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 Corporation 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 2023 to 29 February 2024 (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:
  - Certificate Policy/ Certification Practice Statements ("CP/CPS") as enumerated in Attachment B

  including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the Entrust 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 v1.8.

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 – Extended Validation SSL v1.8.

Our independence and quality management

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 Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner'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 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.

Deloitte.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls 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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Other matters

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

	Matter topic	Matter description
1	**CA not issuing SSL certificates during the Period**	The CA #11 in Attachment A, did not issue any SSL certificates during the Period.

Basis for qualified opinion

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

#	Observation	Relevant WebTrust Criteria
1	As publicly disclosed in Bugzilla 1883843, there were 24 EV SSL certificates issued with cPSuri removed in the policy qualifiers. As a result, a criterion of Principle 2 - 2.2.2 of WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8 has not been met.	**P2 - 2.2.2:** The CA maintains controls to provide reasonable assurance that EV SSL Certificates issued include the minimum requirements for the content of EV SSL Certificates, including: • Certificate Policy Identification requirements • Subscriber Public Key • Certificate Serial Number • Additional Technical Requirements for EV Certificates as established in the EV SSL Guidelines relating to: • EV SSL Subscriber Certificates • EV Subordinate CA Certificates
2	As publicly disclosed in Bugzilla 1886532, for those mis-issued EV SSL certificates reported in Bugzilla 1883843, AffirmTrust did not revoke the impacted certificates within 5 days. As of 30 April 2024, the revocation of impacted certificates was still in progress. As a result, a criterion of Principle 2 - 5.3 of WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8 has not been met.	**P2 - 5.3:** The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or 4. The CA obtains evidence that the validation of domain authorization or control for any Fully–Qualified Domain Name or IP address in the Certificate should not be relied upon.

Deloitte.

#	Observation	Relevant WebTrust Criteria
		And, Subscriber Certificates are revoked within 5 days if any of the following events occurs: 1. The Certificate no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6; 2. The CA obtains evidence that the Certificate was misused; 3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use; 4. The CA is made aware of any circumstance indicating that use of a Fully–Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); 5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully–Qualified Domain Name; 6. The CA is made aware of a material change in the information contained in the Certificate; 7. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement; 8. The CA determines that any of the information appearing in the Certificate is inaccurate; 9. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; 10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or 11. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Opinion

In our opinion, except for the matters described in the preceding section entitled 'Basis for qualified opinion', throughout the period 1 March 2023 to 29 February 2024, 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 – Extended Validation SSL v1.8.

Deloitte.

This report does not include any representation as to the quality of Entrust's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8, nor the suitability of any of Entrust's services for any customer's intended purpose.

Use of the WebTrust seal

AffirmTrust's use of the WebTrust for Certification Authorities – Extended Validation SSL 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

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
May 21, 2024

Deloitte.

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
DV SSL Issuing CAs
9. AffirmTrust Certificate Authority – DV1 10. AffirmTrust Certificate Authority – DVTLS1
OV SSL Issuing CAs
11. AffirmTrust Certificate Authority - OV1

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	2030-12-31 14:06:06			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	2030-12-31 14:08:24			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	2040-12-31 14:10:36			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	2040-12-31 14:20:24			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	40f0bbaa8ae0c098	RSA 2048-bits	RSA SHA-256	2016-11-29 16:42:17	2030-12-02 04:00:00		TLS Web Server Authentication, TLS Web Client Authentication	dbef65370be547cb35d1901f03c1bc88c7a7ea80	CF88915CF996932C2B4CBE3039076D119BB728B4F31E49B63A5022FE65489A12
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	1729551ed68e7fb1edf57300f35d7fd5	RSA 2048-bits	RSA SHA-256	2019-03-21 20:27:54	2030-12-02 04:00:00		TLS Web Server Authentication, TLS Web Client Authentication	dbef65370be547cb35d1901f03c1bc88c7a7ea80	ED3C991466CBC45B5FD1DA281028F9587B8219523647E0CA1B47F2C527D2920F
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	5371c8eb0784fd5108e5d4f3e323ec46	RSA 2048-bits	RSA SHA-256	2019-03-21 20:46:35	2030-12-02 04:00:00		TLS Web Server Authentication, TLS Web Client Authentication	737c9a38683c517c4108fea11f2a1eb461dbcd3c	9DF77488C4B74AC32E3CEC4C643D001D5C3BABFA4001FFD193DCA10C8BE5CB3A
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	3424a1ecf8f0a35fe746b7011c43e844	RSA 2048-bits	RSA SHA-256	2019-03-21 20:38:59	2030-12-02 04:00:00		TLS Web Server Authentication, TLS Web Client Authentication	791eb1c917c71eacb1c714d7c3e87fbcb9509b15	B700BA49AF4D19E72FB15A2DAC3C213BA44C319FA7DA92772B3682E12B781093
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	0202a584c134064dc9f32d207ea37298	EC 384-bits	ECDSA SHA-384	2019-03-21 20:55:07	2030-12-02 04:00:00		TLS Web Server Authentication, TLS Web Client Authentication	c6908c0283d75de3be3b9c2ed5657d2a1060eee5	CDE23A52303C3CA67A4BBBCC9582FF5C9203AA98CB0F387139308CE2289506A2
9	1	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	2030-12-02 04:00:00		TLS Web Server Authentication, TLS Web Client Authentication	33df7a3e027996ebb60cc063fa75bf9222cd91fa	CA4389C89DDFC31BEC26C74B44A8498C58B2D838516FA01B14F1393629E58A40
9	2	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	2030-12-02 04:00:00		TLS Web Server Authentication, TLS Web Client Authentication	33df7a3e027996ebb60cc063fa75bf9222cd91fa	4563B936E35AB97576F5AEF1935D9BC7E9977841F0573BD2E16BCAC9534A6AF9
10	1	CN = AffirmTrust 4K TLS Certification Authority - DVTLS1 O = AffirmTrust C = CA	CN = AffirmTrust 4K TLS Root CA - 2022 O = AffirmTrust C = CA	04e911e082864b911d97267aa3388c5a	RSA 4096-bits	RSA SHA-384	2022-12-14 14:09:01	2040-12-29 19:59:59		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	45c174f7f45d033320f133efb8da6179886f5c96	FB327FE14AB3FEC5C96D9169A8B536382B97B1B325543C3DCD8A10F8C431E103
11	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	2030-12-02 04:00:00		TLS Web Server Authentication, TLS Web Client Authentication	fe60c30da4a29d214f7a784c62c5db14fc3978c4	EA4EE2FAA57AE4B539B63977FE5BB205B6AFB32F7A73B2B363E4BE02CD8A91E9
11	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	2030-12-02 04:00:00		TLS Web Server Authentication, TLS Web Client Authentication	fe60c30da4a29d214f7a784c62c5db14fc3978c4	B5FD6F800334F565036B0999F8310B5B0BD7268395D8B267005697AF7301C5E8

Deloitte.

ATTACHMENT B

LIST OF AFFIRMTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
AffirmTrust Certification Practice Statement	3.16	20 Feb 2024
AffirmTrust Certification Practice Statement	3.15	16 Oct 2023
AffirmTrust Certification Practice Statement	3.14	12 May 2023
AffirmTrust Certification Practice Statement	3.13	31 Jan 2023

AFFIRMTRUST MANAGEMENT'S STATEMENT

Entrust Corporation 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, Canada and Toronto, Ontario, Canada throughout the period 1 March 2023 to 29 February 2024, AffirmTrust has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
    - Certificate Policy/ Certification Practice Statements ("CP/CPS") 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 v1.8.

AffirmTrust management has also reported the following 'bugs' on Mozilla's Bugzilla reporting system:

Bug ID	Summary	Opened	Closed
1883843	EV TLS Certificate cPSuri missing	6-Mar-2024	<In Progress>
1886532	Delayed revocation of EV TLS certificates with missing cPSuri	20-Mar-2024	<In Progress>

Bruce Morton
Director, Entrust Certificate Services
May 21, 2024

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
DV SSL Issuing CAs
9. AffirmTrust Certificate Authority – DV1 10. AffirmTrust Certificate Authority – DVTLS1
OV SSL Issuing CAs
11. AffirmTrust Certificate Authority - OV1

ATTACHMENT B

LIST OF AFFIRMTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
AffirmTrust Certification Practice Statement	3.16	20 Feb 2024
AffirmTrust Certification Practice Statement	3.15	16 Oct 2023
AffirmTrust Certification Practice Statement	3.14	12 May 2023
AffirmTrust Certification Practice Statement	3.13	31 Jan 2023