Deloitte LLP
Bay Adelaide Centre, East Tower
8 Adelaide Street West
Suite 200
Toronto, ON M5H 0A9
Canada

Tel: +1 416 601 6150
Fax: +1 416 601 6400
www.deloitte.ca

INDEPENDENT ASSURANCE REPORT

To the management of Entrust Limited ("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 March 1, 2025 to September 17, 2025 (the "Period") for its CAs as enumerated in Attachment A, Entrust has:

- disclosed its Mark Certificate (MC) practices and procedures in its Certificate Policy/ Certification Practice Statements ("CP/CPS") as enumerated in Attachment B including its commitment to provide Mark Certificates in conformity with Minimum Security Requirements for Issuance of Mark Certificates v1.6, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - Mark Certificate subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority ("RA"), and/or subcontractor) and verified;
  - The integrity of CA keys it manages is established and protected throughout their life cycles.

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Mark Certificates v1.6.

Entrust does not archive keys or issue certificates to Business and Non-Commercial Entities, does not use delegated third parties or subordinate CAs. Accordingly, our procedures did not extend to controls that would address those criteria.

The Minimum Security Requirements for Issuance of Mark Certificates issued by the AuthIndicators Working Group require the CA to operate controls to adhere to the Network and Certificate System Security Requirements. The WebTrust Principles and Criteria for Certification Authorities - Network Security address this requirement and are reported on in a separate report.

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 – Mark Certificates v1.6.

Our independence and quality management

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 Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires the firm to design, implement and operate a system of quality management, including policies or 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*. 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 Mark Certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of Mark certificates;
(2) selectively testing transactions executed in accordance with disclosed Mark 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.

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Emphasis of matters

Without modifying our opinion, we draw attention to the following matters relevant to the scope of our procedures. In accordance with Entrust's transition plan, Entrust has stopped issuing MC as of May 12, 2025. All other public-facing services, including certificate issuance, renewals, and revocations, were discontinued as of September 8, 2025. Entrust did not generate any new cryptographic keys during the audit period; therefore, controls related to key generation were considered out of scope for this engagement.

As part of the transition plan and transfer of ownership of MC key pairs – VMCR1 and VMC2 to Sectigo, key backups were generated by Entrust, formally transported to Sectigo, and remaining copies were subsequently destroyed. While Deloitte independently witnessed the Key Destruction Ceremonies of the VMCR1 key at the Toronto location on September 4, 2025, and the VMC2 key at the Ottawa location on September 16, 2025, we were not engaged to independently observe the key backup procedures, nor did we witness the ceremony associated with the transfer of backup keys to Sectigo.

Opinion

In our opinion, throughout the period March 1, 2025 to September 17, 2025, 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 - Mark Certificates v1.6.

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 – Mark Certificates v1.6., nor the suitability of any of Entrust's services for any customer's intended purpose.

Deloitte.

Use of the WebTrust seal

Entrust's use of the WebTrust for Certification Authorities – Mark Certificates 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

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
November 19, 2025

Deloitte.

ATTACHMENT A

LIST OF IN SCOPE CAs

Verified Marks Certification CA
1. Entrust Verified Mark Root Certification Authority - VMCR1
2. Entrust Verified Mark CA - VMC2

CA IDENTIFYING INFORMATION

CA #	Cert #	Note	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
1	1	1,2	CN=Entrust Verified Mark Root Certification Authority - VMCR1 O=Entrust, Inc. C=US	CN=Entrust Verified Mark Root Certification Authority - VMCR1 O=Entrust, Inc. C=US	743900bd5b07fc63d7e9150452c89bb701680463	RSA 4096-bits	RSA SHA-512	5/7/2021 13:31	12/30/2040 13:31			7323567b2b7845809ab8c27ccca586398b2678c5	7831D95A47D42508CD5C9E6264F9096BAC19F04EB9B7C8BDD35FFFC71C189617
2	1	1,2	CN=Entrust Verified Mark CA - VMC2 O=Entrust, Inc. C=US	CN=Entrust Verified Mark Root Certification Authority - VMCR1 O=Entrust, Inc. C=US	699d8fd758c2c39c1e53d1aa1476d1e6	RSA 4096-bits	RSA SHA-512	5/7/2021 19:23	12/19/2040 23:59		1.3.6.1.5.5.7.3.31	efbc3cb4af3ad0455e7654dfc76478e92d1d743f	C269504B491DBF451A695B953711ADC5CD70975B5FCA1E181EBBD2172CB07E0C

Note:
1- Copy of the key was destroyed during Key Destruction Ceremony on September 4, 2025, or September 16, 2025
2- Backup Key was transferred to Sectigo on August 14, 2025

ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement	3.29	February 21, 2025

ENTRUST MANAGEMENT'S STATEMENT

Entrust Limited ("Entrust") operates the Certification Authority ("CA") services as enumerated in Attachment A, and provides Mark Certificate ("MC") services.

The management of Entrust is responsible for establishing and maintaining effective controls over MC CA operations, including its MC CA business practices disclosure on its website, MC key lifecycle management controls, and MC 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 MC CA services. Based on that assessment, in Entrust management's opinion, in providing its MC CA services at Ottawa, Ontario, Canada, and Toronto, Ontario, Canada, throughout the period March 1, 2025 to September 17, 2025, Entrust has:

- disclosed its Mark certificate practices and procedures in its Certificate Policy/ Certification Practice Statements ("CP/CPS") as enumerated in Attachment B, including its commitment to provide Mark certificates in conformity with the applicable Minimum Security Requirements for Issuance of Mark Certificates v1.6, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
    - MC subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA), and/or subcontractor) and verified;
    - The integrity of CA keys it manages is established and protected throughout their life cycles.

- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Mark Certificates v1.6.

Signed by:
Jim Trovato
89D32B44D9C945B...

Jim Trovato
Director, Product Compliance
November 19, 2025

ATTACHMENT A

LIST OF IN SCOPE CAs

Verified Marks Certification CA
1. Entrust Verified Mark Root Certification Authority - VMCR1 2. Entrust Verified Mark CA - VMC2

ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement	3.29	February 21, 2025