ENTRUST CERTIFICATE SERVICES

Registration Practice Statement

Version: 1.01
October 25, 2024

Revision History

Issue	Date	Changes in this Revision
1.0	September 27, 2024	Initial version.
1.01	October 25, 2024	Update based on Deloitte audit review and other minor changes

TABLE OF CONTENTS

1. Introduction

Entrust is a Registration Authority (RA) responsible for the identity verification prior to the issuance of TLS Certificates (Certificates) and lifecycle management for Certificates issued under SSL.com's CP/CPS (CP/CPS). The CP/CPS is located at https://legal.ssl.com/documents/SSLcom-CP-CPS.pdf.

Entrust operates the RA on behalf of SSL.com and is responsible for ensuring compliance with this RPS and the associated CP/CPS.

1.1 Overview

The requirements in this Registration Practice Statement (RPS) are a subset of the requirements specified in the CP/CPS. Section numbers not included in this RPS are omitted and should be interpreted as no stipulation. If any potential conflict is identified between the provisions of this RPS and the provisions of the CP/CPS, the Entrust and SSL.com Policy Management Authorities (PMAs) will amend the RPS to eliminate any such conflict in accordance with Sections 1.5 and 9.12 below.

With the exception of omitted sections, the format of this RPS is consistent with IETF RFC 3647.

This RPS conforms to the current version of requirements adopted by the CA Browser Forum Baseline Requirements and EV Guidelines.

1.2 Identification Number and Document Name

This document is the Entrust Registration Practice Statement (RPS) and has been approved by the Entrust PMA and the SSL.com PMA.

1.3 PKI participants

1.3.1 Certification authorities

The Certification Authority (CA) issues publicly trusted digital Certificates in accordance with its CPS and performs functions associated with Public Key Infrastructure (PKI) operations, including receiving Certificate requests, issuing, revoking and renewing a Certificate, and maintaining, issuing, and publishing Certificate Revocation Lists (CRLs).

Within the SSL.com PKI hierarchy, SSL.com functions as both the Root CA and Issuing CA.

Note: Within this RPS, the terms "SSL.com" and "CA" are used interchangeably.

1.3.2 Registration authorities

The RA identifies, authenticates, and manages a Certificate Subscriber's Certificate request information. Registration operations are performed by the RA in alignment with relevant sections of CA CP/CPS, and utilize trusted trained personnel and trustworthy systems to provide the necessary assurance.

Entrust functions as an RA in the SSL.com PKI hierarchy.

Note: Within this RPS, the terms "Entrust" and "RA" are used interchangeably.

1.3.3 Certificate Subscribers

A Certificate Subscriber is a natural person or Legal Entity to whom a Certificate is issued and who is legally bound by the TLS Subscriber Agreement posted in the Entrust repository at www.entrust.net/cps ("Subscriber Agreement").

Before identity validation and Certificate issuance, a requesting Certificate Subscriber is defined as an Applicant. Once the Certificate is issued, the Applicant is referred to as a Certificate Subscriber.

1.3.4 Relying parties

A Relying Party is any entity performing transactions, communications or functions which rely on a Certificate facilitated by the RA and issued by the CA.

1.4 Certificate usage

1.4.1 Appropriate Certificate uses

The CA issues TLS Certificates to Certificate Subscribers as designated by the key usage or extended key usage fields defined in the Certificate profile for that product.

1.4.2 Prohibited Certificate uses

Certificates may not be used for any purpose other than those defined in the Certificate profile of the respective product.

1.5 Policy administration

1.5.1 Organization administering the document

The Entrust PMA is responsible for administering this RPS.

1.5.2 Contact information

The Entrust PMA may be reached at:

Entrust Limited
2500 Solandt Road, Suite 100
Ottawa, Ontario
Canada K2K 3G5
Attn: Entrust Certificate Services

Tel: 1-866-267-9297 or 1-613-270-2680
Email: ecs.support@entrust.com

Certificate Problem Reports, such as Certificate misuse, vulnerability reports or external reports of key compromise, must be submitted to https://www.ssl.com/revoke.

1.5.3 Person determining RPS suitability for the policy

The Entrust PMA and the SSL.com PMA are jointly responsible for determining the suitability and applicability of this RPS.

1.5.4 RPS approval procedures

The Entrust PMA and the SSL.com PMA approve this RPS and any material amendments, in accordance with RPS Section 9.12.

1.6 Definitions and acronyms

Capitalized terms and acronyms not otherwise defined in this RPS have the meanings given to them in Section 1.6 of the CP/CPS.

2. Publication and Repository Responsibilities

2.1 Repositories

The following terms and practices referenced in this document are published at the locations listed below:

Document Location	
Registration Practice Statement (RPS)	https://www.entrust.net/CPS
Certificate Policy/ Certification Practice Statement (CP/CPS)	https://www.ssl.com/repository
List of Approved Incorporating and Registration Agencies	https://www.ssl.com/repository
Subscriber Agreements	https://www.entrust.net/CPS
Personal Data Protection Policy	https://www.entrust.com/legal-compliance/data-privacy
Product Privacy Notice	https://www.entrust.com/legal-compliance/data-privacy
Web Privacy Statement	https://www.entrust.com/sites/default/files/documentation/licensingandagreements/web-privacy-statement.pdf

The RA ensures that its repository of legal documents is available at https://www.entrust.net/CPS (the "RA Repository") 24 hours a day, 7 days a week, 365 days a year with at least 99% availability.

The CA's repository provisions are specified in Section 2.1 of the CP/CPS.

2.2 Access controls on repositories

The RA Repository is publicly available on the Internet with read-only access. Only authorized RA personnel have the right to modify files in this RA Repository. Further, the RA applies restrictions and access-control to this RA Repository to protect against enumeration and denial of service (DoS) attacks.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

All Certificates in scope of this RPS adhere to rules for naming and identification and require a Distinguished Name (DN) that complies with ITU X.500 standard for Distinguished Names.

3.1.2 Need for Names to be Meaningful

The RA and CA jointly prepare the End Entity Naming Forms that contain non-null Subject and Issue Distinguished Names (DNs) for all Subscriber Certificates. SSL.com and Entrust review and approve all End Entity Naming Forms. The RA configures its Certificate Applications (Applications) to ensure non-null Subject DNs for all Certificates based on these End Entity Naming Forms

3.1.3 Anonymity or Pseudonymity of Subscribers

Pseudonyms in the Subject DNs are not supported.

3.1.4 Rules for Interpreting Various Name Forms

The Certificates are issued with Distinguished Names interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of Names

As stipulated in the CPS.

3.2 Initial Identity Validation

All Certificate requests received by the RA are verified at the level of assurance appropriate to the Certificate requested. SSL.com issues TLS Certificates with varying and appropriate levels of verification including "Extended Validation" (EV).

The RA inspects any document relied upon for verification for alteration or falsification. Additionally, the RA verifies the identity and status of any Applicant as appropriate and required for the Certificate requested. Alteration or falsification of any document used in this process, and/or falsification or misrepresentation of the identity or status of any Applicant and/or organization referenced in this process, constitutes grounds for disapproval of a Certificate request and/or immediate revocation of any existing Certificate relying upon altered or falsified documents or false or misrepresented identity or status.

All information provided by the Applicant is verified using Reliable Data Sources, as well as Qualified Independent or Government Information Sources (QIIS/QGIS), according to the Certificate's validation level and applicable requirements, before being included in the Certificate.

For EV Certificates, the RA takes all verification steps necessary to satisfy the EV Verification Requirements set forth in the EV Guidelines.

3.2.1 Method to Prove Possession of Private Key

A valid Certificate request establishes possession of the Private Key related to the request.

An Applicant for any Certificate must submit a signed Certificate Signing Request (CSR). This establishes that the Applicant holds the Private Key corresponding to the Public Key to be included in the requested Certificate.

3.2.2 Authentication of Organization Identity

Requests for Certificates which include an organizational identity are verified using the criteria in the Baseline Requirements or the EV Guidelines. Items to be verified may include the legal existence, legal

name, assumed name, legal form, jurisdiction of incorporation or registration of the legal entity, incorporation/registration number, the type of the legal entity, requested address of the legal entity, and the authority of the requesting party, as applicable to the level of verification requested for the Certificate.

The RA inspects any document relied upon for these purposes for alteration or falsification.

If the Applicant requests a TLS Certificate that will contain Subject Identity Information comprised only of the countryName field, then the RA will verify the country associated with the Subject using a verification process meeting the requirements of Section 3.2.2.3 of SSL.com's CP/CPS. If the Applicant requests a TLS Certificate that will contain the countryName field and other Subject Identity Information, then the RA will verify the identity of the Applicant, and the authenticity of the Applicant Representative's Certificate request using a verification process meeting the requirements of Section 3.2.2.1 of SSL.com's CP/CPS.

For OV Certificates, the RA may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement or a government issued tax document.

For EV Certificates, the RA will verify the organization identity in any request for an EV Certificate and follow the EV verification procedures described in the EV Guidelines. In particular, before issuing an EV Certificate, the RA will ensure that all Subject organization information to be included in the EV Certificate conforms to the requirements of, and is verified in accordance with, EV Guidelines and matches the information confirmed and documented by the RA pursuant to its verification processes. Extended validation processes will verify the following:

1. The Applicant's existence and identity, including;
    a. The Applicant's legal existence and identity, as per Section 3.2.2.2 of the EV Guidelines,
    b. The Applicant's physical existence (business presence at a physical address), as per Section 3.2.2.4 of the EV Guidelines,
    c. The Applicant's operational existence (business activity), as per Section 3.2.2.6 of the EV Guidelines, and
    d. The Applicant's assumed name, as per Section 3.2.2.3 of the EV Guidelines (if applicable).
2. A Verified Method of Communication with the entity to be named as the Subject in the Certificate, as per Section 3.2.2.5 of the EV Guidelines;
3. The Applicant's authorization for the EV Certificate, including;
    a. The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester, as per Section 3.2.2.8 of the EV Guidelines,
    b. That a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use, as per Section 3.2.2.9 of the EV Guidelines; and
    c. That a Certificate Approver has signed or otherwise approved the EV Certificate Request, as per Section 3.2.2.10 of the EV Guidelines.

When performing the above, the RA may take additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement. Whenever the use of documentation obtained by an Incorporating Agency or Registration Agency is required in this process, the RA will only use agencies included in SSL.com's approved, at time of issuance, List of Approved Incorporating and Registration Agencies. This list is publicly available at https://www.ssl.com/repository.

3.2.3 Authentication of Individual Identity

The RA performs verification of the identity and authority of the Contract Signer, the Certificate Approver, and the Certificate Requestor associated with Certificate applications that are submitted by an Applicant or Subscriber. In order to establish the accuracy of an individual identity, the RA performs identity and authority verification consistent with the requirements set forth in the EV Guidelines.

3.2.4 Non-verified Subscriber Information

The RA verifies all required information before approving Applications in the production environment.

3.3 Identification and Authentication for Re-key Requests

Re-keying (sometimes called reissuing) refers to the issuance of an entirely new Certificate, using some or all of the information submitted for an existing Certificate and using a newly generated Private Key.

Subscribers may request re-keying of a Certificate prior to the Certificate's expiration.

3.3.1 Identification and Authentication for Routine Re-key

A Subscriber may request re-key of any unexpired Certificate. Any information to be included in the re-keyed Certificate must be validated or may be re-used if permitted under the CP/CPS Section 4.2.1.

3.4 Identification and Authentication for Revocation Requests

Certificate Subscribers may request revocation of their Certificates by authenticating to the RA service, selecting the revocation option, and providing a revocation reason. The RA sends the revocation request to the CA, receives confirmation of the Certificate revocation and notifies the Certificate Subscriber.

The RA may request revocation of Subscriber's Certificates, by authenticating an internal Entrust service, selecting the Certificates to revoke, and providing a revocation reason. The RA sends the revocation request to the CA, receives confirmation of the Certificate revocation and notifies the Certificate Subscriber.

Any other entity (e.g., Relying Parties, Application Software Suppliers, non-Certificate-Subscribers) seeking to revoke a Certificate may submit a Certificate Problem Report as defined in RPS Section 4.9.3.3.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Either the Applicant or an authorized Certificate Requester may submit Certificate requests. Applicants are responsible for the accuracy of any data submitted.

In all cases, the RA shall require identification and authentication sufficient to meet the requirements relevant to the type of Certificate requested.

4.1.2 Enrollment Process and Responsibilities

The RA verifies the identity of Certificate Subscribers in accordance with RPS Section 3.2.2. Certificate Subscribers also electronically accept the Subscriber Agreement which includes terms, conditions, and warranties for their Certificates.

The RA captures and retains the required evidence for the above in accordance with RPS Sections 5.4 and 5.5.

A valid Certificate Signing Request (CSR) must be created and submitted by the Applicant. A valid CSR will be derived from a Key Pair generated by the Applicant or the Applicant's agent. A valid CSR will incorporate the generated Public Key and other such information as required to create the requested Certificate.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

After receiving a Certificate application, Entrust verifies the application information and other information in accordance with Section 3.2. Entrust creates and maintains records to establish that it has performed its required verification tasks and communicates the completion of such performance to SSL.com. SSL.com performs the domain validation, as per Section 4.2.1 of the CP/CPS, which may occur at any time prior to Certificate issuance.

The RA may use the documents and data provided in Section 3.2 to verify Certificate information, or may reuse previous validations themselves, provided that the RA obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 1) 825 days prior to requesting issuance of an OV Certificate or 2) 398 days prior to requesting issuance of an EV Certificate.

4.2.2 Approval or Rejection of Certificate Applications

The RA will reject any Certificate request which cannot be verified.

The RA will reject Certificate requests containing Internal Names or Reserved IP Addresses, as such names cannot be validated according to Section 3.2.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

An applicant will submit Identity information evidence as required for the Certificate type and CSR to Entrust via established submission methods through the Entrust Certificate lifecycle management portal or API.

The RA performs validation of all Identity information sent before issuing any certificate, in accordance with this RPS, which fulfills the requirements of the SSL.com CP/CPS.

SSL.com shall perform Domain Validation of all TLS Certificates requested by Entrust, except for any domains previously validated by SSL.com within the acceptable validation re-use period as described in §4.2.1 of the SSL.com CP/CPS.

The CA issues Certificates based on the above CSRs and notifies the Entrust service via the API.

4.3.2 Notification of Certificate Issuance by the CA to Other Entities

Entrust shall notify the Subscriber of the successful issuance of a Certificate, upon receiving issuance confirmation via the API. Notification will be via established methods used between Entrust and Subscribers, by email or through its Certificate lifecycle management portal.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The RA service displays the information to be put in the Certificate before issuance for the Applicant to review. The Applicant's acceptance is required to issue the Certificate.

The Certificate Subscriber or Certificate Subscriber's agent is responsible for review and verification of information contained in the issued Certificate. The Certificate Subscriber or agent is deemed to have accepted the issued Certificate by taking delivery of the Certificate, in accordance with the provisions of SSL.com's CP/CPS Section 4.4.1.

4.4.2 Publication of the Certificate by the CA

Any Certificate issued by SSL.com shall be published to Entrust via API, or other approved means. Entrust, in turn, shall make the Certificate available to the Subscriber via established means.

4.5 Key pair and Certificate usage

4.5.1 Certificate Subscriber Private Key and Certificate Usage

Subscribers using TLS Certificates issued through the SSL.com PKI are required to protect the Private Key for that Certificate, including:

- Securing the Private Key (and any copies made) to prevent disclosure or compromise
- Using the Private Key and/or Certificate only as authorized by the relevant Subscriber Agreement
- Ceasing use of the Private Key after suffering a Key Compromise
- Using the Certificate only as applicable and for the intended purpose (per the key usage field of that Certificate)

If Entrust becomes aware that a Certificate Subscriber does not protect their private keys or misuses their Certificate, Entrust will notify SSL.com so it may revoke the Certificate in accordance with the CP/CPS Section 4.9.

4.6 Certificate Renewal

Unless otherwise specifically prohibited in this RPS or in the CP/CPS, any Certificate issued utilizing the SSL.com PKI may be renewed if the Certificate meets the following criteria:

- The original Certificate has not been revoked or otherwise flagged
- The Public Key from the original Certificate has not been blocklisted
- The Private Key corresponding to the original Certificate has not suffered a Key Compromise
- All information within the Certificate, other than the notAfter field, remains accurate
- The renewed Certificate's cryptographic security is deemed to remain sufficient for the Certificate's intended lifetime
- The information provided in the request still passes the appropriate validation checks
- No further or additional validation is required beyond repeating the same steps performed originally

Certificates which have either been previously renewed or previously re-keyed may be renewed again so long as the criteria above are met. The original Certificate may be revoked after renewal is complete.

The RA supports 90, 60, 30, 10-1 day renewal notices, which can be modified by the Subscribers.

4.7 Certificate Re-key

For the purposes of this RPS, "Certificate re-keying" means the re-issuance of a Certificate which utilizes a new Key Pair.

Other information used in the original Certificate may or may not be changed when a Certificate is re-keyed.

In all cases where re-keying is requested and/or performed a new Certificate Signing Request (CSR) must be submitted (per Section 4.1.2) to obtain the new Public Key required.

4.7.1 Circumstances for Certificate Re-key

Any Certificate issued utilizing the SSL.com PKI may be re-keyed, unless otherwise specifically prohibited in the SSL.com PKI CP/CPS.

4.7.1.1 Certificate Subscriber private key and Certificate usage

An original Certificate or previously issued Certificate may need to be revoked as a condition of re-keying or the original Certificate may be revoked after re-keying is complete. Whether the revocation needs to happen before or after re-keying is at the discretion of the RA or CA.

4.7.1.2 Loss, theft or compromise

Any Subscriber, agent or authorized entity whose Private Key has been stolen, lost or otherwise compromised SHOULD immediately request re-keying of that Certificate.

The Subscriber SHOULD also request revocation of the Certificate that is associated with the lost, stolen or compromised Private Key.

The RA is not responsible for loss, damages or injury resulting from any compromise of a Private Key.

4.8 Certificate Modification

For the purposes of this RPS, "Certificate modification" means the issuance of a new Certificate in which non-essential information has changed, without changing the Key Pair related to the original Certificate.

The RA does not support the modification of Certificates. If modification is required, subscribers instead must reapply to receive a new Certificate.

4.9 Certificate Revocation and Suspension

Certificates may be revoked for numerous reasons (e.g., Private Key compromised, change in identity information, etc.). The revocation process changes the status of Certificates from "Valid" to "Revoked." Further, this process adds the Certificates to the CRLs based on the status changes. The "Revoked" status remains valid until the expiration of the Certificates. After expiration, this process removes the Certificates from the CRLs.

"Suspended" status is not supported for Certificates.

4.9.1 Circumstances for Revocation

The RA will support the CA in meeting the requirement in CP/CPS Section 4.9.1.1 to revoke a Certificate within 24 hours, based on one or more of the following criteria:

1. The Certificate Subscriber requests in writing to the RA (or CA) to revoke the Certificate for:
    - keyCompromise (RFC 5280 CRLReason #1) (i.e., Certificate Subscriber's Private Key is suspected of compromise)
    - cessationOfOperation (RFC 5280 CRLReason #5) (i.e., Certificate Subscriber will no longer be using the Certificate)
    - affiliationChanged (RFC 5280 CRLReason #3) (i.e., Certificate Subscriber's identifying information in the Certificate has changed)
    - superseded (RFC 5280 CRLReason #4) (i.e., Certificate Subscriber requests a new Certificate to replace an existing Certificate)

2. The Certificate Subscriber notifies the RA (or CA) that the original Certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn)
3. The RA (or CA) obtains evidence that the Certificate Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise)
4. The RA (or CA) is made aware of a demonstrated or proven method that can easily compute the Certificate Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise)
5. The RA (or CA) obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

The RA will support the CA in meeting the requirement in CP/CPS Section 4.9.1.1 to revoke a Certificate within 24 hours and must revoke within 5 days based on one or more of the following criteria:

1. The Certificate no longer complies with requirements in CPS Sections 6.1.5 and 6.1.6 (CRLReason #4, superseded)
2. The RA (or CA) obtains evidence the Certificate was misused (CRLReason #9, privilegeWithdrawn)
3. The RA (or CA) is made aware that a Certificate Subscriber has violated one or more of its material obligations under the Entrust Terms of Use (CRLReason #9, privilegeWithdrawn)
4. The RA (or CA) is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);
5. The RA (or CA) is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
6. The RA (or CA) is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn)
7. The RA (or CA) is made aware that the Certificate was not issued in accordance with the RPS or CP/CPS (CRLReason #4, superseded)
8. The RA (or CA) determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn)
9. The CA's right to issue Certificates is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL Repository or OCSP Responder (CRLReason #5, cessationOfOperation)
10. Revocation is required by this RPS or the CP/CPS for a reason that is not otherwise required as specified by section 4.9.1.1 of the Baseline Requirements (CRLReason #4, superseded)
11. The RA (or CA) is made aware of a demonstrated or proven method that exposes the Certificate Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise)
12. The RA (or CA) receives a lawful and binding ruling from a Government or regulatory body to revoke the Certificate (CRLReason #9, privilegeWithdrawn)

4.9.2 Who Can Request Revocation

Certificate Subscribers or the RA may request revocation of a Certificate as defined in RPS Section 4.9.3.1. Any other entity may submit a Certificate Problem Report as defined in RPS Section 4.9.3.3.

4.9.3 Procedure for Revocation Request

4.9.3.1 Certificate Subscriber Revocation Request

Certificate Subscribers who need to revoke their Certificate, authenticate to the Entrust service, select the Revocation Reason based on RFC 5280, and submit the Revocation Request to the Entrust service as defined in RPS Section 3.4. Entrust service uses the CA's revocation API to submit the Revocation Request to the CA.

Once the CA verifies the authenticity of the request, the CA revokes the Certificate in the CA software and the Certificate status is changed to "Revoked". The revoked Certificate is included in the CRLs in accordance with the CP/CPS.

4.9.3.2 RA Revocation Request

The RA may request revocation of a Subscriber Certificate for reasons specified in Section 4.9.1.1.

Authorized RA personnel who need to revoke a Subscriber's Certificate, authenticate to the Entrust service with multi factors as defined in RPS Section 3.2.3, select the Certificate to be revoked, select the Revocation Reason based on RFC 5280, and submit the Revocation Request to the Entrust service. Entrust service uses the CA's revocation API to submit the Revocation Request to the CA.

Once the CA verifies the authenticity of the request, the CA revokes the Certificate in the CA software and the Certificate status is changed to "Revoked". The CA includes the revoked Certificate serial number in the CRLs in accordance with the CP/CPS.

4.9.3.3 Certificate Problem Report

Any other entity (e.g., Relying Parties, Application Software Suppliers, non-Certificate-Subscribers) seeking to request revocation of a Certificate must follow the instructions for submitting a Certificate Problem Report at https://www.ssl.com/revoke. Certificate Problem Reports (CPR) should be filed to report:

- Suspected Private Key compromise
- Certificate misuse
- Other types of fraud, compromise, misuse, or inappropriate conduct; or
- Any other matters related to the Certificate

The CA investigates the CPR in collaboration with the RA and revokes the Certificate if the Report meets any of the criteria defined in RPS Section 4.9.1 or CP/CPS Section 4.9.1.

4.9.3.4 Revocation Request by Application Software Providers

An Application Software Supplier may request revocation of a Certificate if it believes that a Certificate attribute is deceptive, or that the Certificate is being used for an illicit purpose.

If the request is submitted to the RA, the RA forwards it to the CA without undue delay, who processes it according to CPS section 4.9.3.4.

4.9.4 Revocation Request Grace Period

As Specified in the SSL.com CP/CPS.

4.9.5 Time within Which CA Must Process the Revocation Request

4.9.5.1 Revocation Request

The RA processes Revocation Requests in accordance with RPS Section 4.9.1. For clarity, nothing in this section extends the times within which Certificates must be revoked as stated in s. 4.9.1.

4.9.5.1 Certificate Problem Report

Certificate Problem Reports are handled by the CA in accordance with SSL.com's CP/CPS Section 4.9.5. Per notification by the CA, the RA delivers the preliminary report to the Certificate Subscriber within the required timeframe.

Based on the findings, the CA works with the Certificate Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether the Certificate will be revoked, and if so, a date upon which the CA will revoke the Certificate.

The period from receipt of the Certificate Problem Report or revocation-related notice to the published revocation does not exceed the time frames set forth in RPS Section 4.9.1. The CA determines whether revocation or other appropriate action is warranted and sets a revocation date based on at least the following criteria:

- The nature of the alleged problem (scope, context, severity, magnitude, risk of harm)
- The consequences of revocation (direct and collateral impacts to Certificate Subscribers and Relying Parties)
- The number of Certificate Problem Reports received about a particular Certificate or Certificate Subscriber
- The entity making the complaint
- Relevant legislation.

4.9.6 Revocation Checking Requirement for Relying Parties

As Specified in the SSL.com CP/CPS Section 4.9.6.

4.9.7 CRL Issuance Frequency

As Specified in the SSL.com CP/CPS Section 4.9.7.

4.9.8 Maximum Latency for CRLs

As Specified in the SSL.com CP/CPS Section 4.9.8.

4.9.9 On-line Revocation/Status Checking Availability

As Specified in the SSL.com CP/CPS Section 4.9.9.

4.9.10 On-line Revocation Checking Requirements

As Specified in the SSL.com CP/CPS Section 4.9.10.

4.9.11 Other Forms of revocation Advertisements Available

As Specified in the SSL.com CP/CPS Section 4.9.11.

4.9.12 Special Requirements Re Key Compromise

As Specified in the SSL.com CP/CPS Section 4.9.12.

4.9.13 Circumstances for Suspension

The SSL.com PKI does not support Certificate suspension as specified in the SSL.com CP/CPS Section 4.9.13.

4.9.14 Who Can Request Suspension

No entity is permitted to request suspension of any Certificate issued utilizing the SSL.com PKI as specified in the SSL.com CP/CPS Section 4.9.14.

4.9.15 Procedure for Suspension Request

Certificate suspension is not provided as specified in the SSL.com CP/CPS Section 4.9.15.

4.9.16 Limits on Suspension Period

As Specified in the SSL.com CP/CPS Section 4.9.16.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status information is available via CRL and OCSP responder as specified in the CP/CPS.

4.11 End of Subscription

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy Practices

No Stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

5.1 Physical Security Controls

The RA implements and maintains physical security controls to restrict access to the hardware and software used for the Entrust service.

5.1.1 Site Location and Construction

The RA operates the Entrust service from a secure commercial datacenter. All critical facilities are housed in secure areas with appropriate security barriers and entry controls. These are protected from unauthorized access, damage and/or interference.

5.1.2 Physical Access

The facility containing the RA equipment is designated a two (2) person zone through physical cards. It has 24-hour video surveillance and full-time security presence which monitors and logs all access.

Controls are used to prevent a person from being in the room alone. Alarm systems are used to notify security personnel of any violation of the rules for access to the RA equipment.

Unauthorized personnel needing to enter the physical location of a secure datacenter or the area where RA functions are performed shall never be left without oversight by an authorized person.

5.1.3 Power and Air Conditioning

RA equipment is maintained in a facility which utilizes uninterrupted power supply (UPS) units and automatic backup generators to ensure multiple redundant power sources.

HVAC systems for heating, cooling and ventilation are sufficient to support the operation of the RA system.

5.1.4 Water Exposures

The RA equipment is maintained in a facility which provides protection against water exposures.

5.1.5 Fire Prevention and Protection

The RA equipment is maintained in a facility which is fully wired for fire detection, alarm and suppression. Routine, frequent inspections of all systems are made to assure adequate operation.

5.1.6 Media Storage

Any media used by the RA is securely handled and stored to protect it from damage, theft and unauthorized access.

5.1.7 Waste Disposal

Paper documents or any other printed material containing RA information or related confidential information are securely disposed of by shredding or destruction by an approved service. Removable media containing RA information or related confidential information are securely disposed of by complete destruction of the media, or by the use of an approved utility to wipe or overwrite removable media.

5.1.8 Off-site Backup

An off-site location is used for the storage and retention of RA backup software and data. The off-site storage facility is available to authorized personnel 24 hours per day 7 days per week for the purpose of retrieving software and data. The offsite storage facility has appropriate levels of physical security in place and is protected against fire and unauthorized access.

5.2 Procedural Controls

5.2.1 Trusted Roles

RA functions are performed by individuals working within clearly defined trusted roles. The RA has established the following trusted roles to share responsibility; limit the ability for action by individual participants; and securely separate duties and functions:

- **Verification Specialist:** Responsible for researching, gathering and verifying the accuracy and authenticity of data to be included within Certificates, along with the information collected for new subscriber registrations, Certificate applications, account modifications and renewals through Reliable Data Sources, Qualified Independent Information Sources (QIIS) and Government Information sources.
- **Verification Audit Specialist:** Reviews and approves (or rejects) the documentation submitted by Verification Specialists adhering to this RPS and the supporting Entrust policies and procedures. Will fail any requests that do not meet compliance.
- **Support:** Sends Certificate revocation requests to the CA.
- **System Administrator:** Operates cloud infrastructure for the Entrust service.
- **Network Administrator:** Manages the network for production and pre-production environments.
- **Software Engineer:** Receives temporary access to the production environment for Entrust service to perform specific tasks.
- **Security Officer:** Assists with implementing and maintaining security safeguards for RA operations. Performing key control and oversight activities to monitor compliance with policies, processes, and procedures. Ensuring compliance of pre-authorization conditions required for physical and logical access. Reviewing and revising policies, processes, procedures, and control documents as required. Performing custodial activities for passwords, keys, and other security items. Reporting suspected security violations and breaches.

5.2.2 Number of Persons Required per Task

Systems used to process and approve EV Certificate requests require actions by at least two persons in trusted roles before issuing an EV Certificate.

5.2.3 Identification and Authentication for Each Role

The RA assigns individuals to trusted roles. Individuals acknowledge the roles and responsibilities of their trusted roles and must authenticate to the Entrust system to perform their job functions.

5.2.4 Roles Requiring Separation of Duties

Any trusted role as defined in 5.2.1 intrinsically possesses duties and/or capabilities separate from those in other trusted roles.

As described in 5.2.2, validation of an EV Certificate request requires the participation of both the Verification Specialist and the Verification Audit Specialist

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

The RA verifies the identity and trustworthiness of all employees and contractors as part of the standard onboarding process.

5.3.2 Background Check Procedures

The RA conducts background checks on all employees and contractors as part of the standard on- boarding process. These background checks verify the employees' and contractors' government-issued identity documents, criminal records, work experiences, and education levels.

5.3.3 Training Requirements

The RA gives comprehensive training to individuals assigned to trusted roles to ensure understanding of roles and responsibilities, job functions, security awareness, applicable policies and procedures that includes PII data access and secure handling.

In particular, the RA provides comprehensive training to all Identity Verification Agents that covers the following topics:

- Entrust's identity verification procedures which are based on the requirements in this RPS, Baseline Requirements and the EV Guidelines.
- Common security threats including phishing and other social engineering tactics.
- Potential threats to the identity verification process including remote sessions between Identity Verification Agents and Certificate Subscribers based on publicly-known attacks and specific security events at Entrust.

5.3.4 Retraining Frequency and Requirements

The RA ensures individuals assigned to trusted roles maintain the required skill levels to perform their job functions and successfully pass security awareness training annually.

5.3.5 Job Rotation Frequency and Sequence

The RA minimizes any negative impact to the Entrust service, operations, and security when there are changes to individuals assigned to trusted roles.

5.3.6 Sanctions for Unauthorized Actions

The RA enforces administrative or disciplinary actions, including termination and criminal sanctions, to all employees and contractors that fail to comply with this RPS whether through negligence or malicious intent.

The RA immediately removes an individual assigned to a trusted role after identifying any unauthorized action. The RA reviews details of the unauthorized action and issues a report with the recommended administrative or disciplinary action. The RA may also require the individual to take additional training

5.3.7 Independent Contractor Requirements

Contractors fulfilling trusted roles are subject to all requirements specified in this RPS.

5.3.8 Documentation Supplied to Personnel

The RA provides individuals in trusted roles with documentation for performing their job functions that is periodically updated to accurately reflect the Entrust service, operations, and security measures.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The RA automatically records all security events in audit logs from the Entrust service. This includes at least the following events:

1. creation of accounts;
2. installation of new software or software updates;
3. date and time and other descriptive information concerning backups;
4. date and time of all hardware changes;
5. date and time of audit log dumps;
6. closing and (re)start of systems.

The audit logs record the following information for all entries:

7. Event description
8. Event date and time
9. Identity of individual or system making entry

Further, the RA retains all security audit logs per Sections 5.4.3 and 5.5 to support investigations in case of suspected or verified incidents per Section 5.7.1. Security audit logs are also made available to the Qualified Auditors as requested.

5.4.2 Frequency of Processing Log

The RA automatically generates audit logs from the software applications and infrastructure systems of the Entrust service which processes Certificate lifecycle management events. Audit logs are automatically loaded in a security information and event management (SIEM) system at least daily. The SIEM processes and analyzes the security events in the audit logs. If necessary, the SIEM alerts the RA about potential security incidents.

5.4.3 Retention Period for Audit Log

The RA retains the audit logs from software applications and infrastructure as follows:

- Certificate Life Cycle Event Records: Validity period for Certificate plus 2 years.
- Certificate Subscriber Authentication, Key Activation, and Signing Event Records: 2 years after event occurrence.
- Security Event Records: 2 years after event occurrence.

5.4.4 Protection of Audit Log

The RA continuously monitors the integrity of the application and system audit logging processes. Also, the RA encrypts and protects the audit logs from modification and destruction and ensures only authorized individuals and the Qualified Auditor access the audit logs.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily, in an automated way. Complete backups are created on a weekly basis and are also archived at a remote location.

5.4.6 Audit Collection System

Actual log data is consolidated on a central log server for the RA infrastructure.

5.4.7 Notification to Event-causing Subject

The RA is not required to provide any notice to Subscribers that caused security events in the audit logs.

5.4.8 Vulnerability Assessments

The RA performs quarterly vulnerability scans of the software applications and infrastructure systems. In addition, the RA conducts annual penetration testing on the Entrust service. Further, the RA identifies, reviews, prioritizes, and remediates findings discovered from the vulnerability scans and penetration tests to maintain the integrity of the software applications and infrastructure systems.

The RA reports to the CA all vulnerabilities with a CVSS score 7.0 or above (Critical and High) that might have an impact to the services within the scope of this RPS. In these reports, the RA includes the remediation plans to mitigate and resolve these vulnerabilities in accordance with Section 5.4.8 of SSL.com's CP/CPS. The RA also provides regular updates on the mitigation and remediation actions to the CA.

The RA may perform on-demand vulnerability scans and penetration tests due to significant changes or requests from the CA.

Further, the RA performs annual risk assessments of the Entrust service to:

- Identify foreseeable internal and external threats that may result in unauthorized access, misuse, disclosure, alteration, or destruction of data related to Certificates.
- Assess likelihood and potential damage from threats.
- Determine sufficiency of policies, procedures, and technology to counter such threats.

5.5 Records Archival

5.5.1 Types of Records Archived

The RA will archive all documentation relating to Certificate requests and the verification thereof, and all Certificates and revocation thereof. Additionally, the RA will archive:

- All audit logs as set forth in section 5.4.1;
- Documentation related to the security of their RA systems; and
- Documentation related to the verification, issuance requests, and revocation requests of Certificates.

The RA records all relevant registration information, including at least:

- The details and the evidence of the Subscriber's identity and address;
- The details and the evidence of the Subscriber's business category and registration number, if applicable;
- the details and the evidence of the approval of the Enterprise RA, Certificate Approver and Contract Signer;
- the identity of the Verification Specialist and Verification Audit Specialist who processed or approved the verified data.

5.5.2 Retention Period of for Archive

The RA retains the records and audit logs in an archive for the longer of 2 years based on the record creation timestamp, or as long as defined in RPS Section 5.4.3.

5.5.3 Protection of Archive

The RA encrypts and protects the records and audit logs from modifications and destruction within the archives and ensures only authorized individuals and the Qualified Auditor access the records and Audit Reports in the archive.

5.5.4 Archive Backup Procedures

The RA utilizes secure and verifiable backup procedures to provide a complete and readily accessible backup archive in the event of loss or damage to a primary archive.

Any backup archive is maintained at a separate, secure location from the primary archive. Access to any backup archive shall employ protections equivalent to the security protocols of its primary archive.

5.5.5 Requirements for Time-stamping of Records

The RA logs a time stamp for the creation or modification of all records and Audit Reports in the archive. The time stamp comes from a trusted time source as described in RPS Section 6.8.

5.5.6 Archive Collection System

The RA shall employ internal systems to collect and maintain a primary archive.

5.5.7 Procedures to Obtain and Verify Archive Information

The RA ensures only authorized individuals and the Qualified Auditor access the records and Audit Reports in the archive.

5.6 Key Changeover

See SSL.com Section 5.6 in CP/CPS.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The RA has policies and procedures to respond to security alerts, investigate potential security incidents, and respond to actual security incidents. In addition, the RA has business continuity and disaster recovery plans which are tested at least annually.

The RA informs the CA about any suspected or verified security incidents without undue delay. Further, the RA collaborates with the CA to provide all required information to support the incident investigation, analysis, containment, remediation, and reporting.

5.7.2 Computing Resources, Software and/or Data are Corrupted

The RA maintains a business continuity plan that includes measures to respond to security or availability incidents. The RA investigates security incidents and suspends affected processes as required and restores suspended processes based on the recovery time objective (RTO) for the process.

5.7.3 Entity Private Key Compromise Procedures

Private Key compromise procedures are described in the CP/CPS Section 5.7.3.

5.7.4 Business Continuity Capabilities after a Disaster

The RA maintains a business continuity plan to ensure the availability of the Entrust service in case of security or availability incidents. The business continuity plan also describes the restoration of processes in the event of security or availability incidents.

SSL.com maintains CRL and OCSP access points that Entrust in its role as RA and entities relying on the RA can use to access revocation information. In the event that the Entrust RA operations are not available, SSL.com Administrators have the ability to directly access the CA systems to revoke Certificates.

5.8 CA or RA Termination

The termination of the RA activities is subject to the agreement between Entrust and SSL.com.

Before Entrust terminates RA activities, Entrust shall:

1. Provide notice and information about the termination by sending notice by email and through Certificate lifecycle management portal to all TLS Certificate customers; and
2. Transfer all responsibilities under this RPS to SSL.com.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The Subscriber generates its key pair by itself. Key pair requirements are defined in the CPS.

6.1.2 Private Key Delivery to Subscriber

The key pair is generated by the Subscriber in the Subscriber's secure environment. The Private Key remains in that secure environment, so it is not transferred.

6.1.3 Public Key Delivery to Certificate Issuer

Public key delivery to the RA is done via the Entrust Certificate lifecycle management portal in accordance with Section 3.2.1. After successful validation, the RA sends the request with the public key to the CA.

6.1.4 CA Public Key Delivery to Relying Parties

As stipulated in the CPS.

6.1.5 Key Sizes

As stipulated in the CPS.

6.1.6 Public Key Parameters Generation and Quality Checking

As stipulated in the CPS.

6.1.7 Key Usage Purposes

As stipulated in the CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

As stipulated in the CPS.

6.2.1 Cryptographic Module Standards and Controls

As stipulated in the CPS.

6.2.2 Private Key (N out of M) Multi-person Control

As stipulated in the CPS.

6.2.3 Private Key Escrow

As stipulated in the CPS.

6.2.4 Private Key Backup

As stipulated in the CPS.

6.2.5 Private Key Archival

As stipulated in the CPS.

6.2.6 Private Key Transfer into or from Cryptographic Module

As stipulated in the CPS.

6.2.7 Private Key Storage on Cryptographic Module

As stipulated in the CPS.

6.2.8 Method of Activating Private Key

As stipulated in the CPS.

6.2.9 Method of Deactivating Private Key

As stipulated in the CPS.

6.2.10 Method of Destroying Private Key

As stipulated in the CPS.

6.2.11 Cryptographic Module Rating

As stipulated in the CPS.

6.3 Other Aspects of Key Pair Management

As stipulated in the CPS.

6.3.1 Public Key Archival

As stipulated in the CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

As stipulated in the CPS.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

As stipulated in the CPS.

6.4.2 Activation Data Protection

As stipulated in the CPS.

6.4.3 Other Aspects of Activation Data

As stipulated in the CPS.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The RA ensures the software applications and infrastructure systems are:

- Configured, maintained, and secured using industry best practices.
- Operated on trustworthy software.
- Regularly scanned for malicious code and protected against spyware and viruses.
- Updated with recommended security patches within 6 months of the security patch's availability, unless documented testing determines that the security patch would introduce additional vulnerabilities.

The RA implements MFA where practical and configures the software applications and infrastructure systems to:

- Authenticate identity of users before permitting access.
- Manage privileges of users and limit users to assigned roles.
- Generate and archive audit records for all transactions.
- Enforce domain integrity boundaries for critical security processes.
- Support recovery from system failure.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The RA has system development controls for the Entrust service that cover the following topics:

- All software development follows a documented development process.
- All infrastructure systems and third-party software applications are obtained in a manner that reduces risk of falsification, modification, or tampering.
- All software code maintains integrity and security throughout the development and deployment processes.

6.6.2 Security Management Controls

The RA continuously monitors software application and infrastructure system configurations for potential security incidents and has a release management process to authenticate, modify, install, and manage software applications and infrastructure systems.

6.6.3 Life Cycle Security Controls

No Stipulation.

6.7 Network Security Controls Security Controls

The RA has security controls to protect all operations related to the Entrust service and segments the network into zones based on functional or logical relationships. The same network security controls apply to all software applications and infrastructure systems within the same zone.

These controls observe the standards established in the most recent version of the CA/B

Forum Network and Certificate System Security Requirements (https://cabforum.org/network-security-requirements/).

The RA implements security controls to manage data flows and secure communications within and between networks and zones. These controls rely on gateways, routers, and firewalls which are configured to only allow services, ports, and protocols necessary for operations.

The RA uses only secure communication channels between the Certificate Subscriber and RA, as well as the RA and CA.

The RA only grants authorized individuals in trusted roles access to the networks and zones. The RA also logs access by these individuals to the networks and zones.

The RA continuously monitors the networks and zones for potential security incidents.

6.8 Time-stamping

The RA uses a network time protocol (NTP) with a trusted time source to ensure the accuracy of all time stamping operations.

7. Certificate, CRL and OCSP Profiles

The CA sets the appropriate Certificate, CRL, and OCSP profiles in accordance with CP/CPS Section 7.

8. Compliance Audit and Other Assessment

8.1 Frequency or Circumstances of Assessment

The RA is audited annually by a Qualified Auditor to ensure compliance with the standards described in RPS Section 8.4. Additional audits may take place per request by the CA in case of deficiencies or major changes in the Entrust service.

8.2 Identity/Qualifications of Assessor

The RA engages a Qualified Auditor with the following skills and qualifications to perform any external audits:

- Can conduct an audit that addresses the criteria specified in RPS Section 8.4.
- Employs individuals proficient in the examination of PKI technology; information security tools and techniques; information technology and security auditing; and third-party attestation function.
- Adheres to applicable laws, government regulations, and professional code of ethics.
- Maintains a Professional Liability / Errors and Omissions insurance policy with a minimum of one million US dollars ($1,000,000) in coverage.

8.3 Assessor's Relationship to Assessed Entity

The RA ensures the Qualified Auditor is independent from any relationship that may constitute a conflict of interest or impair the auditor's objective assessment.

8.4 Topics Covered by Assessment

Annual audits are performed in accordance with the WebTrust for Registration Authorities (WTRA) latest applicable program and industry standards as detailed in the current version of the WebTrust Principles and Criteria for Registration Authorities. Audits cover the WebTrust Principles and Criteria for Registration Authorities, including the RA Additional Baseline and Network Security Criteria and Controls.

Internal self-audits address integrity and security aspects of the Entrust service as described in RPS Section 8.7.

8.5 Actions Taken as a Result of Deficiency

The RA informs the CA about any deficiency in a reasonable timeframe and collaborates with the CA in the investigation, analysis, containment, remediation, and reporting.

The RA develops and implements remediation plans to correct deficiencies deemed to constitute material non-compliance with applicable laws, CP/CPS, or standards listed in RPS Section 8.4. The RA submits remediation plans to the CA and any appropriate third-parties, documents all corrective actions to security controls and updates the RPS as required.

The CA may require on-demand audits of the RA after remediation of the deficiency to ensure the effectiveness of corrective actions.

8.6 Communication of Results

The RA communicates its audit results within a reasonable timeframe to the SSL.com PMA and to any third-party entities entitled or required to be notified of audit results by law, regulation, or agreement.

8.7 Self-audits

The RA performs quarterly internal audits on a sample of Certificates issued since the previous internal audit. For each audit, the sample consists of 3 percent of issued OV Certificates and 6 percent of EV Certificates, rounded up to the next highest integer.

The sample is randomly selected by the RA to cover the examination period. The CA may also select a sample of Certificates in accordance with their internal audit processes. In this case, the RA incorporates the CA's sample; if needed, additional samples are randomly selected by the RA to reach the target sample size.

The RA also performs annual self-assessments of the conformance of this RPS to the CP/CPS and the requirements specified in RPS Section 1.1. The RA shares the self-assessment results and any remediation actions with the CA within a reasonable timeframe.

9. Other Business and Legal Matters

9.1 Fees

All fees are made clear to Applicants during the enrollment process through a web interface and/or in any marketing content presented by the RA.

9.2 Financial Responsibility

Subscribers and Relying Parties shall be responsible for the financial consequences to such Subscribers, Relying Parties, and to any other persons, entities, or organizations for any transactions in which such Subscribers or Relying Parties participate and which use Certificates or any services provided in respect to Certificates.

Entrust maintains (a) Commercial General Liability insurance with policy limits of at least two million US dollars (US$2,000,000.00) in coverage; and (b) Professional Liability/Errors and Omissions insurance, with policy limits of at least five million US dollars (US$5,000,000.00) in coverage. Such insurance policies will be carried with companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information is considered the confidential information of Entrust and is protected against unauthorized disclosure using a reasonable degree of care:

1. Internal procedures for handling and processing Certificate applications and revocation requests;
2. Internal security procedures and measures;
3. Information and data on the RA systems and infrastructure;
4. Business continuity, incident response, contingency, and disaster recovery plans;
5. Information held by Entrust as confidential information in accordance with Section 9.4;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this RPS).

For personal data, see section 9.4.2.

9.3.2 Information not with the Scope of Confidential Information

Certificate status information and Certificates issued via the SSL.com PKI, including information included in a Certificate or a Certificate Revocation List are deemed public.

9.3.3 Responsibility to Protect Confidential Information

Entrust and all its employees, agents and contractors are responsible for protecting confidential information. Entrust shall maintain and protect confidential information through thorough training and enforcement programs for all personnel.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

All personal information utilized by any element of the RA functions is protected in accordance with Entrust's privacy policies, statements and practices published at https://www.entrust.com/legal-compliance/data-privacy (collectively, "Privacy Plan").

9.4.2 Information Treated as Private

Entrust treats all personal information about an individual that is not publicly available in the contents of a Certificate, CRL or OCSP as personal information in accordance with the Privacy Plan.

9.4.3 Information not Deemed Private

Subject to applicable law, information included in Certificates is deemed public information and is not subject to protections outlined in section 9.4.2.

9.4.4 Responsibility to Protect Private Information

Entrust personnel are required to protect personal information in accordance with the Privacy Plan. In accordance with Section 5.3, the RA shall train and periodically retrain all personnel to ensure secure handling of and access to private information.

9.4.5 Notice and Consent to Use Private Information

Entrust complies with its Personal Data Protection Policy and ECS Product Privacy Notice as to the use of personal information,. Unless otherwise stated in the RPS, Personal Data Protection Policy, ECS Product Privacy Notice or Subscriber Agreement, a party shall only use information considered confidential after obtaining the Subject's express written consent. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The RA may disclose private information without notice to Applicants or Subscribers when required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property Rights

As stipulated in the CA CP and CPS.

9.6 Representation and Warranties

9.6.1 CA Representations and Warranties

The CA offers the warranties described in its CPS.

9.6.2 RA Representations and Warranties

The RA warrants that:

1. All Certificate management operations conform to the SSL.com CP/CPS and any other related or relevant documents, as reflected in this RPS.
2. Information provided by the RA does not contain any false or misleading information.
3. Any translations provided by the RA are accurate.
4. The RA shall abide by the terms of the Certificate Services Agreement signed with SSL.com as of July 18 2024, as amended (which is agreed to constitute the Registration Authority Agreement (RAA) as defined in the CP/CPS.

9.6.3 Subscriber representations and Warranties

Subscribers must sign a Subscriber Agreement containing the requirements the Subscriber shall meet including protection of their private keys and use of the Certificates before being issued the Certificates.

9.6.4 Relying Parties Representations and Warranties

As stipulated in the SSL.com CP/CPS.

9.6.5 Representations and Warranties of Other Participants

As stipulated in the SSL.com CP/CPS.

9.7 Disclaimers of Warranties

As stipulated in the SSL.com CP/CPS with respect to SSL.com.
EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.2, ALL RA SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE".

TO THE MAXIMUM EXTENT PERMITTED BY LAW, ENTRUST DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

ENTRUST DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE.

No fiduciary duty is created or implied though use of Entrust services by any entity.

9.8 Limitations of Liability

As Stipulated in the Subscriber Agreement.

9.9 Indemnities

As Stipulated in CA CP/CPS.

9.10 Term and Termination

9.10.1 Term

This RPS and any amendments to the RPS are effective when approved by SSL.com and Entrust and remain in effect until replaced with a newer version.

9.10.2 Termination

Unless otherwise specified, the termination of this RPS becomes effective immediately following the publication of a more recent version. Some sections of the RPS may include specific future dates after which certain policies or practices will become effective.

9.10.3 Effect of Termination and Survival

Entrust shall communicate the conditions and effect of this RPS's termination in a manner mutually agreed to by SSL.com and Entrust. At a minimum, all responsibilities related to protecting confidential information will survive termination.

9.11 Individual Notices and Communications with Participants

Unless otherwise set out in in a Subscriber Agreement or elsewhere in this RPS, any notice to be given to Entrust under this RPS, shall be given in writing to the address specified in Section 1.5.2 by prepaid receipted mail, or overnight courier, and shall be effective as follows (i) in the case of courier, on the next business day in Ontario, Canada ("Business Day"), and (ii) in the case of receipted mail, five (5) Business Days following the date of deposit in the mail.

9.12 Amendments

9.12.1 Procedure for Amendment

This RPS is reviewed annually. Prior to enactment, the Entrust PMA and the SSL.com PMA must approve this RPS and any amendments.

9.12.2 Notification Mechanism and Period

Within 7 days of approval of an amendment to the RPS, an updated version of this RPS will be published in accordance with RPS Section 2.1.

9.12.3 Circumstances Under which OID must be Changed

Not applicable.

9.13 Dispute Resolution Provisions

For disputes between the CA and the RA, as stipulated in the RAA.

For disputes between any other party and SSL.com, as stipulated in the CA CP and CPS.

For disputes between any other party and Entrust, except as specified in a legally binding agreement between Entrust and that party, all disputes shall be submitted to mediation in accordance with the Commercial Mediation Rules of the American Arbitration Association which shall take place in English in Ottawa, Ontario. In the event that a resolution to such dispute cannot be achieved through mediation within thirty (30) days, the dispute shall be submitted to binding arbitration. The arbitrator shall have the right to decide all questions of arbitrability. The dispute shall be finally settled by arbitration in accordance with the rules of the American Arbitration Association, as modified by this provision. Such arbitration shall take place in English in Ottawa, Ontario, before a sole arbitrator appointed by the American Arbitration Association (AAA) who shall be appointed by the AAA from its Technology Panel and shall be reasonably knowledgeable in electronic commerce disputes. The arbitrator shall apply the laws of the Province of Ontario, without regard to its conflict of laws provisions, and shall render a written decision within thirty (30) days from the date of close of the arbitration hearing, but no more than one (1) year from the date that the matter was submitted for arbitration. The decision of the arbitrator shall be binding and conclusive and may be entered in any court of competent jurisdiction. In each arbitration, the prevailing party shall be entitled to an award of all or a portion of its costs in such arbitration, including reasonable attorney's fees actually incurred. Nothing in the RPS shall preclude Entrust from applying to any court of competent jurisdiction for temporary or permanent injunctive relief, without breach of this §9.13 and without any abridgment of the powers of the arbitrator, with respect to any (i) alleged action or omission that affects the integrity of a Certificate, or (ii) alleged breach of the RPS. The institution of any arbitration or any action shall not relieve a party of its obligations under the RPS. Any and all arbitrations or legal actions in respect to a dispute that is related to a Certificate or any services provided in respect to a Certificate shall be commenced prior to the end of one (1) year after (i) the expiration or revocation of the Certificate in dispute, or (ii) the date of provision of the disputed service or services in respect to the Certificate in dispute, whichever is sooner. If any arbitration or action in respect to a dispute that is related to a Certificate or any service or services provided in respect to a Certificate is not commenced prior to such time, any party seeking to institute such an arbitration or action shall be barred from commencing or proceeding with such arbitration or action.

9.14 Governing Law

Subject to Section 9.13, as stipulated in the CA CP/CPS.

9.15 Compliance with Applicable Law

This RPS is subject to all applicable laws and regulations, including United States and Canadian restrictions on the export of software and cryptography products. Subject to Section 9.4.5 Notice and Consent to Use Private Information contained in Certificates, Entrust's RA services meet the requirements of applicable data protection laws and have established appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Entrust requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this RPS, then

the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

Any entities operating under this RPS may not assign their rights or obligations without the prior written consent of Entrust. Unless specified otherwise in a contact with a party, Entrust does not provide notice of assignment.

9.16.3 Severability

In the event of a conflict between this RPS and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which Entrust operates the RA functions, Entrust may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations that are subject to that Law. In such event, Entrust shall immediately (and prior to performing RA functions under the modified requirement) include in Section 9.16.3 of this RPS a detailed reference to the Law requiring a modification of this RPS under this section, and the specific modifications to the RPS as implemented by Entrust.

The RA shall also notify the CA of the relevant information newly added to its RPS, so that the CA can comply with Section 9.16.3 of the CPS.

Any modification to an RA practice enabled under this section must be discontinued if and when the Law no longer applies, or the CA/Browser Forum Baseline Requirements (and therefore the SSL.com CP/CPS) are modified to make it possible to comply with both them and the Law simultaneously without reliance on specific modifications within 9.16.3. An appropriate change in practice and modification to this RPS, as outlined above, must be made within 90 days from the date the law becomes effective as to Entrust.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Entrust's failure to enforce a provision of this RPS does not waive Entrust's right to enforce the same provision later or right to enforce any other provision of this RPS. To be effective, waivers must be in writing and signed by Entrust.

9.16.5 Force Majeure

Entrust is not liable for any delay or failure to perform an obligation under this RPS to the extent that the delay or failure is caused by an occurrence beyond Entrust's reasonable control. The operation of the Internet is beyond Entrust's reasonable control.

9.17 Other Provisions

No stipulation.