REPORT OF THE INDEPENDENT ACCOUNTANT

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

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, 2018 to October 31, 2019, 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) ("CP") 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 CP 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 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; 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.

BDO

DigiCert's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion, based on our examination.

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.

DigiCert makes use of external registration authorities for all 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 A. 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 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.

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.

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.

BDO USA, LLP

February 3, 2020

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)	2.12	June 25, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.11	April 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.10	March 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.9	September 11, 2018
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 DN	**SHA2 Thumbprint**	**Valid From**	**Valid To**
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 SSP Intermediate CA - G3	AD67498AB29C54ACF2D95F7F26B5D9EA331FEEAF50C79EEC43C377578CD912E6	11/10/2014	11/10/2017
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 SSP Intermediate CA - G3	1E52EA21F9F98407E31E5DDC957877EFF89A6BD98AA60678479147F7AF66CFBE	5/2/2017	9/29/2024
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, CN=VeriSign Class 3 SSP Intermediate CA - G2	404BA6472C806879A1CD93DC2600AF6B1F22FE7114BDFBBF19C1F23B502B9B8D	5/2/2017	12/5/2020

Symantec Class 3 SSP Intermediate CA - G3			
Subject DN	**SHA2 Thumbprint**	**Valid From**	**Valid To**
C=US, O=CSRA LLC, OU=CSRA FBCA MedHW2, CN=CSRA FBCA C4 CA	3487C536264CFDDCECC6D662BA2035602A582A01517E3D9B290DA48A2AA2B738	2/9/2017	9/28/2024
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC CA - 2	4C6D7E1752CDBFFB71DCD3ED5F71FECB46062A479CECDAE934C5325C45899635	8/31/2017	6/19/2019
C=US, O=CSRA LLC, OU=CSRA FBCA Devices, CN=CSRA FBCA C4 Device CA	34778354B351505FD5A5F612365D9713529267EC71BF799ED4D67DC3FDE72765	2/9/2017	9/28/2024
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I Device CA G2	3422015CDC4E70401317C6EFF1E3DAF5A9F0B3F30A29E1C2B85206DFB692FBE7	8/31/2017	7/20/2019
C=US, O=Eid Passport, Inc., OU=RAPIDGate PIV Interoperable LRA, CN=Eid Passport LRA Content Signer CA 3	F9FB0BF30A04DA8531EA1ABAE9C79DEB707C9C535A09EDBE174EBBEAB5866B97	4/9/2015	9/28/2024
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Agency CA	57B54919F6684CF3024F952EEFD11BEBFD288591FEAB5447969F276D2850D817	8/31/2017	5/16/2019

Symantec Class 3 SSP Intermediate CA - G3			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier CA	37C5BC1E7EE318A7B275D72B00CE8BD631CDB7CE516BA43910E028EDCAC11C9C	8/31/2017	12/4/2020
C=US, O=Booz Allen Hamilton, OU=Certification Authorities, CN=Booz Allen Hamilton Device CA 02	47C80D55A3863792862AA9B4CE24A4AC9AD995EC63C8B5FE3975E9CF871821EE	8/31/2017	7/30/2020
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Device CA	D82E6083FB66F89EECCF6EA589EA20883D9737145D0A0816272AFA5064EA9E89	8/31/2017	5/16/2020
C=US, O=CSC Government Solutions LLC, OU=CSRA FBCA Devices, CN=CSRA FBCA C3 Device CA	DC4B008EADBB510C2CDBD6CE3308BBD3562716741335467E2A534BD35985C194	12/17/2015	9/28/2024
C=US, O=SureID, Inc., CN=SureID Inc. CA2	6CBDA687455D609626023F35CA64C000291D381802C6531F969733917D07550D	4/28/2016	9/28/2024
C=US, O=SureID, Inc., OU=SureID PIV-I, CN=SureID Inc. Device CA1	627B0212DBA9C984B6B9553C4106CEDA429E7E7186ED6FACC9B26617AC20F67D	1/19/2016	9/28/2024
C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier Device CA	91346F838DCD82BDD8F2355F1AC358B132D902BC889E283990B105402F34C7FE	8/31/2017	12/4/2020
C=US, O=Eid Passport, Inc., OU=Eid Passport PIV-I LRA Network, CN=Eid Passport LRA Device 2 CA	6D7982E84718A6FA69C3D5BD02D9ECC0BAC09A3C7923147F3F5879C02A536397	3/10/2015	9/28/2024
C=US, O=CSC Government Solutions LLC, OU=CSRA FBCA MedHW, CN=CSRA FBCA C3 CA	365B15FFE6F545DBAA6F92C8816EAFF8D92976367FA0A3CDFC33CD00127D3B7F	12/17/2015	9/28/2024

VeriSign Class 3 SSP Intermediate CA - G2			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=EID Passport, Inc., CN=EID Passport LRA Content Signer CA 1	27E94347839EBEC763EC441C250AE7E9754BD15C25C47D74EB3C7378D647E453	6/25/2013	12/4/2020
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC Device CA - G2	39C2EDE3BA5237A05F70EA464C12411D43C6F5FD5ECF349A0514A54C86DF45B6	8/21/2013	12/4/2020
C=US, O=EID Passport, Inc., CN=EID Passport LRA CA 1	C510FBDE21FE42B87034A6640B28D527BCD6832F65A49CC0BB53168C9954AC65	6/25/2013	6/24/2020

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:

- 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 various locations in the United States of America, throughout the period November 1, 2018 to October 31, 2019, 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) ("CP"), 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 CP (including sections 1 through 9)
    - DigiCert provides its services in accordance with its CP, Symantec NFSSP CPS, 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;
  - 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
- 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 all 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 A. 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.

_____

Dan Timpson
Chief Technology Officer

February 3, 2020

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)	2.12	June 25, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.11	April 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.10	March 18, 2019
DigiCert Certificate Policy for Symantec Trust Network (STN)	2.9	September 11, 2018
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 DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 SSP Intermediate CA - G3	AD67498AB29C54ACF2D95F7F26B5D9EA331FEEAF50C79EEC43C377578CD912E6	11/10/2014	11/10/2017
C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 SSP Intermediate CA - G3	1E52EA21F9F98407E31E5DDC957877EFF89A6BD98AA60678479147F7AF66CFBE	5/2/2017	9/29/2024
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, CN=VeriSign Class 3 SSP Intermediate CA - G2	404BA6472C806879A1CD93DC2600AF6B1F22FE7114BDFBBF19C1F23B502B9B8D	5/2/2017	12/5/2020

Symantec Class 3 SSP Intermediate CA - G3			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=CSRA LLC, OU=CSRA FBCA MedHW2, CN=CSRA FBCA C4 CA	3487C536264CFDDCECC6D662BA2035602A582A01517E3D9B290DA48A2AA2B738	2/9/2017	9/28/2024
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC CA - 2	4C6D7E1752CDBFFB71DCD3ED5F71FECB46062A479CECDAE934C5325C45899635	8/31/2017	6/19/2019
C=US, O=CSRA LLC, OU=CSRA FBCA Devices, CN=CSRA FBCA C4 Device CA	34778354B351505FD5A5F612365D9713529267EC71BF799ED4D67DC3FDE72765	2/9/2017	9/28/2024
C=US, O=U.S. Government, OU=U.S. Senate, OU=Office of the Sergeant at Arms, CN=Senate PIV-I Device CA G2	3422015CDC4E70401317C6EFF1E3DAF5A9F0B3F30A29E1C2B85206DFB692FBE7	8/31/2017	7/20/2019
C=US, O=Eid Passport, Inc., OU=RAPIDGate PIV Interoperable LRA, CN=Eid Passport LRA Content Signer CA 3	F9FB0BF30A04DA8531EA1ABAE9C79DEB707C9C535A09EDBE174EBBEAB5866B97	4/9/2015	9/28/2024
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Agency CA	57B54919F6684CF3024F952EEFD11BEBFD288591FEAB5447969F276D2850D817	8/31/2017	5/16/2019

Symantec Class 3 SSP Intermediate CA - G3			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier CA	37C5BC1E7EE318A7B275D72B00CE8BD631CDB7CE516BA43910E028EDCAC11C9C	8/31/2017	12/4/2020
C=US, O=Booz Allen Hamilton, OU=Certification Authorities, CN=Booz Allen Hamilton Device CA 02	47C80D55A3863792862AA9B4CE24A4AC9AD995EC63C8B5FE3975E9CF871821EE	8/31/2017	7/30/2020
C=US, O=Eid Passport, Inc., CN=RAPIDGate PIV-I Device CA	D82E6083FB66F89EECCF6EA589EA20883D9737145D0A0816272AFA5064EA9E89	8/31/2017	5/16/2020
C=US, O=CSC Government Solutions LLC, OU=CSRA FBCA Devices, CN=CSRA FBCA C3 Device CA	DC4B008EADBB510C2CDBD6CE3308BBD3562716741335467E2A534BD35985C194	12/17/2015	9/28/2024
C=US, O=SureID, Inc., CN=SureID Inc. CA2	6CBDA687455D609626023F35CA64C000291D381802C6531F969733917D07550D	4/28/2016	9/28/2024
C=US, O=SureID, Inc., OU=SureID PIV-I, CN=SureID Inc. Device CA1	627B0212DBA9C984B6B9553C4106CEDA429E7E7186ED6FACC9B26617AC20F67D	1/19/2016	9/28/2024
C=US, O=Eid Passport, Inc., CN=RAPIDGate-Premier Device CA	91346F838DCD82BDD8F2355F1AC358B132D902BC889E283990B105402F34C7FE	8/31/2017	12/4/2020
C=US, O=Eid Passport, Inc., OU=Eid Passport PIV-I LRA Network, CN=Eid Passport LRA Device 2 CA	6D7982E84718A6FA69C3D5BD02D9ECC0BAC09A3C7923147F3F5879C02A536397	3/10/2015	9/28/2024
C=US, O=CSC Government Solutions LLC, OU=CSRA FBCA MedHW, CN=CSRA FBCA C3 CA	365B15FFE6F545DBAA6F92C8816EAFF8D92976367FA0A3CDFC33CD00127D3B7F	12/17/2015	9/28/2024

VeriSign Class 3 SSP Intermediate CA - G2			
Subject DN	SHA2 Thumbprint	Valid From	Valid To
C=US, O=EID Passport, Inc., CN=EID Passport LRA Content Signer CA 1	27E94347839EBEC763EC441C250AE7E9754BD15C25C47D74EB3C7378D647E453	6/25/2013	12/4/2020
C=US, O=Computer Sciences Corporation, OU=NPS, CN=CSC Device CA - G2	39C2EDE3BA5237A05F70EA464C12411D43C6F5FD5ECF349A0514A54C86DF45B6	8/21/2013	12/4/2020
C=US, O=EID Passport, Inc., CN=EID Passport LRA CA 1	C510FBDE21FE42B87034A6640B28D527BCD6832F65A49CC0BB53168C9954AC65	6/25/2013	6/24/2020