

## Independent Accountants' report on applying specified procedures

*To the Management of Entrust Ltd ("Entrust"), and Management of Entrust Ltd. doing business as AffirmTrust ("AffirmTrust"):*

We have performed the procedures set out in the accompanying attachment, which were developed to address the exception that was identified in the 2018-2019 WebTrust for CA – SSL Baseline with Network Security assurance report.

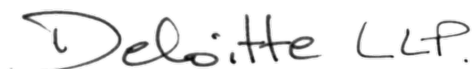
The procedures performed and our findings are set out in the accompanying attachment. This specified procedures engagement was conducted in accordance with the guidelines set out in the CPA Canada Handbook - Assurance, Section 9100, *Reports on the results of applying specified auditing procedures to financial information other than financial statements*.

Our procedures did not constitute an audit of the services provided by Entrust. Accordingly, we do not express any opinion on the assertions made in this report.

The sufficiency of the procedures outlined in this report is solely the responsibility of the specified users of the report. Consequently, we make no representation regarding the sufficiency of the procedures set out therein, either for the purpose for which this report has been requested, or for any other purpose. Had we performed additional procedures, other matters might have come to our attention that would have been reported.

The specified procedures performed relate to information and procedures performed during testing which took place between 25 May 2019 and 22 July 2019. Any projection of the results of the procedures to the future is subject to the risk that the status of Entrust services may have changed.

This report was prepared solely for the information and use of Entrust, and the Browser community (Mozilla, Microsoft Corporation, Google Inc., and Apple Inc.) and is not intended to be and should not be used by anyone other than these specified users.



Chartered Professional Accountants  
Toronto, Ontario, Canada  
25 July 2019

## Appendix A – Specified procedures

The following specified procedures are to be performed under the scope of this engagement.

The “Criteria” refers to the criterion number under WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security 2.3 Principle 4. The “Deficiency” refers to the exceptions reported by Deloitte as part of the 2018-2019 WebTrust for CA – SSL Baseline with Network Security assurance report. The “New control activity” refers to new control activities developed by Entrust. The “Specified procedures performed” refers to the agreed upon procedures performed as part of this engagement. The “Results” refers to the results of performing the agreed upon procedures.

#	Criteria	Deficiency	New control activity	Specified procedures performed	Results
1	P4, 4.3	During the Period, there were instances of some Certificate Systems not undergoing a Vulnerability Scan at least every three (3) months.	<p>Vulnerability scans are performed on the public and private IPs of EDC’s Certificate Systems at least once every 3 months.</p> <p>Vulnerability scans are performed when changes made to EDC’s Certificate Systems’ networks or systems are deemed significant in nature.</p> <p>Vulnerability scans are performed on the public and private IPs of EDC’s Certificate Systems within one week of receipt of a request from the CA/Browser Forum.</p>	<ol style="list-style-type: none"> <li>1. Interviewed management and noted a vulnerability scan of public and private IPs of EDC’s Certificate Systems has been planned for 31 May 2019. Also noted a process has been established to conduct scans when significant changes to networks or systems occur, or within one week when a request is received from the CA/Browser Forum.</li> <li>2. Inspected the vulnerability scan report for the scan completed on 31 May 2019 and noted it included the public and private IPs of EDC’s Certificate Systems.</li> <li>3. Inspected planning information and noted vulnerability scans of EDC’s Certificate Systems are scheduled to occur at 3-month intervals with the next scan planned for the week of 19 August 2019.</li> <li>4. Inspected process documentation and noted defined processes exist to conduct scans when significant network or system changes occur, and within one week of receiving a request from the CA/Browser Forum.</li> </ol>	<b>No exceptions noted.</b>
2	P4, 2.15	During the Period, there were instances where a technical control to restrict remote access to only those devices owned or controlled by Entrust did not operate effectively.	Remote administration access requires VPN, multi-factor authentication and validation that the connection originates from a device owned or controlled by EDC.	<ol style="list-style-type: none"> <li>1. Inspected VPN configuration and noted device validation controls have been implemented and enabled as of 30 May 2019.</li> <li>2. Inspected VPN system logs and noted devices that fail implemented validation controls are denied access.</li> </ol>	<b>No exceptions noted.</b>