PAG
PRINCETON AUDIT GROUP

AICPA/Certification Authority

SSL Baseline with Network Security version 2.3

Independent Auditors Report

December 1, 2018 to November 15, 2019

TrustCor Systems S. de R.L.

Toronto, Canada.

SECTION 1

AUDIT REPORT

A Certified Public Accounting Firm

30 F Chicopee Drive
Princeton, NJ, 08540
Phone: 609-851-2713
www.princetonauditgroup.com

Independent Service Auditor's Report

Year 2019

Princeton Audit Group (PAG)

A Certified Public Accounting Firm

30 F Chicopee Drive
Princeton, NJ, 08540
Phone: 609-851-2713
www.princetonauditgroup.com

The Board of Directors
TrustCor Systems S. de R.L.
371 Front Street West, #227
Toronto, ON. M5V 3S8
CANADA

We have examined the assertion by the management of TrustCor Systems S. de R.L. (TrustCor-CA) for its Certification Authority (CA) operations at Toronto, Ontario, Canada, throughout the period December 1st, 2018 to November 15th, 2019 for its CAs as enumerated in Attachment A, in scope for the SSL Baseline Requirements and Network Security Requirements, TrustCor-CA has:

- Disclosed its SSL certificate lifecycle management business practices in its:
  - ➢ TrustCor CA Certification Practice Statement v 1.5.1 ; and
  - ➢ TrustCor CA Certificate Policy v 1.5.1 ,

  including its commitment to provide SSL certificates in conformance with the CA/Browser Forum Requirements on the TrustCor-CA website, 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 (for registration activities performed by TrustCor-CA)

- 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.

And, for CAs as enumerated in Attachment A :

- 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. TrustCor-CA's management is responsible for its assertion and for specifying the aforementioned Criteria. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). 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.

TrustCor-CA management has disclosed to us the attached matters (Attachment B) that have been posted publicly in the online forums of the Mozilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum. We have considered the nature of these comments in determining the nature, timing and extent of our procedures.

The relative effectiveness and significance of specific controls at TrustCor-CA 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. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, TrustCor-CA'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.

In our opinion TrustCor-CA's 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 TrustCor-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3 criteria, nor the suitability of any TrustCor-CA's services for any customer's intended purpose.

TrustCor-CA's use of the WebTrust for Certification Authorities — SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update the report or provide any additional assurance.

Vijay Khosla, CPA.CITP, CISA, CISM.

V Khosla

Managing Partner

11/15/2019

Princeton Audit Group, Inc.
Princeton, New Jersey 08540
www.princetonauditgroup.com

SECTION 2

TRUSTCOR SSL ASSERTION

TrustCor

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations in accordance with Baseline Requirements for SSL/TLS Certificates and Network Security during the period from December 1st, 2018 through November 15th, 2019

November 15, 2019

TrustCor Systems S. de R.L. ("TrustCor") operates the Certification Authority (CA) services known as the Root and Subordinate CAs, listed in Appendix A, in scope for the SSL Baseline Requirements and Network Security Requirements and provides SSL CA services.

The management of TrustCor is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure in its Certification Practice Statement disclosure on its website, and its SSL 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 TrustCor's CA operations. Furthermore because of changes in conditions, the effectiveness of controls may vary over time.

TrustCor management has assessed its disclosure of its controls over its CA operations. Based on that assessment, in TrustCor management's opinion, in providing its SSL Certification Authority (CA) services from its CA headquarters in Toronto [Ontario, Canada], with its data centers in Phoenix [Arizona, USA], during the period from December 1, 2018 through November 15, 2019, TrustCor has:

- Disclosed its SSL Certificate Life Cycle Management business practices in its:
  - Certificate Policy (version 1.5.1); and
  - Certification Practices Statement (version 1.5.1)

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the TrustCor website, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
  - subscriber information was properly authenticated (for the registration activities performed by TrustCor);
  - the integrity of keys and certificates which it managed were established and protected throughout their life cycles;

- Maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised 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.

- Maintained effective controls to provide reasonable assurances that its 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 – Version 2.3.

Rachel McPherson

Rachel McPherson
Vice President, Operations
November 15, 2019

ATTACHMENT "A"

Certification Practice Statement and Certificate Policy
VERSIONS USED DURING THE AUDIT PERIOD

- For the period: December 1st 2018 — April 19th 2019
  - Certification Practice Statement, version 1.4.2
  - Certificate Policy, version 1.4.2
- For the period: April 19th 2019 – October 21st 2019
  - Certification Practice Statement, version 1.5.0
  - Certificate Policy, version 1.5.0
- For the period: October 21st 2019 – November 15th 2019
  - Certification Practice Statement, version 1.5.1
  - Certificate Policy, version 1.5.1

Which describe the following in-scope Root and Subordinate CAs:

CA ID	Subject	Issuer	Serial	Key Type	Sig Alg	Not Before	Not After	SKI	SHA-256 Fingerprint
Root CA Certificates									
CA-1	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-1	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-1	da:9b:ec:71:f3:03:b0:19	RSA/4096	SHA256/RSA	Feb 4 12:32:16 2016 GMT	Dec 31 17:23:16 2029 GMT	EE:6B:49:3C:7A:3F:0D:E3:B1:09:B7:8A:C8:AB:19:9F:73:33:50:E7	d40e9c86cd8fe468c1776959f49ea774fa548684b6c406f3909261f4dce2575c
CA-2	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-2	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-2	25:a1:df:ca:33:cb:59:02	RSA/4096	SHA256/RSA	Feb 4 12:32:23 2016 GMT	Dec 31 17:26:39 2034 GMT	D9:FE:21:40:6E:94:9E:BC:9B:3D:9C:7D:98:20:19:E5:8C:30:62:B2	0753e940378c1bd5e3836e395daea5cb839e5046f1bd0eae1951cf10fec7c965
ECA-1	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor ECA-1	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor ECA-1	84:82:2c:5f:1c:62:d0:40	RSA/2048	SHA256/RSA	Feb 4 12:32:33 2016 GMT	Dec 31 17:28:07 2029 GMT	44:9E:48:F5:CC:6D:48:D4:A0:4B:7F:FE:59:24:2F:83:97:99:9A:86	5a885db19c01d912c5759388938cafbbdf031ab2d48e91ee15589b42971d039c

DV SSL Subordinate CA Certificates									
CA1-Site	C=PA, ST=Panama, O=TrustCor Systems S. de R.L., OU=TrustCor Network, CN=TrustCor Basic Secure Site (CA1)	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-1 [CA-1]	ff:04:3b:9f:67:7c:dc:49	RSA/ 4096	SHA512 /RSA	Feb 4 13:05:21 2016 GMT	Dec 30 16:20:10 2029 GMT	B7:38:A7:99:92:D7: C6:AA:4E:FB: 3E:D3:1C:4E:BD: 19:C8:E9:92:4D	fe1ecadbdee0e558068ddbc7b33ab78dd57d0dc22fcc1c360119010375b0a61b
CA1-Site 2048	C=PA, ST=Panama, O=TrustCor Systems S. de R.L., OU=TrustCor Network, CN=TrustCor Basic Secure Site 2048 (CA1)	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-1 [CA-1]	60:b9:a6:16:70:dd: 48:f9	RSA/ 2048	SHA256 /RSA	Feb 5 11:47:59 2016 GMT	Dec 30 16:20:10 2029 GMT	70:89:27:66:D4:13: BB:EE:03:57:1D: 89:52:94:89:09:19: 7B:6D:17	4efaaa1040ac2f44d3dee206d9522a288d84ec38ddf59298c926e02f4c9d9aef
OV SSL Subordinate CA Certificates									
CA2-Site	C=PA, ST=Panama, O=TrustCor Systems S. de R.L., OU=TrustCor Network, CN=TrustCor Enhanced Secure Site (CA2)	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-2 [CA-2]	96:6b:e5:90:bb:23:ef: 2a	RSA/ 4096	SHA512 /RSA	Feb 5 12:04:05 2016 GMT	Dec 30 16:20:10 2029 GMT	91:F7:F1:FC:8E:0A: 76:BE:FA:E6:00:05: AF:D7:02:A2:24:CD :5A:9E	3830db8ea1520b6cdf57e1e00a5f1297be11d9e6430c83607176212ff85d2db8
Email S/MIME Subordinate CA Certificates									
CA1-Email	C=PA, ST=Panama, O=TrustCor Systems S. de R.L., OU=TrustCor Network, CN=TrustCor Basic Secure Email (CA1)	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-1 [CA-1]	a6:0d:88:32:19:a3:fd: 59	RSA/ 4096	SHA512 /RSA	Feb 5 11:36:50 2016 GMT	Dec 30 16:20:10 2029 GMT	E4:0B:1D:5B: 9A:AA: 7E:C9:C6:6B: 64:38:76:71:C0:76: CA:97:29:3A	02bef922b32d46dfe7520b0ee7e3eaf588ee2b9cab81b84837e6b955e0759a90
CA2-Email	C=PA, ST=Panama, O=TrustCor Systems S. de R.L., OU=TrustCor Network, CN=TrustCor Enhanced Secure Email (CA2)	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor RootCert CA-2 [CA-2]	0a:f3:e6:12:40:47:17:52	RSA/ 4096	SHA512 /RSA	Feb 5 11:50:28 2016 GMT	Dec 30 16:20:10 2029 GMT	A8:25:C6:DE: 84:F4:28:7A:6C: 7A:A6:03:65:94:51: 0A:16:AC:C9:FE	a6d365161b58539cb44b29d77c648126f33db3c493116c3040e18de3e01a4242
Externally Operated CA Subordinate CA Certificates									
ECA-1 External	C=PA, ST=Panama, O=TrustCor Systems S. de R.L., OU=TrustCor Network, CN=TrustCor External PKI (ECA1)	C=PA, ST=Panama, L=Panama City, O=TrustCor Systems S. de R.L., OU=TrustCor Certificate Authority, CN=TrustCor ECA-1 [ECA-1]	82:25:5d:04:bf:64:fe: 9d	RSA/ 2048	SHA256 /RSA	Feb 5 12:10:46 2016 GMT	Dec 30 16:20:10 2029 GMT	66:C9:D2:44:CC:AD:A5:D6:96:D3:04:12:DF:1D:C5:88:0F: 5C:8D:BA	7882d9faa49a8bb351f0fc6ed685ef1fc51541d0ce0a4222074d1d9e16fdc30b

ATTACHMENT "B"

	Disclosure	Relevant WebTrust Criteria	Publicly Disclosed Link
1	Certificates with non-compliant serial numbers were issued wherein the serial number generation algorithm resulted in 63 bits of entropy instead of the required 64-bit serial numbers. There was a total of 5 impacted certificates, all owned by TrustCor, from first issuance on 11/30/2017 until last issuance on 12/20/2018. The issue was identified and validated on 02/25/2019.	Principle 2, Criterion number 2.1, Baseline Requirements Section 7.1 - The CA maintains controls to provide reasonable assurance that Root, Subordinate, and Subscriber certificates generated by the CA contain certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.	Bugzilla Link