

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 September 2023 to 29 February 2024 (the "Period") for its CAs as enumerated in [Attachment A](#), Entrust has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
 - Certificate Policy/ Certification Practice Statements ("CP/CPS") as enumerated in [Attachment B](#) including its commitment to provide S/MIME 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME 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 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 – S/MIME – Version 1.0.1](#)

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 – S/MIME – Version 1.0.1.

Our independence and quality management

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's statement based on our procedures. We conducted our procedures in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's statement is fairly stated, and, accordingly, included:

- (1) obtaining an understanding of Entrust's S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates;



- (2) selectively testing transactions executed in accordance with disclosed S/MIME certificate lifecycle management practices;
- (3) testing and evaluating the operating effectiveness of the controls; and
- (4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Entrust and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

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

Other matters

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

	Matter topic	Matter description
1	CAs not issuing S/MIME certificates during the Period	The CA #10-12 in Attachment A, did not issue any S/MIME certificates during the Period.

Opinion

In our opinion, throughout the period 1 September 2023 to 29 February 2024, 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 – S/MIME – Version 1.0.1.

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 – S/MIME – Version 1.0.1, 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 – S/MIME Certificates Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

A handwritten signature in black ink that reads "Deloitte LLP." The signature is written in a cursive, flowing style.

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
May 21, 2024



ATTACHMENT A

LIST OF IN SCOPE Cas

Root CAs
1. Entrust.net Certification Authority (2048) 2. Entrust Root Certification Authority 3. Entrust Root Certification Authority – G2 4. Entrust SMIME Root CA - 2022
Intermediate CAs
5. Entrust Certification Authority – ICA1
Secure Email (S/MIME) CAs
6. Class 1 Client CA – SHA256 7. Entrust Class 2 Client CA 8. Entrust Class 2 Client CA – C2CA2 9. Entrust SMIME1 Client CA
CAs capable of issuing S/MIME certificates, which have not issued any S/MIME certificates during the Period
10. Entrust Class 3 Client CA – SHA256 11. Entrust Certification Authority – ES QSig1 12. Entrust Certification Authority – ES QSeal1



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	43DF5774B03E7FEF5FE40D931A7BEDF1BB2E6842738C4E6D3841103D3AA7F339
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	CBCE622D06F9D2C093FAD75CEBB7852EF53FFFF146A0522AB321B3A482B8F8
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	6B143C2005D5539CC22EAB5F772D2A9FE87467FEFFA07FCF0A9F7D28274CA7A
4	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
5	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	5/7/2021 15:32	7/7/2029 16:02		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	C54D8B12C438725C2755B4AD81825F6975CBDA6C258A28FB88247A14F03BD22A
6	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	e249b9ec25deb70cdee550185b48cc08e15f2a6	C6E9E993C258872124AAD3C9C068B6EF23576155F310B305733361E20B17C943
7	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	00bc4d843035b759f0000000051ce1709	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	95AD94E88F5B8604E40E5FFF36B0D348E46C1D5BA06C0E735B72AA396735C415
7	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	00af1c04b2ac8c9fb0000000051ce18e3	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	1A20FEF46482A98BAC6F6C7397C017310AC7F878495438B87A7DE9035C246679
8	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	B14CF550D8F573D93E90963C32A85F851C983C98164F54D78915F6358C954F0E
9	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	E229CD78B38BD7B74AC431FA57E294CBAA35EB238293DEDE04B208218D92BA
10	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	5516151500000000051ce160e	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	069f6f4ea2294e0fcae17bfb69846efadb83b72	33857338361ECFC4858DDFF6B9EF6273E3D8856A89CEA1C0E2C65925D1C87978
11	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	B2874B588A94034798319D5D329DB265F83A47F315BA5831A4970C857166D594



CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Revoked Date	Extended Key Usage	Subject Key Identifier	SHA256 Fingerprint
12	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	1701DE38124C4458F32B88AE7E62AC15876C427A3AD3BBAE8FD1479FF00030 F3



ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement	3.16	20 Feb 2024
Entrust Certificate Services Certification Practice Statement	3.15	16 Oct 2023
Entrust Certificate Services Certification Practice Statement	3.14	20 June 2023



ENTRUST MANAGEMENT'S STATEMENT

Entrust Corporation ("Entrust") operates the Certification Authority ("CA") services as enumerated in [Attachment A](#), and provides S/MIME CA services.

The management of Entrust is responsible for establishing and maintaining effective controls over its S/MIME CA operations, including its S/MIME CA business practices disclosure on its [website](#), S/MIME key lifecycle management controls, and S/MIME 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 S/MIME CA services. Based on that assessment, in Entrust management's opinion, in providing its S/MIME CA services at Ottawa, Ontario, Canada and Toronto, Ontario, Canada, throughout the period 1 September 2023 to 29 February 2024, for its CAs as enumerated in [Attachment A](#), Entrust has:

- disclosed its S/MIME certificate lifecycle management business practices as enumerated in [Attachment B](#), including its commitment to provide S/MIME 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME 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 – S/MIME – Version 1.0.1](#).

A handwritten signature in black ink that reads "Bruce Morton".

Bruce Morton
Director, Entrust Certificate Services
May 21, 2024



ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. Entrust.net Certification Authority (2048) 2. Entrust Root Certification Authority 3. Entrust Root Certification Authority – G2 4. Entrust SMIME Root CA - 2022
Intermediate CAs
5. Entrust Certification Authority – ICA1
Secure Email (S/MIME) CAs
6. Class 1 Client CA – SHA256 7. Entrust Class 2 Client CA 8. Entrust Class 2 Client CA – C2CA2 9. Entrust SMIME1 Client CA
CAs capable of issuing S/MIME certificates, which have not issued any S/MIME certificates during the Period
10. Entrust Class 3 Client CA – SHA256 11. Entrust Certification Authority – ES QSig1 12. Entrust Certification Authority – ES QSeal1



ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

CPS Name	Version	Date
Entrust Certificate Services Certification Practice Statement	3.16	20 Feb 2024
Entrust Certificate Services Certification Practice Statement	3.15	16 Oct 2023
Entrust Certificate Services Certification Practice Statement	3.14	20 June 2023