Deloitte.

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 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 September 18th, 2018 and September 26th, 2018. 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.

Deloitte LLP.

Chartered Professional Accountants
Toronto, Ontario, Canada
September 30th, 2018

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 2.2 Principle 4. The "Deficiency" refers to the exceptions reported by Deloitte as part of the 2017 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	4.6	During the Period, there were instances where upon the discovery of a Critical Vulnerability any of the following did not occur within 96 hours: • Remediation of the vulnerability; • Creation and implementation of a plan to mitigate the vulnerability; or • Documentation of the factual basis for Entrust's determination that the vulnerability does not require remediation. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 4, Criterion 4.6 to not be met.	New processes have been developed, reviewed, and implemented to provide improved monitoring and control of vulnerability management. On a monthly basis vulnerability scans are run to identify all vulnerabilities with a CVSS score of 7 or above and included in a report (ECS DR AT VA Results) which is delivered on Day 3. Owners are identified for each vulnerability / asset pair and then are responsible for providing a 96-hour response and/or remediation of all true critical vulnerabilities. These responses are documented in the SSL Vulnerability Plan report. The 96-hour responses will either be: • A confirmation that the vulnerability is remediated; or, if remediation is not possible within 96 hours • A documented and implemented plan to remediate (giving priority to those vulnerabilities with a high CVSS or systems that lack sufficient compensating controls); or, if remediation is deemed not necessary Documentation to justify why remediation is not necessary (e.g. disagreement with NVD rating, false positive, compensating controls, etc.)	1. Interviewed ECS Ops Management and TVM management to walkthrough the revised process for addressing Critical Vulnerabilities within 96 hours of discovery. 2. Inspected documented vulnerability management process flow and narrative to assess if the new process meets WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security 2.2 Principle 4, Criteria 4.6. 3. Reviewed the "ECS DR AT VA Results" and "SSL Vulnerability Plan" Reports for the months of July 2018, August 2018 and September 2018. For all Critical Vulnerabilities identified, inspected evidence to confirm that one of the following was performed within 96 hours of discovery: a. Remediate the Critical Vulnerability; b. If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: i. Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and ii. Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; OR c. Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: i. The CA disagrees with the NVD rating; ii. The identification is a false positive; iii. The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or iv. Other similar reasons.	**No exceptions noted.**

Deloitte.

www.deloitte.ca

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

© Deloitte LLP and affiliated entities