Registration Practice Statement

Notarize, Inc. (dba Proof.com)
Effective Date: October 11, 2026
Document Version: V.1.3

Table of Contents

1. INTRODUCTION **6**
1.1 Overview 6
1.2 Document name and identification 6
1.3 PKI participants 6
1.3.1 Certification authorities 6
1.3.2 Registration authorities 7
1.3.3 Certificate Subscribers 7
1.3.4 Relying parties 7
1.4 Certificate usage 7
1.4.1 Appropriate certificate uses 7
1.4.2 Prohibited certificate uses 7
1.5 Policy administration 7
1.5.1 Organization administering the document 7
1.5.2 Contact information 8
1.5.3 Person determining RPS suitability for the policy 8
1.5.4 RPS approval procedures 8
1.6 Definitions and acronyms 8
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES **8**
2.1 Repositories 8
2.2 Access controls on repositories 9
3. IDENTIFICATION AND AUTHENTICATION **9**
3.1 Naming 9
3.1.1 Types of names 9
3.1.2 Need for names to be meaningful 9
3.1.3 Anonymity or pseudonymity of subscribers 9
3.1.5 Uniqueness of names 9
3.2 Initial identity validation 10
3.2.1 Method to prove possession of private key 10
3.2.2 Authentication of organization identity 10
3.2.3 Authentication of individual identity 10
3.2.4 Non-verified subscriber information 10
3.3 Identification and authentication for re-key requests 11
3.4 Identification and authentication for revocation request 11
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS **11**
4.1 Certificate Application 11
4.1.1 Who can submit a certificate application 11
4.1.2 Enrollment process and responsibilities 11
4.2 Certificate application processing 12
4.2.1 Performing identification and authentication functions 12
4.2.2 Time to process certificate applications 12

4.3 Certificate issuance 12
4.3.1 CA actions during certificate issuance 12
4.3.2 Notification to subscriber by the CA of issuance of certificate 12
4.4 Certificate acceptance 12
4.4.1 Conduct constituting certificate acceptance 12
4.5 Key pair and certificate usage 13
4.5.1 Certificate Subscriber private key and certificate usage 13
4.6 Certificate renewal 13
4.9 Certificate revocation and suspension 13
4.9.1 Circumstances for revocation 13
4.9.2 Who can request revocation 15
4.9.3 Procedure for revocation request 15
4.9.5 Time within which CA must process the revocation request 16
4.9.6 Revocation checking requirement for relying parties 17
4.9.7 CRL issuance frequency 17
4.9.8 Maximum latency for CRLs (if applicable) 17
4.9.9 On-line revocation/status checking availability 17
4.9.12 Special requirements regarding key compromise 17
4.10 Certificate status services 17
4.10.1 Operational characteristics 17
4.11 End of subscription 18
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 18
5.1 Physical controls 18
5.1.1 Site location and construction 18
5.1.2 Physical access 18
5.1.3 Power and air conditioning 18
5.1.4 Water exposures 18
5.1.5 Fire prevention and protection 19
5.1.8 Off-site backup 19
5.2 Procedural controls 19
5.2.1 Trusted roles 19
5.2.2 Number of persons required per task 19
5.2.3 Identification and authentication for each role 20
5.2.4 Roles requiring separation of duties 20
5.3 Personnel controls 20
5.3.1 Qualifications, experience, and clearance requirements 20
5.3.2 Background check procedures 20
5.3.3 Training requirements 20
5.3.4 Retraining frequency and requirements 21
5.3.5 Job rotation frequency and sequence 21
5.3.6 Sanctions for unauthorized actions 21

5.3.7 Independent contractor requirements 21
5.3.8 Documentation supplied to personnel 21
5.4 Audit logging procedures 21
5.4.1 Types of events recorded 21
5.4.2 Frequency of processing log 22
5.4.3 Retention period for audit log 22
5.4.4 Protection of audit log 22
5.4.5 Audit log backup procedures 22
5.4.6 Audit collection system (internal vs. external) 23
5.4.7 Notification to event-causing subject 23
5.4.8 Vulnerability assessments 23
5.5 Records archival 23
5.5.1 Types of records archived 23
5.5.2 Retention period for archive 24
5.5.3 Protection of archive 24
5.5.4 Archive backup procedures 24
5.5.5 Requirements for time-stamping of records 24
5.5.6 Archive collection system (internal or external) 24
5.5.7 Procedures to obtain and verify archive information 24
5.7 Compromise and disaster recovery 25
5.7.1 Incident and compromise handling procedures 25
5.7.2 Computing resources, software, and/or data are corrupted 25
5.7.3 Entity private key compromise procedures 25
5.7.4 Business continuity capabilities after a disaster 25
5.8 CA or RA termination 25
6. TECHNICAL SECURITY CONTROLS 26
6.1 Key pair generation and installation 26
6.2 Private Key Protection and Cryptographic Module Engineering Controls 26
6.2.8 Method of activating private key 26
6.4 Activation data 26
6.4.1 Activation data generation and installation 26
6.4.2 Activation data protection 26
6.5 Computer security controls 27
6.5.1 Specific computer security technical requirements 27
6.6 Life cycle technical controls 27
6.6.1 System development controls 27
6.6.2 Security management controls 27
6.7 Network security controls 28
6.8 Time-stamping 28
7. CERTIFICATE, CRL, AND OCSP PROFILES 28
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 29

8.1 Frequency or circumstances of assessment 29
8.2 Identity/qualifications of assessor 29
8.3 Assessor's relationship to assessed entity 29
8.4 Topics covered by assessment 29
8.5 Actions taken as a result of deficiency 30
8.6 Communication of results 30
8.7 Self audits 30
9. OTHER BUSINESS AND LEGAL MATTERS 31
9.4 Privacy of personal information 31
9.6 Representations and Warranties 31
9.6.2 RA representations and warranties 31
9.6.3 Subscriber representations and warranties 31
9.10 Term and termination 31
9.10.1 Term 31
9.10.2 Termination 31
9.12 Amendments 31
9.12.1 Procedure for amendment 31
9.12.2 Notification mechanism and period 32
APPENDIX A - DOCUMENT INFORMATION 32

1. INTRODUCTION

Proof is a Registration Authority (RA) responsible for the verification prior to the issuance of Digital Signature Certificates (Certificates) issued under SSL.com's CP/CPS (CP/CPS) which is located at https://legal.ssl.com/documents/SSLcom-CP-CPS.pdf.

Proof (or a third party Operator designated by Proof) 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 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 the provisions of this RPS conflict with the CP/CPS, the CP/CPS prevails.

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 Adobe Approved Trusted List program and published to their site: https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html.

In particular, Certificates are issued and managed per the Adobe Approved Trust List Technical Requirements (AATL-TR).

1.2 Document name and identification

This document is the Proof Registration Practice Statement (RPS) and has been approved by the Proof Policy Management Authority (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 under CA supervision and utilize trusted trained personnel or third parties and trustworthy systems to provide the necessary assurance.

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

1.3.3 Certificate Subscribers

A Certificate Subscriber is a natural person to whom a Certificate is issued and who is legally bound by the Proof Terms of Use.

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 or a Digital Signature facilitated by the RA and issued by the CA.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The CA issues Digital Signature Certificates (Certificates) to Certificate Subscribers by enabling digital signature key usage and Adobe Authentic Documents extended key usage, thus specifying the appropriate Certificate uses.

1.4.2 Prohibited certificate uses

Certificates may not be used for any other purpose (*e.g.*, authentication, code signing, etc.).

1.5 Policy administration

1.5.1 Organization administering the document

The Proof PMA is responsible for administering this RPS.

1.5.2 Contact information

The Proof PMA may be reached at pma@proof.com.

1.5.3 Person determining RPS suitability for the policy

The Proof 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 Proof 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 RA publishes the following terms and practices at its website:

Document	Location
Registration Practice Statement (RPS)	https://www.proof.com/legal/registration-practice-statement
Terms of Use	https://www.proof.com/legal/general-terms
Individual Digital Certificate Supplement	https://www.proof.com/legal/individual-digital-certificate-supplement
Privacy Policy	https://www.proof.com/legal/privacy-policy
Data Processing Addendum	https://www.proof.com/legal/data-processing-addendum

The RA ensures the above Repository of legal documents is available 24 hours a day, 7 days a week, 365 days a year with at least 99% availability.

The RA's Credential Policy and Practice Statement (CPPS) is available upon request by contacting the Proof PMA as defined in RPS Section 1.5.2.

The CA's repository is available at https://www.ssl.com/repository. 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 and anonymously available on the Internet with read-only access. Only authorized RA personnel have rights to modify files in this Repository. Further, the RA applies restrictions and access-control to this 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 adhere to rules for naming and identification, and require a Distinguished Name (DN) that complies with IETF RFC 5280 and the International Telecommunication Union (ITU) X.500: Open Systems Interconnection (ITU X.500) standard.

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 DNs for all End Entity Certificates. SSL.com and Proof review and approve all End Entity Naming Forms. The RA configures the Certificate Applications (Applications) in the Proof service 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.

3.1.5 Uniqueness of names

The RA verifies the uniqueness of Names in the Subject DN that includes the individual's full name and email address.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Private keys of Certificate Subscribers are generated and stored on the CA's hardware security modules (HSMs) based on Applications submitted by the RA. Since the private keys are generated on HSMs, proof-of-possession is not required before issuing the Certificates.

3.2.2 Authentication of organization identity

The RA does not issue Certificates to organizations.

3.2.3 Authentication of individual identity

The RA relies on strong identity proofing, based on a face to face meeting with the Applicant, or a procedure that provides an equivalent assurance. The latter may include any of the following:

- means of secure video communication;
- use of identity verification software/AI;
- hybrid or other methods.

In particular, the RA verifies all Subject DN data in the Applications with a process that meets NIST Special Publication 800-63 Identity Assurance Level 2 (IAL2).

The process is certified as IAL2 compliant by the Kantara Initiative as listed on the Trust Status List: https://kantarainitiative.org/trust-status-list/, and is fully documented in the Proof Credential Policy and Practice Statement (CPPS) which is available upon request by contacting the Proof PMA as defined in RPS 1.5.2.

As part of this identity proofing process, Certificate Subscribers set up login credentials with multiple factors. Certificate Subscribers select complex passwords based on the password policy as the first authentication factor and one of the following methods as a second authentication factor:

- Enrollment codes delivered via short message service (SMS)
- One-time passcodes (OTPs) from a software-based application (*e.g.*, Google Authenticator, Okta Verify, etc.)

3.2.4 Non-verified subscriber information

The RA is granted a waiver by the CA to use non-verified Certificate Subscriber information for Certificates issued in non-production environments. The RA verifies all information before approving Applications in the production environment.

3.3 Identification and authentication for re-key requests

The RA does not support re-keying of Certificates via the Proof service.

3.4 Identification and authentication for revocation request

Certificate Subscribers may request revocation of their Certificates by authenticating to the Proof service with multi factors as defined in RPS Section 3.2.3, selecting the revocation option, and providing a revocation reason. The Proof service sends the revocation requests 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

Applications may only be submitted by:

- Any individual who is to be included in the Subject of the Certificate.
- Any authorized representative of the above individual.
- Any authorized representative of the RA.

Controls apply to prevent issuance of Certificates to Applicants of Countries restricted by U.S. export restriction laws.

4.1.2 Enrollment process and responsibilities

The RA verifies the identity of Certificate Subscribers in accordance with RPS Section 3.2.3. Certificate Subscribers also electronically accept the Proof Terms of Use and Individual Digital Certificate Supplement which include 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.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The RA enrolls Certificate Subscribers through an identity proofing process and requires Certificate Subscribers to set up their authentication factors in accordance with RPS Section 3.2.

The RA requires Certificate Subscribers to complete the identity proofing process and set up their authentication factors in a single session. If Certificate Subscribers do not finish the identity proofing process or authentication factor selection within the session or time frame, the RA rejects the Application.

4.2.2 Time to process certificate applications

The RA will process Applications in a commercially reasonable time frame.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Once the RA approves Applications, the Proof service creates, digitally signs, and sends requests with the Certificate Subscribers' identity information to the application programming interfaces (APIs) operated by the CA.

Once the authenticity of these requests is verified, the CA generates new asymmetric key pairs on the HSMs and new Certificate Signing Requests (CSRs) with the Certificate Subscribers' identity information. The CA issues Certificates based on the above CSRs, installs them on the HSMs and notifies the Proof service via the APIs.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Upon receiving issuance confirmation via the API, the Proof service displays a modal about the Certificate issuance to Certificate Subscribers.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The Proof 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 CP/CPS Section 4.4.1.

4.5 Key pair and certificate usage

4.5.1 Certificate Subscriber private key and certificate usage

Certificate Subscribers are required to protect the authentication factors that provide access to the private keys for their Certificate, as specified in Sections 3 and 4 of the Individual Digital Certificate Supplement.

If a Certificate Subscriber does not protect their authentication factors or misuses their Certificate, the Proof service revokes their Certificate in accordance with RPS Section 4.9.

4.6 Certificate renewal

The RA does not support the renewal of Certificates. Upon expiration, Subscribers instead 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.

Proof does not support "Suspended" status for Certificates.

4.9.1 Circumstances for revocation

The RA (or CA) begins the revocation procedure of 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)

The RA (or CA) should revoke a Certificate within 24 hours and must revoke a Certificate 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 Proof Terms of Use (CRLReason #9, privilegeWithdrawn)
4. The RA (or CA) is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn)
5. The RA (or CA) is made aware that the Certificate was not issued in accordance with the RPS or CP/CPS (CRLReason #4, superseded)
6. The RA (or CA) determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn)
7. The CA's right to issue Certificates is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL Repository (CRLReason #5, cessationOfOperation)
8. Revocation is required by this RPS or the CP/CPS (CRLReason #4, superseded)
9. 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)
10. 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 Proof service, select the Revocation Reason based on RFC 5280, and submit the Revocation Request to the Proof service as defined in RPS Section 3.4. Proof 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 Proof 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 Proof service. Proof 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.

4.9.3.3 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.

4.9.5 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, considering any additional time required for Revocation Requests that entail manual processing by the CA.

4.9.5.2 Certificate problem report

Certificate problem reports are handled by the CA in accordance with CP/CPS Section 4.9.5.2. 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

Relying Parties should validate the authenticity and intended usage of a Certificate using resources described in RPS Section 4.10.1.

4.9.7 CRL issuance frequency

The CA publishes a new CRL with revoked Certificates at least once every 7 days. In the CRL, the “Next Update” field value is not more than 10 days beyond the “This Update” field.

4.9.8 Maximum latency for CRLs (if applicable)

Where applicable, the maximum latency for the CRL is 10 minutes.

4.9.9 On-line revocation/status checking availability

Online Certificate Status Protocol (OCSP) is not supported for Certificates in the Proof service.

4.9.12 Special requirements regarding key compromise

Any entity needs to use the Certificate Problem Report as defined in RPS Section 4.9.3.3 to show evidence of a Private Key Compromise based on one of the following methods:

- Submission of the Private Key itself;
- Submission of a CSR with a Common Name indicating Private Key Compromise (e.g., “This key is compromised”);
- Submission of signed data indicating key compromise by following the instructions to confirm private key matches at Proving Possession of a Private Key.

4.10 Certificate status services

4.10.1 Operational characteristics

The CA automatically generates and publishes CRLs for Digital Signature Certificates to the following URI which it includes in the CRL Distribution Point (CDP) extension of the Certificates:

- CRL Distribution Endpoint: http://crls.ssl.com/Proof.com-docSigning-I-E2.crl

4.11 End of subscription

Certificate Subscribers can terminate their subscriptions by allowing their Certificates to expire without renewing the Certificates. Further, Certificate Subscribers or the RA can revoke the Certificates as defined in RPS Section 4.9.3.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

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

5.1.1 Site location and construction

The RA operates the Proof service from 2 geographic locations, US East and US West, within Amazon Web Services (AWS) which is an Infrastructure-as-a-Service (IaaS) solution. The RA relies on AWS to maintain appropriate security barriers and physical access controls.

5.1.2 Physical access

The RA relies on AWS to secure and protect the physical infrastructure (*e.g.*, servers, routers, etc.) in its data centers from unauthorized access with physical access controls including physical cards and biometric readers. Further, the RA relies on AWS for 24x7x365 video monitoring to record all access to data centers.

5.1.3 Power and air conditioning

The RA relies on AWS to utilize uninterrupted power supply (UPS) units and automatic backup generators to ensure redundant power sources. Further, the RA relies on AWS for heating, ventilation, and air conditioning (HVAC) systems to control temperatures in the data centers to support the operation of the Proof service.

5.1.4 Water exposures

The RA relies on AWS to protect infrastructure from water exposure in the data centers.

5.1.5 Fire prevention and protection

The RA relies on AWS for automatic fire suppression systems in data centers to preserve infrastructure in case of fire.

5.1.8 Off-site backup

The RA backs up software code and data between 2 geographic locations, US East and US West, in AWS and leverages Github, a Software-as-a-Service (SaaS) solution, to store and protect software code. Github backs up the software code in multiple geographic locations.

5.2 Procedural controls

5.2.1 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:

- **Identity Verification Agent:** Addresses issues with automated identity proofing process by reviewing and validating Applicant data and approving or rejecting Applications in the Proof service based on their findings.
- **Certificate Operations:** Manages Subscriber and Identity Verification Agent access to system and certificates.
- **System Administrator**: Operates cloud infrastructure for the Proof.com service.
- **Network Administrator**: Manages the network for production and pre-production environments.
- **Engineering Manager:** Authorizes temporary access to Software Engineers to perform work for on-call shifts.
- **Software Engineer:** Receives temporary access to the production environment for Proof service to perform specific tasks.
- **Security Auditor**: Performs internal audits of controls and reviews and archives audit logs.

5.2.2 Number of persons required per task

The RA requires all software code and infrastructure-as-code changes be peer-reviewed to ensure dual control before merging changes into the main line code branch. The RA also submits and approves changes to deploy authorized code changes to the Proof service as specified in RPS Section 6.6.1 and monitors the Proof service for unauthorized changes.

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 Proof, Github, and AWS services to perform their job functions.

5.2.4 Roles requiring separation of duties

The Security Auditor role is not combined with any operational role, such as Identity Verification Agent, Engineering Manager, or System Administrator. Under the separation of duties principle, a Security Auditor may not audit areas which the same Security Auditor was involved in.

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 should cover the following topics:

- Proof identity verification procedures based on requirements in this RPS, CrP/CrPS, and CP/CPS.
- 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 Proof.

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 annually.

5.3.5 Job rotation frequency and sequence

The RA minimizes any negative impact to the Proof 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 Proof 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 Proof service. This includes at least the following events:

1. Subscriber identity proofing events;
2. Subscriber Certificate issuance events;
3. Subscriber Certificate revocation events;
4. Subscriber Certificate usage events, traced back to Subscriber authentication events per Section 6.2.8;
5. Privileged users authentication events and actions;

6. Successful and unsuccessful access attempts.

The audit logs record the following information for all entries:

- Event description
- Event date and time
- 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 Proof 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

The RA loads all audit logs into the SIEM at least daily which serves as the backup. The SIEM is a SaaS solution and stores the audit logs at data centers in different geographic locations than the Proof service.

5.4.6 Audit collection system (internal vs. external)

The software application and infrastructure system logging processes operate independently from the Proof service. These processes are invoked at start up and only cease at shut down. Further, these processes are not capable of being circumvented.

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 Proof 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 the 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 Proof 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 retains records related to Applications, identity proofing, revocation requests, and audit logs. This includes records (documentation, communication records, etc) related to any processing of the above that is not automatically logged, including cases that the RA personnel address issues with automated identity proofing process per

Section 3.2.3 and process Revocation Requests and Certificate Problem Reports per Section 4.9.3.

Further, the RA preserves copies of the System and Organization Control (SOC 2) and WebTrust RA Audit Reports about the security of the Proof service.

5.5.2 Retention period for archive

The RA retains the records and Audit Reports in an archive for the longer of 3 years based on the record or document time stamp 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 Reports 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 backs up the primary archive based on a long-term storage solution in AWS that replicates this archive across multiple geographic locations. The replicated archives have the same protections as the primary archive.

5.5.5 Requirements for time-stamping of records

The RA logs a time stamp for the creation or modification on 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 (internal or external)

The RA utilizes an external system in AWS to collect and maintain the primary and replicated archives.

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.

5.7 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 Proof 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.

5.8 CA or RA termination

Upon termination, the RA will provide timely notice to all affected parties and perform the following tasks in collaboration with the CA:

- Revoke all unexpired Certificates.
- Destroy the private keys for the RA certificates.
- Transfer all responsibilities to an entity approved by the CA.

The RA will retain records and audit logs specified in 5.5.1 for at least 2 years after any Certificate based on that documentation ceases to be valid to be available for any lawful control.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

Private Keys are generated and stored in HSMs operated by the CA in accordance with its CP/CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.8 Method of activating private key

The RA requires Certificate Subscribers authenticate to the Proof service with multi factor authentication (MFA) based on NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management at Authentication Assurance Level 2 (AAL2).

The RA applies the necessary technical and organizational controls to ensure the security of the management/lifecycle of the MFA factors. In particular, the RA ensures that the compromise of one factor does not lead to the compromise of the other factor.

The CA is responsible for activating the private keys for CA Certificates as defined in CP/CPS Section 6.2.8.

6.4 Activation data

6.4.1 Activation data generation and installation

The CA is responsible for generating and installing the HSM activation data as described in CPS Section 6.4.1.

6.4.2 Activation data protection

The CA protects the HSM activation data as described in CPS Section 6.4.2.

The RA protects the MFA factors that are used to activate the Private Keys in the HSMs by:

- Preventing unauthorized access to the authentication data.
- Encrypting authentication data in-transit and at-rest.
- Establishing secure processes to change MFA factors.

- Restricting administrative access to authorized trusted role members in accordance with RPS Section 5.2.2.

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.

6.6 Life cycle technical controls

6.6.1 System development controls

The RA has system development controls for the Proof 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.

6.7 Network security controls

The RA has security controls to protect all operations related to the Proof 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.

Further, 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.

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

Moreover, 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.

Lastly, 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 CPS Section 7.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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 Proof service.

8.2 Identity/qualifications of assessor

The RA engages an 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 infrastructure 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 andOmissions 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 audits address integrity and security aspects of the Proof 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 that are 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 and 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. The RA also communicates its audit results to any appropriate third-party as legally required.

The CA may notify other interested third-parties (i.e., Adobe) as contractually required.

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 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

9.4 Privacy of personal information

The RA protects all personally identifiable information (PII) from Certificate Subscribers in accordance with its Privacy Policy and its Data Processing Addendum.

9.6 Representations and Warranties

9.6.2 RA representations and warranties

The RA makes the warranties in CP/CPS Section 9.6.2 to the CA.

9.6.3 Subscriber representations and warranties

For each Certificate Application and resulting Digital Signature Certificate, the RA requires Subscriber to agree to its Terms of Use and its Individual Digital Certificate Supplement.

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 Proof 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.

9.12 Amendments

9.12.1 Procedure for amendment

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

9.12.2 Notification mechanism and period

Within 7 days of approval of an RPS amendment, an updated version of this RPS is published in accordance with RPS Section 2.1.

APPENDIX A - DOCUMENT INFORMATION

Version	Date	Changes	Review/Approval
1.0	November 14, 2023	Initial Issue	Proof PMA SSL.com PMA
1.1	January 30, 2024	Added Certificate Operations as a new Trusted Role, updated URL for CRL, and minor grammatical updates	Proof PMA SSL.com PMA
1.2	December 23, 2024	Reviewed RPS based on SSL.com CP/CPS V.1.22 updates and determined no changes were required to RPS	Proof PMA SSL.com PMA
1.3	September 29, 2026	Fixed white spaces; updated Data Privacy Supplement to Data Processing Addendum as well as Digital Certificate Supplement to Individual Digital Certificate Supplement; and changed RFC 822 to RFC 5280	Proof PMA