



REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of SecureTrust,

We have examined for SecureTrust's, a Trustwave Holdings, Inc. division ("SecureTrust"), Certification Authority ("CA") operations at Chicago, Illinois, in the United States of America,

- SecureTrust's disclosure of its SSL certificate lifecycle management business practices in the applicable versions of its SecureTrust Certificate Policy and Certification Practices Statement enumerated in [Attachment A](#), including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on its [repository](#)
- the provision of such services in accordance with its disclosed practices
- the effectiveness of its controls over:
 - key and SSL certificate integrity;
 - the authenticity and confidentiality of SSL subscriber and relying party information;
 - continuity of key and SSL certificate lifecycle management operations;
 - development, maintenance, and operation of CA systems integrity; and
 - meeting the network and certificate system security requirements set forth by the CA/Browser Forum

throughout the period October 1, 2018 to September 30, 2019 for its CAs enumerated in [Attachment B](#), in scope for SSL Baseline Requirements and Network Security Requirements.

SecureTrust's management is responsible for these disclosures and for maintaining effective controls based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#). Our responsibility is to express an opinion based on our examination.

The relative effectiveness and significance of specific controls at SecureTrust 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.

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, throughout the period October 1, 2018 to September 30, 2019, for its CAs enumerated in [Attachment B](#), in all material respects, SecureTrust:

- disclosed its SSL certificate lifecycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the SecureTrust [repository](#)



- provided such services in accordance with its disclosed practices
- maintained effective controls over:
 - key and SSL certificate integrity;
 - the authenticity and confidentiality of SSL subscriber and relying party information;
 - continuity of key and SSL certificate lifecycle management operations;
 - development, maintenance, and operation of CA systems integrity; and
 - meeting the network and certificate system security requirements set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#).

Because of the nature and inherent limitations of controls, SecureTrust’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.

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

Impacted WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security		Control Deficiency Noted
4-3.5	The CA maintains controls to provide reasonable assurance that a human review of application and system logs is performed at least monthly and includes: <ul style="list-style-type: none">• Validating the integrity of logging processes; and• Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly.	Human reviews of application and system logs to validate the integrity of logging processes and test the monitoring, logging, alerting, and log-integrity-verification functions are operating properly were not being performed monthly during the examination period.

In our opinion, except for the effect of the matter described in the preceding table, throughout the period October 1, 2018 to September 30, 2019, SecureTrust has, in all material respects:

- disclosed its SSL certificate lifecycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the SecureTrust [repository](#)
- provided such services in accordance with its disclosed practices
- maintained effective controls over:



- o key and SSL certificate integrity;
- o the authenticity and confidentiality of SSL subscriber and relying party information;
- o continuity of key and SSL certificate lifecycle management operations;
- o development, maintenance, and operation of CA systems integrity; and
- o meeting the network and certificate system security requirements set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#).

Without further modifying our opinion, we noted the following other matters during our procedures:

Matter Topic		Matter Description
1	Certificate Content	Two certificates were issued containing the phrase "Some-State" in the stateOrProvinceName field. This matter has been disclosed by SecureTrust in Mozilla Bug 1551374 .
2	Certificate Validation	During an internal self-audit on April 23, 2019, SecureTrust discovered a certificate that was intended to be an internal only test certificate was issued using a deprecated validation method. The certificate was issued as a public trusted certificate. This matter has been disclosed by SecureTrust in Mozilla Bug 1546776 .
3	Vulnerability Scans	The scope of SecureTrust's vulnerability scanning process did not include all public and private IP addresses for the Certificate System for two of the four quarters during the engagement period.
4	Certificate Audit	One quarterly self-assessment completed by SecureTrust of at least three percent of certificates issued was not performed in a timely manner.

This report does not include any representation as to the quality of SecureTrust's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#), nor the suitability of any of SecureTrust's services for any customer's intended purpose.

BDS USA, LLP

St. Louis, Missouri
November 19, 2019



**ATTACHMENT A - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE
POLICY VERSIONS IN-SCOPE**

Policy Name	Policy Version	Policy Date
SecureTrust Certificate Policy and Certification Practices Statement	Version 6.0	April 24, 2019
Trustwave Certificate Policy and Certification Practices Statement	Version 5.2	November 14, 2018
Trustwave Certificate Policy and Certification Practices Statement	Version 5.1	October 1, 2018



ATTACHMENT B - IN-SCOPE CAs

Root CAs

Subject DN	SHA2 Thumbprint	Valid From	Valid To
CN = XRamp Global Certification Authority O = XRamp Security Services Inc OU = www.xrampsecurity.com C = US	CECDDC905099D8DADFC5B1D209B737CBE2C18CFB2C10C0FF0BCF0D3286FC1AA2	11/1/2004	1/1/2035
CN = SecureTrust CA O = SecureTrust Corporation C = US	F1C1B50AE5A20DD8030EC9F6BC24823DD367B5255759B4E71B61FCE9F7375D73	11/7/2006	12/31/2029
CN = Secure Global CA O = SecureTrust Corporation C = US	4200F5043AC8590EBB527D209ED1503029FBCBD41CA1B506EC27F15ADE7DAC69	11/7/2006	12/31/2029
CN = Trustwave Global Certification Authority O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	97552015F5DDFC3C8788C006944555408894450084F100867086BC1A2BB58DC8	8/23/2017	8/23/2042



Subject DN	SHA2 Thumbprint	Valid From	Valid To
CN = Trustwave Global ECC P256 Certification Authority O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	945BBC825EA554F489D1FD51A73DDF2EA624AC7019A05205225C22A78CCFA8B4	8/23/2017	8/23/2042
CN = Trustwave Global ECC P384 Certification Authority O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	55903859C8C0C3EBB8759ECE4E2557225FF5758BBD38EBD48276601E1BD58097	8/23/2017	8/23/2042



SSL/TLS Issuing CAs

Subject DN	SHA2 Thumbprint	Valid From	Valid To
E = ca@trustwave.com CN = Trustwave Extended Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	EEA36C0FFA3F54FFDB0CF14B3BD34A53EC7B775F54053DD8B07DFD2F8BEC9083	10/13/2014	10/10/2024
E = ca@trustwave.com CN = Trustwave Extended Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	49C58270F70F1BE0B7C19D1BC2C2EBC41E2FDE0D4885D4FA65EF0370ACEC7A00	9/1/2016	9/29/2024
E = ca@trustwave.com CN = Trustwave Secure Global Extended Validation CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	45B2B08E1B58948A028BE13A67C0E20D4B2466AE2B6EC6250EBB10FD6B7F8239	8/12/2015	8/9/2025
E = ca@trustwave.com CN = Trustwave XRamp Global Extended Validation CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	1D0CD7EF3C19265508E20E58B3538964F4A11ADEC8A71D8AB8A8AFF15683C6AE	8/12/2015	8/9/2025



Subject DN	SHA2 Thumbprint	Valid From	Valid To
C = US S = Illinois L = Chicago O = SecureTrust CN = SecureTrust Extended Validation CA, Level 1	DD23355C61D59970423004729795CAEF77AFDB39767A795740D4E04CB6158A99	1/29/2019	1/29/2029
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global Extended Validation CA, Level 1	18626A3B7211128D563469C654557D13C9366D7FCEC8B94DB4F0AA7E05944041	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-256 Extended Validation CA, Level 1	275BF0046E0270178B13B67E4DB150A10197CB71F9A061FAD36B3D76639FE186	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-384 Extended Validation CA, Level 1	29F8E104DF38E612BF4F505365B5D0B0B20DD4E89C908306484EB8374C1E66D8	2/6/2018	2/24/2028
E = ca@trustwave.com CN = Trustwave Organization Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	FF1E0D233196B7EC20BEDFC65988E0AE1985EC6AC332A79ADFFE71B86BC0208A	10/1/2014	9/28/2024



Subject DN	SHA2 Thumbprint	Valid From	Valid To
E = ca@trustwave.com CN = Trustwave Organization Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	58EA0688B7909AAA8EAAA2FFF36F3BBE8F4A2AD03BD70243B3903469DB4890F7	9/1/2016	9/29/2024
C = US S = Illinois L = Chicago O = SecureTrust CN = SecureTrust Organization Validation CA, Level 1	11D9330D1A2398508DD50D3094EB28B1B44900D9928F8C22B25EF7A781BDB403	1/29/2019	1/29/2029
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global Organization Validation CA, Level 1	2E63DC1BECF427F9902B49DE6330FD3E8EEBF88B14E653B3BA2E37D4E4880965	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-256 Organization Validation CA, Level 1	18ABD6E9CA907BB36754D0C046EBB50DD9B95D527824D9581A31B750FCFDBAEF	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-384 Organization Validation CA, Level 1	87D42169B2693551CA205CCF17F06F6E6651F7218CD6D26607BF5BA4DD2F26F2	2/6/2018	2/24/2028



Subject DN	SHA2 Thumbprint	Valid From	Valid To
E = ca@trustwave.com CN = Trustwave Domain Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	859968F9278B4DC82EE30FD118A5D297D284B687CB64CF9755AB8A9D38F2B70F	10/1/2014	9/28/2024
E = ca@trustwave.com CN = Trustwave Domain Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	74F56E1AB339D83E80F2F6E264F894775B426C89B44703DF4FA8A3231163A2BD	9/1/2016	9/29/2024
C = US S = Illinois L = Chicago O = SecureTrust CN = SecureTrust Domain Validation CA, Level 1	5E60965804461930AC27B6DBE3445679EAE4131C22AFB88AF7ACF6A1917B5ABA	1/29/2019	1/29/2029
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global Domain Validation CA, Level 1	6782C6E9ADBF9216E268306D46333FBC674BDEDF86B67BE777079E2C0E36888E	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-256 Domain Validation CA, Level 1	F62E35AAD345FB253863CFC0E65823ACD3E7F0846D19B8326D709C7919A22D7E	2/6/2018	2/24/2028



Subject DN	SHA2 Thumbprint	Valid From	Valid To
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-384 Domain Validation CA, Level 1	C63DF9618FBAF48662BA12ABE87B212CF777C27A446A0FA555D7A9D191148ED7	2/6/2018	2/24/2028

SECURETRUST MANAGEMENT’S ASSERTION

SecureTrust, a Trustwave Holdings, Inc. division (“SecureTrust”), operates the Certification Authority (“CA”) services for its CAs enumerated in [Attachment B](#) in scope for SSL Baseline and Network Security Requirements and provides SSL CA services.

SecureTrust management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL CA services at Chicago, Illinois, in the United States of America, throughout the period October 1, 2018 to September 30, 2019, SecureTrust has:

- disclosed its SSL certificate lifecycle management business practices in applicable versions of its SecureTrust Certificate Policy and Certification Practices Statement enumerated in [Attachment A](#), including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on its [repository](#), and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
 - SSL subscriber information is properly authenticated
- 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.3](#), except for the effect of the matter noted below:

Impacted WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security		Control Deficiency Noted
4-3.5	<p>The CA maintains controls to provide reasonable assurance that a human review of application and system logs is performed at least monthly and includes:</p> <ul style="list-style-type: none"> • Validating the integrity of logging processes; and • Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly. 	<p>Human reviews of application and system logs to validate the integrity of logging processes and test the monitoring, logging, alerting, and log-integrity-verification functions are operating properly were not being performed monthly during the examination period.</p>

A handwritten signature in cursive script, appearing to read "Tom Wallace", is written over a solid horizontal line.

Tom Wallace
Chief Operating Officer, SecureTrust
November 19, 2019

**ATTACHMENT A - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY
VERSIONS IN-SCOPE**

Policy Name	Policy Version	Policy Date
SecureTrust Certificate Policy and Certification Practices Statement	Version 6.0	April 24, 2019
Trustwave Certificate Policy and Certification Practices Statement	Version 5.2	November 14, 2018
Trustwave Certificate Policy and Certification Practices Statement	Version 5.1	October 1, 2018

ATTACHMENT B - IN-SCOPE CAs

Root CAs

Subject DN	SHA2 Thumbprint	Valid From	Valid To
CN = XRamp Global Certification Authority O = XRamp Security Services Inc OU = www.xrampsecurity.com C = US	CECDDC905099D8DADFC5B1D209B737CBE2C18CFB2C10C0FF0BCF0D3286FC1AA2	11/1/2004	1/1/2035
CN = SecureTrust CA O = SecureTrust Corporation C = US	F1C1B50AE5A20DD8030EC9F6BC24823DD367B5255759B4E71B61FCE9F7375D73	11/7/2006	12/31/2029
CN = Secure Global CA O = SecureTrust Corporation C = US	4200F5043AC8590EBB527D209ED1503029FBCBD41CA1B506EC27F15ADE7DAC69	11/7/2006	12/31/2029
CN = Trustwave Global Certification Authority O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	97552015F5DDFC3C8788C006944555408894450084F100867086BC1A2BB58DC8	8/23/2017	8/23/2042

Subject DN	SHA2 Thumbprint	Valid From	Valid To
CN = Trustwave Global ECC P256 Certification Authority O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	945BBC825EA554F489D1FD51A73DDF2EA624AC7019A05205225C22A78CCFA8B4	8/23/2017	8/23/2042
CN = Trustwave Global ECC P384 Certification Authority O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	55903859C8C0C3EBB8759ECE4E2557225FF5758BBD38EBD48276601E1BD58097	8/23/2017	8/23/2042

SSL/TLS Issuing CAs

Subject DN	SHA2 Thumbprint	Valid From	Valid To
E = ca@trustwave.com CN = Trustwave Extended Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	EEA36C0FFA3F54FFDB0CF14B3BD34A53EC7B775F54053DD8B07DFD2F8BEC9083	10/13/2014	10/10/2024
E = ca@trustwave.com CN = Trustwave Extended Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	49C58270F70F1BE0B7C19D1BC2C2EBC41E2FDE0D4885D4FA65EF0370ACEC7A00	9/1/2016	9/29/2024
E = ca@trustwave.com CN = Trustwave Secure Global Extended Validation CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	45B2B08E1B58948A028BE13A67C0E20D4B2466AE2B6EC6250EBB10FD6B7F8239	8/12/2015	8/9/2025
E = ca@trustwave.com CN = Trustwave XRamp Global Extended Validation CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	1D0CD7EF3C19265508E20E58B3538964F4A11ADEC8A71D8AB8A8AFF15683C6AE	8/12/2015	8/9/2025
C = US S = Illinois L = Chicago O = SecureTrust CN = SecureTrust Extended Validation CA, Level 1	DD23355C61D59970423004729795CAEF77AFDB39767A795740D4E04CB6158A99	1/29/2019	1/29/2029

Subject DN	SHA2 Thumbprint	Valid From	Valid To
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global Extended Validation CA, Level 1	18626A3B7211128D563469C654557D13C9366D7FCEC8B94DB4F0AA7E05944041	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-256 Extended Validation CA, Level 1	275BF0046E0270178B13B67E4DB150A10197CB71F9A061FAD36B3D76639FE186	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-384 Extended Validation CA, Level 1	29F8E104DF38E612BF4F505365B5D0B0B20DD4E89C908306484EB8374C1E66D8	2/6/2018	2/24/2028
E = ca@trustwave.com CN = Trustwave Organization Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	FF1E0D233196B7EC20BEDFC65988E0AE1985EC6AC332A79ADFFE71B86BC0208A	10/1/2014	9/28/2024
E = ca@trustwave.com CN = Trustwave Organization Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	58EA0688B7909AAA8EAAA2FFF36F3BBE8F4A2AD03BD70243B3903469DB4890F7	9/1/2016	9/29/2024

Subject DN	SHA2 Thumbprint	Valid From	Valid To
C = US S = Illinois L = Chicago O = SecureTrust CN = SecureTrust Organization Validation CA, Level 1	11D9330D1A2398508DD50D3094EB28B1B44900D9928F8C22B25EF7A781BDB403	1/29/2019	1/29/2029
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global Organization Validation CA, Level 1	2E63DC1BECF427F9902B49DE6330FD3E8EEBF88B14E653B3BA2E37D4E4880965	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-256 Organization Validation CA, Level 1	18ABD6E9CA907BB36754D0C046EBB50DD9B95D527824D9581A31B750FCFDBAEF	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-384 Organization Validation CA, Level 1	87D42169B2693551CA205CCF17F06F6E6651F7218CD6D26607BF5BA4DD2F26F2	2/6/2018	2/24/2028
E = ca@trustwave.com CN = Trustwave Domain Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	859968F9278B4DC82EE30FD118A5D297D284B687CB64CF9755AB8A9D38F2B70F	10/1/2014	9/28/2024

Subject DN	SHA2 Thumbprint	Valid From	Valid To
E = ca@trustwave.com CN = Trustwave Domain Validation SHA256 CA, Level 1 O = Trustwave Holdings, Inc. L = Chicago S = Illinois C = US	74F56E1AB339D83E80F2F6E264F894775B426C89B44703DF4FA8A3231163A2BD	9/1/2016	9/29/2024
C = US S = Illinois L = Chicago O = SecureTrust CN = SecureTrust Domain Validation CA, Level 1	5E60965804461930AC27B6DBE3445679EAE4131C22AFB88AF7ACF6A1917B5ABA	1/29/2019	1/29/2029
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global Domain Validation CA, Level 1	6782C6E9ADBF9216E268306D46333FBC674BDEDF86B67BE777079E2C0E36888E	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-256 Domain Validation CA, Level 1	F62E35AAD345FB253863CFC0E65823ACD3E7F0846D19B8326D709C7919A22D7E	2/6/2018	2/24/2028
C = US S = Illinois L = Chicago O = Trustwave Holdings, Inc. CN = Trustwave Global ECDSA P-384 Domain Validation CA, Level 1	C63DF9618FBAF48662BA12ABE87B212CF777C27A446A0FA555D7A9D191148ED7	2/6/2018	2/24/2028