Deloitte LLP
Bay Adelaide Centre, East Tower
8 Adelaide Street West
Suite 200
Toronto, ON M5H 0A9
Canada

Tel: +1 416 601 6150
Fax: +1 416 601 6400
www.deloitte.ca

INDEPENDENT ASSURANCE REPORT

To the management of Entrust Datacard doing business as AffirmTrust ("AffirmTrust"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on AffirmTrust management's statement that for its Certification Authority (CA) operations in Ottawa, Ontario, Canada and Toronto, Ontario, Canada throughout the period 1 March 2019 to 29 February 2020 (the "Period") for its CAs as enumerated in Attachment A, AffirmTrust has:

- disclosed its SSL certificate lifecycle management business practices in its Certification Practice Statements as enumerated on Attachment B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the AffirmTrust 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 the registration activities performed by AffirmTrust)

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

The information included in Attachment C, '*Other information provided by the CA'* is presented by the management of AffirmTrust to provide additional information to users of this report. This information has not been subjected to our procedures, and, accordingly, we express no opinion on it.

Certification authority's responsibilities

AffirmTrust's management is responsible for its statement, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Deloitte.

Auditor's responsibilities

Our responsibility is to express an opinion on management's statement based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information,* set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's statement is fairly stated, and, accordingly, included:

(1) obtaining an understanding of AffirmTrust's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of AffirmTrust's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at AffirmTrust 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.

Inherent limitations

Because of the nature and inherent limitations of controls, AffirmTrust's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised 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.

Other matters

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

	Matter topic	Matter description
1	**Serial numbers contain only 63 bits of entropy**	In February 2019, it was discovered that an open-source CA software used by some of the in-scope CAs had a bug where only 63 bits of entropy was used to generate certificate serial numbers despite the configuration specifying to use 64 bits. This impacted 7 Intermediate CA certificates and 1 end-entity certificate. 4 of the Intermediate CA certificates and 1 end-entity certificate were revoked as of 22 March 2019. 3 of the Intermediate CA certificates could not be revoked as they are in active production use. 6 of the Intermediate CA certificates were re-signed with serial numbers containing 127 bits of entropy on 21 March 2019.
2	**Legacy Inactive CAs not used during the Period and decommissioned**	The Legacy Inactive CAs (*Attachment A, CA #11 to 20*) did not issue certificates during the Period and remained in an inactive state.

Deloitte.

Basis for qualified opinion

During our procedures, we noted the following which caused a qualification of our opinion:

	Observation	Relevant WebTrust Criteria
1	During the Period, there were instances of some Certificate Systems not undergoing a Vulnerability Scan at least every three (3) months. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1, Principle 4, Criterion 4.3 to not be met. This observation was remediated as of 31 May 2019.	**P4, 4.3:** The CA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following: • Within one (1) week of receiving a request from the CA/Browser Forum; • After any system or network changes that the CA determines are significant; • and • At least every three (3) months

2	During the Period, there were instances where a technical control to restrict remote access to only those devices owned or controlled by AffirmTrust did not operate effectively.
	
	This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1, Principle 4, Criterion 2.15 to not be met.
	
	This observation was remediated as of 31 May 2019.
		P4, 2.15: The CA maintains controls to provide reasonable assurance that it restricts remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when:
		
		• The remote connection originates from a device owned or controlled by the CA or Delegated Third Party;
		• The remote connection is through a temporary, non-persistent encrypted channel that is supported by multifactor authentication; and
		• The remote connection is made to a designated intermediary device meeting the following:
		
		  • Located within the CA's network;
		  • Secured in accordance with the Network and Certificate System Security Requirements; and
		  • Mediates the remote connection to the Issuing System.

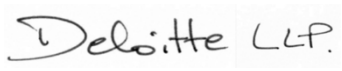
3	During the Period, user access reviews did not always include all relevant users and all relevant systems. Additionally, user access reviews were not performed with sufficient frequency to address the period of September – November 2019. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1, Principle 4, Criterion 2.10 to not be met. This observation was remediated as of 1 December 2019.	**P4, 2.10:** The CA maintains controls to provide reasonable assurance that it reviews all system accounts at least every three (3) months and deactivates any accounts that are no longer necessary for operations.

Deloitte.

Qualified opinion

In our opinion, except for the matters described in the preceding section entitled 'Basis for qualified opinion', throughout the period 1 March 2019 to 29 February 2020, AffirmTrust management's statement, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

This report does not include any representation as to the quality of AffirmTrust's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1, nor the suitability of any of AffirmTrust's services for any customer's intended purpose.



Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
17 April 2020

Deloitte.

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. AffirmTrust Commercial 2. AffirmTrust Networking 3. AffirmTrust Premium 4. AffirmTrust Premium ECC
DV SSL Issuing CAs
5. AffirmTrust Certificate Authority - DV1
OV SSL Issuing CAs
6. AffirmTrust Certificate Authority - OV1
EV SSL Issuing CAs
7. AffirmTrust Extended Validation CA - EV1 8. AffirmTrust Extended Validation CA - EV2 9. AffirmTrust Extended Validation CA - EV3 10. AffirmTrust Extended Validation CA - EVEC1
Legacy Inactive CAs
11. AffirmTrust Commercial Extended Validation CA 12. AffirmTrust Networking Extended Validation CA 13. AffirmTrust Premium Extended Validation CA 14. AffirmTrust Premium ECC Extended Validation CA 15. Trend Micro CA 16. Trend Micro S2 CA 17. AffirmTrust Commercial Extended Validation 18. AffirmTrust Networking Extended Validation 19. AffirmTrust Premium Extended Validation 20. AffirmTrust Premium ECC Extended Validation

Deloitte.

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
1	1	CN=AffirmTrust Commercial O=AffirmTrust C=US	CN=AffirmTrust Commercial O=AffirmTrust C=US	7777062726a9b17c	RSA 2048-bits	RSA SHA-256	2010-01-29 14:06:06 UTC	2030-12-31 14:06:06 UTC			9d93c6538b5ecaaf3f9f1e0fe59995bc24f6948f	0376ab1d54c5f9803ce4b2e201a0ee7eef7b57b636e8a93c9b8d4860c96f5fa7
2	1	CN=AffirmTrust Networking O=AffirmTrust C=US	CN=AffirmTrust Networking O=AffirmTrust C=US	7c4f04391cd4992d	RSA 2048-bits	RSA SHA-1	2010-01-29 14:08:24 UTC	2030-12-31 14:08:24 UTC			071fd2e79cdac26ea240b4b07a50105074c4c8bd	0a81ec5a929777f145904af38d5d509f66b5e2c58fcdb531058b0e17f3f0b41b
3	1	CN=AffirmTrust Premium O=AffirmTrust C=US	CN=AffirmTrust Premium O=AffirmTrust C=US	6d8c1446b1a60aee	RSA 4096-bits	RSA SHA-384	2010-01-29 14:10:36 UTC	2040-12-31 14:10:36 UTC			9dc067a60c22d926f545aba665521127d845ac63	70a73f7f376b60074248904534b11482d5bf0e698ecc498df52577ebf2e93b9a
4	1	CN=AffirmTrust Premium ECC O=AffirmTrust C=US	CN=AffirmTrust Premium ECC O=AffirmTrust C=US	7497258ac73f7a54	EC 384-bits	ECDSA SHA-384	2010-01-29 14:20:24 UTC	2040-12-31 14:20:24 UTC			9aaf297ac011353526513000c36afe40d5aed63c	bd71fdf6da97e4cf62d1647add2581b07d79adf8397eb4ecba9c5e8488821423
5	1	CN=AffirmTrust Certificate Authority - DV1 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Commercial O=AffirmTrust C=US	2c07cff96ce8689a	RSA 2048-bits	RSA SHA-256	2017-01-06 17:55:17 UTC	2030-12-02 04:00:00 UTC	2019-03-21 21:29:22 UTC	TLS Web Server Authentication, TLS Web Client Authentication	33df7a3e027996ebb60cc063fa75bf9222cd91fa	ed8be0e7f03bb876b42e4aaf437bf03a759885f9cc5bae36ded8a8bd8e14e47f
5	2	CN=AffirmTrust Certificate Authority - DV1 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Commercial O=AffirmTrust C=US	580e00b14e86ce35	RSA 2048-bits	RSA SHA-256	2017-04-07 15:10:56 UTC	2030-12-02 04:00:00 UTC		TLS Web Server Authentication, TLS Web Client Authentication	33df7a3e027996ebb60cc063fa75bf9222cd91fa	ca4389c89ddfc31bec26c74b44a8498c58b2d838516fa01b14f1393629e58a40
5	3	CN=AffirmTrust Certificate Authority - DV1 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Commercial O=AffirmTrust C=US	62b4c3eba53918177f127a837b574f96	RSA 2048-bits	RSA SHA-256	2019-03-21 20:21:37 UTC	2030-12-02 04:00:00 UTC		TLS Web Server Authentication, TLS Web Client Authentication	33df7a3e027996ebb60cc063fa75bf9222cd91fa	4563b936e35ab97576f5aef1935d9bc7e9977841f0573bd2e16bcac9534a6af9
6	1	CN=AffirmTrust Certificate Authority - OV1 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Commercial O=AffirmTrust C=US	187e7f3bf66f23cd	RSA 2048-bits	RSA SHA-256	2016-11-29 16:49:28 UTC	2030-12-02 04:00:00 UTC		TLS Web Server Authentication, TLS Web Client Authentication	fe60c30da4a29d214f7a784c62c5db14fc3978c4	ea4ee2faa57ae4b539b63977fe5bb205b6afb32f7a73b2b363e4be02cd8a91e9
6	2	CN=AffirmTrust Certificate Authority - OV1 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Commercial O=AffirmTrust C=US	53f6a611092e528ed963f19149532204	RSA 2048-bits	RSA SHA-256	2019-03-21 20:25:32 UTC	2030-12-02 04:00:00 UTC		TLS Web Server Authentication, TLS Web Client Authentication	fe60c30da4a29d214f7a784c62c5db14fc3978c4	b5fd6f800334f565036b0999f8310b5b0bd7268395d8b267005697af7301c5e8
7	1	CN=AffirmTrust Extended Validation CA - EV1 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Commercial O=AffirmTrust C=US	40f0bbaa8ae0c098	RSA 2048-bits	RSA SHA-256	2016-11-29 16:42:17 UTC	2030-12-02 04:00:00 UTC		TLS Web Server Authentication, TLS Web Client Authentication	dbef65370be547cb35d1901f03c1bc88c7a7ea80	cf88915cf996932c2b4cbe3039076d119bb728b4f31e49b63a5022fe65489a12
7	2	CN=AffirmTrust Extended Validation CA - EV1 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Commercial O=AffirmTrust C=US	1729551ed68e7fb1edf57300f35d7fd5	RSA 2048-bits	RSA SHA-256	2019-03-21 20:27:54 UTC	2030-12-02 04:00:00 UTC		TLS Web Server Authentication, TLS Web Client Authentication	dbef65370be547cb35d1901f03c1bc88c7a7ea80	ed3c991466cbc45b5fd1da281028f9587b8219523647e0ca1b47f2c527d2920f
8	1	CN=AffirmTrust Extended Validation CA - EV2 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Premium O=AffirmTrust C=US	72c3c67f9b2c457b	RSA 2048-bits	RSA SHA-256	2017-05-30 20:15:21 UTC	2030-12-02 04:00:00 UTC	2019-03-21 21:18:18 UTC	TLS Web Server Authentication, TLS Web Client Authentication	737c9a38683c517c4108fea11f2a1eb461dbcd3c	a9ebcfba0299a10436c4c41a2bd75933cb2c7960cf780267ecbe3d5229c19c76
8	2	CN=AffirmTrust Extended Validation CA - EV2 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Premium O=AffirmTrust C=US	5371c8eb0784fd5108e5d4f3e323ec46	RSA 2048-bits	RSA SHA-256	2019-03-21 20:46:35 UTC	2030-12-02 04:00:00 UTC		TLS Web Server Authentication, TLS Web Client Authentication	737c9a38683c517c4108fea11f2a1eb461dbcd3c	9df77488c4b74ac32e3cec4c643d001d5c3babfa4001ffd193dca10c8be5cb3a
9	1	CN=AffirmTrust Extended Validation CA - EV3 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Networking O=AffirmTrust C=US	532092e1e00a15b5	RSA 2048-bits	RSA SHA-256	2017-05-30 20:29:49 UTC	2030-12-02 04:00:00 UTC	2019-03-21 21:22:13 UTC	TLS Web Server Authentication, TLS Web Client Authentication	791eb1c917c71eacb1c714d7c3e87fbcb9509b15	6b63ec3becdecf9f9127235c0995f578d66f77b14d1c7f0fdc2dc060f3c78dd6
9	2	CN=AffirmTrust Extended Validation CA - EV3 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Networking O=AffirmTrust C=US	3424a1ecf8f0a35fe746b7011c43e844	RSA 2048-bits	RSA SHA-256	2019-03-21 20:38:59 UTC	2030-12-02 04:00:00 UTC		TLS Web Server Authentication, TLS Web Client Authentication	791eb1c917c71eacb1c714d7c3e87fbcb9509b15	b700ba49af4d19e72fb15a2dac3c213ba44c319fa7da92772b3682e12b781093
10	1	CN=AffirmTrust Extended Validation CA - EVEC1 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Premium ECC O=AffirmTrust C=US	0ad0428f14541475	EC 384-bits	ECDSA SHA-384	2017-05-30 20:40:17 UTC	2030-12-02 04:00:00 UTC	2019-03-21 21:13:30 UTC	TLS Web Server Authentication, TLS Web Client Authentication	c6908c0283d75de3be3b9c2ed5657d2a1060eee5	59518fc1ef1c337ef34f601e30e623df4d07d3a7b6e402bca2be6e027385c7b8
10	2	CN=AffirmTrust Extended Validation CA - EVEC1 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Premium ECC O=AffirmTrust C=US	0202a584c134064dc9f32d207ea37298	EC 384-bits	ECDSA SHA-384	2019-03-21 20:55:07 UTC	2030-12-02 04:00:00 UTC		TLS Web Server Authentication, TLS Web Client Authentication	c6908c0283d75de3be3b9c2ed5657d2a1060eee5	cde23a52303c3ca67a4bbbcc9582ff5c9203aa98cb0f387139308ce2289506a2

Deloitte.

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
11	1	CN=AffirmTrust Commercial Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Commercial O=AffirmTrust C=US	2926357ea5ca133e	RSA 2048-bits	RSA SHA-256	2010-04-22 02:08:03 UTC	2030-12-31 14:06:06 UTC			a6a117b8ec06ba3e215a8eb82840e1512d4426dc	62f692b7447953d4205ab31b4e34d45a02a12ca45654af8270fecd89e2db3e47
11	2	CN=AffirmTrust Commercial Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Commercial O=AffirmTrust C=US	631bf90c8ab02c81	RSA 2048-bits	RSA SHA-256	2010-05-18 01:36:45 UTC	2030-12-31 14:06:06 UTC			a6a117b8ec06ba3e215a8eb82840e1512d4426dc	241136327dc0aec84973d1fa9b2d0dc027797037ae3ed654564e3b85fc7db221
12	1	CN=AffirmTrust Networking Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Networking O=AffirmTrust C=US	7c519f91f6c988fa	RSA 2048-bits	RSA SHA-1	2010-04-22 02:14:01 UTC	2030-12-31 14:08:24 UTC			7df8b24c5425085d6d27c9ab2b01c33570798064	caf19845b5f9b658f52c3d9aa73a2fcb2a1965fa1f65b54778aab20f1fc720c3
12	2	CN=AffirmTrust Networking Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Networking O=AffirmTrust C=US	239015c7f6788046	RSA 2048-bits	RSA SHA-1	2010-05-18 01:39:24 UTC	2030-12-31 14:08:24 UTC			7df8b24c5425085d6d27c9ab2b01c33570798064	dd0c0be9ce09041f16b72d6b3d62a5b8f538427ec1a42d8331af1b59dfe69446
12	3	CN=AffirmTrust Networking Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Networking O=AffirmTrust C=US	5f0accb65a6bf800	RSA 2048-bits	RSA SHA-256	2015-04-19 22:09:29 UTC	2030-12-31 14:08:24 UTC			7df8b24c5425085d6d27c9ab2b01c33570798064	af639dc0bbb168eff75b15117d888937eb64c1b0453f168d1b8c52ecf04acb93
13	1	CN=AffirmTrust Premium Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium O=AffirmTrust C=US	47c8c927f9f291a1	RSA 4096-bits	RSA SHA-384	2010-04-22 02:16:52 UTC	2040-12-31 14:10:36 UTC			bcdd46bbe4a242fd89d1e6791fd71e41a947fb50	1acdc91964bcfacb317c76eacf1d2dadbe3daff05538a8d4d2cce06e20745fa1
13	2	CN=AffirmTrust Premium Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium O=AffirmTrust C=US	0bcfcf3759c2f586	RSA 4096-bits	RSA SHA-384	2010-05-18 01:40:33 UTC	2040-12-31 14:10:36 UTC			bcdd46bbe4a242fd89d1e6791fd71e41a947fb50	66566fedd60db3ae10910f2a89707cf5159092033a71a75cd86851d735919411
13	3	CN=AffirmTrust Premium Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium O=AffirmTrust C=US	0974f448192f94c4	RSA 4096-bits	RSA SHA-384	2015-09-09 03:04:29 UTC	2030-12-31 11:59:59 UTC			bcdd46bbe4a242fd89d1e6791fd71e41a947fb50	565657f55dd94d6b6e54e132df2a3c9a241c027def14f12d46625e55e9cf58b7
13	4	CN=AffirmTrust Premium Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium O=AffirmTrust C=US	5d544509a0d60aa7	RSA 4096-bits	RSA SHA-384	2015-09-16 02:50:04 UTC	2040-12-31 11:59:59 UTC			bcdd46bbe4a242fd89d1e6791fd71e41a947fb50	d57b9872b1eef8e8032ab2e8cb0e63b685d1655c51c454f23f9975dfa2ad7e0a
14	1	CN=AffirmTrust Premium ECC Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium ECC O=AffirmTrust C=US	5fbc0e888ea4da20	EC 384-bits	ECDSA SHA-384	2010-04-22 02:19:25 UTC	2040-12-31 14:20:24 UTC			01072f8a132c020ea058064ba2a6be08227f26ad	f5d174906c36057fe0dc3b450ea1738612605f9251b12d3103b8be86333ef77f
14	2	CN=AffirmTrust Premium ECC Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium ECC O=AffirmTrust C=US	19269f5e035dfe4b	EC 384-bits	ECDSA SHA-384	2010-04-22 02:20:43 UTC	2040-12-31 14:20:24 UTC			01072f8a132c020ea058064ba2a6be08227f26ad	4e513974092730d1a83f43dcb8ef2621793f51a126d36714f49fe8f639effec0
14	3	CN=AffirmTrust Premium ECC Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium ECC O=AffirmTrust C=US	107caa12ecd68c54	EC 384-bits	ECDSA SHA-384	2010-05-18 01:48:14 UTC	2040-12-31 14:20:24 UTC			01072f8a132c020ea058064ba2a6be08227f26ad	5adcc54514916b02dbf5e065952e9c130bec59421e0fea1ce9647f02050b7ec6
14	4	CN=AffirmTrust Premium ECC Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium ECC O=AffirmTrust C=US	0340f9459bf3d9fe	EC 384-bits	ECDSA SHA-384	2015-09-09 03:05:22 UTC	2030-12-31 11:59:59 UTC			01072f8a132c020ea058064ba2a6be08227f26ad	af872aa2d241957b11608c8e0601a8e2f34b823024f2b24e58bb1b78f00b5e0c
14	5	CN=AffirmTrust Premium ECC Extended Validation CA OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium ECC O=AffirmTrust C=US	2b44f713df170c16	EC 384-bits	ECDSA SHA-384	2015-09-16 02:49:03 UTC	2040-12-31 11:59:59 UTC			01072f8a132c020ea058064ba2a6be08227f26ad	077b75f6b7fa71be4f8121e1ec52faebca0d0aed2dc01711a0f6dcdc38e7bf38
15	1	CN=Trend Micro CA O=Trend Micro Inc C=US	CN=AffirmTrust Networking O=AffirmTrust C=US	4f0c2f8ec227f9ae	RSA 2048-bits	RSA SHA-1	2011-10-04 18:11:57 UTC	2030-12-31 14:08:24 UTC			ad31c7fa02ce67f7651cfbba5fc0bbc5504c67c8	a0dd71da35f5a24301c18b3bcf74b5b62b48fdd667cba3e05fc46956bdea5d93
15	2	CN=Trend Micro CA O=Trend Micro Inc C=US	CN=AffirmTrust Networking O=AffirmTrust C=US	2eed7b3dab645b10	RSA 2048-bits	RSA SHA-1	2011-10-04 18:24:29 UTC	2030-12-31 14:08:24 UTC			ad31c7fa02ce67f7651cfbba5fc0bbc5504c67c8	58c95d17907e743e121cef47d48064d7b3af32b514bea3ef74d290a52d70b96c
15	3	CN=Trend Micro CA O=Trend Micro Inc C=US	CN=AffirmTrust Networking O=AffirmTrust C=US	5af80e98c1530a58	RSA 2048-bits	RSA SHA-1	2011-10-22 19:14:42 UTC	2030-12-31 14:08:24 UTC			ad31c7fa02ce67f7651cfbba5fc0bbc5504c67c8	3f0ae5b3d05652472a108c28546364b31b5a33d01528b555feab21afaebb5b3a
15	4	CN=Trend Micro CA O=Trend Micro Inc C=US	CN=AffirmTrust Networking O=AffirmTrust C=US	3d847c1b4abb3202	RSA 2048-bits	RSA SHA-1	2014-04-29 02:25:55 UTC	2030-12-31 14:08:24 UTC			ad31c7fa02ce67f7651cfbba5fc0bbc5504c67c8	938c4557589b7263d59b2f0f6b84cbeb27efb9b23ba724eb3ccd5b7e2a58716f

Deloitte.

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
16	1	CN=Trend Micro S2 CA O=Trend Micro Inc C=US	CN=AffirmTrust Commercial O=AffirmTrust C=US	5b469990ec759d34	RSA 2048-bits	RSA SHA-256	2014-03-01 23:13:48 UTC	2030-12-31 14:06:06 UTC			b099e1904ef36563289c123f7856ba84c0c73a3d	8cd591f3314bd57bac74b3faee2d70471b5d996a4fe197e64380abaf9e8b3133
17	1	CN=AffirmTrust Commercial Extended Validation OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Commercial O=AffirmTrust C=US	6cf34fe998b2b13a	RSA 2048-bits	RSA SHA-256	2010-01-29 14:13:08 UTC	2030-12-31 14:06:06 UTC			8ef10a21466a38a4c85b21167ef56c9a8eee1efe	c6f613a20b0c98aa9ed4a7e25d4dd19f370a41a3e57efd4ecb0dfd7aeef8c278
18	1	CN=AffirmTrust Networking Extended Validation OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Networking O=AffirmTrust C=US	1c915ed11d3c8994	RSA 2048-bits	RSA SHA-1	2010-01-29 14:15:31 UTC	2030-12-31 14:08:24 UTC			c42bad000f672c6d3c3775d67d3e9dd19c5a5cd8	3ca196de120acc3f6e680ef9c5cdfc39ef89f0fdd33bd68e524025358446a94e
19	1	CN=AffirmTrust Premium Extended Validation OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium O=AffirmTrust C=US	56f1bc77c11d417d	RSA 4096-bits	RSA SHA-384	2010-01-29 14:18:04 UTC	2040-12-31 14:10:36 UTC			684de243d25cbc4152e4b42f518b007f9a01da78	52e3e25bb3a162f210b89c7af98776b259cc9b525aafd24b1a35998438efa94c
20	1	CN=AffirmTrust Premium ECC Extended Validation OU=http://www.affirmtrust.com/resources O=AffirmTrust C=US	CN=AffirmTrust Premium ECC O=AffirmTrust C=US	7b80f268cb93ef80	EC 384-bits	ECDSA SHA-384	2010-01-29 14:23:02 UTC	2040-12-31 14:20:24 UTC			7edbf6081bd80b5e52d979841cc142aa318f1b45	4bd76adb9ad30ef667037bba662393317500595acbd4f0a75e4249daf48ccf85

Deloitte.

ATTACHMENT B

LIST OF AFFIRMTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
AffirmTrust Certification Practice Statement	3.5	12 Oct 2018
AffirmTrust Certification Practice Statement	3.6	31 May 2019
AffirmTrust Certification Practice Statement	3.7	25 Jul 2019
AffirmTrust Certification Practice Statement	3.8	30 Sep 2019

Deloitte.

ATTACHMENT C

Other information provided by the CA

The information included herein is presented by the management of AffirmTrust to provide additional information to users of this report. This information has not been subjected to the procedures of this engagement, and, accordingly, Deloitte LLP express no opinion on it.

Comments on other matters

	Matter topic	Additional AffirmTrust comments
1	**Serial numbers contain only 63 bits of entropy**	Problem has been addressed and disclosed per https://bugzilla.mozilla.org/show_bug.cgi?id=1536287.

AFFIRMTRUST™

AFFIRMTRUST MANAGEMENT'S STATEMENT

Entrust Datacard doing business as AffirmTrust ("AffirmTrust") operates the Certification Authority (CA) services as enumerated in Attachment A, and provides SSL CA services.

The management of AffirmTrust is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate system controls, its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and 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 only provide reasonable assurance with respect to AffirmTrust's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

AffirmTrust management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in AffirmTrust management's opinion, in providing its SSL and non-SSL Certification Authority (CA) services at Ottawa, Ontario, and Toronto, Ontario, throughout the period 1 March 2019 to 29 February 2020, AffirmTrust has:

- disclosed its SSL certificate lifecycle management business practices in its Certification Practice Statements as enumerated on Attachment B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the AffirmTrust 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 the registration activities performed by AffirmTrust)

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

Bruce Morton
Director, Entrust Certificate Manager
17 April 2020

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. AffirmTrust Commercial 2. AffirmTrust Networking 3. AffirmTrust Premium 4. AffirmTrust Premium ECC
DV SSL Issuing CAs
5. AffirmTrust Certificate Authority - DV1
OV SSL Issuing CAs
6. AffirmTrust Certificate Authority - OV1
EV SSL Issuing CAs
7. AffirmTrust Extended Validation CA - EV1 8. AffirmTrust Extended Validation CA - EV2 9. AffirmTrust Extended Validation CA - EV3 10. AffirmTrust Extended Validation CA - EVEC1
Legacy Inactive CAs
11. AffirmTrust Commercial Extended Validation CA 12. AffirmTrust Networking Extended Validation CA 13. AffirmTrust Premium Extended Validation CA 14. AffirmTrust Premium ECC Extended Validation CA 15. Trend Micro CA 16. Trend Micro S2 CA 17. AffirmTrust Commercial Extended Validation 18. AffirmTrust Networking Extended Validation 19. AffirmTrust Premium Extended Validation 20. AffirmTrust Premium ECC Extended Validation

ATTACHMENT B

LIST OF AFFIRMTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
AffirmTrust Certification Practice Statement	3.5	12 Oct 2018
AffirmTrust Certification Practice Statement	3.6	31 May 2019
AffirmTrust Certification Practice Statement	3.7	25 Jul 2019
AffirmTrust Certification Practice Statement	3.8	30 Sep 2019