KPMG LLP
Mission Towers I
Suite 100
3975 Freedom Circle Drive
Santa Clara, CA 95054

Independent Accountant's Report

To the Management of CertiPath, Inc.:

We have examined for CertiPath, Inc.'s (CertiPath) certification authority (CA) operations at Reston, Virginia; New Castle, Delaware; and Mountain View, California, CertiPath's and Symantec's[1] disclosure of its business, key life cycle management, certificate life cycle management, and CA environmental control practices, the consistency of its Certification Practice Statements with its Certificate Policies, the provision of services in accordance with its CA Business Practices Disclosures, and the effectiveness of its controls over key and certificate integrity, the authenticity and confidentiality of subscriber and relying party information, the continuity of key and certificate life cycle management operations, and development, maintenance, and operation of CA systems integrity throughout the period December 1, 2015 to November 30, 2016 for the CertiPath Bridge CA and CertiPath Bridge CA – G2 (collectively referred to as the "CBCA") and the CertiPath Common Policy Root CA and the CertiPath Common Policy Root CA – G2 (collectively referred to as the "CRCA").

These disclosures and controls are the responsibility of CertiPath's and Symantec's management. Our responsibility is to express an opinion on the conformity of these disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities v2.0, based on our examination.

We conducted our examination, which commenced on January 31, 2017 and ended on April 13, 2017, in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of CertiPath's key and certificate life cycle management business practices
(2) obtaining an understanding of CertiPath's and Symantec's controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate life cycle management operations and over development, maintenance and operation of systems integrity;
(3) selectively testing transactions executed in accordance with CertiPath's disclosed key and certificate life cycle management business practices;
(4) testing and evaluating the operating effectiveness of the controls; and
(5) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at CertiPath and Symantec 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.

[1] Symantec Corporation ("Symantec") is an independent service organization that provides certification authority (CA) support services to CertiPath.

We noted the following matters that resulted in a modification of our opinion:

Impacted WebTrust for CAs Criteria		Matters Noted
3.3	The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	It was noted that the 5 year refresh of background checks was not consistently performed for personnel holding Trusted positions, as specified in the CertiPath CBCA and CRCA CPS documents. This caused WebTrust for CAs Criterion 3.3 to not be met from December 1, 2015 to June 15, 2016.
3.10	The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • audit logs are reviewed periodically by authorized personnel.	It was noted that physical access entry and exit logs for a Symantec CA facility were not archived for a minimum of 20 years and 6 months, as specified in CBCA and CRCA CPS document. As a result, we noted that Symantec had not maintained effective controls to meet Principle 3, Criterion 3.10 with respect to the retention of CA facility entry and exit logs. This caused WebTrust for CAs Criterion 3.10 to not be met with respect to the retention of CA facility entry and exit logs from December 1, 2015 to June 15, 2016.

In our opinion, except for the effects of the matters discussed in the preceding paragraphs, throughout the period December 1, 2015 to November 30, 2016, in all material respects:

- CertiPath disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control practices in its:
  - CertiPath X.509 Certificate Policy Version 3.29, dated November 21, 2016 ("CertiPath CP") – published on the CertiPath website (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
  - CertiPath CBCA Certification Practice Statement Version 1.7, dated August 9, 2012 ("CBCA CPS") – restricted to authorized program members, that was consistent with the CertiPath CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
  - CertiPath CRCA Certification Practice Statement Version 1.7, dated August 9, 2012 ("CRCA CPS") – restricted to authorized program members, that was consistent with the CertiPath CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
  - Memorandum of Agreement dated December 9, 2014 between the Federal PKI Policy Authority and CertiPath Inc. ("CBCA FPKI MOA") – restricted to authorized program members (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
- CertiPath and Symantec provided their CA services in accordance with the disclosed practices including:
  - CertiPath CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
  - CBCA CPS that was consistent with the CertiPath CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)

    - CRCA CPS that was consistent with the CertiPath CP (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
    - CBCA FPKI MOA (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
- CertiPath and Symantec maintained effective controls to provide reasonable assurance that:
    - subordinate CA certificate requests were accurate, authenticated, and approved;
- Symantec maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
    - logical and physical access to CA systems and data was restricted to authorized individuals;
    - the continuity of key and certificate management operations was maintained; and
    - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the CBCAs and CRCAs based on the WebTrust Principles and Criteria for Certification Authorities v2.0.

Because of the nature and inherent limitations of controls, CertiPath's and Symantec'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.

This report does not include any representation as to the quality of CertiPath's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.0, nor the suitability of any of CertiPath's services for any customer's intended purpose.

This report is intended solely for the information and use of CertiPath, Symantec, and the Federal PKI Policy Authority and is not intended to be, and should not be, used by anyone other than these named parties.

KPMG LLP

Certified Public Accountants
Santa Clara, CA
April 13, 2017

CertiPath

Assertion by Management as to
its Disclosure of its Business Practices and its Controls
Over its Certification Authority Operations
During the period from December 1, 2015 through November 30, 2016

April 13, 2017

CertiPath, Inc. ("CertiPath") provides the following certification authority services through the CertiPath Bridge CA and CertiPath Bridge CA - G2 (collectively referred to as the CBCA) and the CertiPath Common Policy Root CA and CertiPath Common Policy Root CA - G2 (collectively referred to as the CRCA):

- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

CertiPath's CA Business Practices Disclosures includes the following:

Certification Authorities	**Corresponding CA Business Practices Disclosures**	
	Document Name, Version and Date	**Included Sections**
CBCA	CertiPath X.509 Certificate Policy version 3.29 – dated November 21, 2016 ("CertiPath CP") – published on the CertiPath website	1, 2, 3, 4, 5, 6, 7, 8 and 9
	CertiPath CBCA Certification Practice Statement Version 1.7, dated August 9, 2012 ("CBCA CPS") that is consistent with the CertiPath CP – restricted to authorized program members	1, 2, 3, 4, 5, 6, 7, 8 and 9
	Memorandum of Agreement dated November 18, 2016 between the Federal PKI Policy Authority and CertiPath Inc. ("CBCA FPKI MOA") – restricted to authorized program members	1, 2, 3, 4, 5, 6, 7, 8 and 9
CRCA	CertiPath X.509 Certificate Policy version 3.29 – dated November 21, 2016 ("CertiPath CP") – published on the CertiPath website	1, 2, 3, 4, 5, 6, 7, 8 and 9
	CertiPath CRCA Certification Practice Statement Version 1.7, dated August 6, 2012 ("CRCA CPS") that is consistent with the CertiPath CP – restricted to authorized program members	1, 2, 3, 4, 5, 6, 7, 8 and 9

The management of CertiPath is responsible for establishing and maintaining effective controls over its CBCA and CRCA operations, including its CA business practices disclosure, CA business practices management, and applicable CA environmental controls, CA key life cycle 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 provide only reasonable assurance with respect to CertiPath's CBCA and CRCA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

CertiPath management has assessed the controls over its CBCA and CRCA operations. Based on that assessment, in CertiPath management's opinion, in providing its CBCA and CRCA services at Reston, Virginia; New Castle, Delaware; and Mountain View, California throughout the period December 1, 2015 to November 30, 2016:

- CertiPath disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control practices in its:
  - CertiPath CP – published on the CertiPath website (including sections 1, 2, 3, 4, 5, 6, 7, 8, and 9)
  - CBCA CPS that was consistent with the CertiPath CP (including sections 1, 2, 3, 4, 5, 6, 7, 8, and 9)
  - CRCA CPS that was consistent with the CertiPath CP (including sections 1, 2, 3, 4, 5, 6, 7, 8, and 9)
  - CBCA FPKI MOA (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
- CertiPath provided such services in accordance with disclosed practices including:
  - CertiPath CP – published on the CertiPath website (including sections 1, 2, 3, 4, 5, 6, 7, 8, and 9)
  - CBCA CPS that was consistent with the CertiPath CP (including sections 1, 2, 3, 4, 5, 6, 7, 8, and 9)
  - CRCA CPS that was consistent with the CertiPath CP (including sections 1, 2, 3, 4, 5, 6, 7, 8, and 9)
  - CBCA FPKI MOA (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
- CertiPath maintained effective controls to provide reasonable assurance that:
  - Subordinate CA certificate requests were accurate, authenticated, and approved

based on the WebTrust Principles and Criteria for Certification Authorities v2.0, including the following:

CA Business Practices Disclosure

- Certification Practice Statement
- Certificate Policy

CA Business Practices Management

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

CA Environmental Controls

- Personnel Security
- Monitoring and Compliance

Subordinate CA Certificate Life Cycle Management Controls

- Subordinate CA Certificate Life Cycle Management

CertiPath, Inc.

Jeff Nigriny
President

Assertion of Management as to
its Disclosure of its Business Practices and its Controls
Over its Certification Authority Operations
During the period from December 1, 2015 through November 30, 2016

April 13, 2017

Symantec Corporation, an independent service organization (sub-service provider), provides CertiPath, Inc. (“CertiPath”) with the following third party certification authority (CA) support services for the CertiPath Bridge CA and CertiPath Bridge CA – G2 (collectively referred to as the “CBCA”) and the CertiPath Common Policy Root CA and CertiPath Common Policy Root CA – G2 (collectively referred to as the “CRCA”):

- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of Symantec is responsible for establishing and maintaining effective controls over its CA services supporting the CertiPath CBCA and CRCA operations, including applicable CA environmental controls, CA key management controls, and Subordinate CA certificate life cycle management controls (for systems managed by Symantec on behalf of CertiPath). 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 internal control can provide only reasonable assurance with respect to Symantec’s CA services supporting CertiPath CBCA and CRCA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Symantec management has assessed the applicable CA environmental controls, CA key management controls, and CA certificate life cycle management controls (for systems managed by Symantec on behalf of CertiPath) over CBCA and CRCA operations. Based on that assessment, in Symantec Management’s opinion in providing CA support services to CertiPath for CBCA and CRCA operations in Delaware, New Castle and Mountain View, California during the period from December 1, 2015 through November 30, 2016:

- Symantec provided such services in accordance with the following practices:
  - CertiPath X.509 Certificate Policy version 3.29 – dated November 21, 2016 (“CertiPath CP”) – published on the CertiPath website (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
  - CertiPath CBCA Certification Practice Statement Version 1.7, dated August 9, 2012 (“CBCA CPS”) – restricted to authorized program members (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
  - CertiPath CRCA Certification Practice Statement Version 1.7, dated August 9, 2012 (“CRCA CPS”) – restricted to authorized program members (including sections 1, 2, 3, 4, 5, 6, 7, 8 and 9)
- Symantec maintained effective controls to provide reasonable assurance that:
  - Subordinate CA certificate requests were accurate, authenticated, and approved;
  - the integrity of keys and certificates managed by Symantec on behalf of CertiPath was established and protected throughout their life cycles;

- logical and physical access to CA systems and data was restricted to authorized individuals;
- the continuity of key and certificate life cycle management operations was maintained; and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

based on the WebTrust Principles and Criteria for Certification Authorities v2.0, 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 and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Life Cycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Destruction
- CA Key Archival
- CA Cryptographic Hardware Life Cycle Management

Subordinate CA Certificate Life Cycle Management Controls

- Subordinate CA Certificate Life Cycle Management

except for the effects of the matters noted below:

Impacted WebTrust for CAs Criteria		Issues Noted
3.3	The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	It was noted that the 5 year refresh of background checks was not consistently performed for personnel holding Trusted positions, as specified in the CertiPath CBCA and CRCA CPS documents. As of June 15, 2016, HR has performed a validation of personnel requiring Trusted Status. Management also reiterated internal procedures to ensure that all reinvestigations are consistently performed.

Impacted WebTrust for CAs Criteria		Issues Noted
3.10	The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • audit logs are reviewed periodically by authorized personnel.	It was noted that physical access entry and exit logs for a Symantec CA facility were not archived for a minimum of 20 years and 6 months, as specified in CertiPath's CBCA and CRCA CPS documents, to meet Principle 3, Criterion 3.10. Access log retention requirements for Symantec CA facilities exceed Symantec Corporate Security requirements. Due to recent personnel changes within the Corporate team that manages data retention across the company, CA facility log retention periods were reduced to match corporate security log retention requirements without approval from the Symantec Website Security business unit. As of June 15, 2016, the retention periods of physical access logs have been updated to comply with the respective requirements for CA facilities. In addition, policy updates have been put in place to require supplemental approval and periodic monitoring of data retention requirements moving forward.

Symantec Corporation

Nicolas Popp
Senior Vice President, Information Protection