DIGICERT PKI PLATFORM FOR SHARED SERVICE PROVIDER (FEDERAL) SERVICE DESCRIPTION
(formerly known as Symantec Federal Shared Service Provider PKI)

I. DEFINITIONS

For the purpose of this Service Description, capitalized terms have the meaning defined herein. All other capitalized terms are as defined in the Agreement or the DigiCert CPS for DigiCert PKI Platform for Shared Service Provider (Federal) (which may be called the Symantec Shared Service Provider CPS until it is updated).

"Administrator Certificate" means the Certificate issued by DigiCert to the Trusted Person designated by Customer as the Managed PKI Administrator for the sole purpose of accessing the *Managed PKI Control Center* to perform administrator functions.

"Agreement" means the applicable agreement, which is entered into between DigiCert and Customer and incorporates this Service Description by reference.

"Card Management System" or **"CMS"** means the component implemented by the Customer organization that is used for managing smart card token content and enforcing the PIV policies for PIV Certificates issued.

"Certificate" or **"Digital Certificate"** means a digital representation of information that, at a minimum, 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.

"Certification Practices Statement" or **"CPS"** means a document, as revised from time to time, representing a statement of the practices that a CA and RA employs in issuing Certificates. The DigiCert CPS is published on DigiCert's website. The DigiCert CPS for DigiCert PKI Platform for Shared Service Provider (Federal) (which may be called the Symantec Shared Service Provider CPS until it is updated) attests compliance with the *Certificate Policy for the Federal PKI Common Policy Framework*.

"Erroneous Issuance" means: (a) issuance of a Certificate in a manner not materially in accordance with the procedures required by the DigiCert CPS; (b) issuance of a Certificate to a person other than the one named as the subject of the Certificate; or (c) 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 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, 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 *DigiCert PKI Platform for Shared Service Provider (Federal)*. 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.

"Registration Authority Practices Statement" or **"RPS"** is a subset of the CPS document that includes practices that apply solely to the RA component function (including CMSes). The DigiCert RPS attests compliance with the *Certificate Policy for the Federal PKI Common Policy Framework*.

"Relying Party" is a person who, in the course of secure electronic transmissions with a Subscriber, has received a certificate and a digital signature that is verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

"Relying Party Agreement" or **"RPA"** is a statement of the obligations of the Relying Party, in the course of secure electronic transmissions with a Subscriber, for verifying the validity of a certificate and/or a digital signature and for their decision on whether to rely on the certificate.

"Repository" means the collection of documents located at the link for the repository, which may be accessed from the DigiCert webpage: https://www.websecurity.symantec.com/legal/repository or its successor webpage.

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

"Subscriber" means a person who 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 issuing CA relating to the provision of designated Certificate-related services and governing the Subscriber's rights and obligations relating to the Certificate.

"Trusted Person" is an individual who has gone through strict vetting for trustworthiness and is assigned to a role that oversees, has access to, or operates the trustworthy infrastructures of the CA and RA components and as such may materially affect the issuance or revocation of Certificates.

When the Federal Shared Service Provider (SSP) PKI Certificate 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.

II. SERVICE FEATURES

1. *Services.* Following completion of the requisite installation, DigiCert will provide Customer with the services indicated in this Service Description throughout the term of the service. DigiCert will issue, manage, revoke, and/or renew Certificates in accordance with the instructions provided by Customer and its RAAs. DigiCert will also register Public Keys, provide Public Keys to relying parties, and revoke the registration of Public Keys in response to properly-structured requests submitted by Customer.

Upon Customer's approval of a Certificate Application, DigiCert:
(i) is entitled to rely upon the correctness of the information in each such approved Certificate Application; and (ii) will issue a Certificate for the Certificate Applicant for which such Certificate Application was submitted.

2. *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 constitutes 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.

3. *CA Key Generation.* 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 for use in Customer's Private Hierarchy. Customer's Private Key of each pair will be stored in one or more Certificate Signing Units.

4. *ADDITIONAL SERVICE FEATURES.* 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 Certificates stored in the hardware will be revoked. Administrator Kits consist of a smart card, smart card reader, 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.

III. DIGICERT'S RESPONSIBILITIES

DigiCert will provide the services in a manner that:
1. there are no errors introduced by DigiCert in the Certificate as a result of DigiCert's failure to use reasonable care in creating the Certificate;
2. its issuance of the Certificate(s) complies in all material respects with the DigiCert CPS; and
3. its revocation services and use of a repository conform to the DigiCert CPS in all material respects.

IV. CUSTOMER'S RESPONSIBILITIES

1. *Appointment.* Customer must appoint one or more authorized Customer employees or Trusted Persons as RAA(s). Such RAA(s) are entitled to appoint additional RAAs on Customer's behalf. Customer must cause RAAs receiving Certificates hereunder to abide by the terms of the applicable Subscriber Agreement, which can be found in the Repository.

2. *Administrator Functions.* Customer must comply with the requirements, as appropriate for the appropriate Certificate class stated in the DigiCert 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.

If a RAA ceases to have the authority to act as a RAA on behalf of Customer, Customer must promptly request revocation of the RAA Certificate of such RAA.

3. *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 DigiCert CPS.

4. *Other Responsibilities.* Customer must ensure 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 DigiCert CPS and corresponding RPS, specific to the requirements of the RA and CMS;
(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 Service Description; and
(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.

5. *Federal PKI Policy Compliance.*

(i) In General. DigiCert has the right as CA to take any other reasonable, appropriate and necessary actions as may be required, including updates to the Service, the DigiCert CPS or this Service Description to comply with the Federal PKI Policy Authority's requirements that are now effective or are later promulgated.

(ii) Annual Audit. Without limiting the generality of the foregoing, as Customer performs the RA and CMS functions within the U.S. Federal PKI, Customer must ensure that Customer's RA and CMS functions comply with the requirements set forth in the DigiCert CPS and the *Certificate Policy for Federal PKI Common Policy Framework*, and that such compliance is evidenced by an annual audit as specified therein. Customer must provide DigiCert with such evidence of compliance of the RA and CMS functions on an annual basis. Should any discrepancy be noted in the audit, DigiCert has the right to take appropriate actions as may be required to comply with the Federal PKI Policy Authority.

6. *Audit by DigiCert.* DigiCert may conduct an audit of Customer's procedures no 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 terms of this Service Description, then (i) Customer will pay DigiCert reasonable costs of conducting the audit, and (ii) 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.

7. *Continuing Responsibilities.* In addition to the termination provisions set forth in the Agreement, the revocation and security requirements in this Service Description and the DigiCert CPS will survive termination or expiration of the service until the end of the Operational Period of all Certificates issued hereunder.