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:
  - DigiCert Certificate Policy for Symantec Trust Network (STN) versions as enumerated in Attachment A that is consistent with the Symantec Non-Federal Shared Service Provider ("Symantec NFSSP") PKI Certification Practice Statement ("CPS") version 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:
  - DigiCert Certificate Policy for STN versions as enumerated in Attachment A (including sections 1 through 9)
  - Symantec NFSSP CPS version as set out in Attachment A that is consistent with the DigiCert CPS for STN 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's and Verisign's management are responsible for their respective assertions. Our responsibility is to express an opinion on managements' 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 Non-Federal SSP – Customer Specific CAs as disclosed in the Symantec Non-Federal SSP CPS version 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, does not provide certificate renewal services, and does not provide certificate suspension services. 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' assertions, 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 management's assertions, as referred to above, are fairly stated, in all material respects.

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 Non-Federal Shared Service Provider PKI Certification Practice Statement	2.0	September 15, 2017
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.9	September 11, 2018
Symantec Trust Network (STN) Certificate Policy	2.8.24	September 8, 2017
Memorandum of Agreement between the Federal PKI Policy Authority and Symantec		June 15, 2016

Attachment B – List of CAs In-Scope

Symantec Intermediate CAs			
Subject Name	Serial Number	Valid From Date	Valid To Date
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 SSP Intermediate CA - G3	45B1BEB5F3D47BFBC145F4D9179E22F2	30-Sep-14	29-Sep-24
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, CN=VeriSign Class 3 SSP Intermediate CA - G2	1933CE1133857F9988B1BBB3AE88C67F	6-Dec-10	5-Dec-20
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, CN=VeriSign Class 3 SSP Intermediate CA - G2	316CEB691DCB2E153D9BFA8A121BD52D	6-Dec-10	5-Dec-20
Symantec Class 3 SSP Intermediate CA - G3			
Subject Name	Serial Number	Valid From Date	Valid To Date
C=US, O=Eid Passport, Inc., OU=Eid Passport PIV-I LRA Network, CN=Eid Passport LRA 2 CA	74FA80B580B11F82CDE84EF3AD8E36A4	10-Mar-15	28-Sep-24
C=US, O=CSRA LLC, OU=CSRA FBCA MedHW2, CN=CSRA FBCA C4 CA	2AAA084CCE8D13DC0B3B05B34E325922	9-Feb-17	28-Sep-24
C=US, O=SureID, Inc., CN=SureID Inc. Device CA2	2BF8D00AE1B9D45A0846EDDDCA9CFF45	28-Apr-16	28-Sep-24
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC CA - 2	0F76B14F6E3C3F3D78CC7CABF1E9D1F2	31-Aug-17	19-Jun-19
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I CA G4	52C8B762E38B30212288790964B7AB2C	2-Aug-16	28-Sep-24
C=US, O=CSRA LLC, OU=CSRA FBCA Devices, CN=CSRA FBCA C4 Device CA	22058F804D89EDD93122C840987AC7AB	9-Feb-17	28-Sep-24
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I Device CA G2	50F504C03B7AAFFCB1263AD5FCC202E2	31-Aug-17	20-Jul-19
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I Device CA G4	2879814EEF5B5F6E7BA35946CA23A988	2-Aug-16	28-Sep-24
C=US, O=Eid Passport, Inc., OU=RAPIDGate PIV Interoperable LRA, CN=Eid Passport LRA CA 3	0BD336FF375ECB6E9187B1495254DEFF	9-Apr-15	28-Sep-24
C=US, O=SureID, Inc., OU=SureID PIV-I, CN=SureID Inc. CA1	6353433BC55FBF2E550AB0594D6CE5C3	19-Jan-16	28-Sep-24
C=US, O=Eid Passport, Inc., OU=RAPIDGate PIV Interoperable LRA, CN=Eid Passport LRA Content Signer CA 3	7BC54C654C3A41D738D48AC17AB603AF	9-Apr-15	28-Sep-24
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Agency CA	1384040B5940AC2B5498FBA7593944	31-Aug-17	16-May-19
C=US, O=Symantec Corporation, OU=Healthcare Applications, CN=Symantec Healthcare CA	3B43568D789703A038F80931EFF939A3	31-Aug-17	13-Jul-18

C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier CA	3C3FE36894D0802C73 CB31DD3131490B	31-Aug-17	4-Dec-20
C=US, O=Booz Allen Hamilton, OU=Certification Authorities, CN=Booz Allen Hamilton Device CA 02	29BB1BC2B62C9FBE6 A43D5CA7E1B6DA4	31-Aug-17	30-Jul-20
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Device CA	75815C5B8528355F91 9C9D813DA42BB6	31-Aug-17	16-May-20
C=US, O=CSC Government Solutions LLC, OU=CSRA FBCA Devices, CN=CSRA FBCA C3 Device CA	45AABDFFDAE1621D5 2B260DAF7EF3BD7	17-Dec-15	28-Sep-24
C=US, O=SureID, Inc., CN=SureID Inc. CA2	75C13DBED31093353C 73618EFFDABE6E	28-Apr-16	28-Sep-24
C=US, O=SureID, Inc., OU=SureID PIV-I, CN=SureID Inc. Device CA1	4FF47DFA24D3AA3633 DD4E55DE80F870	19-Jan-16	28-Sep-24
C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier Device CA	7F70E7CA4D45EA30D 19ABF0053132F6D	31-Aug-17	4-Dec-20
C=US, O=Eid Passport, Inc., OU=Eid Passport PIV-I LRA Network, CN=Eid Passport LRA Device 2 CA	404D442E9C09777120 9218AC534936C3	10-Mar-15	28-Sep-24
C=US, O=CSC Government Solutions LLC, OU=CSRA FBCA MedHW, CN=CSRA FBCA C3 CA	48B53C25944E6ED645 339ECF1079FD37	17-Dec-15	28-Sep-24
VeriSign Class 3 SSP Intermediate CA - G2			
Subject Name	Serial Number	Valid From Date	Valid To Date
C=US, O=ICF Incorporated LLC, OU=ICF International, CN=ICFI Device CA	69AEC83167D5026C50 48CF9AA542A672	18-Jan-11	17-Jan-19
C=US, O=ICF Incorporated LLC, OU=ICF International, CN=ICFI PIV Interoperable CA	7EF7F0186038DCFF48 42A2D8F3570BA3	18-Jan-11	17-Jan-18
C=US, O=EID Passport, Inc., CN=EID Passport LRA Content Signer CA 1	684E5892724DE19748 D7F07FA994579F	25-Jun-13	4-Dec-20
C=US, O=State of Colorado, OU=Office of Information Technology, OU=COFRAC, CN=State of Colorado Device CA G2	1BB63AB730B1E01317 988AFECB905347	23-Nov-11	22-Nov-19
C=US, O=HID Global, OU=Certificate Authorities, CN=HIDSigningCA2	59E715132E9E1E8FD2 DC91C4939922F6	19-Jun-12	18-Jun-19
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I CA G2	0954E4BCD441044BCB 144691027E0DB4	21-Jul-11	20-Jul-18
C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier CA	1414A035C1288EC17A D8FD3D1171E211	17-Dec-13	4-Dec-20
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I Device CA G2	74AC3284C494BBB4B4 CF2E3473BB6992	21-Jul-11	20-Jul-19
C=US, O=Booz Allen Hamilton, OU=Certification Authorities, CN=Booz Allen Hamilton Device CA 02	6E9ED777FB55AAF0D7 2BFE4A0E8ED7A8	31-Jul-12	30-Jul-20
C=US, O=ICF Incorporated LLC, OU=ICF International, CN=ICFI PIV Interoperable CA	017F58CF4020CD0DEE 0DF7B5D2C7DF47	18-Jan-11	17-Jan-18
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC CA - 2	547B28C1E722F86897 CF9ADF96940EC6	20-Jun-12	19-Jun-19

C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier Device CA	6F57414BD9853E920C7D5ED295B2C594	17-Dec-13	4-Dec-20
C=US, O=U.S. Government, OU=MCC, CN=Millennium Challenge Corporation Medium HW CA - G2	4CF5B1F83DE78A00C4FBAD4D5E761D08	3-Feb-11	2-Feb-18
C=US, O=Noblis, CN=Noblis CA - G2	476B8E3FF2C064A92171A881DF48F702	29-Jan-13	28-Jan-20
C=US, O=HID Global, OU=Certificate Authorities, CN=HIDSigningDeviceCA1	60FC8E8FA42B5761C8852EE3DD0C64CB	19-Jun-12	18-Jun-20
C=US, O=Symantec Corporation, OU=Healthcare Applications, CN=Symantec Healthcare CA	39286F9F3C17065603D5FEA95110FF42	14-Jul-11	13-Jul-18
C=US, O=State of Kansas, CN=State of Kansas Non Federal SSP CA G2	394F9A116B244FC953D9B46BA1BB53AC	18-Apr-13	17-Apr-20
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC Device CA - G2	46FD677950339931DB54B57754C390E0	15-Aug-13	14-Aug-21
C=US, O=State of Colorado, OU=Office of Information Technology, OU=COFRAC, CN=State of Colorado Medium HW CA G2	635089D2C31B80E8F490C3467F214700	23-Nov-11	22-Nov-18
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC Device CA - G2	6FE860178E583DA94FE0653083AC9632	21-Aug-13	4-Dec-20
C=US, O=Oregon Health Authority, CN=Oregon Health Authority Medium Assurance CA	5D4D7B72BC33A36DF9417223D63B3C69	13-Mar-12	12-Mar-19
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Agency CA	7C5123D5F59B9A2C88ED864873B1EE68	17-May-12	16-May-19
C=US, O=EID Passport, Inc., CN=EID Passport LRA CA 1	2654D448498E78F7C223CF61FC80928C	25-Jun-13	24-Jun-20
C=US, O=Amtrak Police Department, CN=APD MEAS Medium HW CA	455D313EDDF650629DC735F7C13ECB84	16-Jun-11	15-Jun-18
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Device CA	4D32A64D4588CF5241A9D92890AFC152	17-May-12	16-May-20
C=US, O=Symantec Corporation, OU=Organization Signing, CN=Symantec Non Federal SSP Organization Signing CA	36C13DB922580EB96727B8161095EE93	16-Oct-12	15-Oct-19
C=US, O=State of Florida, CN=State of Florida AHCA Medium Assurance CA	0F33D1CE3340916981B8AA5FBD454B79	22-May-12	21-May-19
C=US, O=Booz Allen Hamilton, OU=Certification Authorities, CN=Booz Allen Hamilton CA 02	7B15016346C0BD9532EA3B3EE366E865	31-Jul-12	30-Jul-19

DIGICERT, INC. MANAGEMENT'S ASSERTION

DigiCert, Inc. ("DigiCert") operates the Symantec 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 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.

These 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 versions of its Symantec Non-Federal Shared Service Provider ("Symantec NFSSP") PKI Certification Practice Statement ("CPS") (including sections 1 through 9), DigiCert Certification Practices Statement for Symantec Trust Network (STN) (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 NFSSP CPS is consistent with its Certificate Policy (including sections 1 through 9)
    - DigiCert provides its services in accordance with its Certificate Policy, Certification Practice Statement, and 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)
  - 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 Validation

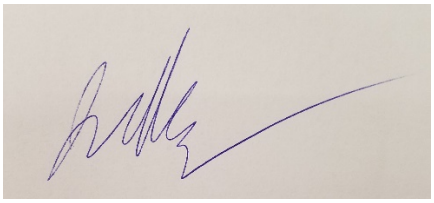
Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

DigiCert makes use of external registration authorities for specific subscriber registration activities for the Symantec Non-Federal SSP – Customer Specific CAs as disclosed in the Symantec Non-Federal SSP CPS version enumerated in Attachment B. Our assertion 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, does not provide certificate renewal services, and does not allow certificate suspension services. 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 Statement and Certificate Policy Versions In-Scope

Policy Name	Version	Date
Symantec Non-Federal Shared Service Provider PKI Certification Practice Statement	2.0	September 15, 2017
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.9	September 11, 2018
Symantec Trust Network (STN) Certificate Policy	2.8.24	September 8, 2017
Memorandum of Agreement between the Federal PKI Policy Authority and Symantec		June 15, 2016

Attachment B – List of CAs In-Scope

Symantec Intermediate CAs			
Subject Name	Serial Number	Valid From Date	Valid To Date
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 SSP Intermediate CA - G3	45B1BEB5F3D47BFBC145F4D9179E22F2	30-Sep-14	29-Sep-24
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, CN=VeriSign Class 3 SSP Intermediate CA - G2	1933CE1133857F9988B1BBB3AE88C67F	6-Dec-10	5-Dec-20
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, CN=VeriSign Class 3 SSP Intermediate CA - G2	316CEB691DCB2E153D9BFA8A121BD52D	6-Dec-10	5-Dec-20
Symantec Class 3 SSP Intermediate CA - G3			
Subject Name	Serial Number	Valid From Date	Valid To Date
C=US, O=Eid Passport, Inc., OU=Eid Passport PIV-I LRA Network, CN=Eid Passport LRA 2 CA	74FA80B580B11F82CDE84EF3AD8E36A4	10-Mar-15	28-Sep-24
C=US, O=CSRA LLC, OU=CSRA FBCA MedHW2, CN=CSRA FBCA C4 CA	2AAA084CCE8D13DC0B3B05B34E325922	9-Feb-17	28-Sep-24
C=US, O=SureID, Inc., CN=SureID Inc. Device CA2	2BF8D00AE1B9D45A0846EDDDCA9CFF45	28-Apr-16	28-Sep-24
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC CA - 2	0F76B14F6E3C3F3D78CC7CABF1E9D1F2	31-Aug-17	19-Jun-19
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I CA G4	52C8B762E38B30212288790964B7AB2C	2-Aug-16	28-Sep-24
C=US, O=CSRA LLC, OU=CSRA FBCA Devices, CN=CSRA FBCA C4 Device CA	22058F804D89EDD93122C840987AC7AB	9-Feb-17	28-Sep-24
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I Device CA G2	50F504C03B7AAFFCB1263AD5FCC202E2	31-Aug-17	20-Jul-19
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I Device CA G4	2879814EEF5B5F6E7BA35946CA23A988	2-Aug-16	28-Sep-24
C=US, O=Eid Passport, Inc., OU=RAPIDGate PIV Interoperable LRA, CN=Eid Passport LRA CA 3	0BD336FF375ECB6E9187B1495254DEFF	9-Apr-15	28-Sep-24
C=US, O=SureID, Inc., OU=SureID PIV-I, CN=SureID Inc. CA1	6353433BC55FBF2E550AB0594D6CE5C3	19-Jan-16	28-Sep-24
C=US, O=Eid Passport, Inc., OU=RAPIDGate PIV Interoperable LRA, CN=Eid Passport LRA Content Signer CA 3	7BC54C654C3A41D738D48AC17AB603AF	9-Apr-15	28-Sep-24
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Agency CA	1384040B5940AC2B5498FBA7593944	31-Aug-17	16-May-19
C=US, O=Symantec Corporation, OU=Healthcare Applications, CN=Symantec Healthcare CA	3B43568D789703A038F80931EFF939A3	31-Aug-17	13-Jul-18
C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier CA	3C3FE36894D0802C73CB31DD3131490B	31-Aug-17	4-Dec-20
C=US, O=Booz Allen Hamilton, OU=Certification Authorities, CN=Booz Allen Hamilton Device CA 02	29BB1BC2B62C9FBE6A43D5CA7E1B6DA4	31-Aug-17	30-Jul-20

C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Device CA	75815C5B8528355F919C9D813DA42BB6	31-Aug-17	16-May-20
C=US, O=CSC Government Solutions LLC, OU=CSRA FBCA Devices, CN=CSRA FBCA C3 Device CA	45AABDFFDAE1621D52B260DAF7EF3BD7	17-Dec-15	28-Sep-24
C=US, O=SureID, Inc., CN=SureID Inc. CA2	75C13DBED31093353C73618EFFDABE6E	28-Apr-16	28-Sep-24
C=US, O=SureID, Inc., OU=SureID PIV-I, CN=SureID Inc. Device CA1	4FF47DFA24D3AA3633DD4E55DE80F870	19-Jan-16	28-Sep-24
C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier Device CA	7F70E7CA4D45EA30D19ABF0053132F6D	31-Aug-17	4-Dec-20
C=US, O=Eid Passport, Inc., OU=Eid Passport PIV-I LRA Network, CN=Eid Passport LRA Device 2 CA	404D442E9C097771209218AC534936C3	10-Mar-15	28-Sep-24
C=US, O=CSC Government Solutions LLC, OU=CSRA FBCA MedHW, CN=CSRA FBCA C3 CA	48B53C25944E6ED645339ECF1079FD37	17-Dec-15	28-Sep-24
VeriSign Class 3 SSP Intermediate CA - G2			
Subject Name	Serial Number	Valid From Date	Valid To Date
C=US, O=ICF Incorporated LLC, OU=ICF International, CN=ICFI Device CA	69AEC83167D5026C5048CF9AA542A672	18-Jan-11	17-Jan-19
C=US, O=ICF Incorporated LLC, OU=ICF International, CN=ICFI PIV Interoperable CA	7EF7F0186038DCFF4842A2D8F3570BA3	18-Jan-11	17-Jan-18
C=US, O=EID Passport, Inc., CN=EID Passport LRA Content Signer CA 1	684E5892724DE19748D7F07FA994579F	25-Jun-13	4-Dec-20
C=US, O=State of Colorado, OU=Office of Information Technology, OU=COFRAC, CN=State of Colorado Device CA G2	1BB63AB730B1E01317988AFECB905347	23-Nov-11	22-Nov-19
C=US, O=HID Global, OU=Certificate Authorities, CN=HIDSigningCA2	59E715132E9E1E8FD2DC91C4939922F6	19-Jun-12	18-Jun-19
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I CA G2	0954E4BCD441044BCB144691027E0DB4	21-Jul-11	20-Jul-18
C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier CA	1414A035C1288EC17AD8FD3D1171E211	17-Dec-13	4-Dec-20
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I Device CA G2	74AC3284C494BBB4B4CF2E3473BB6992	21-Jul-11	20-Jul-19
C=US, O=Booz Allen Hamilton, OU=Certification Authorities, CN=Booz Allen Hamilton Device CA 02	6E9ED777FB55AAF0D72BFE4A0E8ED7A8	31-Jul-12	30-Jul-20
C=US, O=ICF Incorporated LLC, OU=ICF International, CN=ICFI PIV Interoperable CA	017F58CF4020CD0DEE0DF7B5D2C7DF47	18-Jan-11	17-Jan-18
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC CA - 2	547B28C1E722F86897CF9ADF96940EC6	20-Jun-12	19-Jun-19
C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier Device CA	6F57414BD9853E920C7D5ED295B2C594	17-Dec-13	4-Dec-20
C=US, O=U.S. Government, OU=MCC, CN=Millennium Challenge Corporation Medium HW CA - G2	4CF5B1F83DE78A00C4FBAD4D5E761D08	3-Feb-11	2-Feb-18
C=US, O=Noblis, CN=Noblis CA - G2	476B8E3FF2C064A92171A881DF48F702	29-Jan-13	28-Jan-20
C=US, O=HID Global, OU=Certificate Authorities, CN=HIDSigningDeviceCA1	60FC8E8FA42B5761C8852EE3DD0C64CB	19-Jun-12	18-Jun-20
C=US, O=Symantec Corporation, OU=Healthcare Applications, CN=Symantec Healthcare CA	39286F9F3C17065603D5FEA95110FF42	14-Jul-11	13-Jul-18
C=US, O=State of Kansas, CN=State of Kansas Non Federal SSP CA G2	394F9A116B244FC953D9B46BA1BB53AC	18-Apr-13	17-Apr-20

C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC Device CA - G2	46FD677950339931DB54B57754C390E0	15-Aug-13	14-Aug-21
C=US, O=State of Colorado, OU=Office of Information Technology, OU=COFRAC, CN=State of Colorado Medium HW CA G2	635089D2C31B80E8F490C3467F214700	23-Nov-11	22-Nov-18
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC Device CA - G2	6FE860178E583DA94FE0653083AC9632	21-Aug-13	4-Dec-20
C=US, O=Oregon Health Authority, CN=Oregon Health Authority Medium Assurance CA	5D4D7B72BC33A36DF9417223D63B3C69	13-Mar-12	12-Mar-19
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Agency CA	7C5123D5F59B9A2C88ED864873B1EE68	17-May-12	16-May-19
C=US, O=EID Passport, Inc., CN=EID Passport LRA CA 1	2654D448498E78F7C223CF61FC80928C	25-Jun-13	24-Jun-20
C=US, O=Amtrak Police Department, CN=APD MEAS Medium HW CA	455D313EDDF650629DC735F7C13ECB84	16-Jun-11	15-Jun-18
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Device CA	4D32A64D4588CF5241A9D92890AFC152	17-May-12	16-May-20
C=US, O=Symantec Corporation, OU=Organization Signing, CN=Symantec Non Federal SSP Organization Signing CA	36C13DB922580EB96727B8161095EE93	16-Oct-12	15-Oct-19
C=US, O=State of Florida, CN=State of Florida AHCA Medium Assurance CA	0F33D1CE3340916981B8AA5FBD454B79	22-May-12	21-May-19
C=US, O=Booz Allen Hamilton, OU=Certification Authorities, CN=Booz Allen Hamilton CA 02	7B15016346C0BD9532EA3B3EE366E865	31-Jul-12	30-Jul-19

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