Grant Thornton LLP
Grant Thornton Tower
171 N. Clark Street, Suite 200
Chicago, IL 60601-3370

T +312 856 0200
F +312 565 4719
grantthornton.com

INDEPENDENT ACCOUNTANTS' REPORT

To the management of Trustwave Holdings, Inc. ("Trustwave"):

We have examined Trustwave management's assertion that in generating and protecting its TWGCA, TWGP256CA, and TWGP384CA (collectively, "Trustwave Root CAs") on August 23, 2017 at Chicago, Illinois, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
TWGCA	99:E0:19:67:0D:62:DB:76:B3:DA:3D:B8:5B:E8:FD:42:D2:31:0E:87	05:f7:0e:86:da:49:f3:46:35:2e:ba:b2
TWGP256CA	A3:41:06:AC:90:6D:D1:4A:EB:75:A5:4A:10:99:B3:B1:A1:8B:4A:F7	0d:6a:5f:08:3f:28:5c:3e:51:95:df:5d
TWGP384CA	55:A9:84:89:D2:C1:32:BD:18:CB:6C:A6:07:4E:C8:E7:9D:BE:82:90	08:bd:85:97:6c:99:27:a4:80:68:47:3b

Trustwave has:

- followed the CA key generation and protection requirements in its:
  - Trustwave Certificate Policy and Certification Practices Statement Version 4.8 ("CP/CPS"),
- included appropriate, detailed procedures and controls in its Root Key Generation Scripts:
  - TWGCA Root Key and Certificate Generation Ceremony (2017-08-23)
  - TWGP256CA Root Key and Certificate Generation Ceremony (2017-08-23)

  - TWGP384CA Root Key and Certificate Generation Ceremony (2017-08-23)

- maintained effective controls to provide reasonable assurance that the Trustwave Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its Root Key Generation Scripts

- performed, during the root key generation process, all procedures required by the Root Key Generation Scripts

- generated the CA keys in a physically secured environment as described in its CP/CPS

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge

- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.0.

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

We conducted our examination in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of Trustwave's documented plan of procedures to be performed for the generation of the certification authority key pairs for the Trustwave Root CAs;

(2) reviewing the detailed CA key generation scripts for conformance with industry standard practices;

(3) testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;

(4) physical observation of all procedures performed during the root key generation process to ensure that the procedures actually performed on August 23, 2017 were in accordance with the Root Key Generation Scripts for the Trustwave Root CAs; 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.

In our opinion, as of August 23, 2017, Trustwave management's assertion, as referred to below, is fairly stated, in all material respects, based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.0.

This report does not include any representation as to the quality of Trustwave's services beyond those covered by CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.0, nor the suitability of any of Trustwave's services for any customer's intended purpose.

Grant Thornton LLP

Certified Public Accountants
Chicago, Illinois
December 15, 2017

TRUSTWAVE HOLDING, INC. MANAGEMENT'S ASSERTION

Trustwave Holdings, Inc. ("Trustwave") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CAs known as TWGCA, TWGP256CA, and TWGP384CA (collectively, "Trustwave Root CAs"). These CA's will serve as Root CAs for client certificate services. In order to allow the CA's to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA's private signing key. This helps assure the non-refutability of the integrity of Trustwave Root CAs' key pairs, and in particular, the private signing keys.

Trustwave management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in Trustwave Certificate Policy and Certification Practices Statement Version 4.8 ("CP/CPS"), and its Root Key Generation Scripts, which are based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.0.

Trustwave management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

Trustwave management is responsible for establishing and maintaining procedures over its CA root key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the Trustwave Root CAs, and for the CA environment controls relevant to the generation and protection of its CA keys.

Trustwave management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generation and protecting its CA keys for the Trustwave Root CA's on August 23, 2017 at Chicago, Illinois, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
TWGCA	99:E0:19:67:0D:62:DB:76:B3:DA:3D:B8:5B:E8:FD:42:D2:31:0E:87	05:f7:0e:86:da:49:f3:46:35:2e:ba:b2
TWGP256CA	A3:41:06:AC:90:6D:D1:4A:EB:75:A5:4A:10:99:B3:B1:A1:8B:4A:F7	0d:6a:5f:08:3f:28:5c:3e:51:95:df:5d
TWGP384CA	55:A9:84:89:D2:C1:32:BD:18:CB:6C:A6:07:4E:C8:E7:9D:BE:82:90	08:bd:85:97:6c:99:27:a4:80:68:47:3b

Trustwave has:

- followed the CA key generation and protection requirements in its:
  - Trustwave Certificate Policy and Certification Practices Statement Version 4.8 ("CP/CPS"),

- included appropriate, detailed procedures and controls in its Root Key Generation Scripts:
  - TWGCA Root Key and Certificate Generation Ceremony (2017-08-23)
  - TWGP256CA Root Key and Certificate Generation Ceremony (2017-08-23)
  - TWGP384CA Root Key and Certificate Generation Ceremony (2017-08-23)

- maintained effective controls to provide reasonable assurance that the Trustwave Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its Root Key Generation Scripts

- performed, during the root key generation process, all procedures required by the Root Key Generation Scripts

- generated the CA keys in a physically secured environment as described in its CP/CPS

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge

- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

based on CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.0.

Trustwave Holdings, Inc.
Robert J. McCullen
President and Chief Executive Officer
December 15, 2017