

INDEPENDENT ASSURANCE REPORT

To the management of Entrust Corporation (“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 1 March 2022 to 28 February 2023 (the “Period”) for its CAs as enumerated in [Attachment A](#), Entrust has:

- disclosed its Verified Mark (“VM”) certificate practices and procedures in its Certification Practice Statements as enumerated in [Attachment B](#), including its commitment to provide VM certificates in conformity with the applicable Verified Mark Certificate Requirements as set at out at https://bimigroup.org/resources/VMC_Guidelines_latest.pdf, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - VMC 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.0](#).

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 – Verified Mark Certificates v1.0.

Our independence and quality control

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 Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and accordingly maintains a comprehensive system of quality control including documented policies and 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*, set out in the CPA Canada Handbook – Assurance. 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 VM certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of VM certificates;



- (2) selectively testing transactions executed in accordance with disclosed VM 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.

Relative effectiveness of controls

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.

Other matters

Without modifying our opinion, we noted the following other matters during our procedures:

| Matter topic | Matter description |
|----------------------------------|--|
| 1 Mozilla 'bug' responses | As described in management's statement, management has reported or responded to certain 'bugs' on Mozilla's Bugzilla reporting system. Management's statement contains information on their outcome or resolution. |

Practitioner's opinion

In our opinion, throughout the period 1 March 2022 to 28 February 2023, 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 – Verified Mark Certificates v1.0.

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 – Verified Mark Certificates v1.0., nor the suitability of any of Entrust's services for any customer's intended purpose.

Use of the WebTrust seal

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.

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
18th May 2023



ATTACHMENT A

LIST OF IN SCOPE CAs

| |
|---|
| Root CAs |
| 1. Entrust Verified Mark Root Certification Authority - VMCR1 |
| Verified Mark Certificate Issuing CAs |
| 2. Entrust Verified Mark CA - VMC2 |



CA IDENTIFYING INFORMATION

| CA # | Cert # | Subject | Issuer | Serial Number | Key Type | Hash Type | Not Before | Not After | Revoked Date | Extended Key Usage | Subject Key Identifier | SHA256 Fingerprint |
|------|--------|--|--|--|-------------------|-----------------|------------------------|------------------------|--------------|--------------------|--|--|
| 1 | 1 | 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 | 2021-05-07 13:31:48 | 2040-12-30 13:31:48 | | | 7323567b2b7845809ab8c27ccca586398b2678c5 | 7831d95a47d42508cd5c9e6264f9096bac19f04eb9b7c8bdd35ffc71c189617 |
| 2 | 1 | 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 | 2021-05-07 19:23:23 | 2040-12-29 23:59:00 | | 1.3.6.1.5.5.7.3.31 | efbc3cb4af3ad0455e7654dfc76478e92d1d743f | c269504b491dbf451a695b953711adc5cd70975b5fca1e181ebbd2172cb07e0c |



ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

| CPS Name | Version | Date |
|---|---------|-------------|
| Entrust Certificate Services Certification Practice Statement | 3.12 | 31 Jan 2023 |
| Entrust Certificate Services Certification Practice Statement | 3.11 | 30 Sep 2022 |
| Entrust Certificate Services Certification Practice Statement | 3.10 | 18 Feb 2022 |



ENTRUST MANAGEMENT'S STATEMENT

Entrust Corporation ("Entrust") operates the Certification Authority ("CA") services as enumerated in [Attachment A](#), and provides Verified Mark ("VM") Certificate services.

The management of Entrust is responsible for establishing and maintaining effective controls over VM CA operations, including its VM CA business practices disclosure on its [website](#), VM key lifecycle management controls, and VM 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 VM CA services. Based on that assessment, in Entrust management's opinion, in providing its VM CA services at Ottawa, Ontario, and Toronto, Ontario throughout the period 1 March 2022 to 28 February 2023, Entrust has:

- disclosed its Verified Mark certificate practices and procedures in its Certification Practice Statements as enumerated in [Attachment B](#), including its commitment to provide VM certificates in conformity with the applicable Verified Mark Certificate Requirements as set out at https://bimigroup.org/resources/VMC_Guidelines_latest.pdf, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - VMC 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates v1.0](#).

Entrust management has also reported the following 'bugs' on Mozilla's Bugzilla reporting system:

| Bug ID | Summary | Opened | Closed |
|---------|--|-------------|-------------|
| 1737057 | CRLs and OCSP responses not issued as specified in the CPS | 21-Oct-2021 | 8-Mar-2022 |
| 1802916 | EV TLS Certificate incorrect jurisdiction | 28-Nov-2022 | 24-Apr-2023 |
| 1804753 | Delayed Revocation for EV TLS Certificate incorrect jurisdiction | 8-Dec-2022 | 19-Apr-2023 |

Bruce Morton
Director, Entrust Certificate Services
18th May 2023



ATTACHMENT A

LIST OF IN SCOPE CAs

| |
|---|
| Root CAs |
| 1. Entrust Verified Mark Root Certification Authority - VMCR1 |
| Verified Mark Certificate Issuing CAs |
| 2. Entrust Verified Mark CA - VMC2 |



ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

| CPS Name | Version | Date |
|---|---------|-------------|
| Entrust Certificate Services Certification Practice Statement | 3.12 | 31 Jan 2023 |
| Entrust Certificate Services Certification Practice Statement | 3.11 | 30 Sep 2022 |
| Entrust Certificate Services Certification Practice Statement | 3.10 | 18 Feb 2022 |