

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 2020 to 28 February 2021 (the “Period”) for its CAs as enumerated in [Attachment A](#), Entrust has:

- disclosed its code signing (“CS”) certificate lifecycle management business practices in its Certification Practice Statements as enumerated in [Attachment B](#), including its commitment to provide CS certificates in conformity with the Minimum Requirements for Code Signing 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 CS certificates it manages is established and protected throughout their lifecycles; and
 - CS subscriber information is properly authenticated (for the registration activities performed by Entrust)
- maintained effective controls to provide reasonable assurance that:
 - requests for CS Signing Authority and CS Timestamp Authority certificates are properly authenticated; and
 - certificates issued to CS Signing Authorities and CS Timestamp Authorities are not valid for a period longer than specified by the Minimum Requirements for Code Signing Guidelines
- maintained effective controls to provide reasonable assurance that its CS Timestamp Authority is operated in conformity with Minimum Requirements for Code Signing Guidelines

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Publicly Trusted Code Signing v1.0.1](#).

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 – Publicly Trusted Code Signing v1.0.1.

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, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, 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.

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 CS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of CS certificates, CS Signing Authority certificates, and CS Timestamp Authority certificates;
- (2) selectively testing transactions executed in accordance with disclosed CS 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 Entrust 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, Entrust'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.

Practitioner's opinion

In our opinion, throughout the period 1 March 2020 to 28 February 2021, 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 – Publicly Trusted Code Signing v1.0.1.

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 – Publicly Trusted Code Signing v1.0.1, 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 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
22 April 2021



ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Entrust.net Certification Authority (2048)
2. Entrust Root Certification Authority – G2
3. Entrust Root Certification Authority – G4
Code Signing Issuing CAs
4. Entrust Code Signing Certification Authority - L1D
5. Entrust Code Signing CA - OVCS1
Timestamp CAs
6. Entrust Timestamping CA – TS1



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	6dc47172e01cbb0bf62580d895fe2b8ca9ad4f873801e0c10b9c837d21eb177
2	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	43df5774b03e7fef5fe40d931a7bedf1bb2e6b42738c4e6d3841103d3aa7f339
2	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	cbce622d06f9d2c093fad75cebb7852e5f53ffff146ad522ab321b3a4b2bd8f8
2	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	16296e3bef9a64cfede3509f36d700a5cd61c938ec3a955bf36d17d97e16e8d
2	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	6b143c2005d5539cc2e2ab5f772db2a9fe87467effa07fc0a9f7d28274ca7a
3	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	00d9b5437fafa9390f00000005565ad58	RSA 4096-bits	RSA SHA-256	2015-05-27 11:11:16	2037-12-27 11:41:16			9f38c45623c339e8a0716ce8544ce4e83ab1bf67	db3517d1f6732a2d5ab97c533ec70779ee3270a62fb4ac4238372460e6f01e88
4	1	CN=Entrust Code Signing Certification Authority - L1D OU=(c) 2009 Entrust, Inc. OU=www.entrust.net/rpa is incorporated by reference 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	4c0e8c1e	RSA 2048-bits	RSA SHA-256	2011-11-11 15:29:00	2021-11-12 03:28:50			a7b1aac4b606edddca9f88949682d5e74341d125	fa9d6df1af0275300d52a485d036b0543b53dfb4441bec0b8c9a0dff811b6d88
4	2	CN=Entrust Code Signing Certification Authority - L1D OU=(c) 2009 Entrust, Inc. OU=www.entrust.net/rpa is incorporated by reference 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	4c0e8c3a	RSA 2048-bits	RSA SHA-1	2011-11-11 15:41:26	2021-11-12 08:51:52			a7b1aac4b606edddca9f88949682d5e74341d125	8b16d48f721dfab157214b9ace9dda8efba5a06b4eed901806f086d1df8ead37
5	1	CN=Entrust Code Signing CA - OVCS1 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 - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	7ab8c4fc000000051d373d4	RSA 2048-bits	RSA SHA-256	2015-06-09 18:03:40	2025-06-09 18:33:40		Code Signing	7e1a1f1a11745c64c90c1f9401abfd81642ea12c	7fba43a4ccbb37b1ccc2dd11ce0c911da3a2917b0ca0e846056854ef464c50c4
5	2	CN=Entrust Code Signing CA - OVCS1 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 - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	43c10b1c000000051d373da	RSA 2048-bits	RSA SHA-256	2015-06-10 13:46:05	2030-11-10 14:16:05		Code Signing	7e1a1f1a11745c64c90c1f9401abfd81642ea12c	cc5b7a0e5d6771ba348d3d763752f0667026b3531c5396edbe24adce93215723
6	1	CN=Entrust Timestamping CA - TS1 OU=(c) 2015 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	51ce0dd8	RSA 2048-bits	RSA SHA-1	2015-07-15 17:42:06	2029-06-15 23:05:07		Time Stamping	c3c271d27bd76805ae3b399b34250c6203c75768	5f84398236b7e58fa365bf1ae5aa3e441c265fdbc50cf7471799060a27a2381a
6	2	CN=Entrust Timestamping CA - TS1 OU=(c) 2015 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	58da13ff000000051ce0df7	RSA 2048-bits	RSA SHA-256	2015-07-22 19:02:54	2029-06-22 19:32:54		Time Stamping	c3c271d27bd76805ae3b399b34250c6203c75768	44dfcd2c573110e74bf4e85903595f660650ed925b7306542c54e87396671f03



ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement	3.6	30 Sep 2019
Entrust Certificate Services Certification Practice Statement	3.7	30 Sep 2020
Entrust Certificate Services Certification Practice Statement	3.8	31 Dec 2020



ENTRUST MANAGEMENT'S STATEMENT

Entrust Corporation ("Entrust") operates the Certification Authority (CA) services as enumerated in [Attachment A](#), and provides Code Signing ("CS") CA services.

The management of Entrust is responsible for establishing and maintaining effective controls over its CS CA operations, including its CS CA business practices disclosure on its [website](#), CS CA key lifecycle management controls, CS certificate lifecycle management controls, and CS Signing Authority and CS Timestamp Authority 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 CS CA services. Based on that assessment, in Entrust management's opinion, in providing its CS Certification Authority (CA) services at Ottawa, Ontario, and Toronto, Ontario throughout the period 1 March 2020 to 28 February 2021, Entrust has:

- disclosed its extended validation code signing ("CS") certificate lifecycle management business practices in its Certification Practice Statements as enumerated in [Attachment B](#), including its commitment to provide EV CS certificates in conformity with the Minimum Requirements for Code Signing 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 CS certificates it manages is established and protected throughout their lifecycles; and
 - CS subscriber information is properly authenticated (for the registration activities performed by Entrust)
- maintained effective controls to provide reasonable assurance that:
 - requests for CS Signing Authority and CS Timestamp Authority certificates are properly authenticated; and
 - certificates issued to CS Signing Authorities and CS Timestamp Authorities are not valid for a period longer than specified by the Minimum Requirements for Code Signing Guidelines
- maintained effective controls to provide reasonable assurance that its CS Timestamp Authority is operated in conformity with Minimum Requirements for Code Signing Guidelines

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Publicly Trusted Code Signing v1.0.1](#).

Bruce Morton
Director, Entrust Certificate Services
22 April 2021



ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Entrust.net Certification Authority (2048)
2. Entrust Root Certification Authority – G2
3. Entrust Root Certification Authority – G4
Code Signing Issuing CAs
4. Entrust Code Signing Certification Authority - L1D
5. Entrust Code Signing CA - OVCS1
Timestamp CAs
6. Entrust Timestamping CA – TS1



ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement	3.6	30 Sep 2019
Entrust Certificate Services Certification Practice Statement	3.7	30 Sep 2020
Entrust Certificate Services Certification Practice Statement	3.8	31 Dec 2020