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 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, 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 business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statements as enumerated in Attachment B

- maintained effective controls to provide reasonable assurance that Entrust provides its services in accordance with its Certification Practice Statements

- 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, 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 Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA and Cross Certificate Lifecycle Management

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

Entrust has issued cross-certificates to third-party certification authorities which were valid during the Period. The operations of these third-party certification authorities were not in scope for our engagement, and, accordingly, we express no opinion on these third-party certification authorities.

Entrust has additional Issuing CAs not in the scope of this report that chain to Root and/or Intermediate CAs within the scope of this report. These Issuing CAs do not issue TLS Web Server, Code Signing, or Time Stamping certificates. Our procedures did not extend to these Issuing CAs, and, accordingly, we express no opinion on them.

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 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*

Deloitte.

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.

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.
2	**No occurrences of in scope events during the audit period**	During the examination period there were no instances or occurrences of underlying events related to the following control activities: • Section 4.7 CA Key Compromise No key compromise event occurred during the audit period. As underlying event had not occurred, related control activities did not operate during period under audit. • Section 4.11 CA Key Migration No key migration event occurred during the audit period. As underlying event had not occurred, related control activities did not operate during period under audit.

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 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.

Deloitte.

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

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

Deloitte.

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Entrust.net Certification Authority (2048)
2. Entrust Root Certification Authority – EV Root
3. Entrust Root Certification Authority – G2
4. Entrust Root Certification Authority – G4
5. Entrust Root Certification Authority – EC1
6. Entrust Root Certification Authority – CSBR1
7. Entrust Root Certification Authority – VMCR1
8. Entrust Root Certification Authority – 4K EVTLSR 2022
9. Entrust Root Certification Authority – P384 EVTLSR 2022
10. Entrust Root Certification Authority – 4K TLSR 2022
11. Entrust Root Certification Authority – P384 TLSR 2022
12. Entrust Root Certification Authority – SMIMER 2022
Intermediate CAs
13. Entrust Certification Authority – AATL1
14. Entrust Certification Authority – ICA1
OV SSL Issuing CAs
15. Entrust Certification Authority – L1F
16. Entrust Certification Authority – L1K
17. Entrust Certification Authority – OVTLS1
18. Entrust Certification Authority – OVTLS2
19. Entrust Certification Authority – CrowdStrike TLS CA 2022
20. Siemens 2020
21. Entrust Certification Authority – Namirial OV SSL
EV SSL Issuing CAs
22. Entrust Certification Authority – L1E
23. Entrust Certification Authority – L1J
24. Entrust Certification Authority – L1M
25. Entrust Certification Authority – L1N
26. Entrust Certification Authority – QTSP1
27. Entrust Certification Authority – ES QWAC2
28. Entrust Certification Authority - EVTLS1
29. Entrust Certification Authority - EVTLS2
30. Entrust Certification Authority - Namirial EV SSL
Publicly Trusted Code Signing Issuing CAs
31. Entrust Code Signing CA – OVCS1
32. Entrust Code Signing CA – OVCS2
EV Code Signing Issuing CA
33. Entrust Extended Validation Code Signing CA – EVCS1
34. Entrust Extended Validation Code Signing CA – EVCS2
Secure Email (S/MIME) CA
35. Class 1 Client CA – SHA256
36. Entrust Class 2 Client CA
37. Entrust Class 2 Client CA – C2CA2
38. Entrust SMIME1 Client CA
Timestamp CA
39. Entrust Timestamping CA – ES QTS1
40. Entrust Timestamping CA – TS1
41. Entrust Timestamping CA – TS2
Verified Marks Certification CA
42. Entrust Certificate Authority – VMC2

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	SHA256 Fingerprint
1	1	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	3863def8	RSA 2048-bits	RSA SHA-1	1999-12-24 17:50:51	2029-07-24 14:15:12			55e481d11180bed889b908a331f9a1240916b970	6dc47172e01cbcb0bf62580d895fe2b8ac9ad4f873801e0c10b9c837d21eb177
2	1	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	456b5054	RSA 2048-bits	RSA SHA-1	2006-11-27 20:23:42	2026-11-27 20:53:42			6890e467a4a65380c78666a4f1f74b43fb84bd6d	73c176434f1bc6d5adf45b0e76e727287c8de57616c1e6e6141a2b2cbc7d8e4c
3	1	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	4a538c28	RSA 2048-bits	RSA SHA-256	2009-07-07 17:25:54	2030-12-07 17:55:54			6a72267ad01eef7de73b6951d46c8d9f901266ab	43df5774b03e7fef5fe40d931a7bedf1bb2e6b42738c4e6d3841103d3aa7f339
3	2	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	51d33f09	RSA 2048-bits	RSA SHA-1	2014-09-12 17:28:27	2024-09-13 03:12:02			6a72267ad01eef7de73b6951d46c8d9f901266ab	cbce622d06f9d2c093fad75cebb7852ef553ffff146ad522ab321b3a4b2bd8f8
3	3	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	51d33f24	RSA 2048-bits	RSA SHA-1	2014-09-12 19:23:57	2024-09-13 03:12:23			6a72267ad01eef7de73b6951d46c8d9f901266ab	16296e3bef9a64cfede3509f36d700a5cd61cf938ec3a955bf36d17d97e16e8d
3	4	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	51d34044	RSA 2048-bits	RSA SHA-256	2014-09-22 17:14:57	2024-09-23 01:31:53			6a72267ad01eef7de73b6951d46c8d9f901266ab	6b143c2005d5539cc22eab5f772db2a9fe87467feffa07fcf0a9f7d28274ca7a
4	1	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00d9b5437fafa9390f000000005565ad58	RSA 4096-bits	RSA SHA-256	2015-05-27 11:11:16	2037-12-27 11:41:16			9f38c45623c339e8a0716ce8544ce4e83ab1bf67	db3517d1f6732a2d5ab97c533ec70779ee3270a62fb4ac4238372460e6f01e88
5	1	CN=Entrust Root Certification Authority - EC1 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 - EC1 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00a68b79290000000050d091f9	EC 384-bits	ECDSA SHA-384	2012-12-18 15:25:36	2037-12-18 15:55:36			b763e71add8de908a65583a4e06a504165114249	02ed0eb28c14da45165c566791700d6451d7fb56f0b2ab1d3b8eb070e56edff5
5	2	CN=Entrust Root Certification Authority - EC1 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 OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	008011196de613db1600000000051d3575e	EC 384-bits	RSA SHA-256	2016-06-10 14:58:55	2026-11-10 15:28:55			b763e71add8de908a65583a4e06a504165114249	3fde0d36e026b6e8ebe2c28883607c8651de10bd6c1fcad365e560f4ea2f3b03
6	1	CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US	CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US	7ff1a8f9f43ae8876e2dc6ff5e433db2ee30a643	RSA 4096-bits	RSA SHA-512	2021-05-07 13:26:36	2040-12-30 13:26:36			82bad63d97ce9fcf71e89237affdb3b5693557cf	b80847fda453bf6ed876ca7bc046a2481909e15b6ed376e665e7ad09f3864e71
6	2	CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	4e40e43754ede68c0000000051d3947f	RSA 4096-bits	RSA SHA-256	2021-05-07 15:43:45	2030-11-07 16:13:45		Code Signing, Time Stamping	82bad63d97ce9fcf71e89237affdb3b5693557cf	18dd9a467054c74a5ae46182843a6f4ec46d5e338d91adf4e5980b50193fb94b
7	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	7831d95a47d42508cd5c9e6264f9096bac19f04eb9b7c8bdd35fffc71c189617
8	1	CN = Entrust 4K EV TLS Root CA - 2022 O = Entrust, Inc. C = US	CN = Entrust 4K EV TLS Root CA - 2022 O = Entrust, Inc. C = US	72429d8f40dfe46dafbe06ebb533194ce90d6c76	RSA 4096-bits	RSA SHA-384	2022-12-13 12:35:08	2047-12-07 12:35:08			0bdd90d58fbb3f5cbd60a0551a2482863c413041	647987D98D52645DA4D3DE3B80771A0CE02B9B9285E6E86999882170744EC9AA
9	1	CN = Entrust P384 EV TLS Root CA - 2022 O = Entrust, Inc. C = US	CN = Entrust P384 EV TLS Root CA - 2022 O = Entrust, Inc. C = US	097558f5a16c16877bbd064ffd9ce483ba4b040b	EC 384-bits	ECDSA SHA-384	2022-12-13 12:46:44	2047-12-07 12:46:44			137210ae82580fc1389bbcb6a64c05ca8e8468bf	937EF8F12276B3C7A3F58E345D09A6EFF01F862F8D2794441CD84D511825FA0C

Deloitte.

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
10	1	CN = Entrust 4K TLS Root CA - 2022 O = Entrust, Inc. C = US	CN = Entrust 4K TLS Root CA - 2022 O = Entrust, Inc. C = US	57262836aa751a000c16ba28cc86b590fdf225ba	RSA 4096-bits	RSA SHA-384	2022-12-13 12:26:47	2047-12-7 12:26:47			9440ea5affef4963019e09dfe03b803373122056	DD6C44B39401B053DBE61120748BBB0F6056007665C168E5C286750EDC8DF129
11	1	CN = Entrust P384 TLS Root CA - 2022 O = Entrust, Inc. C = US	CN = Entrust P384 TLS Root CA - 2022 O = Entrust, Inc. C = US	453eef32daed9068218d5bea0e83d165042e0f31	EC 384-bits	ECDSA SHA-384	2022-12-13 12:41:45	2047-12-7 12:41:45			c42e807c5f709204864c9e52cb2b67c5076a8293	420332EF876EBE78F2AF5D28AAACDE24AAD0C10F8FFAAC469EFD7BD941929568
12	1	CN = Entrust SMIME Root CA - 2022 O = Entrust, Inc. C = US	CN = Entrust SMIME Root CA - 2022 O = Entrust, Inc. C = US	7da23fcefbbe8849c350f2a511e9b96bb71f8d80	RSA 4096-bits	RSA SHA-384	2022-12-13 13:00:46	2047-12-7 13:00:46			94c8e8468d7f53170305441810ac65e06ea2950d	B7A41ED8096D62716BADC7F530942197A9E7E3175CE05D11D01E7AD6C12DCBA7
13	1	C=US O=Entrust, Inc. CN=Entrust Certification Authority - AATL1	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00c727f51f8f922b020000000005565d8ad	RSA 4096-bits	RSA SHA-512	2020-07-20 15:46:21	2037-12-20 16:16:21		1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5, E-mail Protection	63f184dd03bea39f64fa767a47c4567ec06da020	839f9b91c2e49218a66416df181b984e9be634d12a95483d98a6199fc0788d74
14	1	CN=Entrust Enterprise Intermediate CA - ICA1 O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	3eeb174d9b443ba90000000051ce1981	RSA 2048-bits	RSA SHA-256	2021-05-07 15:32:00	2029-07-07 16:02:00		TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin, Microsoft Encrypted File System, 1.3.6.1.4.1.311.10.3.4.1, 1.3.6.1.4.1.311.67.1.1	c838d40a70dda357a8e596592d1313c920d5dcb3	c54d8b12c438725c2755b4ad81825f6975cbda6c258a2bfbb8247a14f03bd22a
15	1	CN=Entrust Certification Authority - L1F OU=(c) 2016 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - EC1 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00b601913d8553bafa0000000051d4c1f6	EC 384-bits	ECDSA SHA-384	2016-04-05 20:17:29	2037-10-05 20:47:29		TLS Web Server Authentication, TLS Web Client Authentication	2e62f014ee87cdb335033defe4b99efd3bb8a3c9	1835b0e482ea65536fc010e4bc13c060f65668165fba97e2f542ce96ca6dfefc
15	2	CN=Entrust Certification Authority - L1F OU=(c) 2016 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	00a25b1769bad80ad70000000051ce1941	EC 384-bits	RSA SHA-256	2021-02-05 16:34:34	2029-07-05 17:04:34		TLS Web Server Authentication, TLS Web Client Authentication	2e62f014ee87cdb335033defe4b99efd3bb8a3c9	0c5a09db8aedf7d2d1dde14dccc2db6ea959bcf6f010360d836c342c624d7e0e
16	1	CN=Entrust Certification Authority - L1K 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 - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	51d360ce	RSA 2048-bits	RSA SHA-256	2014-08-26 17:07:28	2024-08-27 05:48:52			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	3b6dd5581c9853092007db1bb0106fc61205e88e360543d7cae02d68e7a25ac3
16	2	CN=Entrust Certification Authority - L1K 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 - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	51d360cf	RSA 2048-bits	RSA SHA-256	2014-08-26 17:14:49	2024-08-27 08:34:47			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	3b0cc20384ad7f24eb438f2b80c63ebe003f7f215b8877e418ebb0484028db57
16	3	CN=Entrust Certification Authority - L1K OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	51ce00fe	RSA 2048-bits	RSA SHA-256	2014-10-10 15:23:17	2024-10-11 06:22:47			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	d6c3fc493bacd1df8a1ba30f4ae26254b2a4528e4876081eacc6a16a090aa36a
16	4	CN=Entrust Certification Authority - L1K 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 - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	51d360ee	RSA 2048-bits	RSA SHA-256	2014-10-22 17:05:14	2024-10-23 07:33:22			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	f5c2f23c6518f9d19b6f39beaea4fbae10031ba9dc985ce1563a520da0ad4116
16	5	CN=Entrust Certification Authority - L1K 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 - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	0ee94cc30000000051d37785	RSA 2048-bits	RSA SHA-256	2015-10-05 19:13:56	2030-12-05 19:43:56			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	13efb39a2f6654e8c67bd04f4c6d4c90cd6cab5091bcedc73787f6b77d3d3fe7
16	6	CN = Entrust Certification Authority - L1K OU = (c) 2012 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US	CN = Entrust.net Certification Authority (2048) OU = (c) 1999 Entrust.net Limited OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O = Entrust.net	2e0451ce5d2424c72b5d6576716506d8	RSA 2048-bits	RSA SHA-256	2022-11-25 17:19:43	2029-7-22 20:00:00		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	7f4325cc24107a39441552f27fdc34185802482e164d1794aa415ef1e4206ba7
17	1	CN = Entrust 4K TLS Certification Authority - OVTLS1 O = Entrust, Inc. C = US	CN = Entrust 4K TLS Root CA - 2022 O = Entrust, Inc. C = US	68ca04736adcebbd10432a6bd6ef8a34	EC 384-bits	RSA SHA-256	2022-12-14 14:23:34	2040-12-29 19:59:59		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	a80003c10185b8c0272aa9bc08acfad44abe51a5	9EC6CA44D6ADB5DAEFEFC9D773787E3BB8E1243F5455341B8438A6776869333B
18	1	CN = Entrust P384 TLS Certification Authority - OVTLS2 O = Entrust, Inc. C = US	CN = Entrust P384 TLS Root CA - 2022 O = Entrust, Inc. C = US	68772973693c55320a742ff1433ca0a2	EC 384-bits	RSA SHA-256	2022-12-14 14:25:44	2040-12-29 19:59:59		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	c25b7126ed58efa51419aa2ef60456546f9a39c9	2DB842F824321277291266B230ABC31DE13C1D4B852D6C21C9B1007D5AC20681
19	1	CN = CrowdStrike TLS CA 2022 O = CrowdStrike, Inc. C = US	CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US	309dc7b318912d0ecb7d1df27ab75cdf	RSA 2048-bits	RSA SHA-256	2022-11-15 12:50:48	2030-12-5 20:00:00			55eaa745b99af7b671311a31dfa176fe7692997a	2c4ad64b4e862d7d46424d9fa13ea9a974a62f7c4b608ae1a871424cc9a6873d

Deloitte.

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
20	1	C=DE O=Siemens CN=Siemens Issuing CA Internet Server 2020	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00fabb27ddff80d09a0000000051d39440	RSA 2048-bits	RSA SHA-256	2020-08-10 14:11:48	2030-11-10 14:41:48		TLS Web Server Authentication, TLS Web Client Authentication	c9a757cb86c96107c6c2b48665a91ec1cae1029b	a665007a05efe1889d66a40deecbc6c1a271e919006811fdb8dbd7e0675212d1
21	1	CN = Namirial OV SSL CA 2023 O = Namirial S.p.A C = IT	CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US	17c236215a437f11aae022348b6b7f2d	RSA 2048-bits	RSA SHA-256	2023=-2-9 16:09:10	2030-12-7 8:59:59		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	9a9f6fa5f8fe34fc102deb2f89c6b9d7c692d31e	f4e26beb0279228d96d47b05df744ae6ce6aad888a3b757d249eb3d22d27f4c6
22	1	CN=Entrust Certification Authority - L1E OU=(c) 2009 Entrust, Inc. OU=www.entrust.net/rpa is incorporated by reference O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	008666b02ac1cb54400000000051d3589c	RSA 2048-bits	RSA SHA-256	2019-06-19 16:52:08	2026-11-19 17:22:08		TLS Web Server Authentication, TLS Web Client Authentication	5b418ab2c443c1bdbfc85441559de096adffb9a1	232f6367cf561e00c83e180a9fca8546b3771fb450ebcb4a0526f8349c8ca139
23	1	CN=Entrust Certification Authority - L1J OU=(c) 2016 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - EC1 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	0a83d4803e7e9f510000000051d4c1f7	EC 384-bits	ECDSA SHA-384	2016-04-05 20:19:54	2037-10-05 20:49:54		TLS Web Server Authentication, TLS Web Client Authentication	c3f94503bec8f90b3c4535f3eb72ece7e8eb949b	3447b74b5e500a549983fa2ced73a5642e6aaec78829546158437df66d7435b8
24	1	CN=Entrust Certification Authority - L1M OU=(c) 2014 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	51d346e1	RSA 2048-bits	RSA SHA-256	2014-11-18 20:59:32	2024-11-19 06:33:02		TLS Web Client Authentication, TLS Web Server Authentication	c3f7d0b52a30adaf0d9121703954ddbc8970c73a	ca290389e0d8c62a4083f628a39f52fe3f38b73199cffaf7c0372378a440fb6a
24	2	CN=Entrust Certification Authority - L1M OU=(c) 2014 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	61a1e7d20000000051d366a6	RSA 2048-bits	RSA SHA-256	2014-12-15 15:25:03	2030-10-15 15:55:03		TLS Web Client Authentication, TLS Web Server Authentication	c3f7d0b52a30adaf0d9121703954ddbc8970c73a	75c5b3f01fd1f51a2c447ab7c785d72e69fa9c472c08571e7eadf3b8eabae70c
25	1	CN=Entrust Certification Authority - L1N OU=(c) 2014 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00abec77ff1b410c07000000005565d805	RSA 2048-bits	RSA SHA-256	2017-11-22 20:04:20	2030-12-22 20:34:20		TLS Web Server Authentication, TLS Web Client Authentication	ee47d18571f1fd2db73fbb3e6358771749400e95	b14d5089079c1d8f7649db9a5d3cefb1aac06f66afc49225c5be2aa19fd41a35
26	1	C=ES O=Entrust Datacard Europe S.L. organizationIdentifier=VATES-B81188047 CN=Entrust Certification Authority - QTSP1	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	009c6cf695700c60000000000051d393a6	RSA 2048-bits	RSA SHA-256	2019-07-26 18:31:45	2030-11-26 19:01:45		TLS Web Server Authentication, TLS Web Client Authentication	1cad3f9cd72d2219a19c4be9daf12a33f7fbba0d	681ebc1822b079b97e0404e4687d9b6c0c0892c820f55738a282aae62529bdd8
27	1	CN=Entrust Certification Authority - ES QWAC2 organizationIdentifier=VATES-B81188047 O=Entrust EU, S.L. C=ES	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	7a8872b868a359dab1b02ecf4fc9718d	RSA 2048-bits	RSA SHA-256	2021-11-16 00:00:00	2030-12-01 00:00:00		TLS Web Server Authentication, TLS Web Client Authentication	41cfae2b1d633bcb4cf5904479b65a2489df929c	c97f2f6e6a8adb6ecfe4978f08ca8f6f0123a94784522b610adf6ab51439fc62
28	1	CN = Entrust 4K TLS Certification Authority - EVTLS1 O = Entrust, Inc. C = US	CN = Entrust 4K EV TLS Root CA - 2022 O = Entrust, Inc. C = US	31ef81d7823f9a0f27b5d3085df41ec0	EC 384-bits	ECDSA SHA-384	2022-12-14 14:16:26	2040-12-29 19:59:59		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	9930115c04d2448b259713c665d21616c9678792	AAC8B9394C3BB037662244423534337 1C59E951FF85A151B3FE19C288076E2B5
29	1	CN = Entrust P384 TLS Certification Authority - EVTLS2 O = Entrust, Inc. C = US	CN = Entrust P384 EV TLS Root CA - 2022 O = Entrust, Inc. C = US	2ecf71fbc3f43015ca8bea5edd3dc763	EC 384-bits	ECDSA SHA-384	2022-12-14 14:20:13	2040-12-29 19:59:59		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	2cc1fad3279c77e73038c8c95ca43c02a36775c4	2426C77CFA12EBCDB6B013225496C0E7AAD66D63597AE5EF9A0BEB3830C23EC2
30	1	CN = Namirial EV SSL CA 2023 O = Namirial S.p.A C = IT	CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US	7b0350a7b1d46885af4cc8c740a568b0	RSA 2048-bits	RSA SHA-256	2023-02-09 16:13:06	2030-12-07 8:59:59		Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	eafeeb5847b833d9d2367bc88c677ab1338b8d52	366dd61ece49ef68a7e0705915ece7ee7baa3c5d71b9363cd487e0fe0242a634
31	1	CN=Entrust Code Signing CA - OVCS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	7ab8c4fc0000000051d373d4	RSA 2048-bits	RSA SHA-256	2015-06-09 18:03:40	2025-06-09 18:33:40		Code Signing	7e1a1f1a11745c64c90c1f9401abfd81642ea12c	7fba43a4ccbb37b1ccc2dd11ce0c911da3a2917b0ca0e846056854ef464c50c4
31	2	CN=Entrust Code Signing CA - OVCS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	43c10b1c0000000051d373da	RSA 2048-bits	RSA SHA-256	2015-06-10 13:46:05	2030-11-10 14:16:05		Code Signing	7e1a1f1a11745c64c90c1f9401abfd81642ea12c	cc5b7a0e5d6771ba348d3d763752f0667026b3531c5396edbe24adce93215723
32	1	CN=Entrust Code Signing CA - OVCS2 O=Entrust, Inc. C=US	CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US	71ef5574af3554c35a2c69f66f4b6bcd	RSA 4096-bits	RSA SHA-512	2021-05-07 19:20:45	2040-12-29 23:59:00		Code Signing	ef9fba79b073f2251e789c03529c1b5384de8ded	95f843046bac035572a3ba1b821df8b759467f5b512ddfa8a72f0799447d6368
33	1	CN=Entrust Extended Validation Code Signing CA - EVCS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	417ace390000000051d373bb	RSA 2048-bits	RSA SHA-256	2015-06-09 17:54:53	2025-06-09 18:24:53		Code Signing	2a0a6f322c292021766ab1ac8c3caf938e0e6ba2	57bc151d924c5a43b57b6433a58a93885f773b4631fdecb85c9fc3545529f274

Deloitte.

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
33	2	CN=Entrust Extended Validation Code Signing CA - EVCS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00d9d6b8f20000000051d373d8	RSA 2048-bits	RSA SHA-256	2015-06-10 13:39:51	2025-06-10 14:09:51		Code Signing	2a0a6f322c292021766ab1ac8c3caf938e0e6ba2	091c6319936f0cac4c7b5e027dcca2b2b2a2af4561ea2c71e650c1e3fb905fd0
33	3	CN=Entrust Extended Validation Code Signing CA - EVCS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00878252600000000051d373d9	RSA 2048-bits	RSA SHA-256	2015-06-10 13:42:49	2030-11-10 14:12:49		Code Signing	2a0a6f322c292021766ab1ac8c3caf938e0e6ba2	d04db927c663aa8c853d54716dd6dc2a4b2fef9c3ae1bfb250447fc5d7771e57
34	1	CN=Entrust Extended Validation Code Signing CA - EVCS2 O=Entrust, Inc. C=US	CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US	35afb77b9d341f6afc8f8446ab31352b	RSA 4096-bits	RSA SHA-512	2021-05-07 19:19:52	2040-12-29 23:59:00		Code Signing	ce894f8251aa15a28462ca312361d261fbf8fe78	6510dc50a0d17dc438c2a85d738f558582b6c25361884f3882e207a51f4ed152
35	1	CN=Entrust Class 1 Client CA - SHA256 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	6e61669872bc9c300000000051d3931e	RSA 2048-bits	RSA SHA-256	2019-04-16 15:35:52	2030-11-16 16:05:52		TLS Web Client Authentication, E-mail Protection	e249b9ec25deb70cdee550185b48cc0c8e15f2a6	c6e9e993c258b72124aad3c9c068b6ef23576155f310b305733361e20b17c943
36	1	CN=Entrust Class 2 Client CA OU=(c) 2010 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	00bcb4d843035b759f0000000051ce1709	RSA 2048-bits	RSA SHA-256	2017-06-20 20:34:33	2028-12-20 21:04:33		E-mail Protection, TLS Web Client Authentication	0991a5bae9f22e2a75dfcd7efe77caf2de6b9b24	95ad94e88f5b8604e40e5fff36b0d34be46c1d5ba06c0e735b72aa396735c415
36	2	CN=Entrust Class 2 Client CA OU=(c) 2010 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	00af1c04b2ac8cff9b0000000051ce18e3	RSA 2048-bits	RSA SHA-256	2020-07-29 15:48:30	2029-06-29 16:18:30		E-mail Protection, TLS Web Client Authentication	0991a5bae9f22e2a75dfcd7efe77caf2de6b9b24	1a20fef46482a98bac6f6c7397c017310ac7fb78495438bc7a7de9035c246679
37	1	CN=Entrust Class 2 Client CA - C2CA2 O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	0088068b45c3fdd4640000000051ce1961	RSA 2048-bits	RSA SHA-256	2021-03-16 14:22:40	2029-07-16 14:52:40		TLS Web Client Authentication, E-mail Protection	a2714ad5c264652f8dce2ae2c1b6e70dd0f932e4	b14cf550d8f573d93e90963c32a85fb51c983c98164f54d78915f6358c954f0e
36	1	CN = Entrust Personal Email Certification Authority - SMIME1 O = Entrust, Inc. C = US	CN = Entrust SMIME Root CA - 2022 O = Entrust, Inc. C = US	1bb7bc5a6a4f06be4f716105ecdf2a74	EC 384-bits	ECDSA SHA-384	2022-12-14 14:25:44	2040-12-29 19:59:59		Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	03219b5f18632ec87ef9aedad9179fb6c91b8360	E229CD78B38BD7B74AC431FA57E294CBAA35EB238293DEDE04B20B218D92BA
37	1	CN = Entrust Certification Authority – ES QTS1 OrganizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES	CN = Entrust Digital Signing Root Certification Authority – DSR1 O = Entrust, Inc. C = US	10b5a317770d5c645606941116538cdc	RSA 4096-bits	RSA SHA-256	2022-10-03 11:12:28	2040-12-28 20:00:00		Time Stamping (1.3.6.1.5.5.7.3.8)	696382cac2f1119a714332858bae37ca9676be80	253F463FB19E06D188A1F81AB6A3CA78C9352B08DC94DD74CF05336809363812
38	1	CN=Entrust Timestamping CA - TS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	51ce0dd8	RSA 2048-bits	RSA SHA-1	2015-07-15 17:42:06	2029-06-15 23:05:07		Time Stamping	c3c271d27bd76805ae3b399b34250c6203c75768	5f84398236b7e58fa365bf1ae5aa3e441c265fdcb50cf7471799060a27a2381a
38	2	CN=Entrust Timestamping CA - TS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048)s OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	58da13ff0000000051ce0df7	RSA 2048-bits	RSA SHA-256	2015-07-22 19:02:54	2029-06-22 19:32:54		Time Stamping	c3c271d27bd76805ae3b399b34250c6203c75768	44dfcd2c573110e74bf4e85903595f660650ed925b7306542c54e87396671f03
39	1	CN=Entrust Time Stamping CA - TS2 O=Entrust, Inc. C=US	CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US	25bc2bf329ca107f1ea9ba8885d49d3b	RSA 4096-bits	RSA SHA-512	2021-05-07 19:22:14	2040-12-29 23:59:00		Time Stamping	260ff0c448081bcddd91f55454b6b3b3fc99f108	21e81685b352955b9ed48fb969bd2e4f95cfb85ed1260cf6b7fa70a035d0028f
40	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

Deloitte.

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 Certificate Services Time-stamp Authority Practice Statement	1.0	30 Sep 2022

ENTRUST MANAGEMENT'S STATEMENT

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

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Subordinate CA cross-certification

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, and Toronto, Ontario, throughout the period 1 March 2022 to 28 February 2023, Entrust has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its Certification Practice Statements as enumerated in Attachment B

- maintained effective controls to provide reasonable assurance that Entrust provides its services in accordance with its Certification Practice Statements

- 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 Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA and Cross Certificate Lifecycle Management

Entrust does not escrow and archive its CA keys, does not provide integrated circuit card management services, and does not provide certificate suspension services. Accordingly, our statement does not extend to controls that would address those criteria.

Entrust management has also reported to 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
1748634	Late Revocation for SSL Certificates issued with Un-verified IP Addresses	5-Jan-2022	8-Mar-2022
1766525	TLS Certificate issued with a key that is impacted by the Close Primes vulnerability	26-Apr-2022	30-Aug-2022
1792231	TLS Certificate issued with an incorrect state or province	23-Sep-2022	19-Apr-2023
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 Root Certification Authority – EV Root
2. Entrust Root Certification Authority – G4
3. Entrust Root Certification Authority – EC1
4. Entrust Root Certification Authority – G2
5. Entrust.net Certification Authority (2048)
6. Entrust Root Certification Authority – CSBR1
7. Entrust Root Certification Authority – VMCR1
8. Entrust Root Certification Authority – 4K EVTLSR 2022
9. Entrust Root Certification Authority – P384 EVTLSR 2022
10. Entrust Root Certification Authority – 4K TLSR 2022
11. Entrust Root Certification Authority – P384 TLSR 2022
12. Entrust Root Certification Authority – SMIMER 2022
Intermediate CAs
13. Entrust Certification Authority – AATL1
14. Entrust Certification Authority – ICA1
OV SSL Issuing CAs
15. Entrust Certification Authority – L1F
16. Entrust Certification Authority – L1K
17. Entrust Certification Authority – OVTLS1
18. Entrust Certification Authority – OVTLS2
19. Entrust Certification Authority – CrowdStrike TLS CA 2022
20. Siemens 2020
21. Entrust Certification Authority – Namirial OV SSL
EV SSL Issuing CAs
22. Entrust Certification Authority – L1E
23. Entrust Certification Authority – L1J
24. Entrust Certification Authority – L1M
25. Entrust Certification Authority – L1N
26. Entrust Certification Authority – QTSP1
27. Entrust Certification Authority – ES QWAC2
28. Entrust Certification Authority - EVTLS1
29. Entrust Certification Authority - EVTLS2
30. Entrust Certification Authority - Namirial EV SSL
Publicly Trusted Code Signing Issuing CAs
31. Entrust Code Signing CA – OVCS1
32. Entrust Code Signing CA – OVCS2
EV Code Signing Issuing CA
33. Entrust Extended Validation Code Signing CA – EVCS1
34. Entrust Extended Validation Code Signing CA – EVCS2
Secure Email (S/MIME) CA
35. Class 1 Client CA – SHA256
36. Entrust Class 2 Client CA
37. Entrust Class 2 Client CA – C2CA2
38. Entrust SMIME1 Client CA
Timestamp CA
39. Entrust Timestamping CA – ES QTS1
40. Entrust Timestamping CA – TS1
41. Entrust Timestamping CA – TS2
Verified Marks Certification CA
42. Entrust Certificate Authority – 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
Entrust Certificate Services Time-stamp Authority Practice Statement	1.0	30 Sep 2022
Entrust EU, S.L. Certification Practice Statement	1.7	1 Aug 2022
Entrust EU, S.L. Certification Practice Statement	1.6	30 Nov 2021

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 Corporation ("Entrust"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on Entrust management's statement that for its Document Signing as a Service ("DSaaS") Certification Authority ("CA") operations in Ottawa, Ontario, Canada, Toronto, Ontario, Canada, Denver, Colorado, USA, Dallas, Texas, USA, and Berkshire, United Kingdom, throughout the period 1 March 2022 to 28 February 2023 (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 its Certification Practice Statements as enumerated in Attachment B

- maintained effective controls to provide reasonable assurance that Entrust provides its services in accordance with its Certification Practice Statements

- 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.

Assessment of controls at DSaaS operations in US and UK was limited to the following WebTrust for CA criteria:

CA Environmental Controls

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

CA Key Lifecycle Management Controls

- CA Cryptographic Hardware Lifecycle Management

Deloitte.

Assessment of controls related to DSaaS operations in Canada was limited to the following WebTrust for CA criteria:

CA Environmental Controls

- System Development, Maintenance, and Change Management

Subscriber Key Lifecycle Management Controls

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

Entrust DSaaS operations do not provide CA key generation, storage, archive, or management services, integrated circuit card management services, suspension services and do not provide third-party subordinate CA or cross certificate issuance or management services. Accordingly, our procedures did not extend to controls that would address those criteria.

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 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 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.

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.

Deloitte.

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	**No instances or occurrences of the control activity during the audit period**	During the examination period there were no instances or occurrences of the following control activity: • **WTCA 4.8 Cryptographic Device Life Cycle Management** No cryptographic device life cycle events occurred for US and UK operation during the audit period. As underlying event had not occurred, related control activities did not operate during period under audit and their operating effectiveness was not tested.

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 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.

Deloitte LLP

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

Deloitte.

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Entrust.net Certification Authority (2048) 2. Entrust Root Certification Authority - G4 3. Entrust Digital Signing Root Certification Authority - DSR1
Intermediate CAs
4. Entrust Certification Authority – AATL1
Document Signing CAs
5. Entrust Class 3 Client CA - SHA256 6. Entrust Certification Authority - ES QSig1 7. Entrust Certification Authority - ES QSig2 8. Entrust Certification Authority - ES QSeal1 9. Entrust Certification Authority - ES QSeal2 10. Entrust Certification Authority – DS1
Timestamp CAs
11. Entrust Certification Authority - ES QTS1

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	SHA256 Fingerprint
1	1	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	3863def8	RSA 2048-bits	RSA SHA-1	1999-12-24 17:50:51	2029-07-24 14:15:12			55e481d11180bed889b908a331f9a1240916b970	6dc47172e01cbcb0bf62580d895fe2b8ac9ad4f873801e0c10b9c837d21eb177
2	1	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00d9b5437fafa9390f000000005565ad58	RSA 4096-bits	RSA SHA-256	2015-05-27 11:11:16	2037-12-27 11:41:16			9f38c45623c339e8a0716ce8544ce4e83ab1bf67	db3517d1f6732a2d5ab97c533ec70779ee3270a62fb4ac4238372460e6f01e88
3	1	CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	2d37bcd092d2cb88b67f5ccdab71b39b	RSA 4096-bits	RSA SHA-512	2021-11-12 00:00:00	2030-12-30 00:00:00		1.3.6.1.4.1.311.10.3.12, Time Stamping	a6654181f25b87056addfd8a544e8f987bdc23b8	20fc75acb2cad7978c7b006a9b1523bfdaf5490afcf49652c585e4a12f601c85
3	2	CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US	CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US	6c73c936b185e50b804d5bcec29f83d21a51c1a3	RSA 4096-bits	RSA SHA-512	2021-11-12 18:28:47	2040-12-30 18:28:47			a6654181f25b87056addfd8a544e8f987bdc23b8	e874fe2531eae4a4b6b62f37496bbae90eb1d8fc8cedbebb00a182cfacdc7e61
4	1	CN=Entrust Class 3 Client CA - SHA256 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net	551615150000000051ce160e	RSA 2048-bits	RSA SHA-256	2016-02-25 18:08:16	2029-06-25 18:38:16		TLS Web Client Authentication, E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 2.16.840.1.114027.40.11	069f6f4ea2294e0f0cae17bfb69846efadb83b72	33857338361ecfc4858ddff6b9ef6273e3db856ab9cea1c0e2c65925d1c87978
5	1	C=ES O=Entrust Datacard Europe, S.L. organizationIdentifier=VATES-B81188047 CN=Entrust Certification Authority - ES QSig1	C=US O=Entrust, Inc. CN=Entrust Certification Authority - AATL1	4491ca5825be79842b29b0c37286215f	RSA 4096-bits	RSA SHA-512	2020-07-29 16:33:00	2037-12-19 23:59:00		E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5	5a53088a6130a90dead54397d3983b951e2e6d02	b2874b588a94034798319d5d329db265f83a47f315ba5831a4970cb57166d594
6	1	CN=Entrust Certification Authority - ES QSig2 organizationIdentifier=VATES-B81188047 O=Entrust EU, S.L. C=ES	CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US	3f967d63188a95bf302f82e516cb991d	RSA 4096-bits	RSA SHA-512	2021-11-16 00:00:00	2040-12-29 00:00:00		1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5	f5560d69d7da6ac9d8c9a2096e74bedb80c61700	4671fdead3c5b32d834b36591d41496fcb8a0db7d4f9f4cb9d34eabe0947ee87
7	1	C=ES O=Entrust Datacard Europe, S.L. organizationIdentifier=VATES-B81188047 CN=Entrust Certification Authority - ES QSeal1	C=US O=Entrust, Inc. CN=Entrust Certification Authority - AATL1	13ee348e492f8dd6b5c49cf073f714ab	RSA 4096-bits	RSA SHA-512	2020-07-27 14:39:07	2037-12-19 23:59:00		E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5	5680152395717fe72d90d0cd063a4f67637d3d75	1701de38124c4458f32b88ae7e62ac15876c427a3ad3bbae8fd1479ff00030f3
8	1	CN=Entrust Certification Authority - ES QSeal2 organizationIdentifier=VATES-B81188047 O=Entrust EU, S.L. C=ES	CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US	12f04c327561e6f51e8d39b47e9884e1	RSA 4096-bits	RSA SHA-512	2021-11-16 00:00:00	2040-12-29 00:00:00		Document Signing (1.3.6.1.4.1.311.10.3.12) Unknown Key Usage (1.2.840.113583.1.1.5)	3618256ed95df710057c272eb8ecfa414a60ed1f	8c31d9375128d4b107f07678eebfff2cca26a4cabb462f257f31a36fe7bce104
9	1	CN = Entrust Digital Signing Certification Authority - DS1 O = Entrust, Inc. C = US	CN = Entrust Digital Signing Root Certification Authority - DSR1 O = Entrust, Inc. C = US	536373ce69ce48b59ab6f202780d6d75	RSA 4096-bits	RSA SHA-384	2022-12-14 14:12:49	2040-12-29 19:59:59		Unknown Key Usage (1.3.6.1.5.5.7.3.36) Document Signing (1.3.6.1.4.1.311.10.3.12) Unknown Key Usage (1.2.840.113583.1.1.5)	80a1841c29b421823c0e5d17fbb21ed1a3e2d82d	EEE2B2C76CF4A1DC6E90C14CC1986D120245294833BD6A739EFBD3EBDE9BB972
10	1	CN = Entrust Certification Authority – ES QTS1 OrganizationIdentifier = VATES-B81188047 O = Entrust EU, S.L. C = ES	CN = Entrust Digital Signing Root Certification Authority – DSR1 O = Entrust, Inc. C = US	10b5a317770d5c645606941116538cdc	RSA 4096-bits	RSA SHA-256	2022-10-03 11:12:28	2040-12-28 20:00:00		Time Stamping (1.3.6.1.5.5.7.3.8)	696382cac2f1119a714332858bae37ca9676be80	253F463FB19E06D188A1F81AB6A3CA78C9352B08DC94DD74CF05336809363812
11	1	C=US O=Entrust, Inc. CN=Entrust Certification Authority - AATL1	CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US	00c727f51f8f922b020000000005565d8ad	RSA 4096-bits	RSA SHA-512	2020-07-20 15:46:21	2037-12-20 16:16:21		1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5, E-mail Protection	63f184dd03bea39f64fa767a47c4567ec06da020	839f9b91c2e49218a66416df181b984e9be634d12a95483d98a6199fc0788d74

Deloitte.

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 EU, S.L. Certification Practice Statement	1.7	1 Aug 2022
Entrust EU, S.L. Certification Practice Statement	1.6	30 Nov 2021

ENTRUST MANAGEMENT'S STATEMENT

Entrust Corporation ("Entrust") operates the Document Signing as a Service Certification Authority ("DSaaS CA") services as enumerated in Attachment A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- 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 DSaaS 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 DSaaS CA services. Based on that assessment, in Entrust management's opinion, in providing its DSaaS CA services at Ottawa, Ontario, Canada, Toronto, Ontario, Canada, Denver, Colorado, USA, Dallas, Texas, USA, and Berkshire, United Kingdom, throughout the period 1 March 2022 to 28 February 2023, Entrust has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its Certification Practice Statements as enumerated in Attachment B

- maintained effective controls to provide reasonable assurance that Entrust provides its services in accordance with its Certification Practice Statements

- 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:

DSaaS CA operations in US and UK

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management

- System Access Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Cryptographic Hardware Lifecycle Management

DSaaS CA operations in Canada

Assessment of controls related to DSaaS operations in Canada was limited to the following WebTrust for CA criteria:

CA Environmental Controls

- System Development, Maintenance, and Change Management

Subscriber Key Lifecycle Management Controls

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

Entrust DSaaS operations do not provide CA key generation, storage, archive, or management services, integrated circuit card management services, suspension services and do not provide third-party subordinate CA or cross certificate issuance or management services. Accordingly, our statement does not extend to controls that would address those criteria.

No cryptographic device life cycle events occurred for US and UK operations during the audit period. Accordingly, our statement does not extend to controls that would address those criteria.

Bruce Morton
Director, Entrust Certificate Services
18th May 2023

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Entrust.net Certification Authority (2048) 2. Entrust Root Certification Authority - G4 3. Entrust Digital Signing Root Certification Authority - DSR1
Intermediate CAs
4. Entrust Certification Authority – AATL1
Document Signing CAs
5. Entrust Class 3 Client CA - SHA256 6. Entrust Certification Authority - ES QSig1 7. Entrust Certification Authority - ES QSig2 8. Entrust Certification Authority - ES QSeal1 9. Entrust Certification Authority - ES QSeal2 10. Entrust Certification Authority – DS1
Timestamp CAs
11. Entrust Certification Authority - ES QTS1

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 EU, S.L. Certification Practice Statement	1.7	1 Aug 2022
Entrust EU, S.L. Certification Practice Statement	1.6	30 Nov 2021