DIGICERT PKI PLATFORM SERVICE DESCRIPTION (MPKI 8.x)

(formerly known as Symantec Managed Public Key Infrastructure (PKI) Service)

Service Overview

The DigiCert PKI Platform (MPKI 8.x or greater) ("**Managed PKI Service**" or "**Service**") provides a flexible PKI platform to manage the complete certificate lifecycle to issue new certificates, renew existing certificates, and revoke untrustworthy certificates. Additionally, Managed PKI Service provides the ability to escrow and recover private keys of certificates used to encrypt emails, file systems, or other data, as well as numerous validation services to verify certificates' current status to ensure only trustworthy certificates perform such actions as encrypting data, digitally signing documents, or authenticating on to networks.

This Service Description, with any attachments included by reference, is part of any agreement which incorporates this Service Description by reference (collectively, the "Agreement"), for the Service which is described in this Service Description and is provided by DigiCert.

Table of Contents

- Appendix C – Adobe® Document Signing Services
- Appendix D – LTE Certificate Service
- Appendix E – Manufacturer Certificates

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Features

As a managed service, the Managed PKI Service significantly reduces costs associated with an in-house PKI. For example, customers would need to acquire cryptographic and application server hardware, purchase server and client licenses, and train staff before issuing the first certificate from an in-house PKI deployment. Customers would have to create their own certificate policy (CP) as a principal statement of policy governing the PKI hierarchy, and certification practices statement (CPS), which defines certificate process and procedures as well as trusted roles and responsibilities. The Managed PKI Service is designed as multi-tenant, highly-available environment based on best-of-breed cryptographic and application server hardware. This environment is monitored 24x7x365 by a professionally trained staff that has passed enhanced security background checks, and is audited on a regular basis to maintain *WebTrust* and SOC-2 accreditation.

- The Managed PKI Service creates and manages **Certificate Authority (CA)** hierarchies.
  - The Managed PKI Service is available in the following standard CA hierarchies:
    - DigiCert Trust Network (DTN) (formerly known as the Symantec Trust Network (STN)) – see ***Appendix A***
    - Private Certificate Authority – see ***Appendix B***
    - Adobe® Document Signing Services – see ***Appendix C***
    - LTE Certificate Service – see ***Appendix D***
    - Manufacturer Certificates – see ***Appendix E***
  - Each service account includes at least one CA Certificate for each CA hierarchy that you elect. Additional CA Certificates for a given volume may be purchased later. Any extraction of CA Certificates and/or corresponding key pairs from DigiCert systems and services will be subject to agreement of the parties.
- The Managed PKI Service offers two (2) deployment models, Cloud and Hybrid, to **manage certificate lifecycle**.
  - The Cloud deployment model hosts account, certificate, and key management tools in DigiCert's data centers.
  - The Hybrid deployment model also hosts all account, certificate, and key management tools in DigiCert's data centers, but this model installs registration authority (RA) and directory integration tools in the customer's data center as well.
  - The deployment models are not exclusive and can use a combination of deployment models based on the needs of various PKI projects. Both deployment models work with desktop middleware, PKI Client, designed to dramatically improve the user experience with the certificate lifecycle.

- The Managed PKI Service offers the following **management tools**:
    - **PKI Manager** – PKI Manager is a web portal hosted in DigiCert's data centers for a PKI administrator to perform tasks related to account, user, certificate, and key management.
        - *Account Management*: PKI Manager enables a PKI administrator to view certificate authorities (CAs), number of Seats, and reports associated with their account(s). PKI Manager also allows a PKI administrator to create and assign responsibilities to additional PKI administrators.
        - *User Management*: PKI Manager permits a PKI administrator to add users, revoke users, generate unique enrollment codes for each user, and customize email notifications sent to users. PKI Manager also has the capability to provide users with document and video-based instructions to configure third party applications to work with the newly-issued certificates.
        - *Certificate Management*: PKI Manager enables a PKI administrator to configure certificate profiles for different CAs in their account. As part of these certificate profiles, a PKI administrator sets such parameters as key sizes, key usages, and signing algorithms. A PKI administrator also selects user experience (enrollment through OS/browser or PKI Client) and security protection level. A PKI administrator decides whether or not to escrow private keys of the certificates. Along with configuring certificate profiles, PKI Manager lets a PKI administrator revoke certificates which have become untrustworthy because a user no longer needs a certificate (*e.g.*, a user left the company) or a private key has been comprised (*e.g.*, a user lost a laptop).
        - *Key Management*: PKI Manager provides a PKI administrator with the ability to recover a private key of an encryption certificate.
    - **PKI Certificate Service** – PKI Certificate Service hosts the certificate enrollment web pages in DigiCert's data centers for users (a.k.a., subscribers) to request certificates. These web pages guide users through the necessary steps to request certificates. In addition, these web pages may display instructions, provided by a PKI administrator, to configure third-party products.
    - **Certificate Issuance Center** – Certificate Issuance Center is the certificate engine hosted in DigiCert's data centers. This certificate engine creates certificates based on certificate signing requests submitted from PKI Certificate Service, received from PKI Enterprise Gateway, or sent via Web Services. This certificate engine signs these certificates with the issuing Certificate Authority (CA).
    - **PKI Enterprise Gateway** – PKI Enterprise Gateway is a registration authority (RA) authority application installed in the customer's data center, if desired. This application tightly integrates with a Lightweight Directory Access Protocol (LDAP) source (*e.g.*, Microsoft® Active Directory®) to automatically approve certificate requests and publish certificate data back into the LDAP source.
    - **PKI Client** – PKI Client is an endpoint middleware designed to dramatically improve user experience with the certificate lifecycle. PKI Client is available for desktops on Windows as well as MAC operating systems. In the browser enrollment experience, users use either Microsoft Internet Explorer®, Safari®, Chrome™ or Mozilla® Firefox® to request certificate from certificate enrollment web pages. While this native experience does not require any additional software, the native experience has known usability limitations. For example, Microsoft Internet Explorer produces numerous pop-up windows with

warning messages that often confuse users. In the PKI Client experience, the certificate lifecycle has been streamlined to automate common functions (*i.e.*, certificate renewal) to minimize user involvement. PKI Client also provides centralized policy management functions (*e.g.*, PIN, export, etc.) to protect certificates. Further, PKI Client has the ability to auto-configure third-party products (*e.g.*, wireless, virtual private network clients, etc.) to use certificates. DigiCert Managed PKI Certificate lifecycle management functions are also available on mobile devices such as the iOS that leverages built-in iOS Over-the-Air (OTA) protocol capabilities. This allows the iOS device or application to make certificate enrollment requests via Apple's SCEP protocol. For mobile operating systems such as the Android OS, that don't have an iOS OTA equivalent, DigiCert provides a PKI Client that similarly hides the complexity of configuring the device and application to use the certificate.

- **PKI Web Services** – PKI Web Services hosted in the DigiCert data center provide the capability to programmatically integrate with the Managed PKI Service. A third party application can obtain a certificate policy and perform certificate lifecycle functions such as enroll and renew using the API provided by PKI Web Services.

- The Managed PKI Service offers the following **authentication methods**:
  - **Authentication using Enrollment Code** – With this type of authentication, a PKI administrator can generate a unique enrollment code for each user in order to automatically approve certificate requests. When a PKI administrator sends certificate invitations to users with a link to certificate enrollment web page, the PKI administrator includes the unique enrollment code for that user. Users then include their enrollment code along with any additional information in the certificate enrollment web pages. Certificate Issuance Center compares this enrollment code to the information generated in PKI Manager. If there is a match, Certificate Issuance Center issues a certificate. If the user-entered enrollment code does not match the one that was generated for that user, Certificate Issuance Center gives an error message to the user.
  - **Automated Authentication** – Automated authentication approves certificate requests based on data in a LDAP source (i.e., Microsoft Active Directory). PKI Enterprise Gateway must be installed in a customer's data center and integrated with an LDAP source. When users submit certificate requests via PKI Certificate Service, PKI Enterprise Gateway compares the data in the certificate requests with the LDAP source. If data match, PKI Enterprise Gateway approves certificate requests, signs certificate requests with Registration Authority (RA) certificate, and sends signed certificate requests to Certificate Issuance Center. Else, PKI Enterprise Gateway rejects certificates requests.

- The Managed PKI Service offers the following **certificate validation tools**:
  - **Certificate Revocation List (CRL)** – Many third-party products have the ability to check the certificate's current status (e.g., active, revoked, etc.) through Certificate Revocation List (CRL). A CRL is a black list of revoked certificates that have not yet expired. These products can be configured to download and check most recent CRL on a regular basis. If a certificate appears on the CRL, these products deny access (e.g., will not authenticate onto networks, digitally sign documents, etc.). DigiCert produces a CRL at least once every 24 hours.
  - **Online Certificate Status Protocol (OCSP)** – Many third-party products verify the current status of certificates (e.g., active, revoked, etc.) via Online Certificate Status Protocol (OCSP). While all revoked certificates will appear on a CRL, there is a time delay between the certificate's revocation and next CRL run which may be up to 24 hours for a standard CRL. DigiCert immediately updates the certificates' status upon any change (e.g., revoked, suspended, etc.) which is reflected in near-real time within DigiCert's OCSP tool, Trusted Global Validation (TGV).

- DigiCert offers the following **hardware options** to complement the Managed PKI Service:
    - **SafeNet® PKI Tokens** - DigiCert is an authorized reseller of SafeNet® hardware USB tokens. In addition, these tokens also come with a three (3)-year warranty as described in the Warranty Information Supplement available in the Repository. These tokens meet Federal Information Processing Standard (FIPS) 140-2 and Common Criteria standards.
    - **SafeNet® Hardware Security Modules (HSMs)** – DigiCert is an authorized reseller of SafeNet® Luna® hardware security modules (HSMs) which consists of Luna® PCI cards, Luna® SA network appliances, and Luna® PCM tokens. These HSMs may also include firmware or associated software (such as SafeNet Authentication Client). While these HSMs include a one (1) year basic warranty, DigiCert resells optional SafeNet extended warranty programs for additional charge. These HSMs also meet FIPS 140-2 Level 2 and Common Criteria standards.
        - Title to any HSMs sold will pass to Customer or to any party designated by Customer upon shipment from DigiCert. Delivery of all items is Ex Works (EXW) DigiCert's shipping point – Incoterms 2010. Delivery of HSMs is complete when such are made available to the carrier at DigiCert's shipping point. Freight terms must be collect or third party.
        - If Customer elects to purchase HSMs through DigiCert ("**Customer HSMs**") and have such Customer HSMs stored at DigiCert's datacenter, then Customer HSMs will be stored and protected in the same fashion as DigiCert's own HSMs. Upon any expiration or termination of DigiCert's applicable services provided to Customer, upon Customer's request, DigiCert will transfer Customer HSMs to Customer in accordance with the industry's best practice. Transfer of Customer HSMs will be at no cost to Customer, provided, however, that if Customer requests technical support in connection with the transfer of Customer HSMs, DigiCert will provide transition support under a separately negotiated statement of work that is mutually agreeable to the parties.
- DigiCert offers the following types of **Certificates** or **Seats** through the Managed PKI Service:
    - ***User Seats***: Certificates issued to human Subscribers that authenticate them as users accessing the private network over VPN/WiFi. Certificates issued under such "*User Seats*" allow multiple quantities and different types of user certificates (VPN, WiFi, SMIME, etc. from the *User Seat* Pool) to be issued to these users. One *User Seat* can mean multiple quantities of certificates issued to a single and unique user.
    - ***Device Seats***: Certificates issued to devices (such as laptops, computers, LTE equipment, etc.) as Subscribers to allow such devices to access to a private network. Unlike the *User Seats*, a *Device Seat* means a certificate issued to a device and to be used on one (1) physical device only.
    - ***Server Seats***: Certificates issued to an organization's internal servers as Subscribers to assure such servers' identity to users or devices requesting access to the intranet websites hosted on the servers. Managed PKI Service issues private hierarchy server certificates as part of this solution. Each physical or virtualized server requires a *Server Seat*.
    - ***Organization Certificates***: Certificates issued to an organization or entity as the Subscriber to allow identity assurance (such as in the case of private code signing Certificates) and also digital signatures (as in the case of Word or PDF signing at the organizational level). The following are restrictions for *Organization Certificates*. Customer must not use a code signing, or any other *Organizational Certificate*: (i) for or on behalf of any organization other than Customer organization; (ii) to

perform private 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 malicious or harmful content of any kind including, but not limited to, content that would otherwise have the effect of inconveniencing the recipient of such content; 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).

DigiCert Obligations

- Following completion of the requisite installation, DigiCert will provide Customer with the services specified in this Service Description.
- DigiCert will issue, manage, revoke, and/or renew Certificates in accordance with the instructions provided by Customer and its Managed PKI Administrator(s).
- Upon Customer's approval of a Certificate Application, DigiCert: (1) is entitled to rely upon the accuracy of the information in each such approved Certificate Application; and (2) will issue a Certificate for the Certificate Applicant for which such Certificate Application was submitted.
- Certificates issued or licensed under this Service Description, including Administrator Certificates, will have a maximum Operational Period of twelve (12) months from the date each Certificate is issued.
- During a single CA Key Generation event, DigiCert will generate for Customer, pairs of CA keys for use in signing Certificates issued by DigiCert on behalf of Customer in the DTN or such other hierarchy of Customer's election.
- Customer CA Private Key of each key pair will be stored in one or more hardware security modules.

Customer Responsibilities

DigiCert can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, DigiCert's performance of the Service may be delayed, impaired or prevented, as noted below.

- Setup Enablement: Customer must provide information required for DigiCert to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist DigiCert in delivery of the Service, upon reasonable request by DigiCert.
- Customer must ensure that:
  - all information material to the issuance of a Certificate and validated by or on behalf of Customer is true and correct in all material respects;
  - Customer's approval of Certificate Applications will not result in Erroneous Issuance;
  - Customer's revocation of Certificates complies with the STN CPS or the Adobe CPS (if and as applicable);
  - Customer has substantially complied with the STN CPS or the Adobe CPS (if and as applicable);
  - Customer has substantially complied with the RA requirements (if applicable);
  - Certificate information provided to DigiCert will not infringe the intellectual property rights of any third party (such as domain squatting);
  - information in the Certificate Application(s) (including email address(es)) has not been and will not be used for any unlawful purpose;
  - Customer's Managed PKI Administrator has been (since the time of the Administrator Certificate's creation) and will remain the only person possessing the Administrator Certificate's Private Key, any

challenge phrase, PIN, software, or hardware mechanism protecting the Private Key, and no unauthorized person has had or will have access to such material or information;

- Customer will use the Administrator Certificate exclusively for authorized and legal purposes consistent with this Service Description; and
- Customer will not 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.

Assistance and Technical Support

The support and maintenance commitments of DigiCert are described in the applicable Service Level Agreement available in the Repository.

SERVICE-SPECIFIC TERMS

No Auto-Renewal

Notwithstanding anything to the contrary in the Agreement, there is no automatic renewal of the NSL Service. Before the NSL Service expires, Customer must contact DigiCert or its channel reseller partner to renew.

Service Conditions

- **Administrator Certificate**: Upon Customer's submission of a Certificate Application for an Administrator Certificate and DigiCert's completion of authentication procedures required for the Administrator Certificate, DigiCert will process the Certificate Application. DigiCert will notify Customer whether Customer's Certificate Application for an Administrator Certificate is approved or rejected. Managed PKI Administrator's use of the PIN from DigiCert to pick up the Administrator Certificate or otherwise installing or using the Administrator Certificate will constitute Managed PKI Administrator's acceptance of the Administrator Certificate. After the Managed PKI Administrator picks up or otherwise installs the Administrator Certificate, the Managed PKI Administrator must review the information in it before using it and promptly notify DigiCert of any errors. Upon receipt of such notice, DigiCert may revoke the Administrator Certificate and issue a corrected Administrator Certificate.
- **Survival**: In addition to the termination provisions set forth in the Agreement, the revocation and security requirements in this Service Description and any applicable CPS will survive termination of the Agreement or the applicable order document until the end of the Operational Period of all Certificates issued hereunder.
- **Compliance with Local Laws**: Customer is responsible for ensuring that Customer's acquisition, use, or acceptance of public and private key pairs generated by DigiCert in accordance with this Service Description 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 pairs.
- **Audit Rights**: DigiCert may conduct an audit of Customer's procedures not more than once per year to ensure compliance with the terms of this Service Description. Any such audit will be conducted during business hours upon reasonable written notice to Customer and will not unreasonably interfere with Customer's business activities. Customer must reasonably cooperate with DigiCert in connection with any such audit. If the audit reveals that Customer has breached any term of the Service Description terms and conditions, then: (1) Customer will pay DigiCert's reasonable costs of conducting the audit, and (2) notwithstanding the one audit per year limitation stated above, DigiCert may conduct such further

audits as it deems reasonably necessary to ensure compliance with the terms herein. Routine annual audits may only cover the activities of the immediately preceding year.

- **Use Restrictions**: Certificates issued to Subscribers may not be integrated with or installed in any Relying Party that does not correspond to the applicable Certificate request. Each Certificate must be used only for its intended use as the type of such Certificate indicates.

- Please refer to CA hierarchy specific additional conditions as follows:
  - DigiCert Trust Network (DTN) – see ***Appendix A***
  - Private Certificate Authority – see ***Appendix B***
  - Adobe® Document Signing Services – see ***Appendix C***
  - LTE Certificate Service – see ***Appendix D***
  - Manufacturer Certificates – see ***Appendix E***

- The use of any Service Component in the form of software shall be governed by the license agreement accompanying the software. If no EULA accompanies the Service Component, it shall be governed by the terms and conditions located at http://www.digicert.com/eula. Any additional rights and obligations with respect to the use of such Service Component shall be as set forth in this Service Description.
- Except as otherwise specified in the Service Description, the Service (including any Hosted Service Software Component provided therewith) may use open source and other third party materials that are subject to a separate license.
- DigiCert may update the Service at any time in order to maintain the effectiveness of the Service.
- The Service may be accessed and used globally, subject to applicable export compliance limitations and technical limitations in accordance with the then-current DigiCert standards.

Evaluation License

These terms and conditions apply if Customer is accessing the Service for evaluation purposes.

- ***Use Rights.*** The licenses granted to Customer are for restricted use solely for the purposes of internal, non-commercial, non-production evaluation and interoperability testing of the Service. Customer may not use the Service for any other purposes.
- ***Evaluation Period.*** The licenses granted to Customer are time limited, and continue through the trial end date as specified upon Customer's enrollment for evaluation license (the "Evaluation Period"). Unless Customer purchases a commercial license for the Service, the licenses granted to Customer are terminated upon expiration of the Evaluation Period.
- ***After Termination.*** Customer must cease using the Service upon termination. Any termination will not relieve either party of any obligations that accrued prior to the date of such termination. The terms that by their nature are intended to survive beyond the termination, cancellation, or expiration will survive.
- ***LIMITATION OF LIABILITY.*** IN NO EVENT WILL DIGICERT BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION, ANY LOST REVENUE, LOST PROFITS, OR CONSEQUENTIAL DAMAGES EVEN IF ADVISED OF THEIR POSSIBILITY.
- ***DISCLAIMERS.*** IF THE SERVICE CONTAINS TECHNOLOGY THAT DIGICERT HAS NOT PUBLICLY ANNOUNCED ITS GENERAL AVAILABILITY, THE SERVICE MAY NOT PERFORM AT THE LEVEL OF A FINAL, GENERALLY AVAILABLE PRODUCT. THE SERVICE MAY NOT OPERATE CORRECTLY, AND MAY BE SUBSTANTIALLY MODIFIED PRIOR TO FIRST COMMERCIAL RELEASE, IF ANY. THE PARTIES ACKNOWLEDGE THAT THE SERVICE OR SOFTWARE PROVIDED TO CUSTOMER

PURSUANT TO AND FOR THE PURPOSES OF EVALUATION 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. THE PARTIES FURTHER ACKNOWLEDGE THAT THE SERVICE DESCRIPTION IS SOLELY FOR THE PURPOSE OF DESCRIBING THE SERVICE AND THAT ANY REPRESENTATIONS, WARRANTIES, SERVICE LEVEL COMMITMENTS OR OTHER DIGICERT COMMITMENTS, OBLIGATIONS OR LIABILITIES ARE HEREBY DISCLAIMED BY DIGICERT. NO DIGICERT AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE ANY MODIFICATIONS, EXTENSIONS, OR ADDITIONS TO THIS WARRANTY.

- ***Order of Precedence.*** In the event of any conflict between this Section and any provision of the Agreement, this Section will prevail and supersede such other provisions with respect to the Service while provide for evaluation purposes.

Use of Microsoft Auto Enrollment

If you use the Microsoft Auto Enrollment component of the MPKI Service, then the following MICROSOFT REQUIRED SUPPLEMENTAL OBLIGATIONS will apply:

***(a) 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.

(b) 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.

(c) Server Software Requirements. Customer may use only one (1) copy (unless otherwise specified in the applicable Services Order or Statement of Work**)** 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.

(d) 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 these Service Description terms and conditions with rights to enforce any terms herein that affect any included Microsoft intellectual property or other Microsoft interest related to the terms hereof.

(e) 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.

(f) 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 to Microsoft Customer's identity and the basis for DigiCert's belief of non- compliance*.*

(g) 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.

(h) 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.

SERVICE LEVEL AGREEMENT.

The service availability commitments of DigiCert are described in the applicable Service Level Agreement available in the Repository.

DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Services Description, have the meaning given below:

"**Administrator Certificate**" means the Certificate issued by DigiCert to the Customer employee or such other Trusted Person designated as the Managed PKI Administrator for the sole purpose of accessing the PKI Manager to perform Administrator functions.

> **[For *Appendix D – LTE Certificate Service* only]** "Administrator Certificate" means the client Certificate issued by DigiCert to a Customer appointed Managed PKI Administrator or such other Trusted Person designated as the Managed PKI Administrator for the purpose of accessing the PKI Manager to manage end entity LTE Certificates or Manufacturers Certificates.

"**Affiliated Individual**" means a person that is affiliated to Customer: (1) as an officer, director, employee, partner, contractor, intern, or other person within Customer's organization; or (2) as a person maintaining a contractual relationship with Customer's organization where Customer has business records providing strong assurances of the identity of such person.

"**CA Certificate**" means a Digital Certificate issued to Certification Authority or CA.

"**Certificate**" or "**Digital Certificate**" means a digital record that includes, at a minimum, a name or identity of the issuing CA, the Subscriber, the Subscriber's Public Key, the Certificate's Operational Period, a Certificate serial number, and a digital signature of the issuing CA.

"**Certificate Applicant**" means an individual or organization that requests the issuance of a Certificate by a CA.

"**Certificate Application(s)**" means a request from a Certificate Applicant (or authorized agent) to a CA for the issuance of a Certificate.

"**Certification Authority**" or "**CA**" means a person or entity authorized to issue, suspend, or revoke Certificates.

"**Certificate Management Protocol**" or "**CMP**" means a protocol for auto-enrollment and lifecycle management of the LTE or Manufacturers certificates. Devices will interface directly with the DigiCert PKI system via CMP. The devices must be pre- authorized by a Managed PKI Administrator before the device is permitted to send CMP request to the DigiCert PKI system.

"**Certification Practices Statement**" or "**CPS**" means a document, as revised from time to time, representing a statement of the practices a CA or RA employs in issuing Certificates. The STN CPS and Adobe CPS's are published in the Repository on the applicable DigiCert website.

"**Customer**" means the entity using the service.

"**Erroneous Issuance**" means (a) issuance of a Certificate not materially in accordance with the procedures required by the applicable CPS; (b) issuance of a Certificate to a person, entity or object other than the one named as the subject of the Certificate; or (c) issuance of a Certificate without the authorization of the person, entity or object named as the subject of the Certificate.

"**End User License Agreement**" or "**EULA**" means the terms and conditions accompanying Software.

"**Key Generation**" means the DigiCert procedures for proper generation of Customer CA Public Key and Private Key via a trustworthy process and for storage of the Private Key and documentation thereof.

"**LTE Certificate**" means a message to be stored in a device, including a name, the issuing CA, or a network element in the operator network. The network element may be an Operator Base Station or a Security Gateway or other similar device. In all cases, the LTE Certificate contains the network element's Public Key, Certificate's Operational Period, a Certificate serial number, and a digital signature of the issuing CA.

"**Managed PKI Administrator**" means an employee of the Registration Authority or such other Trusted Person authorized to perform RA tasks.

> **[For *Appendix D – LTE Certificate Service* only]** "Managed PKI Administrator" means a Trusted Employee of Customer or Affiliate that has been designated to perform certain Certificate-related administrative functions described in the Service Description.

"**Manufacturer**" means a business entity that makes devices for distribution and sale.

"**Manufacturers Certificates**" means Certificates issued to devices and embedded on devices at the time of manufacture that typically have a long lifespan of 35-40 years and do not require revocation mechanism.

"**Operational Period**" means a period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with a date and time at which the Certificate expires, or is earlier revoked.

> **[For *Appendix D – LTE Certificate Service* only]** "Operational Period" means a period starting with the date and time a Certificate is issued and ending at the date and time at which the Certificate expires.

"**Operator**" means a business entity that is a subsidiary of the Customer typically from another country or region and is treated as a Sub-account of the Customer by DigiCert.

"**Private Hierarchy**" means a Certification Authority to issue Certificates in a hierarchy other than STN, and a domain consisting of a system of CAs that issue Certificates in a chain leading from Customer's Root CA through one or more CAs to Subscribers in accordance with Customer's practices. Certificates issued in a Private Hierarchy are intended to meet the needs of organizations authorizing their issuance and are not intended for interactions between organizations and/or individuals through public channels.

"**Private Key**" means a mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, decrypt messages or files encrypted (for confidentiality) with the corresponding Public Key.

"**Public Key**" means a mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding Private Key. Depending on the algorithm, Public Keys are also used to encrypt messages or files which can then be decrypted with the corresponding Private Key.

"**Registration Authority**" or "**RA**" means an entity that performs identification and authentication of Certificate Applicants for Certificates, initiates or passes along revocation requests for Certificates, or approves applications for renewal or re-keying of Certificates. A RA is not an agent of a Certificate Applicant. A RA may not delegate the authority to approve Certificate Applications other than to authorized Managed PKI Administrators of the RA.

"**Relying Party**" means a person, entity or object that acts in reliance of a Certificate and/or a digital signature. A Relying Party may, or may not, also be a Subscriber.

"Repository" means the collection of documents located at www.websecurity.symantec.com/legal/repository or https://www.digicert.com/legal-repository/ or any successor website maintained for the purpose of compliance with any applicable CPS.

"**Root CA**" means the top entity in the domain of trusted hierarchy and Root CA is identified by a "Root Certificate".

"**Seat**" means a single Subscriber that is an authorized end user of the Service, without regard to the number of Certificates actually issued to that Subscriber.

"**Service Component**" means Software, as may be required by the Service, which must be installed on each Customer computer, in order to receive the Service. Service Component includes the Software and associated documentation that may be separately provided by DigiCert as part of the Service.

"**Software**" means each DigiCert or licensor software program, in object code format, licensed to Customer by DigiCert and governed by the terms of the accompanying EULA, or this Service Description, as applicable, including without limitation new releases or updates as provided hereunder.

"**Subscriber**" means a person, entity or object that is the subject of, and has been issued, a Certificate, and is capable of using, and is authorized to use, the Private Key that corresponds to the Public Key listed in the Certificate at issue.

"**Subscriber Agreement**" is the agreement executed between a Subscriber and the CA or DigiCert relating to the provision of designated Certificate-related services governing the Subscriber's rights and obligations relating to the Certificate. The Subscriber Agreement is published in the Repository on the DigiCert website.

"**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a DigiCert certificate or a similar document issued by DigiCert, or a written agreement between Customer and DigiCert, that accompanies, precedes or follows the Service.

"**DigiCert Trust Network**" or "**DTN**" means the Certificate-based Public Key Infrastructure formerly known as the Symantec Trust Network (STN) governed by the DigiCert for CPS for Symantec Trust Network (STN) (the "STN CPS"), which enables the worldwide deployment and use of Certificates by DigiCert and its affiliates, and their respective customers, Subscribers, and Relying Parties.

"**Trusted Person**" means an employee, contractor, or consultant of Customer who is responsible for managing infrastructural trustworthiness of Customer, its products, its services, its facilities, and/or its practices.

APPENDICES.

Appendix A: DigiCert Trust Network (DTN) (formerly known as Symantec Trust Network (STN))

DigiCert PKI Platform service provides customers with the ability to issue certificates from the DigiCert Trust Network (DTN). DigiCert has worked with hardware and software vendors to embed the DTN Primary Certificate Authorities (PCAs) into the most popular web browsers, email applications, operating systems, and network appliances. As a result, certificates chaining to one of these PCAs are automatically trusted by these applications. These certificates can generally be used across organizations without any special preparation by either administrators or users. For example, many customers use *DTN* certificates for secure email which digitally signs and/or encrypts email.

Customer electing DTN as a Certificate Authority (CA) is automatically provisioned an issuing CA chaining to Class 2 PCA as part of the account setup. If a customer wants another trademarked name or change any of the default values in the CA, the customer may purchase an option to create additional CAs.

Note: Customers and user must adhere to the *DigiCert Certification Practice Statement (CPS) for Symantec Trust Network (STN)* or its successor CPS to issue, manage, and use these certificates.

ADDITIONAL SERVICE CONDITIONS – Apply to *DigiCert Trust Network* Only

Appointment. DigiCert hereby appoints Customer as a non-DigiCert CA within the DTN pursuant to the STN CPS, and Customer accepts such appointment.

STN CPS. Except for the functions outsourced to DigiCert under this Service Description, Customer must meet all requirements and perform all obligations imposed upon a CA and/or RA within the DTN including but not limited to the STN CPS, as periodically amended. DigiCert will notify the Customer-appointed Managed PKI Administrator of any amendments by posting the information to the PKI Manager.

***Appointment*.** Customer must appoint one or more authorized Customer employees or Trusted Persons as Managed PKI Administrator(s). Such Managed PKI Administrator(s) must be entitled to appoint additional Managed PKI Administrators on Customer's behalf. Customer must cause Managed PKI Administrators receiving Certificates hereunder to abide by the terms of the applicable Subscriber Agreement.

Administrator Functions. Customer must comply with the requirements stated in the STN CPS as periodically amended, including without limitation, requirements for validating the information in Certificate Applications, approving or rejecting such Certificate Applications, and revoking Certificates, using hardware and software designated by DigiCert. Customer must perform such tasks in a competent, professional, and workmanlike manner. Customer must approve a Certificate Application only if the Certificate Applicant is an Affiliated Individual as to Customer. If a Subscriber, who had been issued a Certificate by Customer, ceases to be affiliated with Customer as an Affiliated Individual, then Customer must promptly request revocation of such Subscriber's Certificate through the PKI Manager. If a Managed PKI Administrator ceases to have the authority to act as Managed PKI Administrator on behalf of Customer, then Customer must promptly request revocation of the Administrator Certificate of such Managed PKI Administrator.

Customer's Subscribers. Customer must cause Subscribers receiving Certificates hereunder to abide by the terms of the appropriate Subscriber Agreement, to which they must assent as a condition of enrolling for their Certificates.

Customer will ensure that the terms of such Subscriber Agreement must be no less protective of CAs than those in the STN CPS.

DigiCert's Warranties. DigiCert warrants that: (i) there are no errors introduced by DigiCert in the Certificate information as a result of DigiCert's failure to use reasonable care in creating the Certificate; (ii) its issuance of the Certificate(s) complies in all material respects with the STN CPS; and (iii) its revocation services and use of a repository conform to the STN CPS in all material aspects.

Appendix B: Private Certificate Authority

DigiCert PKI Platform service provides customers with the ability to issue certificates from a private Certificate Authority (CA). DigiCert performs a formal, secure procedure to create private/public key pair for this CA called a key ceremony. These certificates are generally used to control access to organizational resources. For example, many customers only trust their private CA for access to their private network (over VPN or WiFi) to prevent unauthorized access to their networks.

Every customer is automatically provisioned a private Certificate Authority (CA) as part of the account setup. This CA is based on the vetted customer's legal entity name provided to DigiCert for setting up the account. If a customer wants to use another name trademarked to that organization (*e.g.*, a brand name versus a legal entity name) or change any of the default values in the CA, the customer may purchase an option to create additional CAs.

Note: Customers are responsible for defining and following their own Certification Practice Statement (CPS) that governs the issuing, managing, and use of certificates from the applicable private CA.

ADDITIONAL SERVICE CONDITIONS – Apply to *Private Certificate Authority* Only

Appointment. Customer must appoint one or more authorized Customer employees or Trusted Persons as Managed PKI Administrator(s). Such Managed PKI Administrator(s) must be entitled to appoint additional Managed PKI Administrators on Customer's behalf. Customer must cause Managed PKI Administrators receiving Certificates hereunder to abide by the terms of the applicable Subscriber Agreement.

Administrator Functions. Customer must, through its Managed PKI Administrator(s) using hardware and software designated by DigiCert, validate the information in Certificate Applications, approve or reject such Certificate Applications, and instruct DigiCert to issue, renew and revoke Certificates. If a Managed PKI Administrator ceases to have the authority to act as a Managed PKI Administrator on behalf of Customer, Customer must promptly request revocation of the Administrator Certificate of such Managed PKI Administrator.

DigiCert's Warranty. DigiCert warrants that there are no errors introduced by DigiCert in the Certificate information as a result of DigiCert's failure to use reasonable care in creating the Certificate.

Appendix C: Adobe® Document Signing Services

DigiCert PKI Platform service provides customers with the ability to issue certificates from *Adobe® Document Signing Services.* DigiCert has worked with Adobe to have ability to issue certificates automatically trusted by Adobe *Acrobat®, Reader®, and LiveCycle®* products. These certificates are used to digitally sign portable document files (PDF) in these products.

Customer electing Adobe as a Certificate Authority (CA) is automatically provisioned an issuing CA chaining to DigiCert's intermediate CA for Adobe Document Signing Services as part of the account setup. This CA is based on the vetted customer's legal entity name provided to DigiCert for setting up the account. If a customer wants to use another name trademarked to that organization (*e.g.,* a brand name versus a legal Entity name) or change any of the default values in the CA, the customer may purchase an option to create additional CAs.

Note: Customers and user must adhere to the *Adobe CDS Certification Practice Statement (CPS),* or *Adobe ATL CPS,* as applicable, to issue, manage, and use these certificates.

For AATL, Customers can choose between SHA256 and ECC.

ADDITIONAL SERVICE CONDITIONS – Apply to *Adobe® Document Signing Services Only*

Appointment. Customer must appoint one or more authorized Customer employees or Trusted persons as Managed PKI Administrator(s). Such Managed PKI Administrator(s) must be entitled to appoint additional Managed PKI Administrators on customer's behalf. Customer must cause Managed PKI Administrators receiving Certificates hereunder to abide by the terms of the applicable Subscriber Agreement and the CPS.

Administrator Functions. Customer must, through its Managed PKI Administrator(s) using hardware and software designated by DigiCert, validate the information in Certificate Applications, approve or reject such Certificate Applications, and instruct DigiCert to issue, renew and revoke Certificates in accordance with the CPS, published at the PKI Manager and amended from time to time. If a Managed PKI Administrator ceases to have the authority to act as a Managed PKI Administrator on behalf of Customer, Customer must promptly request revocation of the Administrator Certificate of such Managed PKI Administrator.

Customer's Subscribers. Customer must cause Subscribers receiving Certificates hereunder to abide by the terms of the appropriate Subscriber Agreement, to which they must assent as a condition of enrolling for their Certificates. Customer will ensure that the terms of such Subscriber Agreement must be no less protective of CAs than those in the CPS.

DigiCert's Warranty. DigiCert warrants that there are no errors introduced by DigiCert in the Certificate information as a result of DigiCert's failure to use reasonable care in creating the Certificate.

Appendix D: LTE Certificate Service

DigiCert™ LTE Service ("LTES" or "Service") provides customer with an ability to obtain device Certificates in a private hierarchy for integration into operator LTE equipment. Customer or their Operators submits request to DigiCert for LTES through a programmatic interface such as the Certificate Management Protocol (CMP).

ADDITIONAL SERVICE CONDITIONS – Apply to *LTE Certificate Service* Only

Appointment. Customer must appoint one or more authorized Customer and/or Operator employees as Managed PKI Administrators for the entities employing such personnel. Customer must require Managed PKI Administrators receiving Administrator Certificates hereunder to abide by the terms of the applicable Subscriber Agreement associated with such Certificates, and to use Managed PKI Administrator Certificates exclusively for authorized and legal purposes consistent with this Service Description. Customer must immediately request revocation of the applicable Administrator Certificate if the subscriber ceases to be an authorized Managed PKI Administrator.

Administrator Functions. Customer and/or its Operators, as applicable, through the appointed Managed PKI Administrators, must be responsible for:

i. creation of operator sub-account;
ii. creation of certificate profiles;
iii. provide Manufacturer CA Certificates;
iv. provide IP address blocks for validation;
v. register new devices and set up a pre-approval for a future request; and
vi. configure CMP responder URL to on network elements.

Account Authorization and Certificate Issuance. Customer must provide DigiCert advance written authorization of any Operator authorized to receive LTE Certificate issued hereunder, including such Operator's contact information, identification of the individual(s) designated to be Managed PKI Administrator(s) for such Operator (including enrollment information therefore), and the number of LTE Certificates and sites for which each Operator has been authorized. Customer must ensure, and require its Operator(s) to ensure, that each Managed PKI Administrator has been (since the time of the applicable Managed PKI Administrator Certificate's creation) and will remain the only person possessing such Certificate's Private Key, any PIN, software, or hardware mechanism protecting the Private Key, and no unauthorized person has had or will have access to aforementioned material or information.

Upon a Managed PKI Administrator's submission through PKI Manager of a Certificate request for which the requested number of Certificates have been authorized by Customer as stated above, DigiCert is entitled to (i) rely upon the accuracy of the information in each such Certificate request, and (ii) issue and provide such Certificates to the requesting Managed PKI Administrator. Device Certificates issued or licensed under this Service Description will have a validity period of one (1), two (2) or three (3) years from the date the Certificate is issued. DigiCert will fulfill all orders meeting the forgoing requirements in the order received. Notwithstanding any inconsistent provision hereof, the number of Operators that may request Certificates, and the number production sites and Managed PKI Administrators through which Certificates may be requested, will be strictly limited to the number specified in the applicable order document(s).

Manufacturer Flow-Down Obligation. 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.

CA Certificates. Notwithstanding anything to the contrary in this Service Description, DigiCert will create and host, in accordance with DigiCert's standard PKI practices and policies, two (2) Customer Root Certificates and optionally up to two (2) CA Certificates issued under each Root Certificate, which CA Certificates will be used solely for the purpose of providing the Service to Customer hereunder. Additional CA Certificates may be purchased separately. DigiCert will onboard Operators and create sub-accounts for them based on requests from Customer with accordance with standard PKI practices and policies.

IP address configuration. As part of the on-boarding process of a new Operator, a range of valid IP addresses must be provided to DigiCert. DigiCert's System will only respond to CMP requests coming from the valid IP addresses and all other requests not originated from the configured IP addresses will be rejected. This configuration must be performed by the Operator.

Account Activation. Subject to advance purchase, DigiCert will use commercially reasonably efforts to activate sub-accounts based within the United States within ten (10) business days and accounts outside of the United States within a commercially reasonable period upon the following requirements being satisfied: (i) completion of the necessary enrollment process; and (ii) authentication of the Operator and its Managed PKI Administrator(s). These Managed PKI Administrator(s) must be accessible during this period in order for DigiCert to perform authentication in a timely manner.

DigiCert's Warranty. DigiCert warrants that there are no errors introduced by DigiCert in the Certificates issued hereunder as a result of DigiCert's failure to use reasonable care in creating the Certificates.

Appendix E: Manufacturer Certificates

DigiCert PKI Platform service provides customers with the ability to issue Manufacturer certificates in a private hierarchy for integration into Manufacturer's ecosystem-specific devices. Manufacturer certificates are used for device authentication or to encrypt messages sent from the device. Customers use batch interface to request Manufacturer Certificates from DigiCert PKI Platform service.

ADDITIONAL SERVICE CONDITIONS – Apply to *Manufacturer Certificates* Only

Appointment. Customer must appoint one or more authorized Customer employees as Managed PKI Administrators for the entities employing such personnel. Customer must require Managed PKI Administrators receiving Administrator Certificates hereunder to abide by the terms of the applicable Subscriber Agreement associated with such Certificates, and to use Administrator Certificates exclusively for authorized and legal purposes consistent with this Service Description. Customer must immediately request revocation of the applicable Administrator Certificate if the subscriber ceases to be an authorized Service Administrator.

Administrator Functions. Customer and/or its Operators, as applicable, through the appointed Managed PKI Administrators, must be responsible for:

i. creation of sub-accounts;
ii. creation of certificate profiles;
iii. provide Manufacturer CA Certificates; and
iv. submission of batch requests for certificate issuance.

Manufacturer Flow-Down Obligation. 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.

Certificate Issuance. Upon a Service Administrator's submission through PKI Manager of a batch Certificate request, DigiCert is entitled to (i) rely upon the accuracy of the information in each such Certificate request, and (ii) issue and provide such Certificates to the requesting Managed PKI Administrator. DigiCert will fulfill all orders meeting the forgoing requirements in the order received. Notwithstanding any inconsistent provision hereof, the number of Certificates that could be requested, will be strictly limited to the number specified in the applicable order document(s).

Account Activation. Subject to advance purchase, DigiCert will use commercially reasonably efforts to activate accounts based within the United States within ten (10) business days and accounts outside of the United States within a commercially reasonable period upon the following requirements being satisfied: (i) completion of the necessary enrollment process; and (ii) authentication of the Customer and its Managed PKI Administrator(s). These Managed PKI Administrator(s) must be accessible during this period in order for DigiCert to perform authentication in a timely manner.

DigiCert's Warranty. DigiCert warrants that there are no errors introduced by DigiCert in the Certificates issued hereunder as a result of DigiCert's failure to use reasonable care in creating the Certificates.

Private Root CA's Required Terms. Because Manufacturer Certificates operate in a Root CA's Private Hierarchy, DigiCert's provision of Manufacturer Certificates may be conditioned upon Customer's satisfying all the conditions imposed by Root CA as prerequisites to receiving Manufacturer Certificates issued under Root Certificate hosted by DigiCert if Root CA is a third party other than Customer, such as an industry consortium or standard setting body, and such Manufacturer Certificates are intended for use only within the ecosystem managed by such Root CA. Such prerequisites may include without limitation execution of any additional documentation designated by Root CA. **Root CA has absolute authority over issuance of Manufacturer Certificates for their ecosystem, and reserves the right to direct DigiCert not to issue Certificates to Customer. DigiCert disclaims any and all liability in connection with actions taken by Root CA. Root CA retains all proprietary and intellectual property rights that it owns in each Manufacturer Certificates of an ecosystem. Such rights owned by Root CA are licensed to Customer pursuant to documentation designated by Root CA. Customer acknowledges and agrees that, upon Root CA's request, DigiCert may be required to report Customer's identity and all sales of the Certificates.**

END OF SERVICE DESCRIPTION

Version March 2019