DigiCert PKI Platform for CertiPath Service Description
(formerly known as Symantec Managed PKI Service for CertiPath)

Introduction

DigiCert PKI Platform for CertiPath (formerly known as Symantec Managed PKI Service for CertiPath) provides a flexible PKI platform to manage complete lifecycle of certificates which includes the ability to issue, renew, and revoke certificates; escrow and recover private keys; and validate the status of certificates. As a managed service, *DigiCert PKI Platform for CertiPath* significantly reduces the costs associated with an in-house PKI such as acquiring hardware systems, purchasing PKI software licenses, and training staff. Additionally, *DigiCert PKI Platform for CertiPath* reduces the risks in the customer's cross-certification process by leveraging DigiCert's secure, high-available infrastructure which has passed the extensive audit requirements of CertiPath root Certificate Authority (CA).[1]

This service description outlines the primary elements of *DigiCert PKI Platform for CertiPath.* Certain optional components may be described more fully in their respective service descriptions and subject to additional terms.

Capabilities

DigiCert PKI Platform for CertiPath provides the following key capabilities:

- **Digital ID Center**

End users (a.k.a., subscribers) enroll for certificates via Digital ID Center web pages. DigiCert provides two methods – remote hosting and local hosting – to deploy Digital ID center web pages. In remote hosting, DigiCert hosts these web pages within DigiCert's data centers. However, there are only limited customizations allowed to these pages. In local hosting, a Managed PKI (MPKI) sit kit is installed in the customer's data center to host these web pages. The customer can then customize text, logo, and links on these web pages based on the customer's branding guidelines.

- **Control Center**

PKI administrators perform certificate management lifecycle processes (e.g., approval, renewal, revocation, etc.) through Control Center which is hosted within DigiCert's data centers. These administrators ensure certificates are issued to properly authenticated end users in accordance to customer's business practices. Additionally, these administrators are able to monitor account usage, download Certificate Revocation Lists (CRLs), and generate reports. DigiCert allows an unlimited number of PKI administrators to manage an account which enables the customer to set up separation of duties between PKI administrators (*e.g.,* approval certificates versus revocation of certificates).

- **Issuing Center**

Certificates are created and signed through the Issuing Center which is hosted within DigiCert's data centers. Once end users enroll for certificates via the Digital ID Center web pages and PKI administrator approves the certificate requests in Control Center, the Issuing Center creates the certificates and signs these certificates with the customers' Certificate Authority (CA). Issuing Center then sends an email to end users in order to retrieve the certificates.

- **Authentication Methods**

  DigiCert offers three methods for PKI administrators to authenticate end users:

  - **Manual Authentication**

    In manual authentication, the PKI administrators personally review and decide whether to approve or reject certificate requests from end users in Control Center. Due to the time

[1] DigiCert PKI Platform for CertiPath is intended to prepare a company for certification by CertiPath, but does not automatically lead to certification.

required for this effort, this method may not be suitable for customer's that issue high volumes of certificates.

- **Passcode Authentication**
  In passcode authentication, the PKI administrators give unique passcodes to end users to automatically approve certificate requests. The PKI administrators must create and upload a series of passcodes (*e.g.,*100001, 100002, etc.) in Control Center and set up approval guidelines. Next, the PKI administrators give a different passcode to each end user. During certificate enrollment, the end users enter this passcode in the Digital ID center web pages. Issuing Center then compares this passcode to information loaded in Control Center. Lastly, Issuing Center approves or rejects certificate requests based on the approval guidelines.

- **Automated Administration**
  In automated administration, certificate requests are automatically processed by Issuing Center without involvement from PKI administrators. This method requires installing a MPKI site kit that includes Registration Authority (RA) and Automated Administration (AA) servers within the customer's data center. The AA server is also integrated with a data source (*e.g.* Windows AD, LDAP, etc.) to authenticate users. When the end users enroll for certificates via the Digital ID Center web pages, the AA servers compares the data on the certificate requests with the data source. If the data matches, the AA server approves certificate requests. The RA server then signs and sends approved certificate request to Issuing Center. If the data does not match, the AA server rejects certificate requests.

Standard Options

- **Key Management Service**
  PKI administrators can centralize generation of public/private key pairs, back-up private keys, and distribute key recovery through Key Management Service (KMS). KMS ensures maximum security and protection of private keys. Additionally, KMS support dual-key pair which allows for separate issuance and back-up of encryption and signature key pairs. (This Service Description does not provide details of the DigiCert Managed PKI Key Management Service, which is described in a separate service description.)

- **Premium Certificate Revocation List (CRL)**
  Customers can validate current status of certificates (*e.g.,* active, revoked, etc.) via the Premium Certificate Revocation List (CRL). A CRL is a black list of all *revoked* certificates. Customers can configure applications (*e.g.* Microsoft Outlook) to check the CRL. If the certificate appears on the CRL, the application can take the appropriate action such as deny access or refuse to use certificate for encryption or digitally signing. As part of standard service, DigiCert produces a CRL every 24 hours. With Premium CRL, DigiCert generates a CRL every hour.

- **Online Certificate Status Protocol (OCSP)**
  Customers can also validate current status of certificates (*e.g.,* active, revoked, etc.) via the On-line Certificate Status Protocol (OCSP) service. While all *revoked* certificates will appear on a CRL, there is a time delay between the certificate's revocation and the next CRL run which can be up to 1 hour for Premium CRL and 24 hours for standard CRL. Customers may have policies that require the applications to check certificate's status in real-time to take appropriate action. DigiCert immediately updates the certificate's status to OCSP service upon any status changing action (*e.g.* revocation, suspension, etc.). Customers can configure applications to send OCSP requests and receive OCSP responses to check the certificate's status in real-time.

Additional Options

DigiCert PKI Platform for CertiPath also provides the following additional options:

- **MyID Personal Identity Verification (PIV)**
  MyID PIV is a comprehensive identity and card management system designed to deploy smart cards and support a wide variety of smart card types and workflows. This system enables customers to manage complete lifecycle of smart cards. Additionally, this system includes role-based management interface to enroll end users; manage cryptographic keys' issue certificates; and graphically personalize smart cards. Furthermore, this system supports numerous Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS).

- **Professional Services**
  DigiCert offers a wide range of professional services to help customers install MPKI site kit in the customer's data centers; integrate applications with MPKI site kit; and train customer's PKI administrators. Customers can leverage DigiCert's extensive experience with Certificate Policy (CP) and Certification Practice Statements (CPS) to help draft the CPS required by CertiPath.

DIGICERT PKI PLATFORM FOR CERTIPATH SERVICE TERMS AND CONDITIONS

1. DEFINITIONS

"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 Managed PKI Control Center to perform Administrator functions.

"**Agreement**" means the Master Services Agreement or such other agreement entered into between DigiCert and Customer under which the Service Order applicable to this service description is issued.

"Certificate" or **"Digital Certificate"** means a message that, at least, states a name or identifies the issuing CA, identifies the Subscriber, contains the Subscriber's Public Key, identifies the Certificate's Operational Period, contains a Certificate serial number, and contains a digital signature of the issuing CA.

"Certificate Applicant" means a person or authorized agent 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.

"Certificate Signing Unit" or **"CSU"** means a hardware unit or software designed for use in signing Certificates and key storage.

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

"Erroneous Issuance" means: (a) issuance of a Certificate to a person other than the one named as the subject of the Certificate; or (b) issuance of a Certificate without the authorization of the person named as the subject of the Certificate.

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

"Private Hierarchy" means a domain consisting of a system of CAs that issue Certificates in a chain leading from Customer's root CA through one or more Certification Authorities 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. upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding Public Key.

"Private Key" means a mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to 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"** is an entity approved by a CA to assist persons in applying for Certificates and/or revoking (or where authorized, suspending) Certificates, and approving such applications, in connection with the services. An RA is not the agent of a Certificate Applicant. An RA may not delegate the authority to approve Certificate Applications other than to authorized RAAs of the RA.

"Registration Authority Administrator" or **"RAA"** is an employee or such other Trusted Person of an RA that is responsible for carrying out the functions of an RA.

"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.

"Subscriber" means a person or entity 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 and
governing the Subscriber's rights and obligations relating to the Certificate.

"**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.

When the service is sold with Premium Validation, the following additional definitions apply:

"Certificate Revocation List" or **"CRL"** is a periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked certificates' serial numbers, and the specific times and reasons for revocation.

"Online Certificate Status Protocol" or **"OCSP"** is a protocol for providing relying parties with real-time certificate status information, and may be accessed (by Customers who have purchased OCSP support) by querying the appropriate DigiCert™ OCSP Responder at a URL specified by DigiCert.

"Premium CRL(s)" means CRLs which DigiCert updates more frequently than standard CRLs and makes available to Customers who have purchased Premium CRL access at a URL specified by DigiCert.

"Premium Validation" means, collectively, the services by which Premium CRLs, XKMS Validation, and OCSP information are made available to Customers.

2. CUSTOMER'S OBLIGATIONS

(a) Appointment. Customer shall appoint one or more authorized Customer employees or Trusted Persons as RAA(s). Such RAA shall be entitled to appoint additional RAAs on Customer's behalf. Customer shall cause RAAs receiving Certificates hereunder to abide by the terms of the applicable Subscriber Agreement.

(b) Administrator Functions. Customer shall, through its RAA(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 RAA ceases to have the authority to act as a RAA on behalf of Customer, Customer shall promptly request revocation of the RAA Certificate of such RAA.

(c) Survival. In addition to the termination provisions set forth in the Agreement, the revocation and security requirements in these Service Terms and Conditions shall survive termination of this Agreement or the applicable Services Order until the end of the Operational Period of all Certificates issued hereunder.

(d) Customer's Warranties. In addition to the express limited warranties set forth in the Agreement, Customer warrants that: (i) 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; (ii) Customer's approval of Certificate Applications will not result in Erroneous Issuance; (iii) Customer has substantially complied with the RA requirements; (iv) no Certificate information provided to DigiCert infringes the intellectual property rights of any third parties; (v) information in the Certificate Application(s) (including email address(es)) has not been and will not be used for any unlawful purpose; (vi) Customer's RAA has been (since the time of the RAA Certificate's creation) and will remain the only person possessing the RAA Certificate Private Key, or any challenge phrase, PIN, software, or hardware mechanism protecting the Private Key, and no unauthorized person has had or will have access to such materials or information; (vii) Customer will use the RAA Certificate exclusively for authorized and legal purposes consistent with this Agreement; (viii) 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.

(e) 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.

3. DIGICERT'S OBLIGATIONS

(a) Services. Following completion of the requisite installation, DigiCert shall provide Customer with the services indicated in this service description throughout the term of the service. DigiCert shall issue, manage, revoke, and/or renew Certificates in accordance with the instructions provided by Customer and its RAAs. DigiCert shall also register Public Keys, provide Public Keys to relying parties, and revoke the

registration of Public Keys under XKMS in response to properly- structured XKMS requests submitted by Customer. Upon Customer's approval of a Certificate Application, DigiCert: (i) shall be entitled to rely upon the correctness of the information in each such approved Certificate Application; and (ii) shall issue a Certificate for the Certificate Applicant for which such Certificate Application was submitted. Certificates issued or licensed under this Agreement, including RAA Certificates, will have a maximum Operational Period of twelve (12) months from the date each Certificate is issued.

(b) RAA Certificate. Upon DigiCert's completion of authentication procedures required for the RAA Certificate, DigiCert will process Customer's RAA Certificate Application(s). DigiCert will notify Customer whether Customer's RAA Certificate Application is approved or rejected. RAA's use of the PIN from DigiCert to pick up the RAA Certificate or otherwise installing or using the RAA Certificate shall constitute RAA's acceptance of the RAA Certificate. After the RAA picks up or otherwise installs the RAA Certificate, the RAA 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 RAA Certificate and issue a corrected RAA Certificate.

(c) CA Key Generation. During a single CA Key Generation event, DigiCert shall generate for Customer pairs of CA keys for use in signing Certificates issued by DigiCert on behalf of Customer for use in Customer's Private Hierarchy. Customer's Private Key of each pair shall be stored in one or more Certificate Signing Units.

(d) 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.

4. ADDITIONAL TERMS

Each service account includes at least one CA Certificate. Additional CA Certificates for a given volume may be purchased later. Automated administration hardware components become the property of Customer, but upon termination of the service any DigiCert Certificates stored in the hardware will be revoked. Each Administrator Kit consists of a token, software and one (1) Administrator Certificate. Any extraction of CA Certificates and/or corresponding key pairs from the DigiCert systems and services will be subject to agreement of the parties.