

## INDEPENDENT ASSURANCE REPORT

To the management of Entrust Corporation (“Entrust”):

### Scope

We have been engaged, in a reasonable assurance engagement, to report on Entrust 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](#), Entrust 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 Entrust)

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

### Certification authority’s responsibilities

Entrust’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 Entrust’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 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 and correct, 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
<b>1 EV SSL certificates issued with postal code as jurisdiction locality field</b>	As publicly disclosed in <a href="#">Bugzilla 1867130</a> , two (2) EV SSL certificates were issued with postal code inputted in the jurisdiction locality field, instead of a "City" name or a "Null" if no city was required.  These certificates were revoked on 26 November 2023.
<b>2 The OCSP responders of two Root CAs were not updated to sign with SHA-256</b>	As publicly disclosed in <a href="#">Bugzilla 1879602</a> , the OCSP responders for the Entrust.net Certification Authority (2048) and Entrust Root Certification Authority were not updated to sign with SHA-256.  OCSP monitoring was updated to ensure correct OCSP responders sign with SHA-256 on 06 February 2024.

## Basis for qualified opinion

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

#	Observation	Relevant WebTrust Criteria
1	<p>As publicly disclosed in <a href="#">Bugzilla 1883843</a>, <a href="#">1888714</a> and <a href="#">1886467</a>, there were non-compliant EV SSL certificates issued within the audit period, including:</p> <ul style="list-style-type: none"> <li>• 26,644 EV SSL certificates were issued with cPSuri removed in the policy qualifiers;</li> <li>• 1,969 out of that 26,644 impacted EV SSL certificates were issued without CP OID in the certificatePolicies extension; and</li> <li>• 14 EV SSL certificates issued without id-kp-serverAuth</li> </ul> <p>As a result, a criterion of Principle 2 - 2.2.2 and of WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8 has not been met.</p>	<p><b>P2 - 2.2.2:</b> 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:</p> <ul style="list-style-type: none"> <li>• Certificate Policy Identification requirements</li> <li>• Subscriber Public Key</li> <li>• Certificate Serial Number</li> <li>• Additional Technical Requirements for EV Certificates</li> </ul> <p>as established in the EV SSL Guidelines relating to:</p> <ul style="list-style-type: none"> <li>• EV SSL Subscriber Certificates</li> <li>• EV Subordinate CA Certificates</li> </ul>
2	<p>As publicly disclosed in <a href="#">Bugzilla 1886532</a> and <a href="#">1887705</a>, for those mis-issued EV SSL certificates reported in <a href="#">Bugzilla 1883843</a>, <a href="#">1888714</a> and <a href="#">1886467</a>, Entrust did not revoke the impacted certificates within 5 days.</p> <p>As of 30 April 2024, the revocation of impacted certificates was still in progress.</p> <p>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.</p>	<p><b>P2 - 5.3:</b> The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs:</p> <ol style="list-style-type: none"> <li>1. The Subscriber requests in writing that the CA revoke the Certificate;</li> <li>2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;</li> <li>3. The CA obtains evidence that the Subscriber’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or</li> <li>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.</li> </ol> <p>And, Subscriber Certificates are revoked within 5 days if any of the following events occurs:</p> <ol style="list-style-type: none"> <li>1. The Certificate no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6;</li> <li>2. The CA obtains evidence that the Certificate was misused;</li> <li>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;</li> <li>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);</li> </ol>

#	Observation	Relevant WebTrust Criteria
		<ol style="list-style-type: none"><li>5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;</li><li>6. The CA is made aware of a material change in the information contained in the Certificate;</li><li>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;</li><li>8. The CA determines that any of the information appearing in the Certificate is inaccurate;</li><li>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;</li><li>10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or</li><li>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 <a href="http://wiki.debian.org/SSLkeys">http://wiki.debian.org/SSLkeys</a>), or if there is clear evidence that the specific method used to generate the Private Key was flawed.</li></ol>

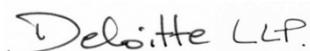
## Opinion

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, Entrust 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 Extended Validation SSL v1.8.

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

Entrust'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  
Chartered Professional Accountants  
Toronto, Ontario, Canada  
May 21, 2024

## ATTACHMENT A

### LIST OF IN SCOPE CAs

<b>Root CAs</b>
<ol style="list-style-type: none"><li>1. Entrust.net Certification Authority (2048)</li><li>2. Entrust Root Certification Authority</li><li>3. Entrust Root Certification Authority – G2</li><li>4. Entrust Root Certification Authority – G4</li><li>5. Entrust Root Certification Authority – EC1</li><li>6. Entrust Root Certification Authority – 4K EVTLSR 2022</li><li>7. Entrust Root Certification Authority – P384 EVTLSR 2022</li></ol>
<b>EV SSL Issuing CAs</b>
<ol style="list-style-type: none"><li>8. Entrust Certification Authority – L1E</li><li>9. Entrust Certification Authority – L1J</li><li>10. Entrust Certification Authority – L1M</li><li>11. Entrust Certification Authority – L1N</li><li>12. Entrust Certification Authority - EVTLS1</li><li>13. Entrust Certification Authority - EVTLS2</li><li>14. Entrust Certification Authority - Namirial EV SSL</li></ol>
<b>Qualified Certificate EV SSL Issuing CAs</b>
<ol style="list-style-type: none"><li>15. Entrust Certification Authority - QTSP1</li><li>16. Entrust Certification Authority - ES QWAC2</li></ol>
<b>OV SSL Issuing CAs</b>
<ol style="list-style-type: none"><li>17. Entrust Certification Authority – L1F</li><li>18. Entrust Certification Authority – L1K</li><li>19. Entrust Certification Authority – CrowdStrike TLS CA 2022</li><li>20. Siemens 2020</li><li>21. Namirial OV SSL CA 2023</li><li>22. Entrust Certification Authority – OVTLS1</li><li>23. Entrust Certification Authority – OVTLS2</li></ol>



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=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	3863def8	RSA 2048-bits	RSA SHA-1	1999-12-24 17:50:51	2029-07-24 14:15:12			55e481d11180bed889b908a331f9a1240916b970	6DC47172E01CBCB08F62580D895FE2B8AC9AD4F873801E0C10B9C837D21EB177
2	1	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	456b5054	RSA 2048-bits	RSA SHA-1	2006-11-27 20:23:42	2026-11-27 20:53:42			6890e467a4a65380c78666a4f1f74b43fb84bd6d	73C176434F1BC6D5ADF4580E76E727287C8DE57616C1E6E6141A2B2CBC7D8E4C
3	1	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	4a538c28	RSA 2048-bits	RSA SHA-256	2009-07-07 17:25:54	2030-12-07 17:55:54			6a72267ad01eef7de73b6951d46c8d9f901266ab	43DF5774B03E7FEF5FE40D931A7BEDF1BB2E6842738C4E6D3841103D3AA7F339
3	2	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	51d33f09	RSA 2048-bits	RSA SHA-1	2014-09-12 17:28:27	2024-09-13 03:12:02			6a72267ad01eef7de73b6951d46c8d9f901266ab	CBCE622D06F9D2C093FAD75CEBB7852EF53FFFF146AD522AB321B3A4B2BD8F8
3	3	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	51d33f24	RSA 2048-bits	RSA SHA-1	2014-09-12 19:23:57	2024-09-13 03:12:23			6a72267ad01eef7de73b6951d46c8d9f901266ab	16296E3BEF9A64CFE3509F36D700A5CD61CF938EC3A955BF36D17D97E16E8D
3	4	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	51d34044	RSA 2048-bits	RSA SHA-256	2014-09-22 17:14:57	2024-09-23 01:31:53			6a72267ad01eef7de73b6951d46c8d9f901266ab	6B143C2005D539CC22EAB5F772DB2A9FE87467FEFFA07FC0A9F7D28274CA7A
4	1	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00d9b5437afa9390f00000005565ad58	RSA 4096-bits	RSA SHA-256	2015-05-27 11:11:16	2037-12-27 11:41:16			9f38c45623c339e8a0716ce8544ce4e83ab1bf67	DB3517D1F6732A2D5AB97C533EC70779EE3270A62F84AC4238372460E6F01E88
5	1	CN=Entrust Root Certification Authority - EC1 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - EC1 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00a68b7929000000050d091f9	EC 384-bits	ECDSA SHA-384	2012-12-18 15:25:36	2037-12-18 15:55:36			b763e71add8de908a65583a4e06a504165114249	02ED0E28C14DA45165C566791700D6451D7F856F082AB1D3B8E8070E56EDFF5
5	2	CN=Entrust Root Certification Authority - EC1 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	008011196de613db16000000051d3575e	EC 384-bits	RSA SHA-256	2016-06-10 14:58:55	2026-11-10 15:28:55			b763e71add8de908a65583a4e06a504165114249	3FDE0D36E02686E8E8E2C28883607C8651DE10BD6C1FCAD365E560F4EA2F3B03
6	1	CN = Entrust 4K EV TLS Root CA - 2022 O = Entrust, Inc. C = US	CN = Entrust 4K EV TLS Root CA - 2022 O = Entrust, Inc. C = US	72429d8f40dfe46dafbe06ebb533194ce90d6c76	RSA 4096-bits	RSA SHA-384	2022-12-13 12:35:08	2047-12-07 12:35:08			0bdd90d58fb3f5cbd60a0551a2482863c413041	647987D98D52645DA4D3DE3B80771A0CE02B9B9285E6E86999882170744EC9AA
7	1	CN = Entrust P384 EV TLS Root CA - 2022 O = Entrust, Inc. C = US	CN = Entrust P384 EV TLS Root CA - 2022 O = Entrust, Inc. C = US	097558f5a16c16877bbd064ffd9ce483ba4b040b	EC 384-bits	ECDSA SHA-384	2022-12-13 12:46:44	2047-12-7 12:46:44			137210ae82580fc1389bbcb6a64c05ca8e8468bf	937EF8F12276B3C7A3F58E345D09A6EFF01F862F8D2794441CD84D511825FA0C
8	1	CN=Entrust Certification Authority - L1E OU=(c) 2009 Entrust, Inc. OU=www.entrust.net/rpa is incorporated by reference O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	008666b02ac1cb5440000000051d3589c	RSA 2048-bits	RSA SHA-256	2019-06-19 16:52:08	2026-11-19 17:22:08		TLS Web Server Authentication, TLS Web Client Authentication	5b418ab2c443c1bdfbc85441559de096adff9a1	232F6367CF561E00C83E180A9FC8A546B3771FB450EBC8A40526F8349C8CA139
9	1	CN=Entrust Certification Authority - L1J OU=(c) 2016 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - EC1 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	0a83d4803e7e9f510000000051d4c1f7	EC 384-bits	ECDSA SHA-384	2016-04-05 20:19:54	2037-10-05 20:49:54		TLS Web Server Authentication, TLS Web Client Authentication	c3f94503bec8f90b3c4535f3eb72ece7e8eb949b	3447B74B5E500A549983FA2CED73A5642E6AAEC78829546158437DF66D7435B8
10	1	CN=Entrust Certification Authority - L1M OU=(c) 2014 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	51d346e1	RSA 2048-bits	RSA SHA-256	2014-11-18 20:59:32	2024-11-19 06:33:02		TLS Web Client Authentication, TLS Web Server Authentication	c3f7d0b52a30adaf0d9121703954ddbc8970c73a	CA290389E0D8C62A4083F628A39F52FE3F38B73199CFFAF7C0372378A440FB6A
10	2	CN=Entrust Certification Authority - L1M OU=(c) 2014 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	61a1e7d20000000051d366a6	RSA 2048-bits	RSA SHA-256	2014-12-15 15:25:03	2030-10-15 15:55:03		TLS Web Client Authentication, TLS Web Server Authentication	c3f7d0b52a30adaf0d9121703954ddbc8970c73a	75C5B3F01FD1F51A2C447AB7C785D72E69FA9C472C08571E7EADF3B8EABAE70C
11	1	CN=Entrust Certification Authority - L1N OU=(c) 2014 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00abec77ff1b410c07000000005565d805	RSA 2048-bits	RSA SHA-256	2017-11-22 20:04:20	2030-12-22 20:34:20		TLS Web Server Authentication, TLS Web Client Authentication	ee47d18571f1fd2b73fbb3e6358771749400e95	B14D5089079C1D8F7649DB9A5D3CFB1AAC066FAFC49225C5BE2AA19FD41A35



CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
12	1	CN = Entrust 4K TLS Certification Authority - EVTLS1 O = Entrust, Inc. C = US	CN = Entrust 4K EV TLS Root CA - 2022 O = Entrust, Inc. C = US	31ef81d7823f9a0f27b5d3085df41e c0	EC 384-bits	ECDSA SHA-384	2022-12-14 14:16:26	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)	9930115c04d2448b259713c665d21616c9678792	AAC8B9394C3BB0376622444235343371C59E951FF85A151B3FE19C288076E2B5
13	1	CN = Entrust P384 TLS Certification Authority - EVTLS2 O = Entrust, Inc. C = US	CN = Entrust P384 EV TLS Root CA - 2022 O = Entrust, Inc. C = US	2ecf71fbc3f43015ca8bea5edd3dc7 63	EC 384-bits	ECDSA SHA-384	2022-12-14 14:20:13	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)	2cc1fad3279c77e73038c8c95ca43c02a36775c4	2426C77CFA12EBDCDB8013225496C0E7AAD66D63597AE5E9A0BEB3830C23EC2
14	1	CN = Namirial EV SSL CA 2023 O = Namirial S.p.A C = IT	CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O = Entrust, Inc. C = US	7b0350a7b1d46885af4cc8c740a56 8b0	RSA 2048-bits	RSA SHA-256	2023-02-09 16:13:06	2030-12-07 8:59:59		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	eafeeb5847b833d9d2367bc88c677ab1338b8d52	3660D61ECE49EF68A7E0705915ECE7EE7BAA3C5D71B9363CD487E0FE0242A634
15	1	CN=Entrust Certification Authority - QTSP1 C=ES O=Entrust Datacard Europe S.L. organizationIdentifier=VATES-B81188047	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	009c6cf695700c600000000051d 393a6	RSA 2048-bits	RSA SHA-256	2019-07-26 18:31:45	2030-11-26 19:01:45		TLS Web Server Authentication, TLS Web Client Authentication	1cad3f9cd72d219a19c4be9daf12a33f7bba0d	681EBC1822B079B97E0404E4687D9B6C0C0892C820F55738A282AAE62529BDD8
16	1	CN=Entrust Certification Authority - ES QWAC2 organizationIdentifier=VATES-B81188047 O=Entrust EU, S.L. C=ES	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	7a8872b868a359dab1b02ecf4fc971 8d	RSA 2048-bits	RSA SHA-256	2021-11-16 00:00:00	2030-12-01 00:00:00		TLS Web Server Authentication, TLS Web Client Authentication	41cfae2b1d633bc4cf5904479b65a2489df929c	C97F2F6E6A8ADB6ECFE4978F08CA8F6F0123A94784522B610ADF6AB51439FC62
17	1	CN=Entrust Certification Authority - L1F OU=(c) 2016 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - EC1 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00b601913d8553bafa0000000051d 4c1f6	EC 384-bits	ECDSA SHA-384	2016-04-05 20:17:29	2037-10-05 20:47:29		TLS Web Server Authentication, TLS Web Client Authentication	2e62f014ee87cd335033defe4b99efd3bb8a3c9	1835B0E482EA65536FC010E4BC13C060F65668165FBA97E2F542CE96CA6DFEFC
17	2	CN=Entrust Certification Authority - L1F OU=(c) 2016 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	00a25b1769bad80ad70000000051c e1941	EC 384-bits	RSA SHA-256	2021-02-05 16:34:34	2029-07-05 17:04:34		TLS Web Server Authentication, TLS Web Client Authentication	2e62f014ee87cd335033defe4b99efd3bb8a3c9	0C5A09DB8AEDF7D2D1DDE14DCCC2D86EA959BCF6F010360D836C342C624D7E0E
18	1	CN=Entrust Certification Authority - L1K OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	51d360ce	RSA 2048-bits	RSA SHA-256	2014-08-26 17:07:28	2024-08-27 05:48:52			82a27074ddbc533cf7bd4f7cd7fa760c60a4cbf	386DD5581C9853092007DB1BB0106FC61205E88E360543D7CAE0D68E7A25AC3
18	2	CN=Entrust Certification Authority - L1K OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	51d360cf	RSA 2048-bits	RSA SHA-256	2014-08-26 17:14:49	2024-08-27 08:34:47			82a27074ddbc533cf7bd4f7cd7fa760c60a4cbf	380CC20384AD7F24EB438F2B80C63EBE003F7F215B8877E418EBB0484028DB57
18	3	CN=Entrust Certification Authority - L1K OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	51ce00fe	RSA 2048-bits	RSA SHA-256	2014-10-10 15:23:17	2024-10-11 06:22:47			82a27074ddbc533cf7bd4f7cd7fa760c60a4cbf	D6C3FC493BACD1DF8A1BA30F4AE2625482A4528E4876081EACC6A16A090AA36A
18	4	CN=Entrust Certification Authority - L1K OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	51d360ee	RSA 2048-bits	RSA SHA-256	2014-10-22 17:05:14	2024-10-23 07:33:22			82a27074ddbc533cf7bd4f7cd7fa760c60a4cbf	F5C2F23C6518F9D19B6F39BEAE4FBAE10031BA9DC985CE1563A520A0AD4116
18	5	CN=Entrust Certification Authority - L1K OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	0ee94cc30000000051d37785	RSA 2048-bits	RSA SHA-256	2015-10-05 19:13:56	2030-12-05 19:43:56			82a27074ddbc533cf7bd4f7cd7fa760c60a4cbf	13EFB39A2F6654E8C67BD04F4C6D4C90CD6CAB50918CEDC73787F6B7D3D3FE7
18	6	CN = Entrust Certification Authority - L1K OU = (c) 2012 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US	CN = Entrust.net Certification Authority (2048) OU = (c) 1999 Entrust.net Limited OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O = Entrust.net	2e0451ce5d2424c72b5d657671650 6d8	RSA 2048-bits	RSA SHA-256	2022-11-25 17:19:43	2029-7-22 20:00:00		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	82a27074ddbc533cf7bd4f7cd7fa760c60a4cbf	7F4325CC24107A39441552F27FDC34185802482E164D1794AA415EF1E4206BA7
19	1	CN = CrowdStrike TLS CA 2022 O = CrowdStrike, Inc. C = US	CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US	309dc7b318912d0ecb7d1df27ab75 cdf	RSA 2048-bits	RSA SHA-256	2022-11-15 12:50:48	2030-12-5 20:00:00			55eaa745b99af7b671311a31dfa176fe7692997a	2C4AD64B4E862D7D46424D9FA13EA9A974A62F7C4B608AE1A871424CC9A6873D
20	1	C=DE O=Siemens CN=Siemens Issuing CA Internet Server 2020	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00fab27dfff80d09a0000000051d3 9440	RSA 2048-bits	RSA SHA-256	2020-08-10 14:11:48	2030-11-10 14:41:48		TLS Web Server Authentication, TLS Web Client Authentication	c9a757cb86c96107c6c2b48665a91ec1cae1029b	A665007A05EFE1889D66A40DEECBC6C1A271E919006811FDB8DBD7E0675212D1



CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
21	1	CN = Namirial OV SSL CA 2023 O = Namirial S.p.A C = IT	CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US	17c236215a437f11aae022348b6b7f2d	RSA 2048-bits	RSA SHA-256	2023-2-9 16:09:10	2030-12-7 8:59:59		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	9a9f6fa5f8fe34fc102deb2f89c6b9d7c692d31e	F4E26BE0279228D96D47B05DF744AE6CE6AAD888A3B757D249E83D22D27F4C6
22	1	CN = Entrust 4K TLS Certification Authority - OV TLS1 O = Entrust, Inc. C = US	CN = Entrust 4K TLS Root CA - 2022 O = Entrust, Inc. C = US	68ca04736adcebbd10432a6bd6ef8a34	EC 384-bits	RSA SHA-256	2022-12-14 14:23:34	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)	a80003c10185b8c0272aa9bc08acfad44abe51a5	9EC6CA44D6ADB5DAEF9FC9D773787E3BB8E1243F5455341B8438A6776869333B
23	1	CN = Entrust P384 TLS Certification Authority - OV TLS2 O = Entrust, Inc. C = US	CN = Entrust P384 TLS Root CA - 2022 O = Entrust, Inc. C = US	68772973693c55320a742ff1433ca0a2	EC 384-bits	RSA SHA-256	2022-12-14 14:25:44	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)	c25b7126ed58efa51419aa2ef60456546f9a39c9	2DB842F824321277291266B230ABC31DE13C1D48852D6C21C981007D5AC20681





ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
<a href="#">Entrust Certificate Services Certification Practice Statement</a>	3.16	20 Feb 2024
<a href="#">Entrust Certificate Services Certification Practice Statement</a>	3.15	16 Oct 2023
<a href="#">Entrust Certificate Services Certification Practice Statement</a>	3.14	20 June 2023
<a href="#">Entrust Certificate Services Certification Practice Statement</a>	3.13	12 May 2023
<a href="#">Entrust Certificate Services Certification Practice Statement</a>	3.12	31 Jan 2023



## ENTRUST MANAGEMENT'S STATEMENT

Entrust Corporation ("Entrust") operates the Certification Authority ("CA") services as enumerated in [Attachment A](#), and provides Extended Validation SSL ("EV SSL") CA services.

The management of Entrust is responsible for establishing and maintaining effective controls over its 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 Entrust's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Entrust management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in Entrust management's opinion, in providing its EV SSL CA services at Ottawa, Ontario, Canada and Toronto, Ontario, Canada throughout the period 1 March 2023 to 29 February 2024, Entrust has:

- disclosed its 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 Entrust)

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

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

Bug ID	Summary	Opened	Closed
1867130	Postal code was added to the jurisdiction locality field in an EV TLS certificate	28-Nov-2023	24-Jan-2024
1883843	EV TLS Certificate cPSuri missing	6-Mar-2024	<In Progress>
1886467	clientAuth TLS Certificates without serverAuth EKU	20-Mar-2024	<In Progress>
1886532	Delayed revocation of EV TLS certificates with missing cPSuri	20-Mar-2024	<In Progress>
1887705	Delayed revocation of clientAuth TLS Certificates without serverAuth EKU	25-Mar-2024	<In Progress>
1888714	EV Certificate missing Issuer's EV Policy OID	29-Mar-2024	<In Progress>

Bruce Morton  
Director, Entrust Certificate Services  
May 21, 2024



ATTACHMENT A

LIST OF IN SCOPE CAs

<b>Root CAs</b>
<ol style="list-style-type: none"><li>1. Entrust.net Certification Authority (2048)</li><li>2. Entrust Root Certification Authority</li><li>3. Entrust Root Certification Authority – G2</li><li>4. Entrust Root Certification Authority – G4</li><li>5. Entrust Root Certification Authority – EC1</li><li>6. Entrust Root Certification Authority – 4K EVTLSR 2022</li><li>7. Entrust Root Certification Authority – P384 EVTLSR 2022</li></ol>
<b>EV SSL Issuing CAs</b>
<ol style="list-style-type: none"><li>8. Entrust Certification Authority – L1E</li><li>9. Entrust Certification Authority – L1J</li><li>10. Entrust Certification Authority – L1M</li><li>11. Entrust Certification Authority – L1N</li><li>12. Entrust Certification Authority - EVTLS1</li><li>13. Entrust Certification Authority - EVTLS2</li><li>14. Entrust Certification Authority - Namirial EV SSL</li></ol>
<b>Qualified Certificate EV SSL Issuing CAs</b>
<ol style="list-style-type: none"><li>15. Entrust Certification Authority - QTSP1</li><li>16. Entrust Certification Authority - ES QWAC2</li></ol>
<b>OV SSL Issuing CAs</b>
<ol style="list-style-type: none"><li>17. Entrust Certification Authority – L1F</li><li>18. Entrust Certification Authority – L1K</li><li>19. Entrust Certification Authority – CrowdStrike TLS CA 2022</li><li>20. Siemens 2020</li><li>21. Namirial OV SSL CA 2023</li><li>22. Entrust Certification Authority – OVTLS1</li><li>23. Entrust Certification Authority – OVTLS2</li></ol>



ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
<a href="#">Entrust Certificate Services Certification Practice Statement</a>	3.16	20 Feb 2024
<a href="#">Entrust Certificate Services Certification Practice Statement</a>	3.15	16 Oct 2023
<a href="#">Entrust Certificate Services Certification Practice Statement</a>	3.14	20 June 2023
<a href="#">Entrust Certificate Services Certification Practice Statement</a>	3.13	12 May 2023
<a href="#">Entrust Certificate Services Certification Practice Statement</a>	3.12	31 Jan 2023

## 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.



## 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	<p>As publicly disclosed in <a href="#">Bugzilla 1883843</a>, there were 24 EV SSL certificates issued with cPSuri removed in the policy qualifiers.</p> <p>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.</p>	<p><b>P2 - 2.2.2:</b> 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:</p> <ul style="list-style-type: none"> <li>• Certificate Policy Identification requirements</li> <li>• Subscriber Public Key</li> <li>• Certificate Serial Number</li> <li>• Additional Technical Requirements for EV Certificates</li> </ul> <p>as established in the EV SSL Guidelines relating to:</p> <ul style="list-style-type: none"> <li>• EV SSL Subscriber Certificates</li> <li>• EV Subordinate CA Certificates</li> </ul>
2	<p>As publicly disclosed in <a href="#">Bugzilla 1886532</a>, for those mis-issued EV SSL certificates reported in <a href="#">Bugzilla 1883843</a>, AffirmTrust did not revoke the impacted certificates within 5 days.</p> <p>As of 30 April 2024, the revocation of impacted certificates was still in progress.</p> <p>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.</p>	<p><b>P2 - 5.3:</b> The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs:</p> <ol style="list-style-type: none"> <li>1. The Subscriber requests in writing that the CA revoke the Certificate;</li> <li>2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;</li> <li>3. The CA obtains evidence that the Subscriber’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or</li> <li>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.</li> </ol>

#	Observation	Relevant WebTrust Criteria
		<p>And, Subscriber Certificates are revoked within 5 days if any of the following events occurs:</p> <ol style="list-style-type: none"> <li>1. The Certificate no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6;</li> <li>2. The CA obtains evidence that the Certificate was misused;</li> <li>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;</li> <li>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);</li> <li>5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;</li> <li>6. The CA is made aware of a material change in the information contained in the Certificate;</li> <li>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;</li> <li>8. The CA determines that any of the information appearing in the Certificate is inaccurate;</li> <li>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;</li> <li>10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or</li> <li>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 <a href="http://wiki.debian.org/SSLkeys">http://wiki.debian.org/SSLkeys</a>), or if there is clear evidence that the specific method used to generate the Private Key was flawed.</li> </ol>

## 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.



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.

A handwritten signature in black ink that reads "Deloitte LLP".

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





ATTACHMENT A

LIST OF IN SCOPE CAs

<b>Root CAs</b>
1. AffirmTrust Commercial 2. AffirmTrust Networking 3. AffirmTrust Premium 4. AffirmTrust Premium ECC
<b>EV SSL Issuing CAs</b>
5. AffirmTrust Extended Validation CA - EV1 6. AffirmTrust Extended Validation CA - EV2 7. AffirmTrust Extended Validation CA - EV3 8. AffirmTrust Extended Validation CA - EVEC1
<b>DV SSL Issuing CAs</b>
9. AffirmTrust Certificate Authority – DV1 10. AffirmTrust Certificate Authority – DVTLS1
<b>OV SSL Issuing CAs</b>
11. AffirmTrust Certificate Authority - OV1



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	70A73F7F376860074248904534B11482D5BF0E698ECC498DF52577EBF2E93B9A
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	BD71FD6DA97E4CF62D1647ADD2581B07D9ADF8397EB4ECBA9C5E8488821423
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	40f0bbaa8e0c098	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	CF88915CF996932C2B4CBE3039076D119B8728B4F31E49B63A5022FE65489A12
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	9DF77488C4B74AC32E3CEC4C643D001D5C3B8AFA4001FFD193DCA10C8BE5C83A
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	791eb1c917c71eacb1c714d7c3e87fbc9509b15	B700BA49AF4D19E72FB15A2DAC3C2138A44C319FA7DA92772B3682E12B781093
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	CDE23A52303C3CA67A4BBBC9582FF5C9203AA98CB0F387139308CE2289506A2
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	4563B936E35A897576F5AEF1935D9BC7E9977841F0573BD2E16BCAC9534A6AF9
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)	45c174f7f45d03320f133efb8da6179886f5c96	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	EA4EE2FAA57AE48539863977FE5B820586AFB32F7A73B2B363E4BE02CD8A91E9
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	B5FD6F800334F565036B0999F8310B580BD7268395D8B267005697AF7301C5E8



ATTACHMENT B

LIST OF AFFIRMTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
<a href="#">AffirmTrust Certification Practice Statement</a>	3.16	20 Feb 2024
<a href="#">AffirmTrust Certification Practice Statement</a>	3.15	16 Oct 2023
<a href="#">AffirmTrust Certification Practice Statement</a>	3.14	12 May 2023
<a href="#">AffirmTrust Certification Practice Statement</a>	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

<b>Root CAs</b>
1. AffirmTrust Commercial 2. AffirmTrust Networking 3. AffirmTrust Premium 4. AffirmTrust Premium ECC
<b>EV SSL Issuing CAs</b>
5. AffirmTrust Extended Validation CA - EV1 6. AffirmTrust Extended Validation CA - EV2 7. AffirmTrust Extended Validation CA - EV3 8. AffirmTrust Extended Validation CA - EVEC1
<b>DV SSL Issuing CAs</b>
9. AffirmTrust Certificate Authority – DV1 10. AffirmTrust Certificate Authority – DVTLS1
<b>OV SSL Issuing CAs</b>
11. AffirmTrust Certificate Authority - OV1

## ATTACHMENT B

## LIST OF AFFIRMTRUST CERTIFICATION PRACTICE STATEMENTS

<b>CPS Name</b>	<b>Version</b>	<b>Date</b>
<a href="#">AffirmTrust Certification Practice Statement</a>	3.16	20 Feb 2024
<a href="#">AffirmTrust Certification Practice Statement</a>	3.15	16 Oct 2023
<a href="#">AffirmTrust Certification Practice Statement</a>	3.14	12 May 2023
<a href="#">AffirmTrust Certification Practice Statement</a>	3.13	31 Jan 2023