BDO

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”):

Scope

We have examined DigiCert management’s assertion, that for its Certification Authority (“CA”) operations at various locations in the United States of America, throughout the period November 1, 2019 to September 30, 2020, 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:
    - DigiCert Shared Service Provider (“DigiCert SSP”) Certification Practice Statement (“CPS”) versions 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 enumerated 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);
    - DigiCert 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;
    - 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 v2.2.

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

Certification Authority's Responsibilities

DigiCert's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.

Independent Accountant's Responsibilities

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 management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgement, including an assessment of the risks of material misstatement of management's 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.

Relative Effectiveness of Controls

The relative effectiveness and significance of specific controls at DigiCert 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.

Inherent Limitations

Because of the nature and inherent limitations of controls, DigiCert'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.

Independent Accountant's Opinion

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of DigiCert's services other than its CA operations at various locations in the United States of America, nor the suitability of any of DigiCert's services for any customer's intended purpose.

Other Matters

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

Matter Topic		Matter Description
1	Certificate Content	For seven (7) out of 45 certificates selected for testing, the Extended Key Usage extension was not present. For nine (9) out of 45 certificates selected for testing, the Extended Key Usage extension has the anyExtendedKeyUsage value. For six (6) out of 45 certificates selected for testing, the Key Usage extension was not marked critical.
2	Certificate Validity Period	For seven (7) out of 45 certificates selected for testing, the Validity Period exceeded three (3) years by one (1) day.

The World Health Organization classified the COVID-19 outbreak as a pandemic in March 2020. Based on the rapid increase in exposure globally, the gravity or length of the impact of the COVID-19 outbreak cannot be estimated at this time.

BDO USA, LLP

February 4, 2021

ATTACHMENT A – POLICY DOCUMENT VERSIONS IN-SCOPE

Policy Name	Version	Date
DigiCert Shared Service Provider Certification Practice Statement	2.2	April 30, 2020
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	1.32	April 14, 2020
X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework	1.31	February 8, 2019
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 DN	**Serial Number**	**Valid From**	**Valid To**
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

VeriSign SSP Intermediate CA - G3			
Subject DN	**Serial Number**	**Valid From**	**Valid To**
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

Symantec SSP Intermediate CA - G4			
Subject DN	**Serial Number**	**Valid From**	**Valid To**
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

Symantec SSP Intermediate CA - G4			
Subject DN	**Serial Number**	**Valid From**	**Valid To**
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:

- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate validation
- Subscriber key generation and management

The management of DigiCert is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its repository, 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 CA 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 various locations in the United States of America, throughout the period November 1, 2019 to September 30, 2020, DigiCert has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its DigiCert Shared Service Provider (“DigiCert SSP”) Certification Practice Statement (“CPS”) and the Memorandum of Agreement (“MoA”) as enumerated in Attachment A

- maintained effective controls to provide reasonable assurance that:
  - DigiCert‘s DigiCert SSP CPS is consistent with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (“FCPF CP”) (including sections 1 through 9)
  - DigiCert provides its services in accordance with its DigiCert SSP CPS, the FCPF CP, and the MoA

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles; and
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - 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 v2.2, including the following:

CA Business Practices Disclosure

- Certificate Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement (CPS) Management

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

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

DigiCert makes use of external registration authorities for all subscriber registration activities for the DigiCert SSP – Customer Specific CAs as disclosed in the DigiCert 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.

DocuSigned by:
Jeremy Rowley
CFF89E6506D0438...

2/4/2021

Jeremy Rowley
Chief Product Officer

ATTACHMENT A – POLICY DOCUMENT VERSIONS IN-SCOPE

Policy Name	Version	Date
DigiCert Shared Service Provider Certification Practice Statement	2.2	April 30, 2020
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	1.32	April 14, 2020
X.509 Certificate Policy For the U.S. Federal PKI Common Policy Framework	1.31	February 8, 2019
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 DN	**Serial Number**	**Valid From**	**Valid To**
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

VeriSign SSP Intermediate CA - G3			
Subject DN	**Serial Number**	**Valid From**	**Valid To**
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

Symantec SSP Intermediate CA - G4			
Subject DN	**Serial Number**	**Valid From**	**Valid To**
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

Symantec SSP Intermediate CA - G4			
Subject DN	**Serial Number**	**Valid From**	**Valid To**
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