Entrust PKIaaS Combined X.509 Certificate Policy/Certificate Practices Statement (PKIaaS CP/CPS)

Version 3.0

22 April, 2026

This CP/CPS states and implements the policy requirements of the X.509 Certificate Policy for Entrust PKIaaS, and all adopted changes.

Document Control

Date	Authors	Description
Feb 2021	Colin Tulloch Bruce Morton Charley Chell Alexandra Stockwell	Initial publication
May 2021	Jonah Guo Bruce Morton Charley Chell Alexandra Stockwell	Updated using PKIaaS 1.1 specs
Jan 2022	Jonah Guo Bruce Morton Alexandra Stockwell	Updated using PKIaaS 1.4 specs
Mar 2022	Jonah Guo Bruce Morton Alexandra Stockwell Blake Morgan	Updated to include the EU data centers New certificate profile updates
Dec 2022	Jonah Guo	Updated to include new certificate profiles
Mar 2023	Jonah Guo	Updated to include new certificate profiles
Jun 2023	Jonah Guo	Updated the default validity from 3 years to 1 year for most of the subscriber certificate profiles.
Oct 2023	Jonah Guo	Updated to include new certificate profiles Updated the subscriber key generation and delivery sections to cover the PCKS #12 scenarios
March 2024	Jonah Guo	Updated to include new certificate profiles
March 2026	Jonah Guo, Peter Dean, Jim Trovato, Alexandra Stockwell, Ngook Kong, Patrick Garritty, Pat Milot, Sean Weldon, Pat Coutu, other SME's.	Transitioned to Combined CP/CPS in RFC 3647, updated for Post Quantum, clarification of Roles & Responsibilities, alignment with current practices, updated assessment information.

SIGNATURE PAGE

JIM TROVATO

Entrust Policy Authority (Print Name)

Signed by:
Jim Trovato
89D32B44D9C945B...

22 April 2026

Entrust Policy Authority (Signature)

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Overview

Entrust PKIaaS provides cloud-based, highly scalable PKI backed by HSM clusters hosted in Entrust data centers. PKIaaS provides an agile PKI backend to applications that require privately trusted Certificates, such as mobile device management, user authentication, IoT, and DevOps. This service is offered under the terms and conditions of a PKIaaS Agreement (See Appendix A for capitalized terms and acronyms).

This CP/CPS:

- Describes the practices and procedures of the Certificate Authorities (CAs) and other PKI participants and forms part of the PKIaaS Agreement under which Entrust makes the PKIaaS available.
- Applies to the Certificate types issued by a Customer's Root CAs or Issuing CAs hosted by Entrust as part of the PKIaaS.
- Applies also to all persons, entities, and organizations, including, without limitation, all CAs, RAs, Applicants, Subscribers, Relying Parties, resellers, co-marketers, and any other persons, entities, or organizations that have a relationship with Entrust in respect to Certificates issued as part of PKIaaS and/or any services provided by Entrust in connection with PKIaaS.
- Is incorporated by reference into all Certificates issued by CAs created as part of PKIaaS.
- Provides Applicants, Subscribers, Relying Parties, resellers, co-marketers, and other persons, entities, and organizations with a statement of the practices and policies of Entrust with respect to PKIaaS. This CP/CPS also provides a statement of the rights and obligations of Entrust, any parties that are acting as RAs, Applicants, Subscribers, Relying Parties, resellers, co-marketers and any other persons, entities, or organizations that may use or rely on Certificates or have a relationship with any of the foregoing in respect to Certificates issued as part of PKIaaS and/or any services provided by Entrust in connection with PKIaaS.
- Excludes PKI components and services deployed, hosted, and operated by the Customer or its delegates, such as root CAs, RA services, and subordinate or cross-certified CAs operated (by any party) outside of PKIaaS.
- Does not cover Entrust-managed PKI, Entrust-managed offline root CA, or any other Entrust PKI services.

1.2 Document name and identification

This document is the Entrust PKIaaS Combined X509 Certificate Policy / Certificate Practices Statement (PKIaaS CP/CPS). The practices stated herein conform to the requirements as defined in this CP/CPS. The CP/CPS policy OID is:

- `2.16.840.1.114027.200.6.10`

The Certificates issued by a Dedicated Root or Issuing CA may assert the above Object Identifier (OID).

1.3 PKI participants

1.3.1 Entrust

Entrust hosts and manages the PKIaaS environment as described in this CP/CPS.

1.3.1.1 The Entrust Policy Management Authority (EPMA)

The EPMA is a cross-functional governance body responsible for policy management and compliance oversight for Entrust Digital Security Solutions (DSS). It operates under the Entrust Compliance Governance Board (CGB). The Vice President of Global Product Management acts as Executive Sponsor. The Director of Product Compliance chairs the EPMA.

The EPMA reviews compliance reporting, evaluates policy and CP/CPS updates, and provides directions and oversight on compliance initiatives to ensure services align with Entrust policies and governance.

1.3.1.2 The Entrust Policy Authority (PA)

In addition to the role of EPMA Chair, Entrust's Director of Product Compliance, serves as the Policy Authority (PA). The PA appoints key compliance roles, defines compliance performance requirements, and oversees overall compliance monitoring with respect to Entrust PKI services. The PA delegates PKI operational oversight to an Operational Authority (OA) and may designate Policy Authority Representatives (PARs) to monitor technical and service compliance of PKI services.

The PA reviews, approves and is the Entrust signatory for CP/CPS/RPS updates.

1.3.1.3 The Entrust Operational Authority (OA)

The Operational Authority (OA) is a Trusted Role appointed by the Policy Authority (PA) and delegated day-to-day responsibility for ensuring that all Entrust operational activities are performed in accordance with this CP/CPS. The OA acts as the operational steward of compliance, translating policy requirements into repeatable procedures, documented controls, and verifiable records.

1.3.2 The Customer

The Customer is responsible for CAs, RA, and Subscribers as described in this CP/CPS.

1.3.2.1 Certification authorities

The PKI environment hosted by Entrust allows the Customer to create and manage CAs. The structure of the Customer environment is comprised of:

- **Root CAs** created by the Customer to serve as PKI trust anchors. The Customer defines the Common Name (CN) of each Online Root CA. Root CAs issue Certificates to the Issuing CAs and OCSP services.
- **Issuing CAs,** each of which is subordinate to a Root CA, created and managed by the Customer and used to issue Certificates to or for Subscribers.

1.3.2.2 Registration authorities

The RA is the person or entity that decides whether a Certificate should be issued in response to a Subscriber request. The Customer is responsible for appointing, instructing, and supervising RAs.

RAs verify Applicant identities and submit certificate issuance requests on their behalf. They are also responsible for Applicant registration, identification, and authentication processes.

RAs are external to PKIaaS and thus outside the scope of this CP/CPS. They interact with PKIaaS through published PKIaaS secure APIs. RAs typically use software applications that interface with the PKIaaS API and provide specific functionality applicable to certificate use.

1.3.2.3 Subscribers

Subscribers may use CA services through an RA appointed to the role by the Customer and responsible, on behalf of the Customer, for:

- Identifying who may be a Subscriber.
- Which people, entities, and devices may receive Certificates.
- Satisfying Customer verification requirements and processes for verifying Subscribers.

Where the Subject of a Certificate is a device or process, the RA is responsible for determining eligibility based on the Subscriber who submitted the application and is responsible for the device or process.

1.3.2.4 Relying parties

The Relying Party is responsible for checking the validity of the Certificate using the appropriate Certificate Status Service. The Customer determines the appropriate Relying Parties for each Certificate type.

1.3.3 Other participants

No stipulation.

1.4 Certificate usage

Private trust Certificates are issued to organizations to allow servers, devices, and individuals to identify themselves and/or communicate securely with entities and services within the organization.

1.4.1 Appropriate certificate uses

The Customer determines the appropriate uses of each Certificate type.

1.4.2 Prohibited certificate uses

All Certificates issued shall be for lawful purposes and consistent with applicable laws, including, without limitation, applicable export or import laws. It is prohibited to use Certificates in any manner that violates the law. In addition, it is not permitted to use any Certificates in a manner that violates the Agreement.

1.5 Policy administration

1.5.1 Organization administering the document

Entrust is responsible for this CP/CPS.

1.5.2 Contact person

Please direct questions pertaining to this CP/CPS to the Entrust Policy Authority (PA) at mpkipa@entrust.com.

1.5.3 Person determining CP/CPS suitability for the policy

This CP/CPS is administered by the Entrust Policy Authority (PA), appointed by the Entrust Policy Management Authority (EMPA). The PA determines the suitability and applicability of proposed changes to this CP/CPS.

1.5.4 CPS approval procedures

Updates to the Certificate Policy (CP) and Certification Practice Statement (CPS) are subject to a formal change management process.

Proposed changes are documented, reviewed for policy and operational impact, and submitted to the Policy Authority (PA) for approval. The PA is responsible for ensuring that all changes remain consistent with applicable standards and with the overall private trust framework.

Upon approval, the PA authorizes release of the updated CP/CPS. The approved version is assigned a new version identifier and effective date. The PA applies a digital signature to the final approved document to ensure authenticity and integrity prior to publication.

The authoritative, current version of the CP/CPS is published in a publicly accessible repository. Material changes may be communicated to relying parties in advance, as determined by the PA.

1.6 Definitions and acronyms

See Appendix A – Definitions and Acronyms.

2.0 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Entrust maintains the Repository to allow access to Certificate-related and Certificate revocation information. The information is accessible through a web interface, available 24/7, and periodically updated as set forth in this CP/CPS. The Repository is the only approved source for CRL and other information about Certificates.

2.2 Publication of certification information

Entrust publishes product documentation, CA Certificates, and CRLs in the Repositories.

Documentation is stored at: https://www.entrust.com/legal-compliance/private-trust

2.3 Time or frequency of publication

The CP/CPS will be reissued and published at least once per year.

2.4 Access controls on repositories

Information published in the Repository is public. Read-only access is unrestricted. Entrust has implemented logical and physical controls to prevent unauthorized write access to its Repositories.

3.0 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names
The Subject names in a Certificate comply with the X.501 Distinguished Name (DN) form.

3.1.2 Need for names to be meaningful
CA Certificates must identify the subject as a Certification Authority and include the Customer organization name. The RA is responsible for ensuring the Subject names in Subscriber Certificates are meaningful to Relying Parties.

3.1.3 Anonymity or pseudonymity of subscribers
No stipulation.

3.1.4 Rules for interpreting various name forms
No Stipulation.

3.1.5 Uniqueness of names
CA distinguished names shall be unique.

3.1.6 Recognition, authentication, and role of trademarks
No Stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key
The CA will perform proof of possession tests for CSRs created using reversible asymmetric algorithms (such as RSA) by validating the signature on the CSR submitted with the Certificate Application.

3.2.2 Authentication of organization identity
Responsibility of the RA.

3.2.3 Authentication of individual identity
Responsibility of the RA.

3.2.4 Non-verified subscriber information
Responsibility of the RA.

3.2.5 Validation of authority
During the initial onboarding process, the Customer identifies who will act as the RA and be responsible for the Customer's RA credentials. A one-time passcode (OTP) used to create the RA credential is generated and securely transmitted to the identified RA.

Validation of Authority for Subscriber Certificates is the responsibility of the RA.

3.2.6 Criteria for Interoperation

Responsibility of the RA.

3.3 Identification and Authentication for Re-Key Requests

The RA is responsible for:

- Identification and Authentication for Routine Re-key
- Identification and Authentication for Re-key after Certificate Revocation

3.4 Identification and Authentication for Revocation Requests

Before revoking Certificates, the RA shall validate the authorization to revoke such Certificate.

4.0 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Application for Certificates issued under this CP/CPS are submitted via electronic means.

4.1.1 Who Can Submit a Certificate Application

Applications for Certificates are submitted via authenticated API request from an RA. Each RA is assigned unique authentication credentials.

4.1.2 Enrollment Process and Responsibilities

The enrollment process includes authentication of the API requests and validation of the certificate request contents.

All communications among PKI components (e.g., CAs, RAs) supporting the Certificate application and issuance process are authenticated and protected from modification. Electronic communication between the Customer or RA enrollment environments, automated RA applications, and the CAs is encrypted and digitally signed.

4.2 Certificate Application Processing

Certificate application processing follows the life cycle outlined in §4.2.1 to §4.2.3 below.

4.2.1 Performing Identification and Authentication Functions

The CA performs verification of the RA by checking that the credentials supplied in the API request entitle the RA to issue Certificates for the designated CA and that the designated CA has license capacity.

The RA will identify and authenticate the Subscriber.

4.2.2 Approval or Rejection of Certificate Applications

Entrust approves a Certificate application if the following conditions are met:

- Request is syntactically valid
- Proof of possession verification passes
- The customer has an available Certificate inventory to consume

4.2.3 Time to Process Certificate Applications

Certificate Application processing is the responsibility of the RA. The CA will respond to API requests with a Certificate or with an error as to why the Certificate was not issued.

4.3 Certificate Issuance

After verifying the information provided with a Certificate Application, an RA operating under a CA may request that a CA issue a Certificate.

4.3.1 CA Actions during Certificate Issuance

Upon receipt of the issuance API request, the CA verifies the integrity of the information in the Certificate request, builds and signs a Certificate, and returns the Certificate in the API response to the API requestor (RA).

The CA will not issue Certificates with a validity period that exceeds the validity period of the corresponding Issuing CA Certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Notification to Subscriber is the responsibility of the RA.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

The CA will provide the Certificate to the RA through an API response.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CA does not provide notification of Certificate issuance to other entities.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Customer is responsible for how Subscriber Private Keys and Certificates are used.

4.5.2 Relying Party Public key and Certificate Usage

The CA provides Certificate status in accordance with this CP/CPS. Relying Party Public key and Certificate usage is outside the scope of this CP/CPS.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Responsibility of the RA.

4.6.2 Who May Request Renewal

Responsibility of the RA.

4.6.3 Processing Certificate Renewal Requests

Certificate renewal is processed the same as Certificate issuance.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification to Subscriber is the responsibility of the RA.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA
The CA will provide the Certificate to the RA through an API response.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities
The CA does not provide notification of Certificate issuance to other entities.

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-key
A Subscriber should request a Certificate with a new Public Key if the Private Key is compromised or at the end of the lifecycle of the Key Pair.

4.7.2 Who May Request Certification of a New Public Key
Responsibility of the RA.

4.7.3 Processing Certificate Re-keying Requests
Certificate re-key is processed the same as Certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber
Notification to Subscriber is the responsibility of the RA.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate
No stipulation.

4.7.6 Publication of the Rey-keyed Certificate by the CA
The CA will provide the Certificate to the RA through an API response.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities
The CA does not provide notification of Certificate issuance to other entities.

4.8 Certificate Modification
Certificate modification is treated the same as issuance. The RA is responsible for submitting the modified CSR and for revoking the replaced certificate.

4.9 Certificate Revocation and Suspension
The CA will revoke a Certificate after receiving a valid revocation request from an RA operating under such CA.

4.9.1 Circumstances for Revocation
Revocation of Issuing CA Certificates may be performed by Entrust in any of the following circumstances:

- The RA requests for a CA Certificate to be revoked. (Note that Root CA Certificates may not be revoked; the Customer must choose whether to delete).
- The RA can be shown to have violated, or is suspected of violating, the requirements of this CP/CPS or the Agreement.

- There is a suspected compromise of the associated private key.
- When the Agreement with Entrust is terminated.

Revocation of Subscriber Certificates is performed when the RA requests that a Subscriber Certificate be revoked.

4.9.2 Who can Request Revocation of a Certificate
The Customer RA may request revocation of any Certificate.

4.9.3 Procedure for Revocation Request
The RA shall request revocation of their Issuing CA Certificate, or of an individual Subscriber Certificate if the RA has a suspicion or knowledge of or a reasonable basis for believing that of any of the following events have occurred:

1. Compromise of the Certificate's Private Key.
2. A Subscriber loses access to the Private Key.
3. Knowledge that the original Certificate request was not authorized.

The RA shall submit revocation requests to the CA via authenticated API.

4.9.4 Certificate Revocation Grace Period
CAs do not apply any grace period. Revocation requests are processed synchronously in sequence with the API request and response.

4.9.5 Time Within Which CA Must Process The Revocation Request
CAs will revoke Certificates upon receipt of a proper revocation request.

4.9.6 Revocation Checking Requirement for Relying Parties
It is recommended that Relying Parties implement revocation checking. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a Certificate whose revocation status cannot be guaranteed.

4.9.7 Revocation Lists Issuance Frequency
CRLs are generated every 24 hours and are valid for 7 days.

The revocation request of a certificate can set an instant CRL update flag. In this case a new CRL will be generated containing the revoked certificate in the requests as soon as reasonably practicable, taking into account operational factors such as system availability and service load.

as possible, depending on the service load.

4.9.8 Maximum Latency for CRLs
No stipulation.

4.9.9 On-line Revocation/Status Checking Availability
On-line revocation/status checking of Certificates is available on a continuous basis by CRL and optionally OCSP.

4.9.10 On-line Revocation Checking Requirements
CAs support OCSP capability using the GET and POST methods for Certificates issued in accordance with this CP/CPS.

The CAs shall sign and issue responses upon request for OCSP for CA Certificates and Subscriber Certificates.

If the OCSP responder receives a request for status of a Certificate serial number that is "unused", the responder will not respond with a "good" status.

The on-line locations of the CRL and the OCSP response are included in the Certificate to support software applications that perform automatic Certificate status checking.

4.9.11 Other Forms of Revocation Advertisements Available
The CA does not provide any other forms of Certificate status.

4.9.12 Special Requirements re: Key Compromise
The Customer RA is responsible for responding to a suspected or confirmed instance of Subscriber Private Key Compromise. If an RA suspects, knows, or is informed of a Subscriber Private Key compromise, it is the responsibility of the RA to take necessary steps to revoke the Certificate, immediately stop using such Certificate, and remove such Certificate from any devices and/or software in which such Certificate has been installed.

4.9.13 Circumstances for Suspension
Suspension of Certificates is to be performed when the RA requests that a Certificate be suspended.

4.9.14 Who Can Request Suspension
The RA may request suspension of any Certificates issued.

4.9.15 Procedure for Suspension Request
The RA shall submit suspension requests to the CA via authenticated API.

4.9.16 Limits on Suspension Period
There is no time limit on suspension, however a suspended certificate may not be restored beyond the certificate validity expiration date.

4.10 Certificate Status Services

4.10.1 Operational Characteristics
Revocation entries on a CRL or OCSP response are not removed until after the expiry date of the revoked Certificate.

4.10.2 Service Availability
The CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions. Certificate status services are available on a continuous basis.

4.10.3 Optional Features
No stipulation.

4.11 End of Subscription
End of subscription is addressed in the Agreement.

4.12 Key Escrow and Recovery
CA and Subscriber key escrow are not supported. Subscriber key recovery is not supported.

4.12.1 Key Escrow and Recovery Policy and Practices
CA Keys can be recovered from a database and HSM backup.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices
No stipulation.

5.0 MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

See below for the practice statement on management, operational and physical controls.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The HSM clusters and Activation Data are located in Tier III, SSAE-18 datacenters or stored in a two-person-controlled safe in a facility where only Entrust-authorized personnel have access. Access to these facilities is restricted to personnel in Trusted Roles.

One or more public cloud facilities host the Certificate issuance, revocation, and status service components. The physical security controls imposed on components residing within a public cloud are outside the scope of this CP/CPS.

5.1.2 Physical Access

Two-person control is required for physical access to the HSM cluster. Alarm mechanisms notify security personnel of any violation of the rules for access to the HSM.

5.1.3 Power and Air Conditioning

The HSM cluster is hosted in Tier III datacenters. The security zone is equipped with:

- Filtered, conditioned, power connected to an appropriately sized UPS and generator.
- Heating, ventilation, and air conditioning as appropriate for a commercial data processing facility.
- Emergency lighting.

Environmental controls conform to local standards and are appropriately secured to prevent unauthorized access and/or tampering with the equipment. Temperature control alarms and alerts are activated upon detection of threatening temperature conditions.

5.1.4 Water Exposures

The HSM cluster is hosted in Tier III datacenters and is not in danger of exposure to water. No liquid, gas, exhaust, etc. pipes traverse the controlled space other than those directly required for the area's HVAC system and for the pre-action fire suppression system. Water pipes for the pre-action fire suppression system are only filled when multiple fire alarms are activated.

5.1.5 Fire Prevention and Protection

The HSM cluster is hosted in Tier III datacenters equipped with fire suppression mechanisms. The facility is fully wired for fire detection, alarm, and suppression. Hosting facilities perform and report to Entrust annually on inspections made to ensure adequate operation.

5.1.6 Media Storage

All media is stored away from sources of heat and from obvious sources of water or other obvious hazards. Electromagnetic media (e.g. tapes) are stored away from obvious sources of strong magnetic fields.

5.1.7 Waste Disposal
Waste containing sensitive information shall be destroyed, such that the information is unrecoverable, before disposal. Media used to store sensitive data shall be destroyed before disposal, such that the information is unrecoverable.

5.1.8 Off-Site Backup
Backups of the CA key material and CA databases, sufficient to recover from system failure, shall be made on a periodic schedule in accordance with the disaster recovery requirements.

5.2 Procedural Controls for the CA

5.2.1 Trusted Roles
Personnel in Trusted Roles will not be assigned other responsibilities that conflict with their operational responsibilities for the CA. Their privileges will be limited to the minimum required to carry out their assigned duties.

5.2.2 Number of Persons Required Per Task
The CA Private Keys are backed up, stored, and recovered only by personnel in Trusted Roles using dual control in a physically secured environment.

5.2.3 Identification and Authentication for Each Role
An individual performing a Trusted Role shall identify and authenticate their identity before being permitted to perform any actions or responsibilities associated with that Trusted Role.

5.2.4 Roles Requiring Separation of Duties
Personnel in Trusted Roles who can deploy to or access production systems do not have the ability to commit software code, and development team members who can commit code cannot deploy to or access production systems.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements
Personnel in Trusted Roles undergo background investigations and are trained for their specific role.

5.3.2 Background Check Procedures
Background checks are conducted as per the Entrust hiring processes.

5.3.3 Training Requirements
Personnel in Trusted Roles receive role-specific training. Where applicable, training will be conducted in the following areas:

- CA security principles and mechanisms.
- PKI duties that they are expected to perform.
- Disaster recovery and business continuity procedures.
- Stipulations of this CP/CPS.

5.3.4 Retraining Frequency and Requirements
No stipulation.

5.3.5 Job Rotation Frequency and Sequence
No stipulation.

5.3.6 Sanctions for Unauthorized Actions
No stipulation.

5.3.7 Contracting Personnel Requirements
Contractor personnel employed to perform functions pertaining to the environment must meet applicable requirements as set forth in this CP/CPS.

5.3.8 Documentation Supplied to Personnel
No stipulation.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded
Significant security events in the CAs are automatically time-stamped and recorded as audit logs. Audit logs are archived periodically. Where these events cannot be electronically (automated) logged, Entrust shall supplement electronic audit logs with digital (manual) logs as necessary.

The foregoing record requirements include, but are not limited to, an obligation to record the following events:

- CA Certificate key lifecycle events, including:
    - CA Private Key generation, backup, storage destruction, and recovery
    - CA certificate requests and CA certificate revocation
    - Cryptographic device lifecycle management events
- Subscriber Certificate lifecycle management events, including:
    - Certificate issuance requests and revocation requests
    - Generation of CRLs
- Security events, including:
    - Successful and unsuccessful PKI system access attempts
    - PKI and security system actions performed
    - Entries to and exits from the facility housing the HSM

5.4.2 Frequency of Processing Data
A Security Information and Event Management (SIEM) system continuously monitors the audit logs. Policy violations and other significant events generate alerts that operations and security teams review for malicious activity.

5.4.3 Retention Period for Security Audit Data
The audit logs are retained on the PKI system for at least three months and periodically archived in accordance with section 5.5.

5.4.4 Protection of Security Audit Data
Audit logs remain stored on the PKI systems until archived in accordance with section 5.5 Only Trusted Role personnel have access to the PKI systems.

5.4.5 Audit Log Backup Procedures
Audit logs are periodically archived in accordance with section 5.5.

5.4.6 Audit Collection System
Audit collection processes are integral to the system and cover its entire deployment time. Should it become apparent that an automated audit system has failed, the Operational Authority will be notified and will consider suspending operations until the audit capability can be restored.

5.4.7 Notification to Event-Causing Subject
No stipulation.

5.4.8 Vulnerability Assessments
Vulnerability scans are conducted monthly to identify system weaknesses and patching requirements for operating systems and supporting infrastructure. Identified vulnerabilities are analyzed and addressed in accordance with Entrust's Patch and Vulnerability Management Standards.

5.4.9 Risk Assessments
Compliance and risks are managed through automated monitoring and periodic review conducted at the discretion of the Policy Authority. This ongoing compliance risk management process continuously identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of Certificate data or Certificate management processes. If required based on insights gathered through automated monitoring and periodic reviews, under the PA and OA, a security plan is established, maintained, and updated as needed to manage and control identified risks.

5.5 Records Archival

5.5.1 Types of Records Archived
The audit logs, data, and revocation information for the CAs are archived, as are data elements necessary to access or verify archive contents.

5.5.2 Retention Period for Archive
Entrust retains audit logs for a maximum of 6 years.

Archive data is protected through logical and administrative security controls appropriate to its sensitivity and retention requirements. PKI-related archive records are stored in secured systems with restricted access limited to authorized Trusted Role personnel. Access controls, monitoring, and retention mechanisms are implemented to prevent unauthorized access, modification, or deletion of archived data and to ensure compliance with applicable retention requirements.

5.5.3 Archive Backup Procedures
No stipulation.

5.5.4 Requirements for Time-Stamping of Records
No stipulation.

5.5.5 Archive Collection System
Archive data will be collected as part of the routine system backup procedures, along with physical materials such as cryptographic modules and datacenter access logs, which will be stored manually.

5.5.6 Procedures to Obtain and Verify Archive Information
No stipulation.

5.6 Key Changeover
CAs will not be re-keyed. CA key pairs will be retired from service at the end of their lifetimes. New CA key pairs will be created as required to support the continuation of CA Services. Each CA will continue to publish CRLs signed with the original key pair until all Certificates issued using that original key pair have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures
For the purposes of this Certificate Policy, a security incident is any event that compromises, or has the potential to compromise, the confidentiality, integrity, or availability of the PKI, including but not limited to:

- Compromise or suspected compromise of CA, RA, or OCSP private keys
- Unauthorized access to CA or RA systems
- Malfunction or failure of PKI systems that may affect certificate issuance, revocation, or status services
- Security events requiring certificate revocation or re-issuance
- Any event requiring notification to Subscribers, Relying Parties, or supervisory authorities under applicable policy or law

All such incidents SHALL be handled in accordance with documented incident response procedures defined in the applicable Entrust Policy, Procedure or Standard, CP/CPS or Registration Practice Statement as determined by the PA.

The disaster recovery plan addresses the following:

1. the conditions for activating the plans
2. resumption procedures
3. a maintenance schedule for the plan
4. awareness and education requirements
5. the responsibilities of the individuals
6. recovery point objective (RPO) of fifteen minutes

7. recovery time objective (RTO) of 24 hours for essential CA operations, which include Certificate revocation, and issuance of Certificate revocation status
8. testing of recovery plans

To mitigate the event of a disaster, the CAs have implemented the following:

1. Datacenters with highly available HSMs and secure on-site and off-site storage of backup HSMs containing copies of all CA Private Keys
2. secure on-site and off-site storage of all requisite activation materials
3. database replication between primary and secondary regions
4. daily database backups within both the primary and secondary regions
5. weekly backup of critical data to a secure off-site storage facility
6. secure off-site storage of the disaster recovery plan and disaster recovery procedures

Entrust maintains geographically distributed physical data centers to support service availability and regional coverage. These facilities include locations near Dallas, Texas, and Denver, Colorado in North America, and Munich and Frankfurt, Germany within the European Union.

Cloud-based components utilize multiple availability zones for high availability and a secondary region for disaster recovery.

Entrust requires rigorous security controls to maintain the integrity of the environment. Entrust views the compromise of the Private Key used by a CA as being very unlikely; however, Entrust has policies and procedures that will be employed in the event of such a compromise. At a minimum, all RAs will be informed as soon as practicable of such a compromise. It is a Customer responsibility to determine whether Certificates signed by the compromised CA must be revoked.

5.7.2 Computing Resources, Software, and/or Data are Corrupted
No stipulation.

5.7.3 Entity Private Key Compromise Procedures
In the event of a compromised RA credential, another Customer RA must ensure that the compromised credential is revoked.

5.7.4 Business Continuity Capabilities After a Disaster
In the event of a disaster that results in the compromise, loss, or destruction of all copies of the CA private signing key (including active, backup, escrowed, or archived instances), the Policy Authority (PA) SHALL be notified at the earliest feasible time.

The PA SHALL assess the impact of the disaster and determine whether CA operations may continue, must be suspended, or may be reestablished. Reestablishment of CA services, if permitted, MAY require generation of new cryptographic key material and issuance under a new CA certificate, subject to PA approval.

Certificates issued under a destroyed, lost, or compromised CA private signing key SHALL no longer be considered trustworthy. The Customer SHALL advise Relying Parties to discontinue reliance on certificates issued under the affected CA.

The CA SHALL maintain documented business continuity and disaster recovery plans that address disaster scenarios, including loss of facilities, systems, or cryptographic keys. These plans SHALL define recovery objectives, roles and responsibilities, and controls designed to ensure the integrity of CA operations. Such plans SHALL be reviewed, tested, and approved by the PA on a periodic basis.

5.8 CA Termination

In the event of termination because the Customer has terminated service, new Customer issuance and revocation operations will be rejected, and publication of certificate status will cease.

6.0 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation

6.1.1 CA Key Pair Generation

At the RA request, an API-based, automated, documented process to generate CA key pairs is executed.

The CA system will perform the following when generating a CA Key Pair:

1. Generate the CA Key Pair in a physically secured environment.
2. Generate the CA Key Pair within hardware cryptographic modules meeting the applicable requirements of §6.2.11
3. Log CA Key Pair generation activities.
4. Maintain adequate controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CP/CPS.

6.1.2 Subscriber Key Pair Generation

The Applicant or Subscriber must generate or initiate a new, secure, and cryptographically sound Key Pair to be used with the Subscriber's Certificate or Applicant's Certificate Application.

Generation of Subscriber key pairs by the CA is limited to Certificate Profiles that permit the use of the PKCS #12 format.

6.1.3 Key Delivery to Subscriber

In the case where the CA generates the Key Pair on behalf of the Subscriber, the Private Key will be delivered to the Subscriber in a cryptographically secure manner with at least 168-bit encryption strength in a PKCS #12 format.

6.1.4 Public Key Delivery to Certificate Issuer

Subscriber Public Keys are delivered to the CA in a Certificate Signing Request as part of the Certificate Application process.

6.1.5 CA Public Key Delivery to Relying Parties

The CA Public Keys are provided to the Relying Parties by the RA.

6.1.6 Key Sizes

For CA and Subscriber Certificates, the key sizes supported are:

- RSA 4096
- RSA 3072
- RSA 2048
- ECDSA P-521
- ECDSA P-384

- ECDSA P-256
- ML-DSA-44
- ML-DSA-65
- ML-DSA-87
- HASH-SLH-DSA-SHA2-128F-WITH-SHA256
- HASH-SLH-DSA-SHA2-192F-WITH-SHA512
- HASH-SLH-DSA-SHA2-256F-WITH-SHA512
- HASH-SLH-DSA-SHAKE-128F-WITH-SHAKE128
- HASH-SLH-DSA-SHAKE-192F-WITH-SHAKE256
- HASH-SLH-DSA-SHAKE-256F-WITH-SHAKE256
- MLDSA44-RSA2048-PSS-SHA256
- MLDSA44-RSA2048-PKCS15-SHA256
- MLDSA44-ECDSA-P256-SHA256
- MLDSA65-RSA3072-PSS-SHA512
- MLDSA65-RSA3072-PKCS15-SHA512
- MLDSA65-RSA4096-PSS-SHA512
- MLDSA65-RSA4096-PKCS15-SHA512
- MLDSA65-ECDSA-P256-SHA512
- MLDSA65-ECDSA-P384-SHA512
- MLDSA87-ECDSA-P384-SHA512
- MLDSA87-RSA3072-PSS-SHA512
- MLDSA87-RSA4096-PSS-SHA512
- MLDSA87-ECDSA-P521-SHA512

6.1.7 Public Key Parameters Generation and Quality Checking

CA Public Keys are generated and protected on a cryptographic module compliant with at least FIPS 140-2 Level 3 certification standards.

Subscriber Public Keys: No stipulation.

6.1.8 Key Usage Purposes

No stipulation.

6.2 Private Key Protection

6.2.1 Cryptographic Module Standards and Control
CA Private Keys must be used and unlocked on cryptographic modules that meet or exceed the requirements as defined in §6.2.11. The cryptographic modules are held in secure facilities.

6.2.2 CA Private Key Multi-Person Control
Upon activation of any CA Private Key, a minimum of two-person control will be established, and it may be implemented as a combination of technical and procedural controls. Resources involved in managing and using the CA Private Keys shall be Trusted Roles.

6.2.3 Private Key Escrow
CA Private Keys are not escrowed.

6.2.4 Private Key Backup
All copies of the CA's Private Key shall be protected in the same manner as the original.

6.2.5 Private Key Archival
CA Private Keys are not archived.

6.2.6 Private Key Transfer into or from Cryptographic Module
CA Private Keys shall be generated by and secured in a cryptographic module. Private Keys are backed up and restored to multiple HSMs to provide high availability and disaster recovery, while remaining secured within the boundary of the cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module
CA Private Keys are secured by a cryptographic module as defined in §6.2.11.

6.2.8 Method of Activating Private Keys
CA Private Keys are activated upon generation and available for automated signing of revocation data and RA-initiated certificate signing.

6.2.9 Private Key Deactivation Methods
CA Private Keys will be deactivated upon termination of service.

6.2.10 Private Signature Key Destruction Method
No stipulation.

6.2.11 Cryptographic Module Rating
CA Key Pairs are generated and protected on a cryptographic module that is compliant with at least FIPS 140-2 Level 3 certification standards.

6.3 Other Aspects of Key Pair Management
See below for the practice statement in other aspects of key pair Management.

6.3.1 Public Key Archival
CA public keys are archived.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

CA Certificate Key Pairs are not reused and therefore are valid for the life of the Certificate, up to, but no more than, 20 years.

There is no stipulation on the usage period of Subscriber certificate key pairs.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CA Private Key activation data is generated by Trusted Role personnel under two-person control using the methods provided by the HSM. If the activation data must be transmitted, it is protected from tampering or disclosure and transmitted separately from the associated cryptographic module.

Activation data for RA private keys is transmitted via an appropriately protected channel, and out-of-band from the associated cryptographic module.

6.4.2 Activation Data Protection

Access to CA Private Key activation data is restricted to Trusted Role personnel. Physical storage of CA Private Key activation data is secured under two-person control as described in §5.1.2.

Protection of activation data for RA private keys is the responsibility of the RA.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

See below for the practice statement on security control.

6.5.1 Specific Computer Security Technical Requirements

The CA systems are physically secure as described in §5.1. The CA systems enforce identification and authentication of users. All Trusted Roles that are authorized to have access to the CAs are required to use hardware tokens in conjunction with a PIN or biometric to gain access to the physical room that contains the CA key material being used for such CAs.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Technical Controls

See below for the practice statement on life-cycle technical controls.

6.6.1 System Development Controls

Systems developed by Entrust are deployed according to Entrust software lifecycle development standards.

6.6.2 Security Management Controls

The configuration of the CA system and any modifications and upgrades shall be documented and controlled. Methods of detecting unauthorized modifications to the CA system and configuration are

in place to ensure integrity of the security software, firmware, and hardware for correct operation. A formal configuration and change management methodology is used to install and maintain the CA system.

6.6.3 Life Cycle Security Controls
No stipulation.

6.7 Network Security Controls
A network firewall protects network access to the CA system. The network firewall limits services allowed to and from the CA system to those required to perform CA functions.

Protection of the CA system is provided against known network attacks. All unused network ports and services are turned off.

Boundary control devices used to protect the network on which PKI systems are hosted are configured to deny all but the necessary services to the CA system.

The CA, network, and all connected ancillary equipment hosted and operated are scanned no less than once per month using recognized tools designed to detect network and system vulnerabilities. The scanning tools are updated prior to each scan with the latest vulnerability signatures. Scans are performed inside the environment, and from outside the environment to identify vulnerabilities that must be mitigated. Identified vulnerabilities are remediated in accordance with the Entrust Patch and Vulnerability Management Standards.

All CA systems and all connected ancillary equipment hosted and operated by Entrust have active virus protection and mitigation as defined in the Entrust malware protection standard.

6.8 Time-stamping
The CA will record the time of all issued Certificates and recorded transactions using the system clock time derived, and periodically corrected, from a recognized time source.

7.0 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

CAs issue Certificates in accordance with the X.509 version 3. Certificate profiles for Root CA Certificate.

7.1.1 Version Numbers

The CA issues X.509 v3 Certificates (*version* field populated with integer "2").

7.1.2 Certificate Extensions

Certificate extensions are set as stipulated in IETF RFC 5280 and in accordance with Appendix A.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP/CPS shall use at least one of the following OIDs for signatures:

Signature Algorithm ID	OID
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) 2}
ecdsa-with-SHA384	ecdsa-with-SHA384 {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) 3}
ecdsa-with-SHA512	ecdsa-with-SHA512 {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) 4}
ML-DSA-44	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-44(17)}

Signature Algorithm ID	OID
ML-DSA-65	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-65(18)}
ML-DSA-87	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-87(19)}
HASH-SLH-DSA-SHA2-128F-WITH-SHA256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 36}
HASH-SLH-DSA-SHA2-192F-WITH-SHA512	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 38}
HASH-SLH-DSA-SHA2-256F-WITH-SHA512	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 40}
HASH-SLH-DSA-SHAKE-128F-WITH-SHAKE128	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 42}
HASH-SLH-DSA-SHAKE-192F-WITH-SHAKE256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 44}
HASH-SLH-DSA-SHAKE-256F-WITH-SHAKE256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 46}
MLDSA44-RSA2048-PSS-SHA256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 37}
MLDSA44-RSA2048-PKCS15-SHA256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 38}
MLDSA44-ECDSA-P256-SHA256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 40}
MLDSA65-RSA3072-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 41}
MLDSA65-RSA3072-PKCS15-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 42}
MLDSA65-RSA4096-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 43}

Signature Algorithm ID	OID
MLDSA65-RSA4096-PKCS15-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 44}
MLDSA65-ECDSA-P256-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 45}
MLDSA65-ECDSA-P384-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 46}
MLDSA87-ECDSA-P384-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 49}
MLDSA87-RSA3072-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 52 }
MLDSA87-RSA4096-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 53 }
MLDSA87-ECDSA-P521-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 54 }

Certificates under this CP/CPS will use the following OIDs for identifying the algorithm for which the subject key was generated:

Algorithm ID	OID
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
ecPublicKey	{iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) 1}
ML-DSA-44	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-44(17)}
ML-DSA-65	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-65(18)}
ML-DSA-87	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-87(19)}

Algorithm ID	OID
HASH-SLH-DSA-SHA2-128F-WITH-SHA256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 36}
HASH-SLH-DSA-SHA2-192F-WITH-SHA512	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 38}
HASH-SLH-DSA-SHA2-256F-WITH-SHA512	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 40}
HASH-SLH-DSA-SHAKE-128F-WITH-SHAKE128	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 42}
HASH-SLH-DSA-SHAKE-192F-WITH-SHAKE256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 44}
HASH-SLH-DSA-SHAKE-256F-WITH-SHAKE256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 4 3 46}
MLDSA44-RSA2048-PSS-SHA256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 37}
MLDSA44-RSA2048-PKCS15-SHA256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 38}
MLDSA44-ECDSA-P256-SHA256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 40}
MLDSA65-RSA3072-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 41}
MLDSA65-RSA3072-PKCS15-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 42}
MLDSA65-RSA4096-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 43}
MLDSA65-RSA4096-PKCS15-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 44}
MLDSA65-ECDSA-P256-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 45}
MLDSA65-ECDSA-P384-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 46}

Algorithm ID	OID
MLDSA87-ECDSA-P384-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 49}
MLDSA87-RSA3072-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 52 }
MLDSA87-RSA4096-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 53 }
MLDSA87-ECDSA-P521-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) alg(6) 54 }

For Certificates encrypted using ECDSA(ecPublicKey) algorithm, the following OIDs are supported to identify EC name curves:

EC Named Curves	OID
ECDSA P-256	{iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) 7}
ECDSA P-384	{iso(1) identified-organization(3) certicom(132) curve(0) 34}
ECDSA P-521	{iso(1) identified-organization(3) certicom(132) curve(0) 35}

7.1.4 Name Forms
The content of the certificate issuer DN field will match the subject DN of the issuing CA to support name chaining as specified in RFC 5280, section 4.1.2.4.

7.1.5 Name Constraints
The nameConstraints extension field is not used in CA Certificates.

7.1.6 Certificate Policy Object Identifier
See below for the practice statement on certificate policy object identifiers.

7.1.6.1 Reserved Certificate Policy Identifiers
No stipulation.

7.1.6.2 Root CA Certificates
Root CA Certificates do not contain the certificate policy object identifiers.

7.1.6.3 Issuing CA Certificates
No stipulation.

7.1.6.4 Subscriber Certificates
No stipulation.

7.1.7 Usage of Policy Constraints Extension
The policyConstraints extension is not used in CA Certificates.

7.1.8 Policy Qualifiers Syntax and Semantics
No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension
Certificate policies extension is marked Not Critical.

7.2 CRL Profile
The following fields of the X.509 version 2 CRL format are used by the CAs:

Field	Description
version	Set to v2
Signature	Identifier of the algorithm used to sign the CRL
Issuer	The full Distinguished Name of the CA issuing the CRL
This update	Time of CRL issuance
Next update	Time of next expected CRL update
Revoked Certificates	List of revoked Certificate information

7.2.1 Version Numbers
No stipulation.

7.2.2 CRL Entry Extensions
CRLs issued support the Authority Key Identifier, crlNumber, invalidityDate, and expiredCertsOnCRL extensions.

7.3 OCSP Profile
OCSP systems operated under this policy shall use OCSP requests and responses in accordance with RFC 6960.

7.3.1 Version Number(s)
No stipulation.

7.3.2 OCSP Extensions
Critical OCSP extensions are not used. OCSP responses include the nonce extension.

7.4 Certificate Profiles Reference

Entrust provides the following set of certificate profiles for authorities and end-entities.

Profiles	URL
Profiles for issuing authority Certificates	https://docs.pkiaas.entrust.com/profiles/browse/authority
Profiles for issuing subscriber Certificates	https://docs.pkiaas.entrust.com/profiles/browse/subscriber

8.0 COMPLIANCE AUDIT AND OTHER ASSESSMENT

8.1 Frequency or Circumstances of Assessment

The environment is assessed through a continuous, automated monitoring and alerting framework designed to provide real-time visibility into the security, integrity, and operational health of all PKI components, instead of periodic point-in-time audits/assessments.

This monitoring framework includes automated controls and system checks that validate configuration baselines, certificate lifecycle activities, CA security posture, access controls, system availability, and policy conformance. Alerts are generated and reviewed when deviations from expected configurations or compliance thresholds occur. This approach is designed to identify and remediate issues promptly, maintain ongoing compliance assurance, reduce operational risk, and support a proactive security and governance model consistent with modern cloud-based service delivery.

Entrust reserves the right to audit the environment at the direction of the Entrust PA.

8.2 Identity/Qualifications of Compliance Auditor

No Stipulation.

8.3 Compliance Auditor's Relationship to Audited Party

No stipulation.

8.4 Topics Covered by Compliance Audit

No stipulation.

8.5 Actions Taken as a Result of Deficiency

No stipulation.

8.6 Communication of Result

No stipulation.

9.0 OTHER BUSINESS AND LEGAL MATTERS

As per the applicable Agreement.

10.0 APPENDIX A – DEFINITIONS AND ACRONYMS

Term	Definition
Applicant	A person, entity, or organization applying for the issuance or renewal of a certificate.
Activation data	Data values, other than keys, that are required to operate cryptographic modules and that need to be protected – for example: • PIN • passphrases • manually held key share
Agreement	A legally binding contract for PKIaaS comprising: • The PKIaaS terms of use • The Entrust General Terms and Conditions available at https://www.entrust.com/general-terms.pdf • An Order for PKIaaS as defined in the General Terms
CA certificate	A certificate for the public key of a CA (Certificate Authority).
Certificate	A digital document issued by the CA that, at a minimum, meets the following: • Identifies the CA issuing it. • Names or otherwise identifies a Subject. • Contains a Public Key of a Key Pair. • Identifies its Operational Period. • Contains a serial number and is digitally signed by a CA. In this CP/CPS, “Certificate” means a certificate issued as part of PKIaaS.
Certificate revocation list (CRL)	A time-stamped list of the serial numbers of Certificates that have been revoked before the expiration of their validity periods
Certification authority (CA)	The technology to create, issue, manage, and revoke Certificates.

Term	Definition
Certificate issuance	The act performed by a CA in creating a certificate listing with the CA as "Issuer".
Certification practice statement (CPS)	A statement of the practices for a CA to issue, manage, revoke, renew, or re-key Certificates.
Cryptographic module	A software, device, or utility for: • Generating key pairs, • Storing cryptographic information. • Performing cryptographic functions.
Customer	The entity that has entered into a PKIaaS Agreement with Entrust.
Digital signature	The transformation of an electronic record by one person using a private key and public key cryptography so that another person having the corresponding public key can determine: • The record transformation was created using the private key corresponding to the public key. • The record has been altered since the transformation was made.
Issuing Certification Authority (Issuing CA)	In the context of a particular certificate, the issuing CA is the CA that issued the certificate.
Key generation	The process of creating a key pair.
Key pair	Two mathematically related cryptographic keys with the following properties. • A message encrypted with one key can only be decrypted with the other. • Even knowing one key, it is believed to be computationally infeasible to discover the other key.
Public cloud	Computing services provided by third-party providers over the public Internet.

Term	Definition
Object identifier (OID)	A unique alphanumeric identifier registered under the ISO registration standard to reference a specific object or object class. In this document, OIDs uniquely identify Certificates and cryptographic algorithms.
Online certificate status protocol (OCSP)	A protocol to validate certificate statuses in real time.
OCSP responder	A service that responds to certificate status requests with one of three responses. • Valid • Invalid • Unknown
Private key	The sensitive key in the key pair protected by the subject and kept secret. The private key can: • Create digital signatures. • Decrypt data previously encrypted using the corresponding public key.
Public key	The non-sensitive key in the key pair. This key: • Is submitted as part of a certificate signing request by the subscriber • Is disclosed in the subsequently-issued certificate. The public key can: • Verify digital signatures created using the corresponding private key. • Encrypt data meant for decryption with the corresponding private key
Public key cryptography	A type of cryptography also known as asymmetric cryptography. This cryptography uses a key pair rather than a single key to secure data authentication and confidentiality.

Term	Definition
Public key infrastructure (PKI)	The architecture, technology, practices, and procedures supporting a security system that uses Certificates and public key cryptography.
Registration Authority (RA)	An individual, organization or process responsible for verifying the identity of a subscriber.
Relying party	A Relying Party is a person, entity, or organization that relies on a Certificate and/or any other information provided in a Repository.
Repository	An online system for storing and retrieving Certificates and other information relevant to Certificates, including certificate validity or revocation information.
Certificate revocation	A permanent invalidation of a certificate from a specific time onward. Revocation includes: • Listing the certificate in CRL. • Preventing users from accessing the certificate once connected to the central infrastructure.
Request for comments (RFC)	A document series for communicating information about the Internet. Some RFCs are designated by the IAB (Internet Architecture Board) as Internet standards. Most RFCs document protocol specifications such as Telnet and FTP.
Root Certification Authority (Root CA)	A top-level CA. That is, a CA whose public key is not certified by another CA.
Subject	The individual, legal entity, organization, or device identified in a certificate. The subject holds the private key corresponding to the public Key in the certificate.
Subscriber	The person, legal entity, or organization that has applied for and has been issued a certificate. Before the identity verification and issuance of a certificate, a subscriber is an Applicant.
Trusted Role	An Entrust employee or contractor with authorized access to or control over PKIaaS.

Term	Definition
Validity period	The intended term of validity of a certificate. This period begins with the latter of the following dates: • The date of issuance stated in the "Issued On" certificate field. • The date stated in the "Valid From" or "Activation" certificate fields. The period ends with the earlier of two dates. If the Certificate has been revoked, the revocation date asserted in the CRL. This CRL is published in the distribution point within the Certificate.
X.500	A series of computer networking recommendation standards covering electronic directory services such as: • Directory access protocol (DAP) • Directory system protocol (DSP) • Directory information shadowing protocol (DISP) • Directory operational bindings management protocol (DOP)
X.509	A standard issued by the ITU-T (Technical committee of the International Telecommunication Union) for public key Certificates and certification path validation.

10.1 Acronyms

Acronym	Definition
ACME	Automatic Certificate Management Environment
ADCS	Microsoft Active Directory Certificate Services
ADDS	Microsoft Active Directory Domain Services
AES	Advanced Encryption Standard
AIA	Authority Information Access
CA	Certification Authority

Acronym	Definition
CAGW	Entrust CA Gateway (API)
CEG	Entrust Certificate Enrollment Gateway
CEP	Certificate Enrollment Policy
CLI	Command-line Interface
CLM	Certificate Lifecycle Management
CMC	Cryptographic Message Syntax
CMP	Certificate Management Protocol
CN	Common Name
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request (PKCS #10)
CSS	Certificate Status Server
CT	Certificate Transparency
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DNS	Domain Name System
ECDSA	Elliptic Curve Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECS	Entrust Certificate Services
EEE	End Entity Enrollment
EST	Enrolment over Secure Transport
FIPS	Federal Information Processing Standard

Acronym	Definition
FQDN	Fully Qualified Domain Name
JDK	Java Development Kit
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
LRA	Local Registration Authority
MDM	Mobile Device Management
MDMWS	Entrust's Mobile Device Management Web Service API
MS-XCEP	X.509 Certificate Enrollment Policy Protocol (CEP)
MS-WSTEP	WS-Trust X.509v3 Token Enrollment Extensions Protocol (WSTEP)
NIST	National Institute of Standards and Technology
PKIaaS	Public Key Infrastructure as a Service
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OTP	One-time Passcode
OVA	Open Virtual Appliance
P12	PKCS (Public Key Cryptography Standards) #12
PA	Policy Authority
PQ	Post-Quantum
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure

Acronym	Definition
RA	Registration Authority
REST	Representational State Transfer
RBAC	Role-Based Access Control
RDN	Relative Distinguished Name
RFC	Request for Comment
RHEL	Red Hat Enterprise Linux
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Subject Alternative Names
SCEP	Simple Certificate Enrollment Protocol
SIEM	Security Information and Event Management
SHA	Secure Hash Algorithms
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
TPM	Trusted Platform Module
URL	Uniform Resource Locator
UEM	Unified Endpoint Management
V2G	Vehicle-to-Grid
VM	Virtual Machine
WHFB	Windows Hello for Business

10.2 Distinguished name (DN) Identifiers

The unique identifier for a subject so it can be located in a directory based on the ITU/CCITT X.500. PKIaaS has no restriction on distinguished names per certificate profile; all certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2

Alias	OID
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

11.0 APPENDIX B – RELATED LINKS

Document	URL
PKIaaS Product Page	https://www.entrust.com/digital-security/certificate-solutions/products/pki/managed-services/pki-as-a-service
PKIaaS Terms and Conditions	https://www.entrust.com/legal-compliance/terms-conditions/entrust-managed-pki
Entrust PKIaaS customer guide	https://docs.pkiaas.entrust.com/

This page intentionally left blank.