provided by DigiCert or obtained on DigiCert's behalf for any other purpose. Anyone receiving an unsolicited email related to DigiCert's products and services should forward the entire message and headers to privacy@digicert.com.

- **Validation Services**: DigiCert uses information provided by Customers to perform Validation Services, in accordance with Industry Standards. DigiCert uses this information as follows: (1) to perform our contracts with Customers that are natural persons; (2) based on the legitimate interest of DigiCert to provide services to Customers that are legal entities; and (3) based on the legitimate interest of Customers to have DigiCert issue Certificates.

Please refer to DigiCert's Master Services Agreement and Certification Practices Statement for details on the terms, conditions, policies and standards regarding the request and issuance of Certificates.

- **Advisory e-mails**: While a Customer account is active, DigiCert will send advisory e-mails to Customers to provide support and security updates in relation to our products and services, as this is necessary for the performance of our contracts with Customers. Advisory emails are used to respond to inquiries, provide support and validation services, provide upgrade information and security updates, inform customers about expiring Certificates, and inform the Customer about ordered products and services. Because advisory emails contain essential information related to the use and security of DigiCert's products and services, Customers are not able to unsubscribe from advisory service emails while their Customer account is active. DigiCert may also use third-party service providers to assist in sending these communications, subject to the same restrictions as mentioned in the "Marketing" sub-heading, above.

- **Technical usage information**: As it is in our legitimate interests to ensure the proper functioning of our Website by personalizing its use, monitoring usage activity and trends, and keeping the Website safe and secure, when you visit the Website, we collect the information sent to us by your computer, mobile phone, or other access device. This information includes: your IP address; device information including, but not limited to, identifier, name, and type of operating

system; mobile network information; and standard web information, such as your browser type and the pages you access on our Website.

- **Customer analytics**: It is in our legitimate interest to analyze information provided by our Customers to track sales, demographics, product usage and related analytics so that we can improve our product offerings and target marketing and sales resources. We create reports and data analyses that are reported internally and occasionally shared with third-party service providers, who are under a duty of strict confidentiality and who are not authorized to use information provided by us for any other purpose than to provide services as directed by us.

Cookies & Tracking Technologies

DigiCert uses cookies, web beacons and log files to automatically gather, analyze, and store technical information about Website visitors. See Cookie Settings for more information.

Sharing with Third Parties

DigiCert will publicly disclose information embedded in an issued Certificate as necessary to provide the services contracted by Customer, in accordance with Industry Standards.(See our Certification Practices Statement for information specific to the various services and products offered by DigiCert.)

When performing its services, DigiCert uses third party sources to confirm or supplement the information that it obtains from a Customer, including information about Individuals. DigiCert uses such information from third-party sources exclusively for the purposes of its Validation Services, based on the legitimate interests of DigiCert and of the Customer to provide services and have a Certificate issued.

DigiCert never sells or provides personal information to third parties for uses apart from assisting DigiCert in servicing our Customers and Website visitors. We will share your personal information with third parties including these categories of recipients:

- IT service providers that provide us with SaaS services including customer relationship management and other database and application software;
- Marketing providers, advertisers and advertising networks that require the data to send you advertisements about our products and select and serve relevant advertisements to you and others;
- Analytics and search engine providers that assist us in the improvement and optimization of the Website;
- Chat-based support software services that allow users to input information, including an email address, to request support and clarify their problem; and
- Credit card and payment providers that help process payments for us (note that we do not store any provided credit card information).

DigiCert will share your information with law enforcement agencies, public authorities or other organizations if legally required to do so, including to meet national security or law enforcement requirements, or if we have a good faith belief that such use is reasonably necessary to:

- comply with a legal obligation, process or request;
- enforce our terms and conditions and other agreements, including investigation of any potential violation thereof;

- detect, prevent or otherwise address security, fraud or technical issues; or

- protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law.

DigiCert will also disclose your information to third parties:

- in the event that we sell any business or assets, in which case we will disclose your data to the prospective buyer of such business or assets; or

- if we or substantially all of our assets are acquired by a third party, in which case information held by us about our users will be one of the transferred assets.

Referrals

If you choose to use our referral service to tell a friend about our Website, we will ask you for your friend's name and email address. We will automatically send your friend a one-time email inviting them to visit the site. DigiCert collects this information for the sole purpose of sending this one-time email and tracking success of the referral program.

If you believe that one of your contacts has provided DigiCert with your personal information, you may contact us at privacy@digicert.com to request that we remove this information from our database.

Blogs

Our Website offers publicly accessible blogs or community forums. Any information you provide in these areas can be read, collected, and used by others who access them.

To request removal or your personal information from our blog or community forums, please contact us at privacy@digicert.com. In some cases, we may not be able to remove your personal information, in which case we will let you know if we are unable to do so and why, as well as additional contact information when applicable.

Social Media Widgets

The Website includes social media features, such as a Facebook "Like" button and widgets, as well as share buttons or interactive mini-programs. These features collect the user's IP address, the pages visited on the Website, and set cookies to enable the features to function properly. Social media features are either hosted by a third party or hosted directly on the Website. Interactions with these features are governed by the privacy notice of the corresponding social media company.

Security

The security of your personal information is of the utmost importance to DigiCert. DigiCert only transmits personal information, including sensitive information (such as credit cards), using transport layer security (TLS, formerly referred to as secure sockets layer or SSL). To learn more about TLS, follow this link: https://www.digicert.com/ssl/.

Unfortunately, no method of transmission over the Internet or electronic storage is 100% secure. While DigiCert strives to use commercially acceptable standards to protect personal information, DigiCert cannot guarantee absolute security. If you have any questions about the security of your personal information, please contact us at dpo@digicert.com.

We take all necessary security and legal precautions to ensure the safety and integrity of the Individual's personal data that we receive from Customer, including, as appropriate, (i) the pseudonymization of personal data; (ii) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) restoring the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) regularly testing, assessing, and evaluating the effectiveness of

technical and organizational measures for ensuring the security of the processing. More information about DigiCert's security practices can be found here and here.

Where We Store Your Data

The DigiCert Group has its parent company based in the United States and our Website is hosted in the United States. Therefore, if you are located outside the United States, the information that you submit to us through our Website will be transferred to the United States. Furthermore, DigiCert performs Validation Services for the EMEA region in its office in South Africa and provides hosting services for certain products in Australia and Japan. Accordingly, depending on your location and the products you are using, Customer data and your personal data will be accessible from and transferred to the United States, South Africa, Australia, Ireland, India and Japan.

Where you have a question, dispute or complaint regarding DigiCert's collection, storage, or use of your personal information, you may ask a question or make a complaint to DigiCert by sending it to privacy@digicert.com. If you are an EU or Switzerland resident, where the dispute or complaint is not satisfactorily resolved or you do not receive a timely response, you may escalate the matter to your European data protection authority free of charge, and DigiCert commits to cooperate with the relevant European data protection authority and will comply with the advice given by this authority with regard to your information which was transferred from the European Union or Switzerland in the context of this Website or through DigiCert's provision of services. You may also contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request. For EU or Switzerland residents, such complaint is without prejudice to your right to launch a claim with the data protection supervisory authority in the country in which you live or work.

Individual Rights over Personal Information

Generally, a Customer or Individual can review, delete inaccuracies, and update personal information through their DigiCert account interface by accessing and editing their Account Profile through the DigiCert service platform they are using. Information and help in accessing and editing the Account Profile can be obtained by contacting DigiCert Support at support@digicert.com or through the phone numbers provided below.

In certain circumstances and where legally available or required in your jurisdiction, Individuals also have the following rights:

- **Access and portability**: You have the right to know whether we process personal data about you, and if we do, to access data we hold about you and certain information about how we use it and who we share it with.

- **Correction, erasure and restriction of processing**: You have the right to require us to correct any personal data held about you that is inaccurate and have incomplete data completed or ask us to delete data (i) where you believe it is no longer necessary for us to hold the personal data; (ii) where we are processing your data on the basis of our legitimate interest and you object to such processing; or (iii) if you believe the personal data we hold about you is being unlawfully processed by us. You can ask us to restrict processing data we hold about you other than for storage purposes if you believe the personal data is not accurate (whilst we verify accuracy); where we want to erase the personal data as the processing we are doing is unlawful but you want us to continue to store; where we no longer need the personal data for the purposes of the processing but you require us to retain the data for the establishment, exercise or defense of legal claims or where you have objected to us processing personal data and we are considering your objection.

Customers and Individuals cannot edit a DigiCert Certificate directly. In order to update information in a Certificate, including personal information, Customers or Individuals must submit a change request through the Customer's Account, and DigiCert will implement the edits or issue a new certificate where applicable. If you have questions about how to submit a change request to your Certificate, please contact DigiCert Support at support@digicert.com or through the phone numbers provided below.

- **Objection**: You have the right to object to our processing of data about you and we will consider your request. Please contact privacy@digicert.com with details of your objection, providing us with detail as to your reasoning so that we can assess whether we have a compelling or overriding interest in continuing to process such data or whether we need to process it in relation to legal claims.

- **Testimonials**: With prior permission from the Customer, DigiCert displays personal testimonials of satisfied Customers on our Website in addition to other endorsements. Customers wishing to update or delete a testimonial should contact DigiCert at privacy@digicert.com.

- **Marketing**: You have the right to ask us not to process your personal data for marketing purposes. You can exercise your right to prevent such processing at any time by contacting us at privacy@digicert.com.

- **Complaints**: In the event that you wish to make a complaint about how we process your personal data, please contact us in the first instance at privacy@digicert.com and we will endeavor to deal with your request. If you are an EU or Switzerland resident, this is without prejudice to your right to launch a claim with the data protection supervisory authority in the European country in which you live or work where you think we have infringed data protection laws.

You can exercise these rights by sending an email to privacy@digicert.com or by mailing DigiCert at the address listed in this notice. Before we respond to your request, we will ask you to verify your identity. Note that these rights may not apply in their entirety in your jurisdiction and are subject to the applicable law of the jurisdiction where you reside. Where exercise of a particular data subject right is not required by law, your request will be handled on a case-by-case basis.

How Long We Store Your Data

We will retain your information as follows:

- Account data and data provided for Validation Services (including to send Advisory e-mails): As long as the account is active, while a Certificate remains unexpired, and in accordance with industry standards, which requires us to maintain the data for 7.5 to 10.5 years (depending on the type of Certificate with which the data is associated) after account cancellation or Certificate expiration. In addition, after account cancellation, we will keep this for as long as necessary to defend against legal claims, resolve disputes or enforce Customer agreements.

- Data provided and collected for marketing and web experience customization purposes: until you notify us that you no longer want us to use your information for marketing and/or web experience customization purposes, by unsubscribing from any marketing email you receive, changing your cookie preferences through consulting our Cookie Settings, or by contacting privacy@digicert.com.

After we no longer have a legitimate basis for retaining your personal data, we may store your information in an aggregated and anonymized format.

EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield

DigiCert participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. We are committed to subjecting all personal data received from European Union (EU) member countries and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Framework's applicable Principles. To learn more about the Privacy Shield Frameworks, and to view our certification, visit the U.S. Department of Commerce's Privacy Shield List, here: https://www.privacyshield.gov.

DigiCert is responsible for the processing of personal data it receives, under each Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. DigiCert complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, DigiCert is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedbackform.truste.com/watchdog/request.

Under certain conditions, more fully described on the Privacy Shield website here, https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

Applicability

Terms of use for software downloaded from DigiCert's Websites may override the terms of this privacy notice, with respect to use of the software.

Our Website includes links to third party websites whose privacy practices may differ from those of DigiCert. If you submit personal information to any of those websites, your information is governed by their privacy policies. We encourage you to carefully read the privacy policies of those third-party websites before you submit any information to those websites.

Changes to This Privacy Notice

If we make material changes to our information practices, we will update this privacy notice and notify interested parties (e.g., by posting a notice on our home page or by emailing affected individuals). Visitors should check the Website regularly to be aware of changes. We encourage you to periodically review this page for the latest information on our privacy practices. Revisions to the privacy notice are effective 30 calendar days after being posted, or as required by applicable law.

Contact

Please contact DigiCert or DigiCert's Europe Data Protection Liaison with any questions or concerns about this privacy notice or our data collection practices:

DigiCert Data Privacy Officer

By mail:

DigiCert, Inc.
Attention: Data Privacy Officer, Aaron Olsen
2801 North Thanksgiving Way
Suite 500
Lehi, Utah 84043
USA

By phone or fax:

Toll Free: 1-800-896-7973 (US & Canada)
Direct: 1-801-701-9600
Fax Toll Free: 1-866-842-0223 (US & Canada)
Fax Direct: 801-705-0481

By email:
dpo@digicert.com

Europe Data Protection Liaison

By mail:

DigiCert Ireland Ltd.
Attention: Europe Data Protection Liaison, Richard Hall
Unit 21, Beckett Way
Park West Business Park
Dublin 12
Ireland

By phone or fax:

Phone:+353 1803 5400
Fax: +353 1861 7990

By email:

richard.hall@digicert.com

For assistance with technical difficulties, including problems with accessing or using your Customer account, please email support@digicert.com.

As noted above, if you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request. For EU or Switzerland residents, this is without prejudice to your right to launch a claim with the data protection supervisory authority in the country in which you live or work.