

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 2021 to 28 February 2022 (the “Period”) for its CAs as enumerated in [Attachment A1](#), Entrust has:

- disclosed its SSL certificate lifecycle management business practices in its Certification Practice Statements 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

And, for its CAs as enumerated in [Attachment A2](#):

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5](#).

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 with Network Security v2.4.1.

Our independence and quality control

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

The firm applies Canadian Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and accordingly maintains a comprehensive system of quality



control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner’s responsibilities

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

- (1) obtaining an understanding of Entrust’s SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of Entrust’s network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- (2) selectively testing transactions executed in accordance with disclosed SSL 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

Because of the nature and inherent limitations of controls, Entrust’s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Other matters

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

| Matter topic | Matter description |
|----------------------------------|--|
| 1 Mozilla ‘bug’ responses | As described in management’s statement, management has reported or responded to certain ‘bugs’ on Mozilla’s Bugzilla reporting system. Management’s statement contains information on their outcome or resolution. |

Practitioner’s opinion

In our opinion, throughout the period 1 March 2021 to 28 February 2022, 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 with Network Security v2.5.

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 with Network Security v2.5, 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.

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
11 May 2022



ATTACHMENT A1

LIST OF IN SCOPE CAs for SSL BASELINE REQUIREMENTS

| |
|---|
| Root CAs |
| <ol style="list-style-type: none">1. Entrust.net Certification Authority (2048)2. Entrust Root Certification Authority3. Entrust Root Certification Authority – G24. Entrust Root Certification Authority – G45. Entrust Root Certification Authority – EC16. Entrust Root Certification Authority – EC2 |
| OV SSL Issuing CAs |
| <ol style="list-style-type: none">13. Entrust Certification Authority – L1C14. Entrust Certification Authority – L1F15. Entrust Certification Authority – L1K16. CRYPTAS OV Issuing CA17. Siemens Issuing CA Internet Server 2020 |
| EV SSL Issuing CAs |
| <ol style="list-style-type: none">18. Entrust Certification Authority – L1E19. Entrust Certification Authority – L1J20. Entrust Certification Authority – L1M21. Entrust Certification Authority – L1N22. CRYPTAS OV Issuing CA |
| Qualified Certificate EV SSL Issuing CAs |
| <ol style="list-style-type: none">23. Entrust Certification Authority - QTSP124. Entrust Certification Authority - DE QWAC125. Entrust Certification Authority - ES QWAC2 |

LIST OF IN SCOPE CAs for NETWORK SECURITY REQUIREMENTS

| |
|---|
| Root CAs |
| <ol style="list-style-type: none"> 1. Entrust.net Certification Authority (2048) 2. Entrust Root Certification Authority 3. Entrust Root Certification Authority – G2 4. Entrust Root Certification Authority – G4 5. Entrust Root Certification Authority – EC1 6. Entrust Root Certification Authority – EC2 7. Entrust Code Signing Root Certification Authority - CSBR1 8. Entrust Digital Signing Root Certification Authority - DSR1 9. Entrust Verified Mark Root Certification Authority - VMCR1 |
| Intermediate CAs |
| <ol style="list-style-type: none"> 10. Entrust Certification Authority - AATL1 11. Entrust Enterprise Intermediate CA - ICA1 12. Siemens Intermediate CA 2021 |
| OV SSL Issuing CAs |
| <ol style="list-style-type: none"> 13. Entrust Certification Authority – L1C 14. Entrust Certification Authority – L1F 15. Entrust Certification Authority – L1K 16. CRYPTAS OV Issuing CA 17. Siemens Issuing CA Internet Server 2020 |
| EV SSL Issuing CAs |
| <ol style="list-style-type: none"> 18. Entrust Certification Authority – L1E 19. Entrust Certification Authority – L1J 20. Entrust Certification Authority – L1M 21. Entrust Certification Authority – L1N 22. CRYPTAS OV Issuing CA |
| Qualified Certificate EV SSL Issuing CAs |
| <ol style="list-style-type: none"> 23. Entrust Certification Authority - QTSP1 24. Entrust Certification Authority - DE QWAC1 25. Entrust Certification Authority - ES QWAC2 |
| Code Signing Issuing CAs |
| <ol style="list-style-type: none"> 26. Entrust Code Signing Certification Authority – L1D 27. Entrust Code Signing CA - OVCS1 28. Entrust Code Signing CA - OVCS2 |
| EV Code Signing Issuing CAs |
| <ol style="list-style-type: none"> 29. Entrust Extended Validation Code Signing CA – EVCS1 30. Entrust Extended Validation Code Signing CA – EVCS2 |
| Secure Email (S/MIME) CAs |
| <ol style="list-style-type: none"> 31. Entrust Class 1 Client CA 32. Entrust Class 1 Client CA - SHA256 33. Entrust Class 2 Client CA 34. Entrust Class 2 Client CA - C2CA2 |
| Timestamp CAs |
| <ol style="list-style-type: none"> 35. Entrust Timestamping CA – TS1 36. Entrust Time Stamping CA – TS2 |
| Verified Mark Certificate CAs |
| <ol style="list-style-type: none"> 37. Entrust Certificate Authority - VMC1 38. Entrust Verified Mark CA - VMC2 |



CA IDENTIFYING INFORMATION

| CA # | Cert # | Subject | Issuer | Serial Number | Key Type | Hash Type | Not Before | Not After | Revoked Date | Extended Key Usage | Subject Key Identifier | SHA256 Fingerprint |
|------|--------|---|---|--|---------------|---------------|---------------------|---------------------|--------------|--|--|--|
| 1 | 1 | CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net | CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net | 3863def8 | RSA 2048-bits | RSA SHA-1 | 1999-12-24 17:50:51 | 2029-07-24 14:15:12 | | | 55e481d11180bed889b908a331f9a1240916b970 | 6dc47172e01c1cb0bf62580d895fe2b8ac9ad4f873801e0c10b9c837d21eb177 |
| 2 | 1 | CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US | 456b5054 | RSA 2048-bits | RSA SHA-1 | 2006-11-27 20:23:42 | 2026-11-27 20:53:42 | | | 6890e467a4a65380c78666a4f174b43fb84bd6d | 73c176434f1bc6d5ad4f5b0e76e727287c8de57616c1e6e6141a2b2cb7d8e4c |
| 3 | 1 | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 4a538c28 | RSA 2048-bits | RSA SHA-256 | 2009-07-07 17:25:54 | 2030-12-07 17:55:54 | | | 6a72267ad01eef7de73b6951d46c8d9f901266ab | 43df5774b03e7ef5fe40d931a7bedf1bb2e6b42738c4e6d3841103d3aa7f339 |
| 3 | 2 | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US | 51d33f09 | RSA 2048-bits | RSA SHA-1 | 2014-09-12 17:28:27 | 2024-09-13 03:12:02 | | | 6a72267ad01eef7de73b6951d46c8d9f901266ab | cbce622d06f9d2c093fad75cebb7852ef53ffff146ad522ab321b3a4b2bd8f8 |
| 3 | 3 | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US | 51d33f24 | RSA 2048-bits | RSA SHA-1 | 2014-09-12 19:23:57 | 2024-09-13 03:12:23 | | | 6a72267ad01eef7de73b6951d46c8d9f901266ab | 16296e3bef9a64cfede3509f36d700a5cd61cf938ec3a955bf36d17d97e16e8d |
| 3 | 4 | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority OU=(c) 2006 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US | 51d34044 | RSA 2048-bits | RSA SHA-256 | 2014-09-22 17:14:57 | 2024-09-23 01:31:53 | | | 6a72267ad01eef7de73b6951d46c8d9f901266ab | 6b143c2005d5539cc22eab5772db2a9fe87467effa07fca9f7d28274ca7a |
| 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 | 00d9b5437fafa9390f00000005565ad58 | RSA 4096-bits | RSA SHA-256 | 2015-05-27 11:11:16 | 2037-12-27 11:41:16 | | | 9f38c45623c339e8a0716ce8544ce4e83ab1bf67 | db3517d1f6732a2d5ab97c533ec70779ee3270a62fb4ac4238372460e6f01e88 |
| 5 | 1 | CN=Entrust Root Certification Authority - EC1 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - EC1 OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 00a68b7929000000050d091f9 | EC 384-bits | ECDSA SHA-384 | 2012-12-18 15:25:36 | 2037-12-18 15:55:36 | | | b763e71add8de908a65583a4e06a504165114249 | 02ed0e28c14da45165c566791700d6451d7fb56f0b2ab1d3b8eb070e56edff5 |
| 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 | 008011196de613db16000000051d3575e | EC 384-bits | RSA SHA-256 | 2016-06-10 14:58:55 | 2026-11-10 15:28:55 | | | b763e71add8de908a65583a4e06a504165114249 | 3fde0d36e026b6e8be2c28883607c8651de10bd6c1fad365e60f4ea2f3b03 |
| 6 | 1 | CN=Entrust Root Certification Authority - EC2 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 - EC2 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 00bbd3315a80485c9900000005565cdaf | EC 521-bits | ECDSA SHA-256 | 2015-05-27 13:29:11 | 2037-12-27 13:59:11 | | | a1f88d67c167c938a415d6005a20823d8f2e0ef3 | f11aaa40753fda0629cbda80e56bb73f3dea1ce2a8b3aa9bc3abfd0123725159 |
| 7 | 1 | CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US | CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US | 7ff1a8f9f43ae8876e2dc6ff5e433db2ee30a643 | RSA 4096-bits | RSA SHA-512 | 2021-05-07 13:26:36 | 2040-12-30 13:26:36 | | | 82bad63d97ce9cf71e89237affdb3b5693557cf | b80847fda453bf6ed876ca7bc046a2481909e15bed376e665e7ad09f3864e71 |
| 7 | 2 | CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 4e40e43754ede68c000000051d3947f | RSA 4096-bits | RSA SHA-256 | 2021-05-07 15:43:45 | 2030-11-07 16:13:45 | | Code Signing, Time Stamping | 82bad63d97ce9cf71e89237affdb3b5693557cf | 18dd9a467054c74a5ae46182843a6f4ec46d5e338d91adf4e5980b50193fb94b |
| 8 | 1 | CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 2d37bcd092d2cb88b67f5ccadab71b39b | RSA 4096-bits | RSA SHA-512 | 2021-11-12 00:00:00 | 2030-12-30 00:00:00 | | 1.3.6.1.4.1.311.10.3.12, Time Stamping | a6654181f25b87056addfd8a544e8f987bdc23b8 | 20fc75acb2cad7978c7b006a9b1523bfdaf5490afcf49652c585e4a12f601c85 |
| 8 | 2 | CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US | CN=Entrust Digital Signing Root Certification Authority - DSR1 O=Entrust, Inc. C=US | 6c73c936b185e50b804d5bcec29f83d21a51c1a3 | RSA 4096-bits | RSA SHA-512 | 2021-11-12 18:28:47 | 2040-12-30 18:28:47 | | | a6654181f25b87056addfd8a544e8f987bdc23b8 | e874fe2531eae4a4b6b62f37496bbae90eb1d8fc8cedbebb00a182cfacdc7e61 |



| CA # | Cert # | Subject | Issuer | Serial Number | Key Type | Hash Type | Not Before | Not After | Revoked Date | Extended Key Usage | Subject Key Identifier | SHA256 Fingerprint |
|------|--------|--|---|--|---------------|---------------|---------------------|---------------------|---------------------|---|--|--|
| 9 | 1 | CN=Entrust Verified Mark Root Certification Authority - VMCR1 O=Entrust, Inc. C=US | CN=Entrust Verified Mark Root Certification Authority - VMCR1 O=Entrust, Inc. C=US | 743900bd5b07fc63d7e9150452c89bb701680463 | RSA 4096-bits | RSA SHA-512 | 2021-05-07 13:31:48 | 2040-12-30 13:31:48 | | | 7323567b2b7845809ab8c27ccca586398b2678c5 | 7831d95a47d42508cd5c9e6264f9096bac19f04eb9b7c8bdd35fff71c189617 |
| 10 | 1 | C=US O=Entrust, Inc. CN=Entrust Certification Authority - AATL1 | CN=Entrust Root Certification Authority - G4 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 00c727f51f8f922b0200000005565d8ad | RSA 4096-bits | RSA SHA-512 | 2020-07-20 15:46:21 | 2037-12-20 16:16:21 | | 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5, E-mail Protection | 63f184dd03bea39f64fa767a47c4567ec06da020 | 839f9b91c2e49218a66416df181b984e9be634d12a95483d98a6199fc0788d74 |
| 11 | 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 | 3eeb174d9b443ba9000000051ce1981 | RSA 2048-bits | RSA SHA-256 | 2021-05-07 15:32:00 | 2029-07-07 16:02:00 | | TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin, Microsoft Encrypted File System, 1.3.6.1.4.1.311.10.3.4.1, 1.3.6.1.4.1.311.67.1.1 | c838d40a70dda357a8e596592d1313c920d5dcb3 | c54d8b12c438725c2755b4ad81825f975cbda6c258a2bfb8247a14f03bd22a |
| 12 | 1 | CN=Siemens Intermediate CA 2021 O=Siemens C=DE | CN=Entrust Enterprise Intermediate CA - ICA1 O=Entrust, Inc. C=US | 22c541ff0bb7bf2214f84b9669f69d75 | RSA 4096-bits | RSA SHA-256 | 2021-06-09 00:00:00 | 2025-08-09 00:00:00 | | E-mail Protection, TLS Web Client Authentication, 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 | 8e47059c577d6060cb48ccf7a2604ed2eb00ba62 | 817d76354988c8e88d799e6ebb873a1033d54e1718f026d7835987932d3bc7b6 |
| 12 | 2 | CN=Siemens Intermediate CA 2021 O=Siemens C=DE | CN=Entrust Enterprise Intermediate CA - ICA1 O=Entrust, Inc. C=US | 1cc223abe7a3f1461e85a6b8a92af2f7 | RSA 4096-bits | RSA SHA-256 | 2021-06-15 00:00:00 | 2025-08-15 00:00:00 | 2021-10-14 17:03:35 | E-mail Protection, TLS Web Client Authentication, 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 | 8e47059c577d6060cb48ccf7a2604ed2eb00ba62 | 455aaf6e80421171e484b3115a8383a07f09596bd9ba8c9bc540c9cbb8f92b3 |
| 13 | 1 | CN=Entrust Certification Authority - L1C OU=(c) 2009 Entrust, Inc. OU=www.entrust.net/rpa 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 | 4c0e8c1d | RSA 2048-bits | RSA SHA-256 | 2011-11-11 15:26:22 | 2021-11-11 17:45:09 | | | 1ef1ab8906f8490f013377ee147aee197c93284d | ca971c936c699bc5d6a609d2529f03a60f6e141a2cf12be72313da50ca64e17 |
| 13 | 2 | CN=Entrust Certification Authority - L1C OU=(c) 2009 Entrust, Inc. OU=www.entrust.net/rpa 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 | 4c0e8c39 | RSA 2048-bits | RSA SHA-1 | 2011-11-11 15:40:40 | 2021-11-12 02:51:17 | | | 1ef1ab8906f8490f013377ee147aee197c93284d | 0ee4daf71a85d842d23f4910fd4c909b7271861931f1d5feac868225f2700e2 |
| 14 | 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 | 00b601913d8553bafa000000051d4c1f6 | EC 384-bits | ECDSA SHA-384 | 2016-04-05 20:17:29 | 2037-10-05 20:47:29 | | TLS Web Server Authentication, TLS Web Client Authentication | 2e62f014ee87c3353033defe4b99efd3bb8a3c9 | 1835b0e482ea65536fc010e4bc13c060f65668165fba97e2f542ce96ca6dfefc |
| 14 | 2 | CN=Entrust Certification Authority - L1F OU=(c) 2016 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net | 00a25b1769bad80ad7000000051ce1941 | EC 384-bits | RSA SHA-256 | 2021-02-05 16:34:34 | 2029-07-05 17:04:34 | | TLS Web Server Authentication, TLS Web Client Authentication | 2e62f014ee87c3353033defe4b99efd3bb8a3c9 | 0c5a09db8aedf7d2d1dde14dccc2db6ea959bcf6f010360d836c342c624d7e0e |
| 15 | 1 | CN=Entrust Certification Authority - L1K OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 51d360ce | RSA 2048-bits | RSA SHA-256 | 2014-08-26 17:07:28 | 2024-08-27 05:48:52 | | | 82a27074ddbc533fc7bd4f7cd7fa760c60a4cbf | 3b6dd5581c9853092007db1bb0106fc61205e88e360543d7cae02d68e7a25ac3 |
| 15 | 2 | CN=Entrust Certification Authority - L1K OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 51d360cf | RSA 2048-bits | RSA SHA-256 | 2014-08-26 17:14:49 | 2024-08-27 08:34:47 | | | 82a27074ddbc533fc7bd4f7cd7fa760c60a4cbf | 3b0cc20384ad7f24eb438f2b80c63ebe003f7f215b8877e418ebb0484028db57 |
| 15 | 3 | CN=Entrust Certification Authority - L1K OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net | 51ce00fe | RSA 2048-bits | RSA SHA-256 | 2014-10-10 15:23:17 | 2024-10-11 06:22:47 | | | 82a27074ddbc533fc7bd4f7cd7fa760c60a4cbf | d6c3fc493bacd1df8a1ba30f4ae26254b2a4528e4876081eacc6a16a090aa36a |
| 15 | 4 | CN=Entrust Certification Authority - L1K OU=(c) 2012 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 51d360ee | RSA 2048-bits | RSA SHA-256 | 2014-10-22 17:05:14 | 2024-10-23 07:33:22 | | | 82a27074ddbc533fc7bd4f7cd7fa760c60a4cbf | f5c2f23c6518f9d19b6f39beaea4fbae10031ba9dc985ce1563a520da0ad4116 |
| 15 | 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 | 0ee94cc3000000051d37785 | RSA 2048-bits | RSA SHA-256 | 2015-10-05 19:13:56 | 2030-12-05 19:43:56 | | | 82a27074ddbc533fc7bd4f7cd7fa760c60a4cbf | 13efb39a2f6654e8c67bd04f4c6d4c90cd6cab5091bcedc73787f6b77d3d3fe7 |
| 16 | 1 | CN=CRYPTAS OV Issuing CA O=CRYPTAS it-Security GmbH C=AT | 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 | 325141290f2323266b9d21c1f7bea575 | RSA 2048-bits | RSA SHA-256 | 2021-06-18 00:00:00 | 2030-12-01 00:00:00 | 2022-02-24 00:00:00 | TLS Web Server Authentication, TLS Web Client Authentication | b8d708f51ca58fa6455213f2f4d505b773aa204a | faecdd05d9f2e5fe8498de56cdf895c0a697094e1773dede5fce2001b4c7b152 |



| CA # | Cert # | Subject | Issuer | Serial Number | Key Type | Hash Type | Not Before | Not After | Revoked Date | Extended Key Usage | Subject Key Identifier | SHA256 Fingerprint |
|------|--------|--|---|-----------------------------------|---------------|---------------|---------------------|---------------------|---------------------|--|--|---|
| 16 | 2 | CN=CRYPTAS OV Issuing CA O=CRYPTAS it-Security GmbH C=AT | 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 | 7650788c314c05b358d4c2da8d4d69a2 | RSA 2048-bits | RSA SHA-256 | 2021-07-09 00:00:00 | 2030-12-01 00:00:00 | 2021-06-18 00:00:00 | TLS Web Server Authentication, TLS Web Client Authentication | b8d708f51ca58fa6455213f2f4d505b773aa204a | 452f1df0e4eb3943f5d0714f55f5bc15597083eb9297b025e8e53049504cd1de |
| 17 | 1 | C=DE O=Siemens CN=Siemens Issuing CA Internet Server 2020 | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 00fab27dfff80d09a000000051d39440 | 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 |
| 18 | 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 | 008666b02ac1cb5440000000051d3589c | 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 | 5b418ab2c443c1bdfc85441559de096adffb9a1 | 232f6367cf561e00c83e180a9fca8546b3771fb450ebcb4a0526f8349c8ca139 |
| 19 | 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 | 0a83d4803e7e9f51000000051d4c1f7 | 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 | 3447b74b5e500a549983fa2ced73a5642e6aac78829546158437df66d7435b8 |
| 20 | 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 | ca290389e0d8c62a4083f628a39f52fe3f38b73199cfa7c0372378a440fb6a |
| 20 | 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 | 61a1e7d2000000051d366a6 | 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 |
| 21 | 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 | 00abec77ff1b410c0700000005565d805 | 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 |
| 22 | 1 | CN=CRYPTAS EV Issuing CA O=CRYPTAS it-Security GmbH C=AT | 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 | 1d6a0a7890840919beb89ebc49aa288 | RSA 2048-bits | RSA SHA-256 | 2021-06-18 00:00:00 | 2030-12-01 00:00:00 | 2022-02-24 00:00:00 | TLS Web Server Authentication, TLS Web Client Authentication | fcdb7e9a08c2549d98185dba2d116e08617ea75f | 1ec0afc3ed9f2badca068e0c2d81f9c62ef9752316317b788662b3edad38075 |
| 22 | 2 | CN=CRYPTAS EV Issuing CA O=CRYPTAS it-Security GmbH C=AT | 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 | 3a132e504ef6a5c1e3276851e0f462be | RSA 2048-bits | RSA SHA-256 | 2021-07-09 00:00:00 | 2030-12-01 00:00:00 | 2021-06-18 00:00:00 | TLS Web Server Authentication, TLS Web Client Authentication | fcdb7e9a08c2549d98185dba2d116e08617ea75f | 679b5d3305a168c4b7642b34337e57c4679ba0b1e3639127fcb74c6e62919eb |
| 22 | 2 | CN=CRYPTAS EV Issuing CA O=CRYPTAS it-Security GmbH C=AT | 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 | 4ee7fe99fe7320e41b2b6ed671a57480 | RSA 2048-bits | RSA SHA-256 | 2021-07-09 00:00:00 | 2030-12-01 00:00:00 | 2021-06-18 00:00:00 | TLS Web Server Authentication, TLS Web Client Authentication | fcdb7e9a08c2549d98185dba2d116e08617ea75f | eff58b03b76bab94b092f603752bfff7b0812be1d159fbc44ca746c77a652d576 |
| 23 | 1 | C=ES O=Entrust Datacard Europe S.L. organizationIdentifier=VATES-B81188047 CN=Entrust Certification Authority - QTSP1 | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 009c6cf695700c600000000051d393a6 | 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 | 1cad3f9cd72d2219a19c4be9daf12a33f7fba0d | 681ebc1822b079b97e0404e4687d9b6c0c0892c820f5738a282aae62529bdd8 |
| 24 | 1 | C=DE O=Entrust Datacard Deutschland GmbH organizationIdentifier=VATDE-119264316 CN=Entrust Certification Authority - DE QWAC1 | 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 | 00ec8a269b09be4e9d000000051d39423 | RSA 2048-bits | RSA SHA-256 | 2020-07-29 19:16:08 | 2030-11-29 19:46:08 | 2022-02-24 00:00:00 | TLS Web Server Authentication, TLS Web Client Authentication | 19233ae746ebe4d894e2f7daf1b3f8aa95340e63 | ca14cf9b309ba032bb21910c1aedae4d29fe0656b4f8bfa23cbe94d431c0674 |
| 25 | 1 | CN=Entrust Certification Authority - ES QWAC2 organizationIdentifier=VATES-B81188047 O=Entrust EU, S.L. C=ES | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 7a8872b868a359dab1b02ecf4c9718d | 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 | c97f2f6e6a8adb6ecfe4978f08ca8f6f0123a94784522b610ad6ab51439f62 |
| 26 | 1 | CN=Entrust Code Signing Certification Authority - L1D OU=(c) 2009 Entrust, Inc. OU=www.entrust.net/rpa 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 | 4c0e8c1e | RSA 2048-bits | RSA SHA-256 | 2011-11-11 15:29:00 | 2021-11-12 03:28:50 | | | a7b1aac4b60edddca9f88949682d5e74341d125 | fa9d6df1af0275300d52a485d0360543b5dfb441bec0b8c9a0dff811b6d88 |



| CA # | Cert # | Subject | Issuer | Serial Number | Key Type | Hash Type | Not Before | Not After | Revoked Date | Extended Key Usage | Subject Key Identifier | SHA256 Fingerprint |
|------|--------|--|--|------------------------------------|---------------|-------------|---------------------|---------------------|---------------------|--|--|--|
| 26 | 2 | CN=Entrust Code Signing Certification Authority - L1D OU=(c) 2009 Entrust, Inc. OU=www.entrust.net/rpa 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 | 4c0e8c3a | RSA 2048-bits | RSA SHA-1 | 2011-11-11 15:41:26 | 2021-11-12 08:51:52 | | | a7b1aac4b606edddca9f88949682d5e74341d125 | 8b16d48f721dfab157214b9ace9dda8efba5a06b4eed901806f086d1df8ead37 |
| 27 | 1 | CN=Entrust Code Signing CA - OVCS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 7ab8c4fc0000000051d373d4 | RSA 2048-bits | RSA SHA-256 | 2015-06-09 18:03:40 | 2025-06-09 18:33:40 | | Code Signing | 7e1a1f1a11745c64c90c1f9401abfd81642ea12c | 7ba43a4ccb37b1ccc2dd11ce0c911da3a2917b0ca0e846056854ef464c50c4 |
| 27 | 2 | CN=Entrust Code Signing CA - OVCS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 43c10b1c0000000051d373da | RSA 2048-bits | RSA SHA-256 | 2015-06-10 13:46:05 | 2030-11-10 14:16:05 | | Code Signing | 7e1a1f1a11745c64c90c1f9401abfd81642ea12c | cc5b7a0e5d6771ba348d3d763752f0667026b3531c5396edbe24adce93215723 |
| 28 | 1 | CN=Entrust Code Signing CA - OVCS2 O=Entrust, Inc. C=US | CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US | 71ef574af3554c35a2c69f66f4b6bcd | RSA 4096-bits | RSA SHA-512 | 2021-05-07 19:20:45 | 2040-12-29 23:59:00 | | Code Signing | ef9fba79b073f2251e789c03529c1b5384de8ded | 95f843046bac035572a3ba1b821df8b759467f5b512ddfa8a72f0799447d6368 |
| 29 | 1 | CN=Entrust Extended Validation Code Signing CA - EVCS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 417ace390000000051d373bb | RSA 2048-bits | RSA SHA-256 | 2015-06-09 17:54:53 | 2025-06-09 18:24:53 | | Code Signing | 2a0a6f322c292021766ab1ac8c3caf938e0e6ba2 | 57bc151d924c5a43b57b6433a58a93885f773b4631fdec8b5c9fc3545529f274 |
| 29 | 2 | CN=Entrust Extended Validation Code Signing CA - EVCS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 00d9d6b8f20000000051d373d8 | RSA 2048-bits | RSA SHA-256 | 2015-06-10 13:39:51 | 2025-06-10 14:09:51 | | Code Signing | 2a0a6f322c292021766ab1ac8c3caf938e0e6ba2 | 091c6319936f0cac4c7b5e027dcca2b2a2af4561ea2c71e650c1e3fb905fd0 |
| 29 | 3 | CN=Entrust Extended Validation Code Signing CA - EVCS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 0087825260000000051d373d9 | RSA 2048-bits | RSA SHA-256 | 2015-06-10 13:42:49 | 2030-11-10 14:12:49 | | Code Signing | 2a0a6f322c292021766ab1ac8c3caf938e0e6ba2 | d04db927c663aa8c853d54716dd6dc2a4b2fef9c3ae1bf250447f5d7771e57 |
| 30 | 1 | CN=Entrust Extended Validation Code Signing CA - EVCS2 O=Entrust, Inc. C=US | CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US | 35afb77b9d341f6afc8f8446ab31352b | RSA 4096-bits | RSA SHA-512 | 2021-05-07 19:19:52 | 2040-12-29 23:59:00 | | Code Signing | ce894f8251aa15a28462ca312361d261fbf8fe78 | 6510dc50a0d17dc438c2a85d738f558582b6c25361884f3882e207a51f4ed152 |
| 31 | 1 | CN=Entrust Class 1 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 | 4c0e8c1b | RSA 2048-bits | RSA SHA-256 | 2011-11-11 15:25:51 | 2021-11-11 23:27:50 | | | 4790a4a10a4320bfd07454b894fac47bb5b61c05 | 8cb3d21bbb255dbfeafa1a27d1d1f70320dc84564297bce82e29b8f2e461f270 |
| 31 | 2 | CN=Entrust Class 1 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 | 4c0e8c37 | RSA 2048-bits | RSA SHA-1 | 2011-11-11 15:34:41 | 2021-11-12 07:51:23 | | | 4790a4a10a4320bfd07454b894fac47bb5b61c05 | c23a1f8315538a8651816e9932c044eb856c01fd99771690c863671d2c48564 |
| 31 | 3 | CN=Entrust Class 1 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 | 0b67c935a1727c830000000051ce1708 | RSA 2048-bits | RSA SHA-256 | 2017-06-20 20:30:55 | 2028-12-20 21:00:55 | 2022-02-24 00:00:00 | E-mail Protection, TLS Web Client Authentication | 4790a4a10a4320bfd07454b894fac47bb5b61c05 | 357decc5622f89239ffd1c91c1366a0951ba4db5fd384f518cc4ae85d2dae3a5 |
| 32 | 1 | CN=Entrust Class 1 Client CA - SHA256 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust Root Certification Authority - G2 OU=(c) 2009 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | 6e61669872bc9c300000000051d3931e | RSA 2048-bits | RSA SHA-256 | 2019-04-16 15:35:52 | 2030-11-16 16:05:52 | | TLS Web Client Authentication, E-mail Protection | e249b9ec25deb70cdee550185b48cc0c8e15f2a6 | c6e9e993c258b72124aad3c9c068b6ef23576155f310b305733361e20b17c943 |
| 33 | 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 | 4c0e8c1c | RSA 2048-bits | RSA SHA-256 | 2011-11-11 15:26:05 | 2021-11-12 00:18:35 | | | 0991a5bae9f22e2a75dfcd7efe77caf2de6b9b24 | 27524e32bb2177cbbf0a716f78a71242714fc92f0a447130d91666c716a78107 |
| 33 | 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 | 4c0e8c38 | RSA 2048-bits | RSA SHA-1 | 2011-11-11 15:38:34 | 2021-11-12 00:17:34 | | | 0991a5bae9f22e2a75dfcd7efe77caf2de6b9b24 | 8504a0350036b18594b1f47b6a3bd3513e28b045bc7dbfe5b08d8f3049cd3cfe |
| 33 | 3 | CN=Entrust Class 2 Client CA OU=(c) 2010 Entrust, Inc. OU=www.entrust.net/CPS is incorporated by reference O=Entrust, Inc. C=US | CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net | 00bcb4d843035b759f0000000051ce1709 | RSA 2048-bits | RSA SHA-256 | 2017-06-20 20:34:33 | 2028-12-20 21:04:33 | | E-mail Protection, TLS Web Client Authentication | 0991a5bae9f22e2a75dfcd7efe77caf2de6b9b24 | 95ad94e88f5b8604e40e5fff36b0d34b646c1d5ba06c0e735b72aa396735c415 |



| CA # | Cert # | Subject | Issuer | Serial Number | Key Type | Hash Type | Not Before | Not After | Revoked Date | Extended Key Usage | Subject Key Identifier | SHA256 Fingerprint |
|------|--------|---|--|-----------------------------------|---------------|-------------|---------------------|---------------------|---------------------|--|--|--|
| 33 | 4 | 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 | 00af1c04b2ac8c99b0000000051ce18e3 | 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 |
| 34 | 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 | 0088068b45c3fdd464000000051ce1961 | 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 |
| 35 | 1 | CN=Entrust Timestamping CA - TS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net | 51ce0dd8 | RSA 2048-bits | RSA SHA-1 | 2015-07-15 17:42:06 | 2029-06-15 23:05:07 | | Time Stamping | c3c271d27bd76805ae3b399b34250c6203c75768 | 5f84398236b7e58fa365bf1ae5aa3e441c265fdbc50c7471799060a27a2381a |
| 35 | 2 | CN=Entrust Timestamping CA - TS1 OU=(c) 2015 Entrust, Inc. - for authorized use only OU=See www.entrust.net/legal-terms O=Entrust, Inc. C=US | CN=Entrust.net Certification Authority (2048) OU=(c) 1999 Entrust.net Limited OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O=Entrust.net | 58da13ff0000000051ce0df7 | RSA 2048-bits | RSA SHA-256 | 2015-07-22 19:02:54 | 2029-06-22 19:32:54 | | Time Stamping | c3c271d27bd76805ae3b399b34250c6203c75768 | 44dfcd2c573110e74bf4e85903595f660650ed925b7306542c54e87396671f03 |
| 36 | 1 | CN=Entrust Time Stamping CA - TS2 O=Entrust, Inc. C=US | CN=Entrust Code Signing Root Certification Authority - CSBR1 O=Entrust, Inc. C=US | 25bc2bf329ca107f1ea9ba8885d49d3b | RSA 4096-bits | RSA SHA-512 | 2021-05-07 19:22:14 | 2040-12-29 23:59:00 | | Time Stamping | 260ff0c448081bccdd91f55454b6b3b3fc99f108 | 21e81685b352955b9ed48fb969bd2e4f95cfb85ed1260cf6b7fa70a035d0028f |
| 37 | 1 | CN=Entrust Certificate Authority - VMC1 OU=(c) 2018 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 | 00b3d227db33085e17000000051d3931f | RSA 2048-bits | RSA SHA-256 | 2019-04-16 15:45:43 | 2030-11-16 16:15:43 | 2022-02-24 00:00:00 | 1.3.6.1.5.5.7.3.31 | 8bb63976d03490a63f62e164ea3ebcf47c46a173 | 7dbdfc6bd4463d4e22479bda4e4a973f58ac94845db0b86c0f69eb3d719691a |
| 38 | 1 | CN=Entrust Verified Mark CA - VMC2 O=Entrust, Inc. C=US | CN=Entrust Verified Mark Root Certification Authority - VMCR1 O=Entrust, Inc. C=US | 699d8fd758c2c39c1e53d1aa1476d1e6 | RSA 4096-bits | RSA SHA-512 | 2021-05-07 19:23:23 | 2040-12-29 23:59:00 | | 1.3.6.1.5.5.7.3.31 | efbc3cb4af3ad0455e7654dfc76478e92d1d743f | c269504b491dbf451a695b953711adc5cd70975b5fca1e181ebbd2172cb07e0c |



ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

| CPS Name | Version | Date |
|--|---------|-------------|
| Entrust Certificate Services Certification Practice Statement | 3.8 | 31 Dec 2020 |
| Entrust Certificate Services Certification Practice Statement | 3.9 | 19 Jul 2021 |
| Entrust Certificate Services Certification Practice Statement | 3.10 | 18 Feb 2022 |
| ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS) | 1.4 | 18 Dec 2020 |
| ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS) | 1.5 | 7 May 2021 |
| ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS) | 1.5.1 | 15 Nov 2021 |
| ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS) | 1.6 | 30 Nov 2021 |
| ENTRUST DATACARD DEUTSCHLAND GMBH Certification Practice Statement (CPS) | 1.3 | 18 Dec 2020 |



ENTRUST MANAGEMENT'S STATEMENT

Entrust Corporation ("Entrust") operates the Certification Authority (CA) services as enumerated in [Attachment A1](#), and provides SSL CA services.

Entrust Corporation ("Entrust") operates the Certification Authority (CA) services as enumerated in [Attachment A2](#), and provides SSL and non-SSL CA services.

The management of Entrust is responsible for establishing and maintaining effective controls over its SSL and non-SSL CA operations, including its network and certificate system controls, its SSL CA business practices disclosure on its [website](#), SSL key lifecycle management controls, and SSL 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. In Entrust management's opinion, in providing its SSL and non-SSL Certification Authority (CA) services at Ottawa, Ontario, and Toronto, Ontario, throughout the period 1 March 2021 to 28 February 2022, Entrust has:

- disclosed its SSL certificate lifecycle management business practices in its Certification Practice Statements 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5](#).

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

| Bug ID | Summary | Opened | Closed |
|---------|--|------------|------------|
| 1696227 | Entrust – Incorrect Jurisdiction Country Value in an EV Certificate | 2021-03-03 | 2021-07-15 |
| 1712106 | Invalid localityName | 2021-05-20 | 2021-12-13 |
| 1728796 | Incorrect value in Business Category field for Government Entities | 2021-09-02 | 2021-12-13 |
| 1731887 | Test Website Certificates Expired | 2021-09-21 | 2021-10-20 |
| 1737057 | CRLs and OCSP responses not issued as specified in the CPS | 2021-10-21 | 2022-03-08 |
| 1744827 | SSL Certificates issued with Unverified IP Addresses | 2021-12-07 | 2022-01-14 |
| 1748634 | Late Revocation for SSL Certificates issued with Unverified IP Addresses | 2022-01-05 | 2022-03-08 |

Bruce Morton
Director, Entrust Certificate Services
10 May 2022



ATTACHMENT A1

LIST OF IN SCOPE CAs for SSL BASELINE REQUIREMENTS

| |
|---|
| Root CAs |
| <ol style="list-style-type: none">1. Entrust.net Certification Authority (2048)2. Entrust Root Certification Authority3. Entrust Root Certification Authority – G24. Entrust Root Certification Authority – G45. Entrust Root Certification Authority – EC16. Entrust Root Certification Authority – EC2 |
| OV SSL Issuing CAs |
| <ol style="list-style-type: none">13. Entrust Certification Authority – L1C14. Entrust Certification Authority – L1F15. Entrust Certification Authority – L1K16. CRYPTAS OV Issuing CA17. Siemens Issuing CA Internet Server 2020 |
| EV SSL Issuing CAs |
| <ol style="list-style-type: none">18. Entrust Certification Authority – L1E19. Entrust Certification Authority – L1J20. Entrust Certification Authority – L1M21. Entrust Certification Authority – L1N22. CRYPTAS OV Issuing CA |
| Qualified Certificate EV SSL Issuing CAs |
| <ol style="list-style-type: none">23. Entrust Certification Authority - QTSP124. Entrust Certification Authority - DE QWAC125. Entrust Certification Authority - ES QWAC2 |



ATTACHMENT A2

LIST OF IN SCOPE CAs for NETWORK SECURITY REQUIREMENTS

| |
|---|
| Root CAs |
| <ol style="list-style-type: none"> 1. Entrust.net Certification Authority (2048) 2. Entrust Root Certification Authority 3. Entrust Root Certification Authority – G2 4. Entrust Root Certification Authority – G4 5. Entrust Root Certification Authority – EC1 6. Entrust Root Certification Authority – EC2 7. Entrust Code Signing Root Certification Authority - CSBR1 8. Entrust Digital Signing Root Certification Authority - DSR1 9. Entrust Verified Mark Root Certification Authority - VMCR1 |
| Intermediate CAs |
| <ol style="list-style-type: none"> 10. Entrust Certification Authority - AATL1 11. Entrust Enterprise Intermediate CA - ICA1 12. Siemens Intermediate CA 2021 |
| OV SSL Issuing CAs |
| <ol style="list-style-type: none"> 13. Entrust Certification Authority – L1C 14. Entrust Certification Authority – L1F 15. Entrust Certification Authority – L1K 16. CRYPTAS OV Issuing CA 17. Siemens Issuing CA Internet Server 2020 |
| EV SSL Issuing CAs |
| <ol style="list-style-type: none"> 18. Entrust Certification Authority – L1E 19. Entrust Certification Authority – L1J 20. Entrust Certification Authority – L1M 21. Entrust Certification Authority – L1N 22. CRYPTAS OV Issuing CA |
| Qualified Certificate EV SSL Issuing CAs |
| <ol style="list-style-type: none"> 23. Entrust Certification Authority - QTSP1 24. Entrust Certification Authority - DE QWAC1 25. Entrust Certification Authority - ES QWAC2 |
| Code Signing Issuing CAs |
| <ol style="list-style-type: none"> 26. Entrust Code Signing Certification Authority – L1D 27. Entrust Code Signing CA - OVCS1 28. Entrust Code Signing CA - OVCS2 |
| EV Code Signing Issuing CAs |
| <ol style="list-style-type: none"> 29. Entrust Extended Validation Code Signing CA – EVCS1 30. Entrust Extended Validation Code Signing CA – EVCS2 |
| Secure Email (S/MIME) CAs |
| <ol style="list-style-type: none"> 31. Entrust Class 1 Client CA 32. Entrust Class 1 Client CA - SHA256 33. Entrust Class 2 Client CA 34. Entrust Class 2 Client CA - C2CA2 |
| Timestamp CAs |
| <ol style="list-style-type: none"> 35. Entrust Timestamping CA – TS1 36. Entrust Time Stamping CA – TS2 |
| Verified Mark Certificate CAs |
| <ol style="list-style-type: none"> 37. Entrust Certificate Authority - VMC1 38. Entrust Verified Mark CA - VMC2 |



ATTACHMENT B

LIST OF ENTRUST CERTIFICATION PRACTICE STATEMENTS

| CPS Name | Version | Date |
|--|---------|-------------|
| Entrust Certificate Services Certification Practice Statement | 3.8 | 31 Dec 2020 |
| Entrust Certificate Services Certification Practice Statement | 3.9 | 19 Jul 2021 |
| Entrust Certificate Services Certification Practice Statement | 3.10 | 18 Feb 2022 |
| ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS) | 1.4 | 18 Dec 2020 |
| ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS) | 1.5 | 7 May 2021 |
| ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS) | 1.5.1 | 15 Nov 2021 |
| ENTRUST DATACARD EUROPE S.L. Certification Practice Statement (CPS) | 1.6 | 30 Nov 2021 |
| ENTRUST DATACARD DEUTSCHLAND GMBH Certification Practice Statement (CPS) | 1.3 | 18 Dec 2020 |