Deloitte.

Deloitte LLP
Bay Adelaide Centre, East Tower
22 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 Ltd. doing business as AffirmTrust ("AffirmTrust"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on AffirmTrust management's assertion that for its Certification Authority (CA) operations in Ottawa, Ontario, Canada and Toronto, Ontario, Canada throughout the period 1 June 2017 to 28 February 2018 (the "Period") for its CAs as enumerated in Attachment A, AffirmTrust has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its Certification Practice Statements as enumerated in Attachment B, including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines 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 EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by AffirmTrust)

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.0.

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 assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.0.

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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion 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 assertion is fairly stated, and, accordingly, included:

(1) obtaining an understanding of AffirmTrust’s EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
(2) selectively testing transactions executed in accordance with disclosed EV 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	**EV2, EV3, and EVEC1 CAs placed in production**	The EV2, EV3, and EVEC1 Issuing CAs (*Attachment A, CA #8 to 10*) were cross-signed by the Premium, Networking, and Premium ECC Roots respectively (*Attachment A, CA #3, 2, and 4*) on 30 May 2017 and placed into production on 1 June 2017. These CA’s respective asymmetric key pairs were generated within their secure cryptographic modules on 4 May 2017 and remained in a non-active state until 30 May 2017.
2	**Certificates issued containing metadata in the jurisdictionST subject field**	33 certificates issued from the EV1 CA during the Period contained metadata of ‘???’ in the jurisdictionST subject field. The correct jurisdiction information in non-Latin characters was captured in the registration authority system and was subject to standard verification procedures. A technical encoding issue when the information was transferred from the registration authority system to the CA system to issue the certificate resulted in the non-Latin characters being replaced by question marks. Relevant patches were applied to correct this issue on 19 April 2017.

Opinion

In our opinion, throughout the period 1 June 2017 to 28 February 2018, AffirmTrust management’s assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.0.

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 – Extended Validation SSL v1.6.0, nor the suitability of any of AffirmTrust's services for any customer's intended purpose.

Use of the WebTrust seal

AffirmTrust's use of the WebTrust for Certification 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.

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
21 May 2018

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs

1. AffirmTrust Commercial
2. AffirmTrust Networking
3. AffirmTrust Premium
4. AffirmTrust Premium ECC

EV SSL Issuing CAs

5. AffirmTrust Extended Validation CA - EV1
6. AffirmTrust Extended Validation CA - EV2
7. AffirmTrust Extended Validation CA - EV3
8. AffirmTrust Extended Validation CA - EVEC1

Deloitte.

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	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 Extended Validation CA - EV1 OU=See www.affirmtrust.com/repository O=AffirmTrust C=CA	CN=AffirmTrust Commercial O=AffirmTrust C=US	0bcc5321d219ce0c	RSA 2048-bits	RSA SHA-256	2016-11-28 21:17:29 UTC	2030-12-02 04:00:00 UTC	TLS Web Server Authentication, TLS Web Client Authentication	dbef65370be547cb35d1901f03c1bc88c7a7ea80	1e4ad482c8f9b6157bd8aeac27e5a0f02b06a2cb373dfae889fe798bf523f3ec
5	2	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
6	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	TLS Web Server Authentication, TLS Web Client Authentication	737c9a38683c517c4108fea11f2a1eb461dbcd3c	a9ebcfba0299a10436c4c41a2bd75933cb2c7960cf780267ecbe3d5229c19c76
7	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	TLS Web Server Authentication, TLS Web Client Authentication	791eb1c917c71eacb1c714d7c3e87fbcb9509b15	6b63ec3becdecf9f9127235c0995f578d66f77b14d1c7f0fdc2dc060f3c78dd6
8	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	TLS Web Server Authentication, TLS Web Client Authentication	c6908c0283d75de3be3b9c2ed5657d2a1060eee5	59518fc1ef1c337ef34f601e30e623df4d07d3a7b6e402bca2be6e027385c7b8

Deloitte.

ATTACHMENT B

LIST OF AFFIRMTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
AffirmTrust Certification Practice Statement	3.1	06-Mar-2017
AffirmTrust Certification Practice Statement	3.2	8-Dec-2017

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
2	**Certificates issued containing metadata in the jurisdictionST subject field**	All customers were advised of this issue shortly after it was discovered and were given the option to revoke and replace their certificates.

AFFIRMTRUST™

AFFIRMTRUST MANAGEMENT'S ASSERTION

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

The management of AffirmTrust is responsible for establishing and maintaining effective controls over EV SSL CA operations, including its EV SSL CA business practices disclosure on its website, EV SSL key lifecycle management controls, and EV 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 EV SSL CA services. Based on that assessment, in AffirmTrust management's opinion, in providing its EV SSL Certification Authority (CA) services at Ottawa, Ontario, and Toronto, Ontario throughout the period 1 June 2017 to 28 February 2018, AffirmTrust has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its Certification Practice Statements as enumerated in Attachment B, including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines 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 EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by AffirmTrust)

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.0.

Bruce Morton
CA Operations Manager
21 May 2018

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. AffirmTrust Commercial 2. AffirmTrust Networking 3. AffirmTrust Premium 4. AffirmTrust Premium ECC
EV SSL Issuing CAs
5. AffirmTrust Extended Validation CA - EV1 6. AffirmTrust Extended Validation CA - EV2 7. AffirmTrust Extended Validation CA - EV3 8. AffirmTrust Extended Validation CA - EVEC1

AFFIRMTRUST™

ATTACHMENT B

LIST OF AFFIRMTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
AffirmTrust Certification Practice Statement	3.1	06-Mar-2017
AffirmTrust Certification Practice Statement	3.2	8-Dec-2017