

INDEPENDENT AUDITOR'S REPORT

To the management of Entrust Ltd. ("Entrust"):

We have audited Entrust management's [assertion](#) that for its Certification Authority (CA) operations at Ottawa, Ontario, and Toronto, Ontario throughout the period 1 March 2016 to 28 February 2017 for its CAs as enumerated in [Attachment A](#), Entrust has:

- disclosed its extended validation code signing ("EV 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 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 CS certificates it manages is established and protected throughout their lifecycles; and
 - EV CS subscriber information is properly authenticated (for the registration activities performed by Entrust)
- maintained effective controls to provide reasonable assurance that:
 - requests for EV CS Signing Authority and EV CS Timestamp Authority certificates are properly authenticated; and
 - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum
- maintained effective controls to provide reasonable assurance that its EV CS Timestamp Authority is operated in conformity with CA/Browser Forum Guidelines

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.4](#).

Entrust's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our audit.

We conducted our audit in accordance with the standards for assurance engagements set out in the CPA Handbook – Assurance, and, accordingly, included:

- (1) obtaining an understanding of Entrust's EV CS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV CS certificates, EV CS Signing Authority certificates, and EV CS Timestamp Authority certificates;
- (2) selectively testing transactions executed in accordance with disclosed EV 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 our audit provides a reasonable basis for our opinion.

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.

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, unauthorized 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.

In our opinion, throughout the period 1 March 2016 to 28 February 2017, Entrust management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.4.

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 Code Signing v1.4, nor the suitability of any of Entrust's services for any customer's intended purpose.

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.

A handwritten signature in black ink that reads "Deloitte LLP". The signature is written in a cursive, flowing style.

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario
17 May 2017



ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Entrust Root Certification Authority
2. Entrust Root Certification Authority – G2
EV Code Signing Issuing CAs
3. Entrust Extended Validation Code Signing CA – EVCS1
Timestamp CAs
4. Entrust Timestamping CA – TS1



CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
1	1	C=US O=Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference OU=(c) 2006 Entrust, Inc. CN=Entrust Root Certification Authority	C=US O=Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference OU=(c) 2006 Entrust, Inc. CN=Entrust Root Certification Authority	456B5054	rsaEncryption	(2048 bit)	sha1WithRSAEncryption	Nov 27 20:23:42 2006 GMT	Nov 27 20:53:42 2026 GMT	68:90:E4:67:A4:A6:53:80:C7:86:66:A4:F1:F7:4B:43:FB:84:BD:6D	73:C1:76:43:4F:1B:C6:D5:AD:F4:5B:0E:76:E7:27:28:7C:8D:E5:76:16:C1:E6:E6:14:1A:2B:2C:BC:7D:8E:4C
2	1	C=US O=Entrust, Inc. OU=See www.entrust.net/legal-terms OU=(c) 2009 Entrust, Inc. - for authorized use only CN=Entrust Root Certification Authority - G2	C=US O=Entrust, Inc. OU=See www.entrust.net/legal-terms OU=(c) 2009 Entrust, Inc. - for authorized use only CN=Entrust Root Certification Authority - G2	4A538C28	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	Jul 7 17:25:54 2009 GMT	Dec 7 17:55:54 2030 GMT	6A:72:26:7A:D0:1E:EF:7D:E7:3B:69:51:D4:6C:8D:9F:90:12:66:AB	43:DF:57:74:B0:3E:7F:EF:5F:E4:0D:93:1A:7B:ED:F1:BB:2E:6B:42:73:8C:4E:6D:38:41:10:3D:3A:A7:F3:39
2	2	C=US O=Entrust, Inc. OU=See www.entrust.net/legal-terms OU=(c) 2009 Entrust, Inc. - for authorized use only CN=Entrust Root Certification Authority - G2	C=US O=Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference OU=(c) 2006 Entrust, Inc. CN=Entrust Root Certification Authority	51D34044	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	Sep 22 17:14:57 2014 GMT	Sep 23 01:31:53 2024 GMT	6A:72:26:7A:D0:1E:EF:7D:E7:3B:69:51:D4:6C:8D:9F:90:12:66:AB	6B:14:3C:20:05:D5:53:9C:C2:2E:AB:5F:77:2D:B2:A9:FE:87:46:7F:EF:FA:07:FC:F0:A9:F7:D2:82:74:CA:7A
3	1	C=US O=Entrust, Inc. OU=See www.entrust.net/legal-terms OU=(c) 2015 Entrust, Inc. - for authorized use only CN=Entrust Extended Validation Code Signing CA - EVCS1	C=US O=Entrust, Inc. OU=See www.entrust.net/legal-terms OU=(c) 2009 Entrust, Inc. - for authorized use only CN=Entrust Root Certification Authority - G2	8782526000000 00051D373D9	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	Jun 10 13:42:49 2015 GMT	Nov 10 14:12:49 2030 GMT	2A:0A:6F:32:2C:29:20:21:76:6A:B1:AC:8C:3C:AF:93:8E:0E:6B:A2	D0:4D:B9:27:C6:63:AA:8C:85:3D:54:71:6D:D6:DC:2A:4B:2F:EF:9C:3A:E1:BF:B2:50:44:7F:C5:D7:77:1E:57
4	1	C=US O=Entrust, Inc. OU=See www.entrust.net/legal-terms OU=(c) 2015 Entrust, Inc. - for authorized use only CN=Entrust Timestamping CA - TS1	O=Entrust.net OU=www.entrust.net/CPS_2048 Incorp. by ref. (limits liab.) OU=(c) 1999 Entrust.net Limited CN=Entrust.net Certification Authority (2048)	58DA13FF00000 00051CE0DF7	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	Jul 22 19:02:54 2015 GMT	Jun 22 19:32:54 2029 GMT	C3:C2:71:D2:7B:D7:68:05:AE:3B:39:9B:34:25:0C:62:03:C7:57:68	44:DF:CD:2C:57:31:10:E7:4B:F4:E8:59:03:59:5F:66:06:50:ED:92:5B:73:06:54:2C:54:E8:73:96:67:1F:03



ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement for Extended Validation (EV) Certificates	1.9	12-Feb-2016
Entrust Certificate Services Certification Practice Statement for Extended Validation (EV) Certificates	2.0	01-Feb-2017

ENTRUST MANAGEMENT'S ASSERTION

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

The management of Entrust is responsible for establishing and maintaining effective controls over its EV CS CA operations, including its EV CS CA business practices disclosure on its [website](#), EV CS CA key lifecycle management controls, EV CS certificate lifecycle management controls, and EV CS Signing Authority and EV 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 EV CS CA services. Based on that assessment, in Entrust management's opinion, in providing its EV CS Certification Authority (CA) services at Ottawa, Ontario, and Toronto, Ontario throughout the period 1 March 2016 to 28 February 2017, Entrust has:

- disclosed its extended validation code signing ("EV 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 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 CS certificates it manages is established and protected throughout their lifecycles; and
 - EV CS subscriber information is properly authenticated (for the registration activities performed by Entrust)
- maintained effective controls to provide reasonable assurance that:
 - requests for EV CS Signing Authority and EV CS Timestamp Authority certificates are properly authenticated; and
 - certificates issued to EV CS Signing Authorities and EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum
- maintained effective controls to provide reasonable assurance that its EV CS Timestamp Authority is operated in conformity with CA/Browser Forum Guidelines

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing v1.4](#).

Bruce Morton
CA Operations Manager
17 May 2017

ATTACHMENT A**LIST OF IN SCOPE CAs**

Root CAs
1. Entrust Root Certification Authority
2. Entrust Root Certification Authority – G2
EV Code Signing Issuing CAs
3. Entrust Extended Validation Code Signing CA – EVCS1
Timestamp CAs
4. Entrust Timestamping CA – TS1

ATTACHMENT B**LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS**

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement for Extended Validation (EV) Certificates	1.9	12-Feb-2016
Entrust Certificate Services Certification Practice Statement for Extended Validation (EV) Certificates	2.0	01-Feb-2017