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 CertiPath, Inc.:

We have examined for CertiPath, Inc.'s ("CertiPath") and DigiCert, Inc.'s ("DigiCert"), an independent service organization that provides certification authority support services, Certification Authority ("CA") operations at Reston, Virginia, Mountain View, California, and New Castle, Delaware, USA, throughout the period November 1, 2017 to October 31, 2018,

- CertiPath's disclosures of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices, the consistency of its Certification Practice Statements with its Certificate Policy, and the provision of services in accordance with its Certificate Policy, Certification Practice Statements, and Memorandum of Agreement between the Federal Public Key Infrastructure Policy Authority and CertiPath ("Memorandum of Agreement"), as listed in Attachment B; and

- the effectiveness of CertiPath's and DigiCert's controls over key and certificate integrity, the authenticity and confidentiality of subscriber and relying party information, the continuity of key and certificate lifecycle management operations, and development, maintenance, and operation of CA systems integrity throughout the period November 1, 2017 to October 31, 2018 for the CAs enumerated in Attachment A.

CertiPath's and DigiCert's management are responsible for these disclosures and for maintaining effective controls, based on WebTrust Principles and Criteria for Certification Authorities v2.1. Our responsibility is to express an opinion, based on our examination.

The relative effectiveness and significance of specific controls at CertiPath and 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 subordinate CAs and relying party locations and we have not evaluated the effectiveness of such controls.

CertiPath does not escrow its CA keys, does not provide subscriber key lifecycle management, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Our examination, which commenced on September 4, 2018 and ended on April 8, 2019, 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 throughout the period November 1, 2017 to October 31, 2018, for the CAs enumerated in Attachment A, in all material respects, CertiPath and DigiCert has:

- disclosed CertiPath's business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of CertiPath's Certification Practice Statements (including sections 1 through 9), Certificate

- Policy (including sections 1 through 9), and Memorandum of Agreement (including sections 1 through 9)

- provided its CA services in accordance with CertiPath's disclosed practices, including applicable versions of the Certification Practice Statements, Certificate Policy, 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; 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.

During our examination, we noted the following, which caused a modification of our opinion:

Impacted WebTrust Trust Principles and Criteria for Certification Authorities		Certificate Policy Reference	Control Deficiency Noted
3.8	Business Continuity Management The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • the storage of backups of systems, data and configuration information at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery.	5.7.4 Business Continuity Capabilities after a Disaster - In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request revocation of its certificates. Further, the CA shall re-establish operations by following the procedures for CA key loss or compromise detailed in Section 5.7.3 above.	DigiCert does not have documented disaster recovery procedures specific to the handing of CA operations and no test is conducted to determine the capabilities to recover CA operations from the secondary facility.

Impacted WebTrust Trust Principles and Criteria for Certification Authorities		Certificate Policy Reference	Control Deficiency Noted
	The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation or degradation of the CA's services.		

Because of the nature and inherent limitations of controls, CertiPath's and 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, except for the matter noted in the preceding table, throughout the period November 1, 2017 to October 31, 2018 CertiPath and DigiCert has, in all material respects:

- disclosed CertiPath's business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of CertiPath's Certification Practice Statements (including sections 1 through 9), Certificate Policy (including sections 1 through 9), and Memorandum of Agreement (including sections 1 through 9)

- provided its CA services in accordance with CertiPath's disclosed practices, including applicable versions of the Certification Practice Statements, Certificate Policy, 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; 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.

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

BDO USA, LLP

St. Louis, Missouri
April 8, 2019

Attachment A

List of CAs In-Scope

CertiPath Bridge CA ("CBCA")			
Subject Name	Serial Number	Valid From Date	Valid To Date
CN = CertiPath Bridge CA OU = Certification Authorities O = CertiPath LLC C = US	38 ef 47 1b a1 6f 9d d8 f8 fa e4 c9 a1 84 6f 9c	6/13/2011	2/21/2021
CN = CertiPath Bridge CA - G2 OU = Certification Authorities O = CertiPath LLC C = US	42 f4 67 0e 39 2a 72 2b 3e ce 45 68 40 5f 85 39	11/3/2010	11/3/2020
CertiPath Common Policy Root CA ("CRCA")			
Subject Name	Serial Number	Valid From Date	Valid To Date
CN = CertiPath Common Policy Root Certification Authority OU = Certification Authorities O = CertiPath LLC C = US	5a 83 83 2b 25 f2 7a fe 03 ec 6c 4c 7c db af 72	6/13/2011	2/21/2021
CN = CertiPath Common Policy Root Certification Authority - G2 OU = Certification Authorities O = CertiPath LLC C = US	63 fd ae a2 8d 52 0d 5b 79 c5 1d 28 90 fc eb da	11/3/2010	11/3/2020

Attachment B

CertiPath CBCA Certification Practice Statement Version In-Scope

The CertiPath CBCA Certification Practice Statement is consistent with the CertiPath X.509 Certificate Policy and restricted to authorized program members.

CPS Name	Version	Effective Date
CertiPath CBCA Certification Practice Statement	1.8	July 11, 2017

CertiPath CRCA Certification Practice Statement Version In-Scope

The CertiPath CRCA Certification Practice Statement is consistent with the CertiPath X.509 Certificate Policy and restricted to authorized program members.

CPS Name	Version	Effective Date
CertiPath CRCA Certification Practice Statement	1.8	July 11, 2017

CertiPath X.509 Certificate Policy Versions In-Scope

The CertiPath X.509 Certificate Policy is published on the CertiPath website.

CP Name	Version	Effective Date
CertiPath X.509 Certificate Policy	3.34	April 16, 2018
CertiPath X.509 Certificate Policy	3.33	January 15, 2018
CertiPath X.509 Certificate Policy	3.32	March 20, 2017

Memorandum of Agreement Version In-Scope

The Memorandum of Agreement pertains to the CertiPath Bridge CAs and is restricted to authorized program members.

Memorandum Name	Effective Date
Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and CertiPath, Inc.	November 28, 2016

CertiPath, Inc. Management's Assertion

CertiPath, Inc. ("CertiPath") and DigiCert, Inc. ("DigiCert"), an independent service organization that provides certification authority support services, operates the Certification Authority ("CA") services for its CAs enumerated in Attachment A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of CertiPath is responsible for establishing controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, applicable CA environmental controls, CA key lifecycle management controls, and subordinate CA 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 CertiPath's Certification Authority operations. Furthermore, because of changes in its conditions, the effectiveness of controls may vary over time.

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

- disclosed its business, key lifecycle management, certificate lifecycle management, and applicable CA environmental control practices in the applicable versions of its Certification Practice Statements (including sections 1 through 9), Certificate Policy (including sections 1 through 9), and Memorandum of Agreement between the Federal Public Key Infrastructure Policy Authority and CertiPath ("Memorandum of Agreement") (including sections 1 through 9), as listed in Attachment B

- maintained effective controls to provide reasonable assurance that:
    - CertiPath's Certification Practice Statements are consistent with its Certificate Policy; and
    - CertiPath provides its services in accordance with its Certificate Policy, Certification Practice Statements, and Memorandum of Agreement

- maintained effective controls to provide reasonable assurance that subordinate CA certificate requests are accurate, authenticated, and approved

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

CA Business Practices Disclosure

- Certification 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
- Personnel Security
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

Certificate Lifecycle Management Controls

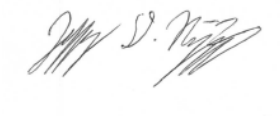
- Subscriber Registration

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

CertiPath does not escrow its CA keys, does not provide subscriber key lifecycle management, and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

CertiPath, Inc.



_____

Jeff Nigriny
President
April 8, 2019

Attachment A

List of CAs In-Scope

CertiPath Bridge CA ("CBCA")			
Subject Name	Serial Number	Valid From Date	Valid To Date
CN = CertiPath Bridge CA OU = Certification Authorities O = CertiPath LLC C = US	38 ef 47 1b a1 6f 9d d8 f8 fa e4 c9 a1 84 6f 9c	6/13/2011	2/21/2021
CN = CertiPath Bridge CA - G2 OU = Certification Authorities O = CertiPath LLC C = US	42 f4 67 0e 39 2a 72 2b 3e ce 45 68 40 5f 85 39	11/3/2010	11/3/2020
CertiPath Common Policy Root CA ("CRCA")			
Subject Name	Serial Number	Valid From Date	Valid To Date
CN = CertiPath Common Policy Root Certification Authority OU = Certification Authorities O = CertiPath LLC C = US	5a 83 83 2b 25 f2 7a fe 03 ec 6c 4c 7c db af 72	6/13/2011	2/21/2021
CN = CertiPath Common Policy Root Certification Authority - G2 OU = Certification Authorities O = CertiPath LLC C = US	63 fd ae a2 8d 52 0d 5b 79 c5 1d 28 90 fc eb da	11/3/2010	11/3/2020

Attachment B

CertiPath CBCA Certification Practice Statement Version In-Scope

The CertiPath CBCA Certification Practice Statement is consistent with the CertiPath X.509 Certificate Policy and restricted to authorized program members.

CPS Name	Version	Effective Date
CertiPath CBCA Certification Practice Statement	1.8	July 11, 2017

CertiPath CRCA Certification Practice Statement Version In-Scope

The CertiPath CRCA Certification Practice Statement is consistent with the CertiPath X.509 Certificate Policy and restricted to authorized program members.

CPS Name	Version	Effective Date
CertiPath CRCA Certification Practice Statement	1.8	July 11, 2017

CertiPath X.509 Certificate Policy Versions In-Scope

The CertiPath X.509 Certificate Policy is published on the CertiPath website.

CP Name	Version	Effective Date
CertiPath X.509 Certificate Policy	3.34	April 16, 2018
CertiPath X.509 Certificate Policy	3.33	January 15, 2018
CertiPath X.509 Certificate Policy	3.32	March 20, 2017

Memorandum of Agreement Version In-Scope

The Memorandum of Agreement pertains to the CertiPath Bridge CAs and is restricted to authorized program members.

Memorandum Name	Effective Date
Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and CertiPath, Inc.	November 28, 2016

DigiCert, Inc. Management's Assertion

DigiCert, Inc. ("DigiCert") is an independent service organization that provides certification authority support services for CertiPath, Inc. ("CertiPath"), who operates the Certification Authority ("CA") services for its CAs enumerated in Attachment A. DigiCert provides the following CA support services to CertiPath's CA:

- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

The management of DigiCert is responsible for establishing controls over its operations, to support CertiPath's CA business practices disclosures on CertiPath's website, applicable CA environmental controls, CA key lifecycle management controls, and subordinate CA 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 support services. Furthermore, because of changes in its conditions, the effectiveness of controls may vary over time.

DigiCert's management has assessed CertiPath's disclosure of its certificate practices and DigiCert's controls to provide its CA support services to CertiPath's CA. During our assessment we noted the following observations which caused the relevant criteria to not be met:

Impacted WebTrust Trust Principles and Criteria for Certification Authorities		Certificate Policy Reference	Control Deficiency Noted
3.8	Business Continuity Management The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure	5.7.4 Business Continuity Capabilities after a Disaster In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request revocation of its certificates. Further, the CA shall re-establish	DigiCert does not have documented disaster recovery procedures specific to the handing of CA operations and no test is conducted to determine the capabilities to recover CA operations from the secondary facility.

Impacted WebTrust Trust Principles and Criteria for Certification Authorities		Certificate Policy Reference	Control Deficiency Noted
	cryptographic device and activation materials) at an alternate location; • the storage of backups of systems, data and configuration information at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery. The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation or degradation of the CA's services.	operations by following the procedures for CA key loss or compromise detailed in Section 5.7.3 above.	

Based on that assessment, in DigiCert management's opinion, except for the matters described in the preceding table, in providing its CA support services at Mountain View, California, USA; and New Castle, Delaware, USA, throughout the period November 1, 2017 to October 31, 2018, DigiCert has:

- 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

- 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, including the following:

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management

- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

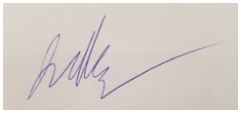
CA Key Lifecycle Management Controls

- 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

Certificate Lifecycle Management Controls

- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

DigiCert, Inc.



_____

Jeremy Rowley

Executive VP of Product

April 8, 2019