

## 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 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 – v1.0.3](#)

### 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 – v1.0.3.

### 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 Update on delayed revocation | As publicly disclosed Bug# <a href="#">1910237</a> three certificates were issued with errors, which were documented in <a href="#">Bugs #1906467</a> and <a href="#">1906470</a> . The issue was identified following a linting report conducted on July 2, 2024. Entrust completed an internal investigation by July 3, 2024, and revoked the certificates on July 8, 2024. |

Basis for qualified opinion

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

| Observation                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Relevant portion of WebTrust - CA for S/MIME Criteria                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| As publicly disclosed in Bug # <a href="#">1906467</a> ; One (1) certificate, issued on July 2, 2024, was mis-issued because a mailbox address in the subject commonName was not included.<br><br>As a result relevant portion of the criterion 2.13 in Principle 2 of WebTrust Principles and Criteria for Certification Authorities – S/MIME – v1.0.3 was not met.                                                                                                           | <b>P2 - 2.13:</b> The CA maintains controls to provide reasonable assurance that for Subscriber certificates issued:<br>•The subjectAltName extension is present and contains at least one entry                                                                                                                                                                                                                                    |
| As publicly disclosed in Bug # <a href="#">1906470</a> ; two (2) S/MIME certificates, issued on October 5, 2023, were issued with a mailbox address case mismatch between the subject name and the subjectAltName. Identified two mis-issued certificates were revoked in July 2024.<br><br>As a result relevant portion of the criterion 2.14 in Principle 2 of <a href="#">WebTrust Principles and Criteria for Certification Authorities – S/MIME – v1.0.3</a> was not met. | <b>P2 - 2.14:</b> The CA maintains controls to provide reasonable assurance that it does not include a Mailbox Address in a Mailbox Field except as verified in accordance with Section 3.2.2 of the S/MIME Baseline Requirements.<br>•All Mailbox Addresses in the subject field or entries of type dirName of this extension SHALL be repeated as rfc822Name or otherName values of type id-on-SmtpUTF8Mailbox in this extension. |
| As publicly disclosed in Bug # <a href="#">1914065</a> ; 1,039 S/MIME certificates were missing verification of the OU and did not                                                                                                                                                                                                                                                                                                                                             | <b>P2-2.15:</b> The CA maintains controls to provide reasonable assurance that Subject information of Certificates                                                                                                                                                                                                                                                                                                                  |

| Observation                                                                                                                                                                                                                                                                                                                                                                                                                   | Relevant portion of WebTrust - CA for S/MIME Criteria                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>comply with S/MIME Baseline Requirements (BRs) section 7.1.4.2.2.c.</p> <p>As a result relevant portion of the criterion 2.15 in Principle 2 of <a href="#">WebTrust Principles and Criteria for Certification Authorities – S/MIME – v1.0.3</a> was not met.</p>                                                                                                                                                          | <p>conforms to the S/MIME Baseline Requirements, including:</p> <ul style="list-style-type: none"><li>•commonName</li><li>•organizationName</li><li>•organizationalUnitName</li><li>•organizationalIdentifier</li><li>•givenName</li><li>•Pseudonym</li><li>•serialNumber</li><li>•emailAddress</li><li>•title</li><li>•streetAddress</li><li>•localityName</li><li>•stateOrProvinceName</li><li>•postalCode</li><li>•countryName</li><li>•Subject Information for Root and Subordinate CA certificates</li></ul> |
| <p>As publicly disclosed in Bug# <a href="#">1914065</a>, 1,039 certificates were identified as mis-issued due to the lacking of OU field on August 15, 2024. Entrust initiated and completed its investigation by August 19, 2024.</p> <p>As a result relevant part of the criterion 5.2 in Principle 2 of <a href="#">WebTrust Principles and Criteria for Certification Authorities – S/MIME – v1.0.3</a> was not met.</p> | <p><b>P2-5.2:</b> The CA maintains controls to provide reasonable assurance that it:</p> <ul style="list-style-type: none"><li>•begins 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.</li></ul>                                                                                                                                                                    |

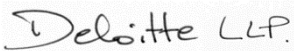
Opinion

In our opinion, except for the matters described in the table presented in the ‘Basis for qualified opinion’ section above, 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 – S/MIME – v1.0.3

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 – v1.0.3, 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.



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

## ATTACHMENT A

### LIST OF IN SCOPE CAs

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Root Cas</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <ul style="list-style-type: none"><li>1. Entrust.net Certification Authority (2048)</li><li>2. Entrust Root Certification Authority- EV Root</li><li>3. Entrust Root Certification Authority – G2</li><li>4. Entrust Root Certification Authority – G4</li><li>5. Entrust Root Certification Authority – EC1</li><li>6. Entrust Root Certification Authority - SMIMER 2022</li><li>7. AffirmTrust Commercial</li><li>8. AffirmTrust Networking</li><li>9. AffirmTrust Premium</li><li>10. AffirmTrust Premium ECC</li></ul> |
| <b>Intermediate Cas</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <ul style="list-style-type: none"><li>11. Entrust Certification Authority – AATL1</li><li>12. Entrust Certification Authority – ICA1</li></ul>                                                                                                                                                                                                                                                                                                                                                                              |
| <b>OV SSL Issuing Cas</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <ul style="list-style-type: none"><li>13. Entrust Certification Authority – L1K</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Secure Email (S/MIME) CA</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <ul style="list-style-type: none"><li>14. Class 1 Client CA – SHA256</li><li>15. Entrust Class 2 Client CA</li><li>16. Entrust Class 2 Client CA – C2CA2</li><li>17. Entrust SMIME1 Client CA</li><li>18. Entrust SMIME2 Client CA</li></ul>                                                                                                                                                                                                                                                                                |
| <b>Document Signing CA</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <ul style="list-style-type: none"><li>19. Entrust Class 3 Client CA - SHA256</li><li>20. Entrust Certification Authority - ES QSeal1</li><li>21. Entrust Certification Authority – ES QSig1</li></ul>                                                                                                                                                                                                                                                                                                                       |



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)<br>OU=(c) 1999 Entrust.net Limited<br>OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)<br>O=Entrust.net       | CN=Entrust.net Certification Authority (2048)<br>OU=(c) 1999 Entrust.net Limited<br>OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)<br>O=Entrust.net       | 3863def8                           | RSA 2048-bits | RSA SHA-1     | 12/24/1999 17:50 | 7/24/2029 14:15  |              |                    | 55e481d11180bed889b908a331f9a1240916b970 | 6DC47172E01CBCB0BF62580D895FE2B8AC9AD4F873801E0C10B9C837D21E8177  |
| 2    | 1      | CN=Entrust Root Certification Authority<br>OU=(c) 2006 Entrust, Inc.<br>OU=www.entrust.net/CPS is incorporated by reference<br>O=Entrust, Inc.<br>C=US                | CN=Entrust Root Certification Authority<br>OU=(c) 2006 Entrust, Inc.<br>OU=www.entrust.net/CPS is incorporated by reference<br>O=Entrust, Inc.<br>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<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US  | CN=Entrust Root Certification Authority - G2<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>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<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US  | CN=Entrust Root Certification Authority<br>OU=(c) 2006 Entrust, Inc.<br>OU=www.entrust.net/CPS is incorporated by reference<br>O=Entrust, Inc.<br>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<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US  | CN=Entrust Root Certification Authority<br>OU=(c) 2006 Entrust, Inc.<br>OU=www.entrust.net/CPS is incorporated by reference<br>O=Entrust, Inc.<br>C=US                | 51d33f24                           | RSA 2048-bits | RSA SHA-1     | 9/12/2014 19:23  | 9/13/2024 3:12   |              |                    | 6a72267ad01eef7de73b6951d46c8d9f901266ab | 16296E3BEF9A64CFEDE3509F36D700A5CD61CF938EC3A9558F36D17D97E16E8D  |
| 3    | 4      | CN=Entrust Root Certification Authority - G2<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US  | CN=Entrust Root Certification Authority<br>OU=(c) 2006 Entrust, Inc.<br>OU=www.entrust.net/CPS is incorporated by reference<br>O=Entrust, Inc.<br>C=US                | 51d34044                           | RSA 2048-bits | RSA SHA-256   | 9/22/2014 17:14  | 9/23/2024 1:31   |              |                    | 6a72267ad01eef7de73b6951d46c8d9f901266ab | 6B143C2005D5539CC22EAB5F772DB2A9FE87467FEFFA07FCF0A9F97D28274CA7A |
| 3    | 5      | CN=Entrust Root Certification Authority - G2<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US  | CN=Entrust Root Certification Authority<br>OU=(c) 2006 Entrust, Inc.<br>OU=www.entrust.net/CPS is incorporated by reference<br>O=Entrust, Inc.<br>C=US                | 525c32e349faf48525bc8d7810d7aabb67 | 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<br>OU=(c) 2015 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US  | CN=Entrust Root Certification Authority - G4<br>OU=(c) 2015 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US  | 00d9b5437fafa9390f00000005565ad58  | 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<br>OU=(c) 2012 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US | CN=Entrust Root Certification Authority - EC1<br>OU=(c) 2012 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US | 00a68b79290000000050d091f9         | EC 384-bits   | ECDSA SHA-384 | 12/18/2012 15:25 | 12/18/2037 15:55 |              |                    | b763e71add8de908a65583a4e06a504165114249 | 02ED0E828C14DA45165C566791700D6451D7FB56F0B2AB1D3B8EB070E56EDFF5  |



| 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<br>OU=(c) 2012 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US | CN=Entrust Root Certification Authority<br>OU=(c) 2006 Entrust, Inc.<br>OU=www.entrust.net/CPS is incorporated by reference<br>O=Entrust, Inc.<br>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 SMIME Root CA - 2022<br>O = Entrust, Inc.<br>C = US                                                                                                      | CN = Entrust SMIME Root CA - 2022<br>O = Entrust, Inc.<br>C = US                                                                                                     | 7da23fcefbbe8849c350f2a511e9b96bb71f8d80 | RSA 4096-bits | RSA SHA-384 | 2022-12-13 13:00:46 | 2047-12-7 13:00:46 |              |                                                                                                                                                                 | 94c8e8468d7f53170305441810ac65e06ea2950d  | B7A41ED8096D62716BAD7C7F530942197A9E7E3175CE05D11D01E7AD6C12DCBA7 |
| 6    | 2      | CN = Entrust SMIME Root CA - 2022<br>O = Entrust, Inc.<br>C = US                                                                                                      | CN = Entrust Root Certification Authority - G2<br>O = Entrust, Inc.<br>CN = US                                                                                       | 58cbd5fa3076485c180ac1e25747447d         | RSA 4096-bits | RSA SHA-256 | 5/17/2023 19:22:00  | 12/7/2030 23:59:00 |              |                                                                                                                                                                 | 94c8e8468d7f53170305441810ac65e06ea2950d  | E8A2B838DE5365BE0BE83AAECC646A104B5C1A2CD03D4534F6CFCF4BDA1533E0  |
| 7    | 1      | CN = AffirmTrust Commercial<br>O = AffirmTrust<br>C = US                                                                                                              | CN = AffirmTrust Commercial<br>O = AffirmTrust<br>C = US                                                                                                             | 7777062726a9b17c                         | RSA 2048-bits | RSA SHA-256 | 01/29/2010 09:06    | 12/31/2030 09:06   |              |                                                                                                                                                                 | 9d93c6538b5ecaa3f9f1e0fe59995bc24f6948f   | 0376AB1D54C5F9803CE4B2E201A0EE7EEF7B57B636E8A93C9B8D4860C96F5FA7  |
| 8    | 1      | CN = AffirmTrust Networking<br>O = AffirmTrust<br>C = US                                                                                                              | CN = AffirmTrust Networking<br>O = AffirmTrust<br>C = US                                                                                                             | 7c4f04391cd4992d                         | RSA 2048-bits | RSA SHA-256 | 01/29/2010 9:08     | 12/31/2030 09:08   |              |                                                                                                                                                                 | 071fd2e79cdac26ea240b4b07a50105074c4c8bd  | 0A81EC5A929777F145904AF38D5D509F66B5E2C58FCD8531058B0E17F3FB41B   |
| 9    | 1      | CN = AffirmTrust Premium<br>O = AffirmTrust<br>C = US                                                                                                                 | CN = AffirmTrust Networking<br>O = AffirmTrust<br>C = US                                                                                                             | 6d8c1446b1a60aee                         | RSA 2048-bits | RSA SHA-256 | 01/29/2010 9:10     | 12/31/2030 09:10   |              |                                                                                                                                                                 | 9dc067a60c22d926f545aba665521127d845ac63  | 70A73F7F376B60074248904534B11482D58F0E698ECC498DF52577EBF2E93B9A  |
| 10   | 1      | CN = AffirmTrust Premium ECC<br>O = AffirmTrust<br>C = US                                                                                                             | CN = AffirmTrust Premium ECC<br>O = AffirmTrust<br>C = US                                                                                                            | 7497258ac73f7a54                         | RSA 2048-bits | RSA SHA-256 | 01/29/2010 9:20     | 12/31/2040 09:20   |              |                                                                                                                                                                 | 9aaf297ac011353526513000c36afe40d5aed63c  | BD71FDf6DA97E4CF62D1647ADD2581B07D79ADF8397EB4ECBA9C5E8488821423  |
| 11   | 1      | CN=Entrust Certification Authority - AATL1<br>O=Entrust, Inc.<br>C=US                                                                                                 | OU=(c) 2015 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc. C=US                                                    | 00c727f51f8f922b02000000005565d8ad       | RSA 4096-bits | RSA SHA-512 | 7/20/2020 15:46     | 12/20/2037 16:16   |              | 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5, E-mail Protection                                                                                                | 63f184dd03bea39f64fa767a47c4567ec06da020  | 839F9B91C2E49218A66416DF181B984E9BE634D12A95483D98A6199FC0788D74  |
| 12   | 1      | CN=Entrust Enterprise Intermediate CA - ICA1<br>O=Entrust, Inc.<br>C=US                                                                                               | CN=Entrust.net Certification Authority (2048)<br>OU=(c) 1999 Entrust.net Limited<br>OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)<br>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 Smart card login, 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  | C54D8B12C438725C2755B4AD81825F6975CBDA6C258A2BFB88247A14F03BD22A  |
| 13   | 1      | CN=Entrust Certification Authority - L1K<br>OU=(c) 2012 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US      | CN=Entrust Root Certification Authority - G2<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US | 79851D5CBC895C56D97FEF2D5CF3D6           | RSA 2048-bits | RSA SHA-256 | 10/05/2015 19:13    | 12/05/2030 19:43   |              |                                                                                                                                                                 | 82a27074ddbcb533fcf7bd4f7cd7fa760c60a4cbf | 052C0174E806F9474AEC865129A04867F385087B631393B4D8A7F26B43733348  |
| 13   | 2      | CN=Entrust Certification Authority - L1K<br>OU=(c) 2012 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US      | CN=Entrust Root Certification Authority - G2<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US | 51d360cf                                 | RSA 2048-bits | RSA SHA-256 | 8/26/2014 17:14     | 8/27/2024 8:34     |              |                                                                                                                                                                 | 82a27074ddbcb533fcf7bd4f7cd7fa760c60a4cbf | 3B0CC20384AD7F24EB438F2B80C63EBE003F7F215B8877E418EBB0484028DB57  |
| 13   | 3      | CN=Entrust Certification Authority - L1K<br>OU=(c) 2012 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US      | CN=Entrust.net Certification Authority (2048)<br>OU=(c) 1999 Entrust.net Limited<br>OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)<br>O=Entrust.net      | 51ce00fe                                 | RSA 2048-bits | RSA SHA-256 | 10/10/2014 15:23    | 10/11/2024 6:22    |              |                                                                                                                                                                 | 82a27074ddbcb533fcf7bd4f7cd7fa760c60a4cbf | D6C3FC4938ACD1DF8A1BA30F4AE26254B2A4528E4876081EACCGA16A090AA36A  |



| CA # | Cert # | Subject                                                                                                                                                                    | Issuer                                                                                                                                                                  | Serial Number                       | Key Type      | Hash Type   | Not Before          | Not After           | Revoked Date | Extended Key Usage                                                                                 | Subject Key Identifier                   | SHA256 Fingerprint                                               |
|------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|---------------|-------------|---------------------|---------------------|--------------|----------------------------------------------------------------------------------------------------|------------------------------------------|------------------------------------------------------------------|
| 13   | 4      | CN=Entrust Certification Authority - L1K<br>OU=(c) 2012 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US           | CN=Entrust Root Certification Authority - G2<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US    | 51d360ee                            | RSA 2048-bits | RSA SHA-256 | 10/22/2014 17:05    | 10/23/2024 7:33     |              |                                                                                                    | 82a27074ddbcb533cf7bd4f7cd7fa760c60a4cbf | F5C2F23C6518F9D19B6F39BEAEA4FBAE10031BA9DC985CE1563A520DA0AD4116 |
| 13   | 5      | CN=Entrust Certification Authority - L1K<br>OU=(c) 2012 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US           | CN=Entrust Root Certification Authority - G2<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US    | 0ee94cc30000000051d37785            | RSA 2048-bits | RSA SHA-256 | 10/5/2015 19:13     | 12/5/2030 19:43     |              |                                                                                                    | 82a27074ddbcb533cf7bd4f7cd7fa760c60a4cbf | 13EFB39A2F6654E8C67BD04F4C6D4C90CD6CAB5091BCEDC73787F6B77D3D3FE7 |
| 13   | 6      | CN = Entrust Certification Authority - L1K<br>OU = (c) 2012 Entrust, Inc. - for authorized use only<br>OU = See www.entrust.net/legal-terms<br>O = Entrust, Inc.<br>C = US | CN = Entrust.net Certification Authority (2048)<br>OU = (c) 1999 Entrust.net Limited<br>OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)<br>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)<br>Client Authentication (1.3.6.1.5.5.7.3.2)             | 82a27074ddbcb533cf7bd4f7cd7fa760c60a4cbf | 7F4325CC24107A39441552F27FDC34185802482E164D1794AA415EF1E4206BA7 |
| 14   | 1      | CN=Entrust Class 1 Client CA - SHA256<br>OU=(c) 2015 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US              | CN=Entrust Root Certification Authority - G2<br>OU=(c) 2009 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>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 | C6E9E993C258B72124AAD3C9C068B6EF23576155F3108305733361E20B17C943 |
| 15   | 1      | CN=Entrust Class 2 Client CA<br>OU=(c) 2010 Entrust, Inc.<br>OU=www.entrust.net/CPS is incorporated by reference<br>O=Entrust, Inc.<br>C=US                                | CN=Entrust.net Certification Authority (2048)<br>OU=(c) 1999 Entrust.net Limited<br>OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)<br>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 |
| 15   | 2      | CN=Entrust Class 2 Client CA<br>OU=(c) 2010 Entrust, Inc.<br>OU=www.entrust.net/CPS is incorporated by reference<br>O=Entrust, Inc.<br>C=US                                | CN=Entrust.net Certification Authority (2048)<br>OU=(c) 1999 Entrust.net Limited<br>OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)<br>O=Entrust.net         | 00af1c04b2ac8cff9b00000000051ce18e3 | 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 |
| 16   | 1      | CN=Entrust Class 2 Client CA - C2CA2<br>O=Entrust, Inc.<br>C=US                                                                                                            | CN=Entrust.net Certification Authority (2048)<br>OU=(c) 1999 Entrust.net Limited<br>OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)<br>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 |
| 17   | 1      | CN = Entrust Personal Email Certification Authority - SMIME1<br>O = Entrust, Inc.<br>C = US                                                                                | CN = Entrust SMIME Root CA - 2022<br>O = Entrust, Inc.<br>C = US                                                                                                        | 1bb7bc5a6a4f06be4f716105ecd2a74     | RSA 4096-bits | SHA-384     | 2022-12-14 18:31    | 2040-12-29 23:59    |              | E-mail Protection, TLS Web Client Authentication                                                   | 03219B5F18632EC87EF9AEDAD9179FB6C91B8360 | 97E229CD78B38BD7B74AC431FA57E294CBAA35EB238293DEDE04820B218D92BA |
| 18   | 1      | CN = Entrust Enterprise Email CA - SMIME2<br>O = Entrust, Inc.<br>C = US                                                                                                   | CN = Entrust SMIME Root CA - 2022<br>O = Entrust, Inc.<br>C = US                                                                                                        | 1ab5936d245a2fe43421c2ef6513e3f3    | RSA 4096-bits | SHA-384     | 2024-06-26 16:05    | 2040-12-29 23:59:59 |              | E-mail Protection, TLS Web Client Authentication                                                   | E08815F1C58A919DBF95E8E676AD71CD0780F87F | D9F628050929FC422B1FCB73C11496923D7D80E155769A134313C0E5E81F82A8 |
| 19   | 1      | CN=Entrust Class 3 Client CA - SHA256<br>OU=(c) 2015 Entrust, Inc. - for authorized use only<br>OU=See www.entrust.net/legal-terms<br>O=Entrust, Inc.<br>C=US              | CN=Entrust.net Certification Authority (2048)<br>OU=(c) 1999 Entrust.net Limited<br>OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)<br>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 |
| 20   | 1      | CN=Entrust Certification Authority - ES<br>QSeal1<br>C=ES<br>O=Entrust Datacard Europe, S.L.<br>organizationIdentifier=VATES-B81188047                                     | CN=Entrust Certification Authority - AATL1<br>C=US<br>O=Entrust, Inc.                                                                                                   | 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 |
| 21   | 1      | CN=Entrust Certification Authority - ES<br>QSig1<br>C=ES<br>O=Entrust Datacard Europe, S.L.<br>organizationIdentifier=VATES-B81188047                                      | CN=Entrust Certification Authority - AATL1<br>C=US<br>O=Entrust, Inc.                                                                                                   | 4491ca5825be79842b29b0c37286215f    | RSA 4096-bits | RSA SHA-512 | 2020-07-29 16:33:00 | 2037-12-19 23:59:00 | 2024-09-25   | E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5                                   | 5a53088a6130a90dead54397d3983b951e2e6d02 | B2874B588A94034798319D5D329DB265F83A47F315BA5831A4970CB57166D594 |

**ATTACHMENT B****LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS**

| <b>CPS Name</b>                                                               | <b>Version</b> | <b>Date</b>   |
|-------------------------------------------------------------------------------|----------------|---------------|
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.29           | 21 Feb 2025   |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.28           | 21 Nov 2024   |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.27           | 7 Nov 2024    |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.26           | 15 Oct 2024   |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.25           | 9 Oct 2024    |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.24           | 19 Sept 2024  |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.23           | 11 Sept 2024  |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.22           | 31 July 2024  |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.21           | 14 May 2024   |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.20           | 26 March 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.19           | 25 March 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.18           | 22 March 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.17           | 21 March 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.16           | 20 Feb 2024   |
| <a href="#">Entrust EU, S.L. Certification Practice Statement</a>             | 2.2            | 27 Jan 2025   |
| <a href="#">Entrust EU, S.L. Certification Practice Statement</a>             | 2.1            | 1 May 2024    |
| <a href="#">Entrust EU, S.L. Certification Practice Statement</a>             | 2.0            | 31 Oct 2023   |
| <a href="#">AffirmTrust Certification Practice Statement</a>                  | 3.18           | 15 Jan 2025   |
| <a href="#">AffirmTrust Certification Practice Statement</a>                  | 3.17           | 21 Mar 2024   |
| <a href="#">AffirmTrust Certification Practice Statement</a>                  | 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 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 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 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 – v1.0.3](#)

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

| Bug ID  | Summary                                                                 | Opened    | Closed     |
|---------|-------------------------------------------------------------------------|-----------|------------|
| 1906467 | S/MIME mailbox address not in subjectAltName                            | 7/2/2024  | 11/13/2024 |
| 1906470 | S/MIME mailbox address case mismatch between subject and subjectAltName | 7/3/2024  | 12/5/2024  |
| 1910237 | Delayed Revocation for S/MIME certificates                              | 7/27/2024 | 11/13/2024 |
| 1914065 | S/MIME certificates lacking OU verification                             | 8/20/2024 | 02/28/2025 |

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

Bruce Morton  
Director, Entrust Certificate Services  
June 27, 2025



## ATTACHMENT A

### LIST OF IN SCOPE CAs

|                                                       |
|-------------------------------------------------------|
| <b>Root Cas</b>                                       |
| 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 - SMIMER 2022 |
| 7. AffirmTrust Commercial                             |
| 8. AffirmTrust Networking                             |
| 9. AffirmTrust Premium                                |
| 10. AffirmTrust Premium ECC                           |
| <b>Intermediate Cas</b>                               |
| 11. Entrust Certification Authority – AATL1           |
| 12. Entrust Certification Authority – ICA1            |
| <b>OV SSL Issuing Cas</b>                             |
| 13. Entrust Certification Authority – L1K             |
| <b>Secure Email (S/MIME) CA</b>                       |
| 14. Class 1 Client CA – SHA256                        |
| 15. Entrust Class 2 Client CA                         |
| 16. Entrust Class 2 Client CA – C2CA2                 |
| 17. Entrust SMIME1 Client CA                          |
| 18. Entrust SMIME2 Client CA                          |
| <b>Document Signing CA</b>                            |
| 19. Entrust Class 3 Client CA - SHA256                |
| 20. Entrust Certification Authority - ES QSeal1       |
| 21. Entrust Certification Authority – ES QSig1        |

## ATTACHMENT B

### LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

| CPS Name                                                                      | Version | Date         |
|-------------------------------------------------------------------------------|---------|--------------|
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.29    | 21 Feb 2025  |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.28    | 21 Nov 2024  |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.27    | 7 Nov 2024   |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.26    | 15 Oct 2024  |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.25    | 9 Oct 2024   |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.24    | 19 Sept 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.23    | 11 Sept 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.22    | 31 July 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.21    | 14 May 2024  |



|                                                                               |      |               |
|-------------------------------------------------------------------------------|------|---------------|
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.20 | 26 March 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.19 | 25 March 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.18 | 22 March 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.17 | 21 March 2024 |
| <a href="#">Entrust Certificate Services Certification Practice Statement</a> | 3.16 | 20 Feb 2024   |
| <a href="#">Entrust EU, S.L. Certification Practice Statement</a>             | 2.2  | 27 Jan 2025   |
| <a href="#">Entrust EU, S.L. Certification Practice Statement</a>             | 2.1  | 1 May 2024    |
| <a href="#">Entrust EU, S.L. Certification Practice Statement</a>             | 2.0  | 31 Oct 2023   |
| <a href="#">AffirmTrust Certification Practice Statement</a>                  | 3.18 | 15 Jan 2025   |
| <a href="#">AffirmTrust Certification Practice Statement</a>                  | 3.17 | 21 Mar 2024   |
| <a href="#">AffirmTrust Certification Practice Statement</a>                  | 3.16 | 20 Feb 2024   |