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 and Toronto, Ontario, Canada, throughout the period 1 March 2024 to 28 February 2025 (the "Period") for its CAs as enumerated in Attachment A, Entrust has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Certificate Policy/ Certification Practice Statements ("CP/CPS") as enumerated on Attachment B including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Entrust website, and provided such services in accordance with its disclosed practices

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

- 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 – SSL Baseline – v2.8.

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.

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 – SSL Baseline - v2.8.

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

Deloitte.

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	**Updates to CPS Versions Addressing EV SSL Certificate Issues and Client Authentication**	CPS V3.17 was updated on March 21, 2024, to correct mis-issued EV SSL certificates, as reported in Bugzilla 1883843. However, the update did not completely and accurately address details of Client Authentication, which was publicly disclosed in Bugzilla 1887753. Consequently, CPS V3.1.8 was updated on March 22, 2024.
2	**Updates to CPS Version Addressing typographical (text placement) error**	CPS V3.1.8 dated March 22, 2024, was updated to require the policyQualifier for the EV certificate profile, as reported in Bugzilla 1890896. However, it was inadvertently added to the OV certificate profile, where it is not required. This error was corrected in CPS V3.20 on March 26, 2024.

In course of our procedures, we have identified two records of the certificate related to CA#18 - L1K in ATTACHMENT A, with different SHA fingerprints. We have disclosed both of these records as Cert # 18.1 and Cert # 18.5 in ATTACHMENT A. We identified these records in crt.sh.

Basis for qualified opinion

During our procedures, we noted the following which caused a qualification of our opinion:

#	Observation	Relevant WebTrust SSL BR Criteria
1	As publicly disclosed in Bug #1886467, there were 1,161 SSL certificates issued without id-kp-serverAuth attribute.	**P2 - 2.5:** The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved

Deloitte.

#	Observation	Relevant WebTrust SSL BR Criteria
	Revocation was completed by June 2024. As a result, a criterion of 2.5 of Principle 2 WebTrust for Certification Authorities – SSL Baseline v2.8 has not been met.	Certificate Policy Identifiers) of Subscriber certificates generated conform to the Baseline Requirements.
2	As publicly disclosed in Bug #1890123 regarding the mis-issued EV SSL certificates reported in Bugzilla 1883843 and 1890898, a preliminary incident report was not provided within the required 24-hour timeframe. As publicly disclosed in Bug #1885754, regarding mis-issued EV SSL certificates, Technical Support Specialist team did not provide a preliminary report to the Subscriber and the entity who filed the CPR within the required 24-hour timeframe. As a result, a criterion of 5.2 of Principle 2 of WebTrust for Certification Authorities – SSL Baseline v2.8 has not been met.	**P2 – 5.2** The CA maintains controls to provide reasonable assurance that it: •has the capability to accept and acknowledge Certificate Problem Reports on a 24x7 basis; •identifies high priority Certificate Problem Reports; •begin investigation of Certificate Problem Reports within 24 hours and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report: •decides whether revocation or other appropriate action is warranted; •if revocation is deemed the appropriate action, the elapsed time from receipt of the Certificate Problem Report or revocation request and revocation status information does not exceed the timelines in SSL Baseline Requirements 4.9.1.1; and •where appropriate, forwards such complaints to law enforcement.
3	As publicly disclosed in Bug #1887705, for those mis-issued SSL certificates reported in Bug #1886467, Entrust did not revoke the impacted certificates within 5 days. Revocation was completed by June 2024. As a result, a criterion of 2.5 of Principle 2 WebTrust for Certification Authorities – SSL Baseline v2.8 has not been met.	**P2 - 5.3:** The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or 4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); 5. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon. And, Subscriber Certificates are revoked within 5 days if any of the following events occurs: 1. The Certificate no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6; 2. The CA obtains evidence that the Certificate was misused; 3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use; 4. The CA is made aware of any circumstance indicating that use of a Fully–Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g., a court or arbitrator has
4	As publicly disclosed in Bug #1887705, regarding the mis-issued EV SSL certificates reported in Bugs # 1883843, 1888714, and 1886467, Entrust did not revoke the impacted certificates within the required 5-day period. A total of 1,175 certificates were affected, and their revocation was delayed. As a result, a criterion of 5.3 of Principle 2 WebTrust for Certification Authorities – SSL Baseline v2.8 has not been met.	

#	Observation	Relevant WebTrust SSL BR Criteria
		revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); 5. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully–Qualified Domain Name; 6. The CA is made aware of a material change in the information contained in the Certificate; 7. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement; 8. The CA determines that any of the information appearing in the Certificate is inaccurate; 9. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; 10. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or 11. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Opinion

In our opinion, except for the matters described in the preceding section entitled 'Basis for qualified opinion', throughout the period 1 March 2024 to 28 February 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 – SSL Baseline v2.8.

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 – SSL Baseline v2.8, 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

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
June 27, 2025

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 – 4K EVTLSR 2022 7. Entrust Root Certification Authority – P384 EVTLSR 2022 8. Entrust Root Certification Authority – 4K TLSR 2022 9. Entrust Root Certification Authority – P384 TLSR 2022 10. AffirmTrust Commercial 11. AffirmTrust Networking 12. AffirmTrust Premium 13. AffirmTrust Premium ECC 14. AffirmTrust 4K TLSR 2022
DV SSL Issuing CAs
15. AffirmTrust Certificate Authority – DV1 16. AffirmTrust Certificate Authority – DVTLS1
OV SSL Issuing CAs
17. Entrust Certification Authority – L1F 18. Entrust Certification Authority – L1K 19. Entrust Certification Authority – OVTLS1 20. Entrust Certification Authority – OVTLS2 21. Entrust Certification Authority – CrowdStrike TLS CA 2022 22. Siemens 2020 23. Entrust Certification Authority – Namirial OV SSL 24. AffirmTrust Certificate Authority – OV1
EV SSL Issuing Cas
25. Entrust Certification Authority – L1E 26. Entrust Certification Authority – L1J 27. Entrust Certification Authority – L1M 28. Entrust Certification Authority – L1N 29. Entrust Certification Authority – QTSP1 30. Entrust Certification Authority – ES QWAC2 31. Entrust Certification Authority - EVTLS1 32. Entrust Certification Authority - EVTLS2 33. Entrust Certification Authority - Namirial EV SSL 34. AffirmTrust Extended Validation CA – EV1 35. AffirmTrust Extended Validation CA – EV2 36. AffirmTrust Extended Validation CA – EV3 37. AffirmTrust Extended Validation CA – EVEC1

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	12/24/1999 17:50	7/24/2029 14:15			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	11/27/2006 20:23	11/27/2026 20:53			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	7/7/2009 17:25	12/7/2030 17:55			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	9/12/2014 17:28	9/13/2024 3:12			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	9/12/2014 19:23	9/13/2024 3:12			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	9/22/2014 17:14	9/23/2024 1:31			6a72267ad01eef7de73b6951d46c8d9f901266ab	6B143C2005D5539CC22EAB5F772DB2A9FE87467FEFFA07FCF0A9F7D28274CA7A
3	5	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	525c32e349f48525bc8d7810d7aabb67	RSA 2048-bits	RSA SHA-256	3/06/2024 16:00	11/26/2026 23:59			6a72267ad01eef7de73b6951d46c8d9f901266ab	65F0358FC93934CD5AAC43122F37948D7BD042D148E6FD88B2E65AA9AC399DDD
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	5/27/2015 11:11	12/27/2037 11:41			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	12/18/2012 15:25	12/18/2037 15:55			b763e71add8de908a65583a4e06a504165114249	02ED0EB28C14DA45165C566791700D6451D7FB56F0B2AB1D3B8EB070E56EDFF5

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
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	008011196de613db160000000051d3575e	EC 384-bits	RSA SHA-256	6/10/2016 14:58	11/10/2026 15:28			b763e71add8de908a65583a4e06a504165114249	3FDE0D36E026B6E8EBE2C28883607C8651DE10BD6C1FCAD365E560F4EA2F3B03
6	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	647987D98D52645DA4D3DE3B80771A0CE02B9B9285E6E869998821707 44EC9AA
6	2	CN = Entrust 4K EV TLS Root CA - 2022 O = Entrust, Inc. C = US	CN = Entrust Root Certification Authority - G2 O=Entrust, Inc. C = US	ac9a58d8637568d2cdfddc1c7955cc	RSA 4096-bits	RSA SHA-256	2024-03-06 15:31	2030-12-06 23:59			0bdd90d58fbb3f5cbd60a0551a2482863c413041	E821B11129110567F1607F0B0F368EC78D811418F0C48CC425450F63EB88095D
7	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
8	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
8	2	CN = Entrust 4K TLS Root CA - 2022 O = Entrust, Inc. C = US	CN = Entrust Root Certification Authority - G2 O = Entrust, Inc. C = US	2ef8e1b306cf96a867406dbedb4e688e	RSA 4096-bits	RSA SHA-256	2024-03-06 15:23:21	2030-12-06 23:59:59	2024-08-02		9440EA5AFFEF4963019E09DFE03B803373122056	E255DA2D54ECFD16FB6426A38A83399E7E39F6A01E96E649CD850FB0FDFF54EB
9	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
10	1	CN = AffirmTrust Commercial O = AffirmTrust C = US	CN = AffirmTrust Commercial O = AffirmTrust C = US	7777062726a9b17c	RSA 2048-bits	RSA SHA-256	01/29/2010 09:06	12/31/2030 09:06			9d93c6538b5ecaaf3f9f1e0fe59995bc24f6948f	0376AB1D54C5F9803CE4B2E201A0EE7EEF7B57B636E8A93C9B8D4860C96F5FA7
11	1	CN = AffirmTrust Networking O = AffirmTrust C = US	CN = AffirmTrust Networking O = AffirmTrust C = US	7c4f04391cd4992d	RSA 2048-bits	RSA SHA-256	01/29/2010 9:08	12/31/2030 09:08			071fd2e79cdac26ea240b4b07a50105074c4c8bd	0A81EC5A929777F145904AF38D5D509F66B5E2C58FCDB531058B0E17F3F0B41B
12	1	CN = AffirmTrust Premium O = AffirmTrust C = US	CN = AffirmTrust Networking O = AffirmTrust C = US	6d8c1446b1a60aee	RSA 2048-bits	RSA SHA-256	01/29/2010 9:10	12/31/2030 09:10			9dc067a60c22d926f545aba665521127d845ac63	70A73F7F376B60074248904534B11482D5BF0E698ECC498DF52577EBF2E93B9A
13	1	CN = AffirmTrust Premium ECC O = AffirmTrust C = US	CN = AffirmTrust Premium ECC O = AffirmTrust C = US	7497258ac73f7a54	RSA 2048-bits	RSA SHA-256	01/29/2010 9:20	12/31/2040 09:20			9aaf297ac01135526513000c36afe40d5aed63c	BD71FDF6DA97E4CF62D1647ADD2581B07D79ADF8397EB4ECBA9C5E8488821423
14	1	CN = AffirmTrust 4K TLS Root CA - 2022 O = AffirmTrust C = CA	CN = AffirmTrust 4K TLS Root CA - 2022 O = AffirmTrust C = CA	4261723e9b00a227d3bd5871e2d5b404687473a5	RSA 2096-bits	RSA SHA-256	12/13/2022	12/07/2047			07875af4076871d9661be264788037805cdef727	A7DEDF5A842167DD12FDAA0F2080E73295B8B8BEA71B2094EA0950945A482FC1
14	2	CN = AffirmTrust 4K TLS Root CA - 2022 O = AffirmTrust C = CA	CN = AffirmTrust Premium O = AffirmTrust C = CA	050f8ba96a256314f2893d9ba3315b1a	RSA 4096-bits	RSA SHA-256	3/6/2024	12/30/2040	08/02/2024		07875AF4076871D9661BE264788037805CDEF727	B0A178E06B7A7274F0B2A640F6A03BF003AB1EDE8693770D5D2741B2D2F01980
15	1	CN = AffirmTrust Certificate Authority - DV1 O = See www.affirmtrust.com/repository ON = AffirmTrust CN = CA	CN = AffirmTrust Commercial ON = AffirmTrust CN = US	6345009686538276405	RSA 2048-bits	RSA SHA-256	2017-04-07 15:10	2030-12-02 04:00		TLS Web Server Authentication, TLS Web Client Authentication	33DF7A3E027996EBB60CC063FA75BF9222CD91FA	CA4389C89DDFC31BEC26C74B44A8498C58B2D838516FA01B14F1393629E58A40
15	2	CN = AffirmTrust Certificate Authority - DV1 O = See www.affirmtrust.com/repository ON = AffirmTrust CN = CA	CN = AffirmTrust Commercial ON = AffirmTrust CN = US	62b4c3eba53918177f127a837b574f96	RSA 2048-bits	RSA SHA-256	2019-03-21 20:21	2030-12-02 04:00		TLS Web Server Authentication, TLS Web Client Authentication	33DF7A3E027996EBB60CC063FA75BF9222CD91FA	4563B936E35AB97576F5AEF1935D9BC7E9977841F0573BD2E16BCAC9534A6AF9
16	1	CN = AffirmTrust 4K TLS Certification Authority - DVTLS1 O = AffirmTrust C = CAS	CN = AffirmTrust 4K TLS Root CA - 2022 O = AffirmTrust C = CA	04e911e082864b911d97267aa3388c5a	RSA 4096-bits	SHA384	2022-12-14 18:09:01	2040-12-29 23:59:59		TLS Web Server Authentication, TLS Web Client Authentication	45c174f7f45d033320f133efb8da6179886f5c96	FB327FE14AB3FEC5C96D9169A8B536382B97B1B325543C3DCD8A10F8C431E103

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
17	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	b601913d8553bafa0000000051d4c1f6	EC 384-bits	ECDSA SHA-384	4/5/2016 20:17	10/5/2037 20:47		TLS Web Server Authentication, TLS Web Client Authentication	2e62f014ee87cdb335033defe4b99efd3bb8a3c9	1835B0E482EA65536FC010E4BC13C060F65668165FBA97E2F542CE96CA6DFEFC
17	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 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	a25b1769bad80ad70000000051ce1941	EC 384-bits	RSA SHA-256	2/5/2021 16:34	7/5/2029 17:04		TLS Web Server Authentication, TLS Web Client Authentication	2e62f014ee87cdb335033defe4b99efd3bb8a3c9	0C5A09DB8AEDF7D2D1DDE14DCCC2DB6EA959BCF6F010360D836C342C624D7E0E
18	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	79851D5CBC895C56D97FEF2D5CF3D6	RSA 2048-bits	RSA SHA-256	10/05/2015 19:13	12/05/2030 19:43			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	052C0174E806F9474AEC865129A04867F385087B631393B4D8A7F26B43733348
18	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	8/26/2014 17:14	8/27/2024 8:34			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	3B0CC20384AD7F24EB438F2B80C63EBE003F7F215B8877E418EBB0484028DB57
18	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	10/10/2014 15:23	10/11/2024 6:22			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	D6C3FC493BACD1DF8A1BA30F4AE26254B2A4528E4876081EACC6A16A090AA36A
18	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	10/22/2014 17:05	10/23/2024 7:33			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	F5C2F23C6518F9D19B6F39BEAEA4FBAE10031BA9DC985CE1563A520DA0AD4116
18	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	10/5/2015 19:13	12/5/2030 19:43			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	13EFB39A2F6654E8C67BD04F4C6D4C90CD6CAB5091BCEDC73787F6B77D3D3FE7
18	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

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
18	7	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	8/26/2014 17:07	8/27/2024 5:48			82a27074ddbc533fcf7bd4f7cd7fa760c60a4cbf	3B6DD5581C9853092007DB1BB0106FC61205E88E360543D7CAE02D68E7A25AC3
19	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
20	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	2DB842F8243212772912668230ABC31DE13C1D4B852D6C21C9B1007D5AC20681
21	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
22	1	CN=Siemens Issuing CA Internet Server 2020 O=Siemens C=DE	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
23	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
24	1	CN= AffirmTrust Certificate Authority – OV1 OU= See www.affirmtrust.com/repository ON= AffirmTrust C=CA	CN= AffirmTrust Commercial ON= AffirmTrust C=US	1764987999490089933	RSA 2048-bits	RSA SHA-256	11/11/2016	2030-12-02			FE60C30DA4A29D214F7A784C62C5DB14FC3978C4	EA4EE2FAA57AE4B539B63977FE5BB205B6AFB32F7A73B2B363E4BE02CD8A91E9
24	2	CN= AffirmTrust Certificate Authority – OV1 OU= See www.affirmtrust.com/repository ON= AffirmTrust C=CA	CN= AffirmTrust Commercial ON= AffirmTrust C=US	53f6a611092e528ed963f19149532204	RSA 2048-bits	RSA SHA-256	2019-03-21 20:25	2030-12-02 04:00		TLS Web Server Authentication, TLS Web Client Authentication	FE60C30DA4A29D214F7A784C62C5DB14FC3978C4	B5FD6F800334F565036B0999F8310B5B0BD7268395D8B267005697AF7301C5E8
25	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
26	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	0a83d4803e7e9f5100000000051d4c1f7	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
27	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
27	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
28	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	00abec77ff1b410c070000000005565d805	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

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
29	1	CN=Entrust Certification Authority - QTSP1 C=ES O=Entrust Datacard Europe S.L. organizationIdentifier=VATES-B81188047	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
30	1	CN=Entrust Certification Authority - ES QWAC2 ON=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
31	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
32	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
33	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
34	1	CN= AffirmTrust Extended Validation CA - EV1 OU= See www.affirmtrust.com/repository ON= AffirmTrust C= CA	CN= AffirmTrust Commercial ON= AffirmTrust C= US	4679446353986764952	RSA 2048-bits	RSA SHA-256	2016-11-29 04:00	2030-12-02 04:00			DBEF65370BE547CB35D1901F03C1BC88C7A7EA80	CF88915CF996932C2B4CBE3039076D119BB728B4F31E49B63A5022FE65489A12
34	2	CN= AffirmTrust Extended Validation CA - EV1 OU= See www.affirmtrust.com/repository ON= AffirmTrust C= CA	CN= AffirmTrust Commercial ON= AffirmTrust C= US	1729551ed68e7fb1edf57300f35d7fd5	RSA 2048-bits	RSA SHA-256	2019-03-21 20:27:00	2030-12-02 04:00			DBEF65370BE547CB35D1901F03C1BC88C7A7EA80	ED3C991466CBC45B5FD1DA281028F9587B8219523647E0CA1B47F2C527D2920F
35	1	CN= AffirmTrust Extended Validation CA – EV2 OU= See www.affirmtrust.com/repository ON= AffirmTrust C= CA	CN= AffirmTrust Premium ON= AffirmTrust C= US	5371c8eb0784fd5108e5d4f3e323ec46	RSA 2048-bits	RSA SHA-256	2019-03-21 20:46:35	2030-12-02 04:00:00			737C9A38683C517C4108FEA11F2A1EB461DBCD3C	9DF77488C4B74AC32E3CEC4C643D001D5C3BABFA4001FFD193DCA10C8BE5CB3A
36	1	CN= AffirmTrust Extended Validation CA – EV3 OU= See www.affirmtrust.com/repository ON= AffirmTrust C= CA	CN= AffirmTrust Networking ON= AffirmTrust C= US	3424a1ecf8f0a35fe746b7011c43e844	RSA 2048-bits	RSA SHA-256	2019-03-21 20:46:35	2030-12-02 04:00:00			791EB1C917C71EACB1C714D7C3E87FBCB9509B15	B700BA49AF4D19E72FB15A2DAC3C213BA44C319FA7DA92772B3682E12B781093
37	1	CN= AffirmTrust Extended Validation CA – EVEC1 OU= See www.affirmtrust.com/repository ON= AffirmTrust C= CA	CN= AffirmTrust Premium ECC ON= AffirmTrust C= US	0202a584c134064dc9f32d207ea37298	EC 384-bits	ECDSA SHA-384	2019-03-21 20:55	2030-12-02 04:00		TLS Web Server Authentication, TLS Web Client Authentication	C6908C0283D75DE3BE3B9C2ED5657D2A1060EEE5	CDE23A52303C3CA67A4BBBCC9582FF5C9203AA98CB0F387139308CE2289506A2

Table – New Root/Subordinate CAs deployed in production during Audit Period

New Root CA	Subject Key Identifier	Key Generation Details
Entrust Root Certification Authority – 4K ClientR 2024	143879FBB5583B6138F45DE28B32A7A507E27507	Key was generated on April 30, 2021 Key Name – 300006.
Entrust Root Certification Authority – P384 ClientR 2024	6C79BDFE09E30965CD682D370EB693E60CFFC314	Key was generated on November 22, 2022 Key Name – 500053.
Entrust Root Certification Authority – Client1	**4775F09CF5BD101D755B9EF38C855733A535330D**	Key was generated on April 30, 2021 Key Name – 300006.
Entrust Root Certification Authority – Client2	**1B21F09CADC08D0C57561B429C4DF2A77815CAC2**	Key was generated on November 22, 2022 Key Name – 500053.

ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement	3.29	21 Feb 2025
Entrust Certificate Services Certification Practice Statement	3.28	21 Nov 2024
Entrust Certificate Services Certification Practice Statement	3.27	7 Nov 2024
Entrust Certificate Services Certification Practice Statement	3.26	15 Oct 2024
Entrust Certificate Services Certification Practice Statement	3.25	9 Oct 2024
Entrust Certificate Services Certification Practice Statement	3.24	19 Sept 2024
Entrust Certificate Services Certification Practice Statement	3.23	11 Sept 2024
Entrust Certificate Services Certification Practice Statement	3.22	31 July 2024
Entrust Certificate Services Certification Practice Statement	3.21	14 May 2024
Entrust Certificate Services Certification Practice Statement	3.20	26 March 2024
Entrust Certificate Services Certification Practice Statement	3.19	25 March 2024
Entrust Certificate Services Certification Practice Statement	3.18	22 March 2024
Entrust Certificate Services Certification Practice Statement	3.17	21 March 2024
Entrust Certificate Services Certification Practice Statement	3.16	20 Feb 2024
Entrust EU, S.L. Certification Practice Statement	2.2	27 Jan 2025
Entrust EU, S.L. Certification Practice Statement	2.1	1 May 2024
Entrust EU, S.L. Certification Practice Statement	2.0	31 Oct 2023
AffirmTrust Certification Practice Statement	3.18	15 Jan 2025
AffirmTrust Certification Practice Statement	3.17	21 Mar 2025
AffirmTrust Certification Practice Statement	3.16	20 Feb 2024

ENTRUST MANAGEMENT'S STATEMENT

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

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 1 March 2024 to 28 February 2025, Entrust has:

- disclosed its SSL certificate lifecycle management business practices in its:
    - Certificate Policy/ Certification Practice Statements ("CP/CPS") as enumerated on Attachment B

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Entrust website, and provided such services in accordance with its disclosed practices

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

- 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 – SSL Baseline – v2.8.

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

Bug ID	Summary	Opened	Closed
1887705	Delayed revocation of clientAuth TLS Certificates without serverAuth EKU	03/25/2024	07/05/2024
1887753	Late CPS Update	03/25/2024	07/12/2024
1883843	EV TLS Certificate cPSuri missing	3/6/2024	8/13/2024
1886467	ClientAuth TLS Certificates without serverAuth EKU	3/20/2024	6/28/2024
1888714	EV Certificate missing Issuer's EV Policy OID	3/29/2024	7/11/2024
1885754	CPR was not responded to in 24 hours	3/16/2024	9/13/2024
1890123	Failed to provide a preliminary incident report according to TLS BR 4.9.5	4/6/2024	8/13/2024
1890901	Delayed incident report - CPS typographical (text placement) error	4/10/2024	5/5/2024

Bruce Morton
Director, Entrust Certificate Services
June 27, 2025

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 – 4K EVTLSR 2022
7. Entrust Root Certification Authority – P384 EVTLSR 2022
8. Entrust Root Certification Authority – 4K TLSR 2022
9. Entrust Root Certification Authority – P384 TLSR 2022
10. AffirmTrust Commercial
11. AffirmTrust Networking
12. AffirmTrust Premium
13. AffirmTrust Premium ECC
14. AffirmTrust 4K TLSR 2022
DV SSL Issuing CAs
15. AffirmTrust Certificate Authority – DV1
16. AffirmTrust Certificate Authority – DVTLS1
OV SSL Issuing CAs
17. Entrust Certification Authority – L1F
18. Entrust Certification Authority – L1K
19. Entrust Certification Authority – OVTLS1
20. Entrust Certification Authority – OVTLS2
21. Entrust Certification Authority – CrowdStrike TLS CA 2022
22. Siemens 2020
23. Entrust Certification Authority – Namirial OV SSL
24. AffirmTrust Certificate Authority – OV1
EV SSL Issuing Cas
25. Entrust Certification Authority – L1E
26. Entrust Certification Authority – L1J
27. Entrust Certification Authority – L1M
28. Entrust Certification Authority – L1N
29. Entrust Certification Authority – QTSP1
30. Entrust Certification Authority – ES QWAC2
31. Entrust Certification Authority - EVTLS1
32. Entrust Certification Authority - EVTLS2
33. Entrust Certification Authority - Namirial EV SSL
34. AffirmTrust Extended Validation CA – EV1
35. AffirmTrust Extended Validation CA – EV2
36. AffirmTrust Extended Validation CA – EV3
37. AffirmTrust Extended Validation CA – EVEC1

ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement	3.29	21 Feb 2025
Entrust Certificate Services Certification Practice Statement	3.28	21 Nov 2024
Entrust Certificate Services Certification Practice Statement	3.27	7 Nov 2024
Entrust Certificate Services Certification Practice Statement	3.26	15 Oct 2024
Entrust Certificate Services Certification Practice Statement	3.25	9 Oct 2024
Entrust Certificate Services Certification Practice Statement	3.24	19 Sept 2024
Entrust Certificate Services Certification Practice Statement	3.23	11 Sept 2024
Entrust Certificate Services Certification Practice Statement	3.22	31 July 2024
Entrust Certificate Services Certification Practice Statement	3.21	14 May 2024
Entrust Certificate Services Certification Practice Statement	3.20	26 March 2024
Entrust Certificate Services Certification Practice Statement	3.19	25 March 2024
Entrust Certificate Services Certification Practice Statement	3.18	22 March 2024
Entrust Certificate Services Certification Practice Statement	3.17	21 March 2024
Entrust Certificate Services Certification Practice Statement	3.16	20 Feb 2024
Entrust EU, S.L. Certification Practice Statement	2.2	27 Jan 2025
Entrust EU, S.L. Certification Practice Statement	2.1	1 May 2024
Entrust EU, S.L. Certification Practice Statement	2.0	31 Oct 2023
AffirmTrust Certification Practice Statement	3.18	15 Jan 2025
AffirmTrust Certification Practice Statement	3.17	21 Mar 2025
AffirmTrust Certification Practice Statement	3.16	20 Feb 2024