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. ("CertiPath"):

Scope

We have examined the assertions by the management of CertiPath and DigiCert, Inc. ("DigiCert"), an independent subservice organization that provides Public Key Infrastructure ("PKI") management services to CertiPath, that for its Certification Authority ("CA") operations in California and Utah, in the United States of America, for its CAs enumerated in Attachment B, CertiPath and DigiCert have:

- disclosed CertiPath's business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in applicable versions of its CertiPath X.509 Certificate Policy ("CP") (including sections 1 through 9), CertiPath CBCA Certification Practice Statement ("CBCA CPS") and CertiPath CRCA Certification Practice Statement ("CRCA CPS") (collectively the "CPSs") (including sections 1 through 9), and Memorandum of Agreements between the United States Federal Public Key Infrastructure Policy Authority and CertiPath, Inc. ("MOA") (including all sections and Attachments), as enumerated in Attachment A

- provided its CA services in accordance with its disclosed practices, including:
  - CertiPath's CP (including sections 1 through 9);
  - CertiPath's CBCA CPS and CRCA CPS that are consistent with CertiPath's CP (including sections 1 through 9); and
  - the MOAs (including all sections and Attachments)

- 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

throughout the period October 1, 2021 to September 30, 2022 based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

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

Certification Authority's Responsibilities

CertiPath and DigiCert management are responsible for their respective assertions, including the fairness of their presentation, and the provision of their described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Practitioner's Responsibilities

Our responsibility is to express an opinion on CertiPath's and DigiCert's management's assertions based on our examination. 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 judgment, 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 subscriber and relying party locations, and we have not evaluated the effectiveness of such controls.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Independent Accountant's Opinion

In our opinion, CertiPath's and DigiCert's management assertions, as referred to above, are fairly stated, in all material respects.

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

BDO USA, LLP

February 21, 2023

ATTACHMENT A – POLICIES IN-SCOPE

CertiPath CBCA Certification Practice Statement Version In-Scope

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

Document Name	Version	Effective Date
CertiPath CBCA Certification Practice Statement	2.0	August 28, 2020

CertiPath CRCA Certification Practice Statement Version In-Scope

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

Document Name	Version	Effective Date
CertiPath CRCA Certification Practice Statement	2.0	August 28, 2020

CertiPath X.509 Certificate Policy Versions In-Scope

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

Document Name	Version	Effective Date
CertiPath X.509 Certificate Policy	3.44	October 13, 2021
CertiPath X.509 Certificate Policy	3.43	May 12, 2021

Memorandum of Agreement Version In-Scope

The Memorandum of Agreement pertains to the CertiPath Bridge CA 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
Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and CertiPath, Inc.	May 16, 2022

ATTACHMENT B – LIST OF CAs IN-SCOPE

CertiPath Bridge CA ("CBCA")			
Subject Name	Serial Number	Valid From	Valid To
CN = CertiPath Bridge CA - G3 OU = Certification Authorities O = CertiPath C = US	12 17 51 7b 7a b3 a9 9a 58 3e b0 08 1a 0d 84 33	1/21/2020	1/20/2040

CertiPath Common Policy Root CA ("CRCA")			
Subject Name	Serial Number	Valid From	Valid To
CN = CertiPath Common Policy Root Certification Authority - G2 OU = Certification Authorities O = CertiPath LLC C = US	59 ea fd 3a 27 1b 46 d9 34 8f e9 5d 13 39 45 51	11/4/2010	11/3/2030

CERTIPATH, INC. MANAGEMENT'S ASSERTION

CertiPath, Inc. ("CertiPath") and DigiCert, Inc. ("DigiCert"), an independent subservice organization that provides Public Key Infrastructure ("PKI") management services to CertiPath, operate the Certification Authority ("CA") services for the CAs enumerated in Attachment B, and provide the following CA services:

- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA and cross certificate lifecycle management

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, 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 CA operations. Furthermore, because of changes in 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 in California and Utah, in the United States of America, CertiPath has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in applicable versions of its CertiPath X.509 Certificate Policy ("CP") (including sections 1 through 9), CertiPath CBCA Certification Practice Statement ("CBCA CPS") and CertiPath CRCA Certification Practice Statement ("CRCA CPS") (collectively the "CPSs") (including sections 1 through 9), and Memorandum of Agreements between the United States Federal Public Key Infrastructure Policy Authority and CertiPath, Inc. ("MOA") (including all sections and Attachments), as enumerated in Attachment A

- provided its CA services in accordance with its disclosed practices, including:
  - CertiPath's CP (including sections 1 through 9)
  - CertiPath's CBCA CPS and CRCA CPS that are consistent with CertiPath's CP (including sections 1 through 9); and
  - the MOAs (including all sections and Attachments)

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

throughout the period October 1, 2021 to September 30, 2022 based on the WebTrust Principles and Criteria for Certification Authorities v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certification Practice Statement Management
- Certificate Policy Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Personnel Security
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA and Cross Certificate Lifecycle Management

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

CertiPath, Inc.

DocuSigned by:
867086ABD4CF40C...

2/21/2023

Jeff Nigriny
CEO

ATTACHMENT A – POLICIES IN-SCOPE

CertiPath CBCA Certification Practice Statement Version In-Scope

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

Document Name	Version	Effective Date
CertiPath CBCA Certification Practice Statement	2.0	August 28, 2020

CertiPath CRCA Certification Practice Statement Version In-Scope

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

Document Name	Version	Effective Date
CertiPath CRCA Certification Practice Statement	2.0	August 28, 2020

CertiPath X.509 Certificate Policy Versions In-Scope

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

Document Name	Version	Effective Date
CertiPath X.509 Certificate Policy	3.44	October 13, 2021
CertiPath X.509 Certificate Policy	3.43	May 12, 2021

Memorandum of Agreement Version In-Scope

The Memorandum of Agreement pertains to the CertiPath Bridge CA 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
Memorandum of Agreement between the United States Federal Public Key Infrastructure Policy Authority and CertiPath, Inc.	May 16, 2022

ATTACHMENT B - LIST OF CAs IN-SCOPE

CertiPath Bridge CA ("CBCA")			
Subject Name	Serial Number	Valid From	Valid To
CN = CertiPath Bridge CA - G3 OU = Certification Authorities O = CertiPath C = US	12 17 51 7b 7a b3 a9 9a 58 3e b0 08 1a 0d 84 33	1/21/2020	1/20/2040

CertiPath Common Policy Root CA ("CRCA")			
Subject Name	Serial Number	Valid From	Valid To
CN = CertiPath Common Policy Root Certification Authority - G2 OU = Certification Authorities O = CertiPath LLC C = US	59 ea fd 3a 27 1b 46 d9 34 8f e9 5d 13 39 45 51	11/4/2010	11/3/2030

DIGICERT, INC. MANAGEMENT'S ASSERTION

DigiCert, Inc. ("DigiCert") provides Public Key Infrastructure ("PKI") management services to CertiPath, Inc. ("CertiPath"), who operates the Certification Authority ("CA") services for the CAs enumerated in Attachment B. DigiCert provides the following PKI services to CertiPath:

- 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 PKI services. Furthermore, because of changes in 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 PKI services to CertiPath. Based on that assessment, in DigiCert management's opinion, in providing its PKI services at California and Utah, in the United States of America, throughout the period October 1, 2021 to September 30, 2022, 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

- 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 v2.2.2, including the following:

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and 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.

DocuSigned by:
Jeremy Rowley
CFF89E6506D0438...

2/21/2023

Jeremy Rowley
Chief Information Security Officer