Auditor’s Report

To the Management of Entrust Ltd. (Entrust):

We have audited the assertion by the management of Entrust that in providing its Certification Authority (CA) services at Ottawa, Ontario, as of 31 March 2013, Entrust has suitably designed its practices and procedures based on the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria version 1.1, for its:

- Entrust.net Secure Server Certification Authority (SSL Root CA), Entrust.net Certification Authority (2048 Root CA), Entrust Root Certification Authority (EV Root CA), Entrust Root Certification Authority – G2 (G2 Root CA), and Entrust Root Certification Authority – EC1 (EC1 Root CA)
- L1A CA and L1E CA – EV SSL Issuing CAs
- L1B CA and L1C CA – Non-EV SSL Issuing CAs

Other CAs within Entrust’s PKI environment, including CAs subordinated from or cross-certified to any of those CAs listed above whether managed by Entrust or by a third party were not subject to our audit.

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

Our audit was conducted in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants (CICA) and, accordingly, included (1) obtaining an understanding of Entrust’s SSL certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of SSL certificates; (2) evaluating the suitability of the design of practices and procedures; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

Management has not placed its EC1 Root CA in operation and, therefore, additional changes may be made to the design of the controls before the EC1 Root CA is implemented. We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of Entrust’s controls, individually or in the aggregate.

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.

In our opinion, Entrust’s management’s assertion, as of 31 March 2013, is fairly stated, in all material respects, in accordance with the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria version 1.1.

This report does not include any representation as to the quality of Entrust’s certification services beyond those covered by the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria version 1.1, or the suitability of any of Entrust’s services for any customer's intended purpose.
Deloitte LLP
Chartered Accountants
Toronto, Ontario
10 May 2013
The management of Entrust Ltd. (Entrust) has assessed the disclosure of its certificate practices and its controls over its SSL - CA services located at Ottawa, Ontario as at 31 March 2013. Based on that assessment, in Entrust Management’s opinion, in providing its SSL - CA services

- Entrust.net Secure Server Certification Authority (SSL Root CA), Entrust.net Certification Authority (2048 Root CA), Entrust Root Certification Authority (EV Root CA), Entrust Root Certification Authority – G2 (G2 Root CA), and Entrust Root Certification Authority – EC1 (EC1 Root CA)
- L1A CA and L1E CA – EV SSL Issuing CAs
- L1B CA and L1C CA – Non-EV SSL Issuing CAs

at Ottawa, Ontario as at 31 March 2013, Entrust has:

- Disclosed its Certificate practices and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- Maintained effective controls to provide reasonable assurance that:
  o The Certificate Policy and/or Certificate Practice Statement are available on a 24x7 basis and updated annually;
  o Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  o The integrity of keys and certificates it manages was established and protected throughout their life cycles;
  o Logical and physical access to CA systems and data was restricted to authorized individuals;
  o The continuity of key and certificate management operations was maintained; and
  o CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

in accordance with the AICPA/CICA WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria version 1.1.

Bruce Morton
CA Operations Manager
10 May 2013