Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 S Hanley Rd, Suite 800
St. Louis, MO 63105

REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of DigiCert, Inc. ("DigiCert"):

We have examined the assertions by the management of DigiCert and VeriSign, Inc. ("Verisign"), an independent service organization that provides datacenter hosting services to DigiCert, that for its Certification Authority ("CA") operations at Mountain View, California, USA and New Castle, Delaware, USA, throughout the period November 1, 2017 to October 31, 2018, for its CAs as enumerated in Attachment B, DigiCert has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Symantec Shared Service Provider ("Symantec SSP") Certification Practice Statement ("CPS") version as enumerated in Attachment A that is consistent with the X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework ("FCPF CP") versions as set out in Attachment A (including sections 1 through 9); and
  - Memorandum of Agreement as set out in Attachment A between the Federal PKI Policy Authority and DigiCert (including all sections)

- provided its CA services in accordance with its disclosed practices, including:
  - FCPF CP versions as set out in Attachment A (including sections 1 through 9);
  - Symantec SSP CPS version as set out in Attachment A that is consistent with the FCPF CP versions as set out in Attachment A (including sections 1 through 9); and
  - Memorandum of Agreement as set out in Attachment A between the Federal PKI Policy Authority and DigiCert (including all sections)

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by DigiCert); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

based on the WebTrust Principles and Criteria for Certification Authorities v2.1.

DigiCert and Verisign's management are responsible for their respective assertions. Our responsibility is to express an opinion on management's assertions, based on our examination.

The relative effectiveness and significance of specific controls at DigiCert and Verisign and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

DigiCert makes use of external registration authorities for specific subscriber registration activities for the Symantec SSP – Customer Specific CAs as disclosed in the Symantec SSP CPS versions enumerated in Attachment B. Our examination did not extend to the controls exercised by these external registration authorities.

DigiCert does not escrow its CA keys, does not provide Integrated Circuit Card Lifestyle Management services to subscribers, and does not provide certificate renewal services. DigiCert does not provide subordinate CA certificate lifecycle management services to third parties. Accordingly, our examination did not extend to controls that would address those criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether managements' assertions are fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about managements' assertions. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of managements' assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, DigiCert's and Verisign's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, throughout the period November 1, 2017 to October 31, 2018, DigiCert and Verisign managements' assertions, as referred to above, are fairly stated, in all material respects.

Without modifying our opinion, we noted the following other matters during our procedures:

Matter Topic		Matter Description
1	Certificate Policy IDs	For 1 out 45 certificates sampled the certificate policies extension asserts an ID that is not in the Fed SSP CPS.

This report does not include any representation as to the quality of DigiCert's or Verisign's services other than its CA operations at Mountain View, California, USA and New Castle, Delaware, USA, nor the suitability of any of DigiCert's or Verisign's services for any customer's intended purpose.

BDO USA, LLP

St. Louis, Missouri
January 29, 2019

Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope

Policy Name	Version	Date
Symantec Shared Service Provider Certification Practice Statement	2.0	September 15, 2017
X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework	1.30	October 4, 2018
X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework	1.29	May 10, 2018
X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework	1.28	April 4, 2018
X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework	1.27	June 29, 2017
Memorandum of Agreement between the Federal PKI Policy Authority and Symantec		August 2, 2017

Attachment B – List of CAs In-Scope

Symantec Intermediate CAs			
Subject Name	Serial Number	Valid From Date	Valid To Date
Country = US, Organization = VeriSign, Inc., Common Name = VeriSign SSP Intermediate CA - G3	0196	12/10/2010	12/9/2020
Country = US, Organization = Symantec Corporation, Common Name = Symantec SSP Intermediate CA - G4	258e	11/12/2014	11/12/2024
Customer Specific CAs Under Symantec VeriSign SSP Intermediate CA- G3			
Subject Name	Serial Number	Valid From Date	Valid To Date
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Transportation, Common Name = U.S. Department of Transportation SSP Agency CA G3	5ffe0acfa12b6147f3275b2bbad93fff	12/10/2010	12/9/2017
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Transportation, Common Name = U.S. Department of Transportation SSP Device CA G3	179bfaecc0894387a691c8406c0ec5fd	12/10/2010	12/9/2018
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Energy, Common Name = Naval Reactors SSP Agency CA G2	27b128bb46171be1c10bb00fdec27219	12/10/2010	12/9/2017
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Energy, Common Name = Naval Reactors SSP Device CA G2	1241bf8c5b2199238f253e80a2e2ba92	12/10/2010	12/9/2018
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Agency CA G2	312c238615ef33b963936445acc9ec4e	5/12/2011	5/11/2018
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Device CA G2	0672492e01f52b8877283bd69879f81a	9/19/2011	9/18/2019
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Education, Common Name = U.S. Department of Education Device CA - G3	01e8bc81c9dcc387bb9453a65947d18a	10/20/2011	10/19/2019
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Education, Common Name = U.S. Department of Education Agency CA - G3	0a8159718adc92ac10a506acb577ceab	10/20/2011	10/19/2018
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Railroad Retirement Board, Organizational Unit = U.S. Railroad Retirement Board, Common Name = RRB Device CA	6553ac4de4277693ce6bae5b1e539160	12/8/2011	12/7/2019
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Device CA G2	79be7fc4f70304db13a113f850d469e5	9/19/2011	12/8/2020

Customer Specific CAs Under Symantec SSP Intermediate CA- G4			
Subject Name	Serial Number	Valid From Date	Valid To Date
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Device CA G3	3e81873cdd063ef174e5fb08c93fd06a	11/25/2014	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Transportation, Common Name = U.S. Department of Transportation Device CA G4	2c0218167772fb57416ad571c9e5f1ee	12/11/2014	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Transportation, Common Name = U.S. Department of Transportation Agency CA G4	61a90f3e5ff532f9fe6209d931279a82	12/11/2014	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Agency CA G3	100f05dd316ca819d9d39febc661b326	11/25/2014	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = Department of Commerce, Common Name = Bureau of the Census Agency CA	2355994850457c656b1b9a58e3fc3f98	7/30/2015	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Education, Common Name = U.S. Department of Education Agency CA - G4	224ad7d35a9d34350671f9b8be45a23a	7/21/2015	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Energy, Common Name = Naval Reactors SSP Device CA G3	6463446c4368d0f89d12bc6f335265	12/10/2015	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Energy, Common Name = Naval Reactors SSP Agency CA G3	18876cd9ffd738ab7e69350ecc9d41f8	12/10/2015	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Education, Common Name = U.S. Department of Education Device CA - G4	2f58bf30b1bb5bf1a6d4996b2e5d8809	7/21/2015	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Device CA G4	52dc1355e4a05be7ca3f40d56c583e51	2/20/2018	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Agency CA G4	2d70005a7b73dda0c795f5f43c4607b9	2/20/2018	11/11/2024

DIGICERT, INC. MANAGEMENT'S ASSERTION

DigiCert, Inc. ("DigiCert") operates the Certification Authority ("CA") services for its CAs as enumerated in Attachment B and provides the following CA services:

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate validation
- Subscriber key generation and management
- Subordinate CA certification

The management of DigiCert is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to DigiCert's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

DigiCert management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in DigiCert management's opinion, in providing its CA services at Mountain View, California, USA and New Castle, Delaware, USA, throughout the period November 1, 2017 to October 31, 2018, DigiCert has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable version of its Symantec Shared Service Provider ("Symantec SSP") Certification Practice Statement ("CPS") (including sections 1 through 9), versions of its X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework ("FCPF CP") (including sections 1 through 9), and the Memorandum of Agreement as enumerated in Attachment A

- maintained effective controls to provide reasonable assurance that:
    - DigiCert's Symantec SSP CPS is consistent with the FCPF CP (including sections 1 through 9)
    - DigiCert provides its services in accordance with its Symantec SSP CPS, the FCPF CP, and the Memorandum of Agreement

- maintained effective controls to provide reasonable assurance that:

  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by DigiCert); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

based on WebTrust Principles and Criteria for Certification Authorities v2.1, including the following:

CA Business Practices Disclosure
- Certificate Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management
- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Lifecycle Management Controls
- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

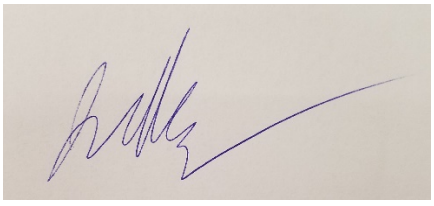
Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

DigiCert makes use of external registration authorities for specific subscriber registration activities for the Symantec SSP – Customer Specific CAs as disclosed in the Symantec SSP CPS versions enumerated in Attachment B. Our assertion did not extend to the controls exercised by these external registration authorities.

DigiCert does not perform subscriber registration activities, does not escrow its CA keys, does not provide Integrated Circuit Card Lifestyle Management services to subscribers, and does not provide certificate renewal services. DigiCert does not provide subordinate CA certificate lifecycle management services to third parties. Accordingly, our assertion does not extend to controls that would address those criteria.

DigiCert, Inc.



_____

Jeremy Rowley

Executive VP of Product

January 29, 2019

Attachment A - Certification Practice Statements and Certificate Policy Versions In-Scope

Policy Name	Version	Date
Symantec Shared Service Provider Certification Practice Statement	2.0	September 15, 2017
X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework	1.30	October 4, 2018
X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework	1.29	May 10, 2018
X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework	1.28	April 4, 2018
X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework	1.27	June 29, 2017
Memorandum of Agreement between the Federal PKI Policy Authority and Symantec		August 2, 2017

Attachment B – List of CAs In-Scope

Symantec Intermediate CAs			
Subject Name	Serial Number	Valid From Date	Valid To Date
Country = US, Organization = VeriSign, Inc., Common Name = VeriSign SSP Intermediate CA - G3	0196	12/10/2010	12/9/2020
Country = US, Organization = Symantec Corporation, Common Name = Symantec SSP Intermediate CA - G4	258e	11/12/2014	11/12/2024
Customer Specific CAs Under Symantec VeriSign SSP Intermediate CA- G3			
Subject Name	Serial Number	Valid From Date	Valid To Date
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Transportation, Common Name = U.S. Department of Transportation SSP Agency CA G3	5ffe0acfa12b6147f3275b2bbad93fff	12/10/2010	12/9/2017
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Transportation, Common Name = U.S. Department of Transportation SSP Device CA G3	179bfaecc0894387a691c8406c0ec5fd	12/10/2010	12/9/2018
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Energy, Common Name = Naval Reactors SSP Agency CA G2	27b128bb46171be1c10bb00fdec27219	12/10/2010	12/9/2017
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Energy, Common Name = Naval Reactors SSP Device CA G2	1241bf8c5b2199238f253e80a2e2ba92	12/10/2010	12/9/2018
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Agency CA G2	312c238615ef33b963936445acc9ec4e	5/12/2011	5/11/2018
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Device CA G2	0672492e01f52b8877283bd69879f81a	9/19/2011	9/18/2019
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Education, Common Name = U.S. Department of Education Device CA - G3	01e8bc81c9dcc387bb9453a65947d18a	10/20/2011	10/19/2019
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Education, Common Name = U.S. Department of Education Agency CA - G3	0a8159718adc92ac10a506acb577ceab	10/20/2011	10/19/2018
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Railroad Retirement Board, Organizational Unit = U.S. Railroad Retirement Board, Common Name = RRB Device CA	6553ac4de4277693ce6bae5b1e539160	12/8/2011	12/7/2019
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Device CA G2	79be7fc4f70304db13a113f850d469e5	9/19/2011	12/8/2020
Customer Specific CAs Under Symantec SSP Intermediate CA- G4			
Subject Name	Serial Number	Valid From Date	Valid To Date
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Device CA G3	3e81873cdd063ef174e5fb08c93fd06a	11/25/2014	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of	2c0218167772fb57416ad571c9e5f1ee	12/11/2014	11/11/2024

Transportation, Common Name = U.S. Department of Transportation Device CA G4			
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Transportation, Common Name = U.S. Department of Transportation Agency CA G4	61a90f3e5ff532f9fe6209d931279a82	12/11/2014	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Agency CA G3	100f05dd316ca819d9d39febc661b326	11/25/2014	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = Department of Commerce, Common Name = Bureau of the Census Agency CA	2355994850457c656b1b9a58e3fc3f98	7/30/2015	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Education, Common Name = U.S. Department of Education Agency CA - G4	224ad7d35a9d34350671f9b8be45a23a	7/21/2015	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Energy, Common Name = Naval Reactors SSP Device CA G3	6463446c4368d0f89d12bc6f335265	12/10/2015	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Energy, Common Name = Naval Reactors SSP Agency CA G3	18876cd9ffd738ab7e69350ecc9d41f8	12/10/2015	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Department of Education, Common Name = U.S. Department of Education Device CA - G4	2f58bf30b1bb5bf1a6d4996b2e5d8809	7/21/2015	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Device CA G4	52dc1355e4a05be7ca3f40d56c583e51	2/20/2018	11/11/2024
Country = US, Organization = U.S. Government, Organizational Unit = U.S. Nuclear Regulatory Commission, Common Name = NRC SSP Agency CA G4	2d70005a7b73dda0c795f5f43c4607b9	2/20/2018	11/11/2024

Assertion by Management of VeriSign, Inc. Regarding Its Controls Over DigiCert Certification Authority Operations Hosted in New Castle, Delaware During the Period November 1, 2017 to October 31, 2018

VeriSign, Inc. ("Verisign"), an independent service organization (sub-service provider), provides datacenter hosting services to DigiCert, Inc.("Digicert") for its Federal SSP and Non-Federal SSP Certification Authority operations ("CAs") hosted in New Castle, Delaware.

The management of Verisign is responsible for establishing and maintaining effective controls over its datacenter hosting services for the Federal SSP and Non-Federal SSP CAs hosted in New Castle, Delaware including CA environmental controls (limited to physical and environmental security), in accordance with applicable versions of the X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework, DigiCert Certificate Policy for Symantec Trust Network (STN), Symantec Shared Service Provider Certification Practice Statement, and Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to Verisign's datacenter hosting services for the Federal SSP and Non-Federal SSP CAs hosted in New Castle, Delaware. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its datacenter hosting services for the Federal SSP and Non-Federal SSP CA operations. Based on that assessment, in Verisign management's opinion, in providing its datacenter hosting services in New Castle, Delaware during the period November 1, 2017 to October 31, 2018, Verisign has maintained effective controls to provide reasonable assurance that physical access to CA systems is restricted to authorized individuals based on the WebTrust Principles and Criteria for Certification Authorities v2.1, including the following:

CA Environmental Controls
- Physical and Environmental Security

VeriSign, Inc.

Pool, Dave Digitally signed by Pool, Dave Date: 2019.01.29 07:48:59 -08'00'

Joseph David Pool
Senior Vice President, Technology Services

DATE