

## Report of the Independent Accountant

To the Management of Trustwave Holdings, Inc.:

We have examined Trustwave Holdings, Inc. (“Trustwave”) management’s assertion for its Certification Authority (“CA”) operations at Chicago, Illinois throughout the period October 1, 2017 to September 30, 2018 for its XRamp Global Certification Authority, SecureTrust CA, Secure Global CA, Trustwave Global Certification Authority, Trustwave Global ECC P256 Certification Authority, and Trustwave Global ECC P384 Certification Authority. Trustwave has:

- disclosed its business, key lifecycle management, certificate lifecycle management and CA environmental control practices in its:
  - Trustwave Certificate Policy and Certification Practices Statement (“CP/CPS”),
    - § Version 5.0, dated January 31, 2018
    - § Version 4.8, dated August 23, 2017
- maintained effective controls to provide reasonable assurance that:
  - Trustwave provides its services in accordance with its CP/CPS
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated (for the registration activities performed by Trustwave)
- 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 v 2.0. Trustwave'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 Trustwave 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.

Trustwave does not escrow its CA keys, does not provide subscriber key generation services, does not provide subscriber key storage and recovery services, does not provide integrated circuit card lifecycle management services, does not provide subscriber key management services, does not provide certificate renewal services, does not provide certificate suspension services, and does not provide subordinate CA certificate lifecycle management 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 required 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 misstatements 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, Trustwave'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 conclusion 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 Trustwave's services other than its CA operations at Chicago, Illinois, nor the suitability of any of Trustwave's services for any customer's intended purpose.

Trustwave's use of the WebTrust<sup>SM/TM</sup> for Certificate Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

*Grant Thornton LLP*

Chicago, Illinois  
November 30, 2018

## Trustwave Holdings, Inc. Management's Assertion

As set forth in Appendix A, Trustwave Holdings, Inc. ("Trustwave") operates Certification Authority ("CA") services known as XRamp Global Certification Authority, SecureTrust CA, Secure Global CA, Trustwave Global Certification Authority, Trustwave Global ECC P256 Certification Authority, Trustwave Global ECC P384 Certification Authority, and provides the following CA services:

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of Trustwave 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, and 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 only provide reasonable assurance with respect to Trustwave's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Trustwave management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in Trustwave management's opinion, in providing its CA services at Chicago, Illinois, throughout the period October 1, 2017 to September 30, 2018, Trustwave has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Trustwave Certificate Policy and Certification Practices Statement ("CP/CPS"),
    - Version 5.0, dated January 31, 2018
    - Version 4.8, dated August 23, 2017
- maintained effective controls to provide reasonable assurance that:
  - Trustwave provides its services in accordance with its CP/CPS
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated (for the registration activities performed by Trustwave)

- 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 Version 2.0, including the following:

#### **CA Business Practices Disclosure**

- Certificate Policy and Certification Practices Statement (“CP/CPS”)

#### **CA Business Practices Management**

- Certificate Policy Management
- Certificate Practice Statement Management

#### **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 Lifecycle Management Controls**

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

#### **Certificate Lifecycle Management Controls**

- Subscriber Registration
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation



Trustwave Holdings, Inc.

Art Wong

Chief Executive Officer

November 30, 2018

## Appendix A

### ROOTS:

subject=C = US, OU = [www.xrampsecurity.com](http://www.xrampsecurity.com), O = XRamp Security Services Inc, CN = XRamp Global Certification Authority  
SHA256  
Fingerprint=CE:CD:DC:90:50:99:D8:DA:DF:C5:B1:D2:09:B7:37:CB:E2:C1:8C:FB:2C:10:C0:FF:0B:CF:0D:32:86:FC:1A:A2

subject=C = US, O = SecureTrust Corporation, CN = SecureTrust CA  
SHA256  
Fingerprint=F1:C1:B5:0A:E5:A2:0D:D8:03:0E:C9:F6:BC:24:82:3D:D3:67:B5:25:57:59:B4:E7:1B:61:FC:E9:F7:37:5D:73

subject=C = US, O = SecureTrust Corporation, CN = Secure Global CA  
SHA256  
Fingerprint=42:00:F5:04:3A:C8:59:0E:BB:52:7D:20:9E:D1:50:30:29:FB:CB:D4:1C:A1:B5:06:EC:27:F1:5A:DE:7D:AC:69

subject= /C=US/ST=Illinois/L=Chicago/O=Trustwave Holdings, Inc./CN=Trustwave Global Certification Authority  
SHA256  
Fingerprint=97:55:20:15:F5:DD:FC:3C:87:88:C0:06:94:45:55:40:88:94:45:00:84:F1:00:86:70:86:BC:1A:2B:B5:8D:C8

subject= /C=US/ST=Illinois/L=Chicago/O=Trustwave Holdings, Inc./CN=Trustwave Global ECC P256 Certification Authority  
SHA256  
Fingerprint=94:5B:BC:82:5E:A5:54:F4:89:D1:FD:51:A7:3D:DF:2E:A6:24:AC:70:19:A0:52:05:22:5C:22:A7:8C:CF:A8:B4

subject= /C=US/ST=Illinois/L=Chicago/O=Trustwave Holdings, Inc./CN=Trustwave Global ECC P384 Certification Authority  
SHA256  
Fingerprint=55:90:38:59:C8:C0:C3:EB:B8:75:9E:CE:4E:25:57:22:5F:F5:75:8B:BD:38:EB:D4:82:76:60:1E:1B:D5:80:97

### SSL/TLS Certificate Issuing CAs:

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Secure Global Extended Validation CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)  
SHA256  
Fingerprint=45:B2:B0:8E:1B:58:94:8A:02:8B:E1:3A:67:C0:E2:0D:4B:24:66:AE:2B:6E:C6:25:0E:BB:10:FD:6B:7F:82:39

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave XRamp Global Extended Validation CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)  
SHA256  
Fingerprint=1D:0C:D7:EF:3C:19:26:55:08:E2:0E:58:B3:53:89:64:F4:A1:1A:DE:C8:A7:1D:8A:B8:A8:AF:F1:56:83:C6:AE

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Extended Validation SHA256 CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)  
SHA256  
Fingerprint=EE:A3:6C:0F:FA:3F:54:FF:DB:0C:F1:4B:3B:D3:4A:53:EC:7B:77:5F:54:05:3D:D8:B0:7D:FD:2F:8B:EC:90:83

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Extended Validation SHA256 CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)  
SHA256  
Fingerprint=49:C5:82:70:F7:0F:1B:E0:B7:C1:9D:1B:C2:C2:EB:C4:1E:2F:DE:0D:48:85:D4:FA:65:EF:03:70:AC:EC:7A:00

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Organization Validation SHA256 CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)  
SHA256  
Fingerprint=FF:1E:0D:23:31:96:B7:EC:20:BE:DF:C6:59:88:E0:AE:19:85:EC:6A:C3:32:A7:9A:DF:FE:71:B8:6B:C0:20:8A

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Organization Validation SHA256 CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)  
SHA256  
Fingerprint=58:EA:06:88:B7:90:9A:AA:8E:AA:A2:FF:F3:6F:3B:BE:8F:4A:2A:D0:3B:D7:02:43:B3:90:34:69:DB:48:90:F7

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Domain Validation SHA256 CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)  
SHA256  
Fingerprint=85:99:68:F9:27:8B:4D:C8:2E:E3:0F:D1:18:A5:D2:97:D2:84:B6:87:CB:64:CF:97:55:AB:8A:9D:38:F2:B7:0F

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Domain Validation SHA256 CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)  
SHA256  
Fingerprint=74:F5:6E:1A:B3:39:D8:3E:80:F2:F6:E2:64:F8:94:77:5B:42:6C:89:B4:47:03:DF:4F:A8:A3:23:11:63:A2:BD

subject=/CN=Trustwave Global Domain Validation CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US  
SHA256  
Fingerprint=67:82:C6:E9:AD:BF:92:16:E2:68:30:6D:46:33:3F:BC:67:4B:DE:DF:86:B6:7B:E7:77:07:9E:2C:0E:36:88:8E

subject=/CN=Trustwave Global Extended Validation CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US  
SHA256  
Fingerprint=18:62:6A:3B:72:11:12:8D:56:34:69:C6:54:55:7D:13:C9:36:6D:7F:CE:C8:B9:4D:B4:F0:AA:7E:05:94:40:41

subject=/CN=Trustwave Global Organization Validation CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US  
SHA256  
Fingerprint=2E:63:DC:1B:EC:F4:27:F9:90:2B:49:DE:63:30:FD:3E:8E:EB:F8:8B:14:E6:53:B3:BA:2E:37:D4:E4:88:09:65

subject=/CN=Trustwave Global ECDSA P-256 Domain Validation CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US  
SHA256  
Fingerprint=F6:2E:35:AA:D3:45:FB:25:38:63:CF:C0:E6:58:23:AC:D3:E7:F0:84:6D:19:B8:32:6D:70:9C:79:19:A2:2D:7E

subject=/CN=Trustwave Global ECDSA P-256 Extended Validation CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=27:5B:F0:04:6E:02:70:17:8B:13:B6:7E:4D:B1:50:A1:01:97:CB:71:F9:A0:61:FA:D3:6B:3D:76:63:9F:E1:86

subject= /CN=Trustwave Global ECDSA P-256 Organization Validation CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=18:AB:D6:E9:CA:90:7B:B3:67:54:D0:C0:46:EB:B5:0D:D9:B9:5D:52:78:24:D9:58:1A:31:B7:50:FC:FD:BA:EF

subject= /CN=Trustwave Global ECDSA P-384 Domain Validation CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=C6:3D:F9:61:8F:BA:F4:86:62:BA:12:AB:E8:7B:21:2C:F7:77:C2:7A:44:6A:0F:A5:55:D7:A9:D1:91:14:8E:D7

subject= /CN=Trustwave Global ECDSA P-384 Extended Validation CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=29:F8:E1:04:DF:38:E6:12:BF:4F:50:53:65:B5:D0:B0:B2:0D:D4:E8:9C:90:83:06:48:4E:B8:37:4C:1E:66:D8

subject= /CN=Trustwave Global ECDSA P-384 Organization Validation CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=87:D4:21:69:B2:69:35:51:CA:20:5C:CF:17:F0:6F:6E:66:51:F7:21:8C:D6:D2:66:07:BF:5B:A4:DD:2F:26:F2

### Secure Email (S/MIME) CAs:

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave S/MIME SHA256 CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)

SHA256

Fingerprint=5C:4B:C5:97:29:1A:B9:C7:02:3F:B6:44:5F:D6:03:81:A6:5C:60:DD:D4:04:F1:24:E5:FA:14:3F:E9:8B:05:F3

### Combined Secure Email (S/MIME) and Client Authentication CAs:

subject= /CN=Trustwave Global Client CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=95:81:1E:24:BE:C4:1B:5F:2B:CC:CA:FE:EA:DA:77:11:40:4E:DF:66:04:B8:FF:11:9C:2E:43:35:00:99:0B:EB

subject= /CN=Trustwave Global ECDSA P-256 Client CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=D2:BB:94:89:EF:AC:F4:8A:D6:B3:42:D3:39:C0:42:95:30:58:E8:F5:DA:42:26:ED:3E:76:CA:70:C1:72:E0:53

subject= /CN=Trustwave Global ECDSA P-384 Client CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=84:C1:5D:35:B6:E2:F2:F4:1E:4A:45:E8:7B:D3:E9:6C:19:53:A4:FE:EF:19:6E:42:5C:80:46:65:0A:75:CE:07

## Code Signing CAs:

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Code Signing CA, Level 2", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)

SHA256

Fingerprint=95:46:9A:45:EE:12:F3:A7:D1:CA:88:0A:2F:52:44:2E:28:63:59:39:23:FE:C0:8A:F6:BC:AB:23:75:45:9E:9B

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Code Signing SHA256 CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)

SHA256

Fingerprint=F4:20:94:9B:B5:5A:46:2D:9B:92:74:49:E4:9D:A2:3F:68:3A:B4:B6:16:6E:05:81:58:08:F5:D9:FD:36:64:6B

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Code Signing SHA256 CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)

SHA256

Fingerprint=53:A8:12:9F:71:A9:82:7D:03:70:46:70:72:0C:37:50:61:82:11:55:C0:76:E8:6A:49:0D:6E:B8:71:E0:3A:F0

subject=/CN=Trustwave Global Code Signing CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=4D:10:A0:86:86:67:31:C0:E1:61:74:19:21:14:C6:07:6C:79:95:DD:54:93:00:6D:D2:05:4E:FB:D1:69:AE:2B

subject=/CN=Trustwave Global ECDSA P-256 Code Signing CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=73:0E:02:CD:3A:FD:48:9F:DB:9D:70:8F:67:4B:45:FA:8C:FD:73:AB:92:6B:94:85:5B:2C:03:76:F9:A5:28:D9

subject=/CN=Trustwave Global ECDSA P-384 Code Signing CA, Level 1/O=Trustwave Holdings, Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=7F:2A:89:0E:8D:9A:FD:B9:C0:F0:8A:F1:CB:8D:DA:18:C5:80:2C:5B:EA:50:E0:B1:80:71:D3:CF:97:3A:46:BD

## Client Authentication CAs:

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = Trustwave Client Authentication Certification Authority

SHA256

Fingerprint=B9:8F:D5:97:83:CE:A8:FE:08:AD:61:EC:7A:A9:1E:53:93:13:8E:72:43:4E:9F:95:00:01:F9:5F:EF:10:DF:38

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Client Authentication SHA256 CA, Level 1", emailAddress = [ca@trustwave.com](mailto:ca@trustwave.com)

SHA256

Fingerprint=7F:E2:0C:EE:E2:B6:97:2D:86:25:42:06:0A:E9:A8:8F:EA:5E:43:A9:77:A7:FB:25:C9:52:46:F7:F7:6C:06:68

## Timestamping CAs:

subject=C = US, ST = Illinois, L = Chicago, O = "Trustwave Holdings, Inc.", CN = "Trustwave Timestamping CA, Level 1"

SHA256

Fingerprint=EF:5A:E8:BB:F2:14:33:77:79:B8:A3:07:30:96:26:38:BB:3A:FE:10:0C:61:5A:49:73:0F:70:9A:25:18:86:1B

subject= /CN=Trustwave Global Timestamping CA, Level 1/O=Trustwave Holdings,  
Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=64:3B:81:C9:0B:35:05:BF:AF:F8:0E:AA:C9:EE:28:C9:F4:06:36:2A:8F:56:DD:26:EC:FA:29:33:59:58:C8:56

subject= /CN=Trustwave Global ECDSA P-256 Timestamping CA, Level 1/O=Trustwave Holdings,  
Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=7F:C2:9B:85:6B:23:EE:FC:3A:5E:68:77:5E:0B:37:DC:32:06:27:FD:5C:19:36:8B:B6:83:97:EE:21:9A:66:7A

subject= /CN=Trustwave Global ECDSA P-384 Timestamping CA, Level 1/O=Trustwave Holdings,  
Inc./L=Chicago/ST=Illinois/C=US

SHA256

Fingerprint=F7:5E:65:42:0A:D6:C0:18:D9:15:BB:BA:40:A7:71:22:B3:0A:CF:D4:17:DA:3A:88:5E:4C:4C:D9:E0:65:A4:15