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 business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in it's Certificate Policy/ Certification Practice Statements ("CP/CPS") as enumerated in Attachment B

- maintained effective controls to provide reasonable assurance that Entrust provides its services in accordance with its CP/CPS

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by Entrust); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2

Entrust does not escrow or archive its CA keys and subscriber keys, does not provide integrated circuit card management services, does not provide certificate suspension services and does not use external Registration Authorities. Accordingly, our procedures did not extend to controls that would address those criteria.

During the course of our procedures, we noted that certain controls defined within the applicable criteria were not triggered during the audit period due to the absence of relevant operational events. Specifically, activities such as the generation of CA keys (including root CA keys), CA key migration, and the registration, renewal, rekey, issuance, and distribution of subordinate CA certificates and cross-certificates did not occur. While these controls are documented within Entrust's Certification Practice Statement (CPS), their operational effectiveness could not be evaluated during this engagement.

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 v2.2.2.

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,* 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 key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
(2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business 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, 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.

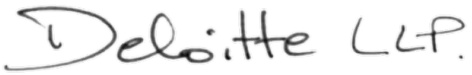
Opinion

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 v2.2.2.

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 v2.2.2, 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
November 19, 2025

Deloitte.

ATTACHMENT A

LIST OF IN SCOPE CAs

Shared Root CAs
1. Entrust Root Certification Authority - G3 2. Entrust Root Certification Authority – PRIV TLSR 2022 3. Entrust 4K Client Root CA - 2024 4. Entrust P384 Client Root CA - 2024
Client Authentication CAs
5. Entrust 4K Client CA - Client1 6. Entrust P384 Client CA – Client2
Shared SSL Issuing CAs
7. Entrust Private Trust SSL CA - PrivSSL1 8. Entrust Private TLS Certification Authority – PrivTLS1
Shared Mobile Device Certificate Issuing CAs
9. Entrust Certification Authority - L1H
eSIM Issuing CAs
10. Entrust eSIM Certification Authority

Deloitte.

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	SHA-256 Fingerprint
1	1	CN=Entrust Root Certification Authority - G3 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G3 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00c2bb63ea0000000050d0b5a1	RSA 2048-bits	RSA SHA-1	12/18/2012 17:57	18/12/2030 18:27			b57501ee41c7ca7a3ff2fc5a56c776060b066c66	158399559E3085027D3CD7E813923F8B54E54FF725E67E70D0286BB1D502DE64
2	1	CN = Entrust 4K Private TLS Root CA - 2022 O = Entrust, Inc. C = US	CN = Entrust 4K Private TLS Root CA - 2022 O = Entrust, Inc. C = US	78c885e63beff8175f17bf14e228e04739cac23f	RSA 4096-bits	RSA SHA-384	12/13/2022 12:56	12/07/2047 12:56			dd1adb235f00ee1989276d1210f0c8143329ccc2	822F5EAFA4E17C27B1904610132EFF00A2005DA0C9AC113C3F5A81F3CDC06E5F
3	1	CN = Entrust 4K Client Root CA – 2024 O = Entrust, Inc. C = US	CN = Entrust 4K Client Root CA - 2024 O = Entrust, Inc. C = US	2FB1D7468F0B138D4D6FDDA5D0F815395F48543D	RSA 4096-bits	RSA SHA-384	7/24/2024 14:00	7/23/2049 14:00			143879FBB5583B6138F45DE28B32A7A507E27507	621A840CDEECFDDB20B2528E5E8AE5CBA6D2FDC23020BC7BA04FA90F54833D74
4	1	CN=Entrust P384 Client Root CA - 2024 O=Entrust, Inc. C=US	CN=Entrust P384 Client Root CA - 2024 O=Entrust, Inc. C=US	1e3bdb63c66d0904c2c68263cee6845535199faa	384 bits	ECDSA SHA-384	7/24/2024 14:09	7/23/2049 14:09			6C79BDFE09E30965CD682D370EB693E60CFFC314	481F0E1B0874D84B189FF83A694D27B30ECD2A477AB3289E976C7FA1A6BD255B
5	1	CN = Entrust 4K Client CA - Client1 O = Entrust C = US	CN = Entrust 4K Client Root CA – 2024 O = Entrust, Inc. C = US	24de798d488441a7d026db305996043a	RSA 4096-bits	RSA SHA-384	7/24/2024 17:45	12/29/2040 23:59			4775F09CF5BD101D755B9EF38C855733A535330D	58C8CEAC8C50BA2ADFF1AF675AFAD118A0125B4B0070834B070C16F646D85D17
6	1	CN = Entrust P384 Client CA – Client2 ON = Entrust C = US	CN=Entrust P384 Client Root CA - 2024 O=Entrust, Inc. C=US	5c305c4ffc05841af97cb8a2aecf8879	384 bits	ECDSA SHA-384	7/24/2024 17:49	12/29/2040 23:59			1B21F09CADC08D0C57561B429C4DF2A77815CAC2	307F34CDBAFABFDBC8952ED153DEC54E0D0B5F60784159580D409D26A7C7C91A
7	1	CN=Entrust Private Trust SSL CA - PrivSSL1 O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G3 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	51aeabf74ef4aad8400562aac1bfae41	RSA 2048-bits	RSA SHA-256	07/28/2021 00:00	12/18/2030 00:00:00		TLS Web Server Authentication, TLS Web Client Authentication	63266b9530c1a8201083325162296262db7ea4d7	48AC388ECE21B6700DAB974CD884F38D84BE15446D924254CBF5E9DCB4CB4B3B
8	1	CN = Entrust Private TLS Certification Authority - PrivTLS1 O = Entrust, Inc. C = US	CN = Entrust 4K Private TLS Root CA - 2022 O = Entrust, Inc. C = US	516744af30940fef988fa7ccc7593761	RSA 4096-bits	RSA SHA-384	12/14/2022 18:28	12/29/2040 23:59			a4f626d81868bc199b69241e76260edac7b4c8e8	30B892723B8457269C4D7A71EA521EECFF9242C7A4C582F63DFAF93DA3FA74F4
9	1	CN=Entrust Certification Authority - L1H OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G3 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	591fa9d50000000051d35641	RSA 2048-bits	RSA SHA-256	10/06/2015 15:12	12/06/2030 15:42			90915cfb528ff4fbbb373e03ff39631ea0691b81	1897FA1EBC96E0BA416326C135AFDBEAE8A8C1A7913D8C5456ECA44BDBD12E69
	2	CN=Entrust Certification Authority - L1H OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G3 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00d0e3f4a00000000051d35642	RSA 2048-bits	RSA SHA-1	10/06/2015 15:14	12/06/2030 15:44			90915cfb528ff4fbbb373e03ff39631ea0691b81	29F1CA3D679DAA79C91685648366AABDF578ADD83867164C80A84D08A46D9638
10	1	CN=Entrust eSIM Certification Authority OU=(c) 2016 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust eSIM Certification Authority OU=(c) 2016 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	008cb8193ecce671ec00000000582c8a7a	EC 256-bits	ECDSA SHA-256	11/16/2016 16:04	10/16/2051 16:34			16704b7f351e3607f18c4b70005c3a003dfd414a	94457E185C7059DDD484FBA87F86D10C2EE89E95571982C4DF3DE67E8F52007C

ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement for Private Trust Certificates	2.7	January 15, 2025

ENTRUST MANAGEMENT'S STATEMENT

Entrust Limited ("Entrust") operates the Certification Authority ("CA") services as enumerated in Attachment A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management

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

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its Certificate Policy/Certification Practice Statements ("CP/CPS") as enumerated in Attachment B

- maintained effective controls to provide reasonable assurance that Entrust provides its services in accordance with its CP/CPS

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
    - subscriber information is properly authenticated (for the registration activities performed by Entrust); and
    - subordinate CA certificate requests are accurate, authenticated, and approved

- 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 v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement ("CPS")

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Entrust does not escrow or archive its CA keys and subscriber keys, does not provide integrated circuit card management services, does not provide certificate suspension services and does not use external Registration Authorities. Accordingly, our procedures did not extend to controls that would address those criteria.

Signed by:
Jim Trovato
89D32B44D9C945B...

Jim Trovato
Director, Product Compliance
November 19, 2025

ATTACHMENT A

LIST OF IN SCOPE CAs

Shared Root CAs
1. Entrust Root Certification Authority - G3 2. Entrust Root Certification Authority – PRIV TLSR 2022 3. Entrust 4K Client Root CA - 2024 4. Entrust P384 Client Root CA - 2024
Client Authentication CAs
5. Entrust 4K Client CA - Client1 6. Entrust P384 Client CA – Client2
Shared SSL Issuing CAs
7. Entrust Private Trust SSL CA - PrivSSL1 8. Entrust Private TLS Certification Authority – PrivTLS1
Shared Mobile Device Certificate Issuing CAs
9. Entrust Certification Authority - L1H
eSIM Issuing CAs
10. Entrust eSIM Certification Authority

ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement for Private Trust Certificates	2.7	January 15, 2025