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

Version 1.0

13 July 2026

This CP/CPS states and implements the policies and practice requirements of Entrust Verified PKIaaS, and all adopted changes.

Document Control

Issue	Date	Changes in this Revision
1.0	July 13, 2026	Initial Version for Verified PKIaaS.

SIGNATURE PAGE

JIM TROVATO

_____

Entrust Verified PKI as a Service Policy Authority (Print Name)

Signed by:
Jim Trovato
89D32B44D9C945B...

13 July 2026

_____ _____

Entrust Verified PKI as a Service Policy Authority (Signature)

Table of Contents

1.0 INTRODUCTION

1.1 Overview

This document constitutes the Certificate Policy and Certification Practice Statement (CP/CPS) for Verified PKI as a Service (Verified PKIaaS). This service provides a high assurance private trust public key infrastructure in which Certification Authority (CA) operations and specified Registration Authority (RA) functions are performed by Entrust within a controlled and audited environment.

Verified PKIaaS is fully hosted and operated, including the operation of hardware security modules (HSMs) within Entrust data centers. The environment is subject to independent audit in accordance with WebTrust for Certification Authorities criteria.

Under this model, Entrust, as the service provider, performs all CA roles associated with certificate issuance and lifecycle management. Entrust RAs or approved Enterprise RAs perform RA roles. Subscribers interact with the service through defined roles that enable administrative control and authorization of certificate requests within their organization.

This CP/CPS follows the structure of RFC 3647 and, where applicable, draws upon industry standards for high assurance public key infrastructures. Cryptographic and operational parameters defined in this section reflect the private trust model of this CP/CPS and may differ from requirements applicable to publicly trusted certificates.

In addition, this CP/CPS:

- Describes the policies, practices, and procedures governing the PKI participants identified in §1.3, the operation of Entrust Verified PKIaaS CAs and RAs, and the issuance, management, and use of Entrust Verified PKIaaS Certificates.

- Applies to all individuals, entities, and organizations that have a relationship with Entrust with respect to Certificates issued as part of Verified PKIaaS and/or any services provided by Entrust in connection with Verified PKIaaS, including without limitation Applicants, Subscribers, and Relying Parties.

- Is incorporated by reference into each Verified PKIaaS Agreement and each Subscriber Agreement.

- Applies exclusively to private trust services and does not govern publicly trusted certificates. The control framework is designed to meet applicable WebTrust for Certification Authorities criteria as applied to private PKI environments.

Subscribers and Relying Parties are responsible for reviewing the current version of this CP/CPS before accepting, using, or relying upon any Certificate that is generated through Entrust Verified PKIaaS.

1.2 Document Name and Identification

This document is called the Entrust Verified PKIaaS Combined X.509 Certificate Policy & Certification Practices Statement (Verified PKIaaS CP/CPS). This document replaces the Entrust Certificate Services Certification Practice Statement for Private Trust Certificates v.2.8 Nov 17, 2025 (Predecessor CPS)

Certificates issued by the Verified PKIaaS CAs MAY contain the Object Identifier arc:

- joint-iso-itu-t (2)
- Country (16)
- Us (840)
- Organization (1)
- Entrust (114027)
- cp (200)
- Verified PKIaaS (7)
- certificate type (X), or simply:

`2.16.840.1.114027.200.7.X` where X= Certificate type.

Certain CAs may continue to assert OIDs that were defined in the Predecessor CPS. Additional Policy OIDs remain valid for Certificates issued under those CAs.

Verified PKIaaS Policy OIDs

Object	Policy OID
object identifier arc	2.16.840.1.114027.200.7.
CP/CPS	2.16.840.1.114027.200.7.1
TLS Certificates	2.16.840.1.114027.200.7.2
TLS Certificates (Shared CA-OV)	2.16.840.1.114027.200.7.2.1
TLS Certificates (Shared CA-DV)	2.16.840.1.114027.200.7.2.2
TLS Certificates (TLS Dedicated CA - OV)	2.16.840.1.114027.200.7.2.5
TLS Certificates (TLS Dedicated CA - DV)	2.16.840.1.114027.200.7.2.6
Mobile Device Certificates	2.16.840.1.114028.10.1.9.4
Device Identity Certificates	2.16.840.1.114027.200.7.5.1
eSIM eUICC Manufacturer CA	2.23.146.1.2.1.2
eSIM SM-DP+ TLS Server Certificates	2.23.146.1.2.1.3
eSIM SM-DP+ Application Authentication Certificates	2.23.146.1.2.1.4
eSIM SM-DP+ Profile Binding Certificates	2.23.146.1.2.1.5
eSIM SM-DS TLS Server Certificates	2.23.146.1.2.1.6

Compliance information is available in the Repository at: www.entrust.com/legal-compliance/pki

1.3 PKI Participants

1.3.1 Policy Authority (PA)

Entrust is the Policy Authority (PA) for Entrust Verified PKIaaS. The PA is responsible for defining and approving certificate policy and certification practice requirements, appointing individuals to PKI roles, and overseeing compliance with applicable policies and standards.

The PA may delegate PKI operational oversight to an Operational Authority (OA) and may designate Policy Authority Representatives (PARs) to support monitoring of technical and service compliance.

The PA reviews, approves, and is the Entrust signatory for all Certificate Policy (CP) and Certification Practice Statement (CPS) updates.

1.3.2 Operational Authority (OA)

Entrust is the Operational Authority (OA) appointed by the Policy Authority (PA) and delegated day-to-day responsibility for ensuring that all 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.

1.3.3 Certification Authorities (CA)

The CA may accept Certificate Signing Requests (CSRs) and Public Keys from Applicants whose identity has been verified as provided herein by an RA. If a Certificate Application is verified, the verifying RA will send a request to a CA for the issuance of a Certificate. The CA will create a Certificate containing the Public Key and identification information contained in the request sent by the RA to that CA. The Certificate created in response to the request will be digitally signed by the CA.

Verified PKIaaS Certification Authorities are operated by Entrust for its Customers, and include CAs that are Shared CAs and Dedicated CAs. Compliance information regarding CAs is available in the Repository: www.entrust.com/legal-compliance/pki

1.3.4 Registration Authorities (RA)

RAs under the CA may accept Certificate Applications from Applicants and perform verification of the information contained in such Certificate Applications, according to the procedures established by the Policy Authority. An RA may send a request to such CA to issue a Certificate to the Applicant.

Only Entrust or Enterprise RAs approved by Entrust are permitted to perform RA functions under this CP/CPS. Entrust will only approve Enterprise RAs after an Entrust RA has verified the proposed Enterprise RA's authorization to act on behalf of the Enterprise.

An approved Enterprise RA may, as stated in this CPS:

i. Authorize certificate requests submitted by Subscribers within the Enterprise, confirming that the Subscriber is entitled, based on their affiliation with the Enterprise, to obtain the requested Certificate;

a. For TLS Certificates, authorize requests only where the Fully Qualified Domain Name (FQDN) is within a domain approved for the Subscriber's Enterprise, and the Subject organization name corresponds to a member of the Enterprise;

ii. Authorize the revocation of Certificates issued to a member of the Enterprise.

1.3.5 Subscribers

Subscribers may use Certificates to support transactions and communications. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant. The Customer determines which individuals and entities are entitled to be Applicants/Subscribers for Certificates under this CP/CPS.

1.3.6 Relying Parties

Relying Parties are any individuals or entities that rely on the validity of certificates issued under this CP/CPS. Relying Parties are responsible for evaluating whether a certificate is appropriate for their intended use and for verifying certificate status.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued under this CP/CPS are intended for use by Subscribers and Relying Parties in accordance with applicable agreements and for the purposes defined by the key usage and extended key usage fields included in the certificate.

Permitted uses include, but are not limited to:

- Authentication including system or Device authentication
- Digital signature, including code signing (where applicable)
- Encryption

Certificate usage SHALL be consistent with the defined assurance level, validation processes, and applicable service requirements.

1.4.2 Prohibited Certificate Uses

The use of all Certificates issued by the CA SHALL only be for lawful purposes and consistent with applicable laws, including without limitation, applicable export or import laws.

Certificates and related services are not intended for use in applications where failure of the Certificate could result in death, personal injury, or severe physical or property damage, including the monitoring, operation or control of nuclear facilities, mass transit systems, aircraft navigation or communications systems, air traffic control, weapon systems, medical devices or direct life support machines, and all such uses are prohibited.

Certificates SHALL not be relied upon outside the scope of the applicable certificate profile or intended application context.

1.5 Policy Administration

1.5.1 Organization Administering the Document
The CP/CPS is administered by Entrust.

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
The CP/CPS is administered by the Entrust Policy Authority (PA). The PA determines the suitability and applicability of change requests to this CP/CPS.

1.6 Definitions & Acronyms
See Appendix A.

2.0 PUBLICATION AND REPOSITORY RESPONSIBILITIES

Entrust maintains the authoritative Repository for Verified PKIaaS. This CP/CPS and CA Certificates are published through the Entrust Repository, and the most recently published version supersedes all prior editions upon its effective date.

2.1 Repositories

Entrust maintains Repositories to provide 24x7 web-based access to Certificate-related and revocation information. Repository content is updated periodically as specified in this CP/CPS and represents the authoritative source for CRLs and other Certificate information. Entrust operates in accordance with the latest version of the CP/CPS published in the Repository.

The compliance documentation Repository is available at: https://www.entrust.com/legal-compliance/pki.

2.2 This Publication of Certification Information

Entrust publishes its CP/CPS, CA Certificates and CRLs in the Repositories.

2.3 Time or Frequency of Publications

The CP/CPS is reviewed at least annually and is updated or re-issued as required in accordance with the applicable document control process.

2.4 Access Controls on Repositories

All information published in the Repository is designated as public information. The Certification Authority (CA) SHALL protect its Repositories from unauthorized access, modification, insertion, or deletion. Public read access to certificates, certificate status information (CRLs and/or OCSP responses), and approved policy and practice documentation SHALL be unrestricted. Write and administrative access to Repositories SHALL be limited to authorized personnel or trusted systems using authenticated, role-based access controls. Repository changes SHALL be authorized, logged, and monitored, and controls SHALL be in place to protect the integrity and availability of Repository information.

Archived documents are preserved to support audit, compliance, and non-repudiation requirements and are protected against unauthorized modification.

3.0 IDENTIFICATION AND AUTHENTICATION

The Policy Authority defines and mandates the identification and authentication requirements applicable to all entities operating under this CP/CPS, including CAs, RAs and Enterprise RAs.

Identification and authentication procedures are designed to ensure that only authorized individuals and systems are granted access to PKI functions and sensitive assets. These procedures may include, but are not limited to strong authentication mechanisms, role separation, and periodic access reviews.

The Policy Authority may update or refine identification and authentication requirements as necessary to address changes in security risk, regulatory requirements, or operational practices. Where applicable, Entrust may implement additional controls consistent with this CP/CPS and subject to approval by the Policy Authority.

3.1 Naming

The Policy Authority mandates the verification practices for verifying identification and authentication, and may, in its discretion, update such practices.

3.1.1 Types of Names

Before issuing a Certificate, the RAs ensure that all information in the Certificate conforms to the requirements of, and has been verified in accordance with, the procedures prescribed in this CP/CPS and matches the information confirmed and documented by the RA pursuant to its verification processes. RAs perform these functions under the oversight of the CA.

The Subject names in a Certificate comply with the X.501 Distinguished Name (DN) form. The CAs use a single naming convention as set forth below.

TLS Certificates	
Distinguished Name	(i) "Country Name" (C) which is the two-letter ISO 3166 code for the country of the Subscriber; (ii) "Organization Name" (O) which is the name of the Subscriber organization in the case of a corporation, partnership, or other entity; (iii) "Common Name" (CN) which is the hostname, the fully qualified hostname or path used in the DNS of the secure server; (iv) "Locality" (L), which is the city or locality of the Subscriber organization's place of business; and (v) "State" (ST) (if applicable), which is the state or province of the Subscriber organization's place of business.
"Subject Alternative Name" (SAN)	The fully qualified hostname or path used in the DNS of the secure server on which the Subscriber is intending to install the TLS Certificate. There may be multiple SANs in each Private TLS Certificate.

Mobile Device Certificates	
Distinguished Name	i. C="Country Name" (C) which is the two-letter ISO 3166 code for the country of the Subscriber; ii. O= "Organization Name" (O) which is the name of the Subscriber organization in the case of a corporation, partnership, or other entity; iii. OU = <organization unit of Subscriber> (optional) iv. CN =< A unique alpha-numeric identifier representing the Device, a Device name controlled by the Subscriber, or a combination of a unique alpha-numeric identifier and Device name, as approved by the Subscriber
Subject Alternative Name" (SAN)	An email address associated with the Device or Subscriber.

Client Authentication Certificates	
Distinguished Name	i. "Country Name" (C) which is the two-letter ISO 3166 code for the of the Subscriber; ii. "Organization Name" (O) which is the name of the Subscriber organization in the case of a corporation, partnership, or other entity; iii. "Common Name" (CN) which is the hostname, the fully qualified hostname or path used in the DNS of the secure server; iv. "Locality" (L), which is the city or locality of the Subscriber organization's place of business; and v. "State" (ST) (if applicable), which is the state or province of the organization's place of business.
Subject Alternative Name" (SAN)	The email address of the Subscriber.

3.1.2 Need for Names to be Meaningful

The Certificates issued pursuant to this CP/CPS are meaningful only if the names that appear in the Certificates can be understood and used by Relying Parties. Names used in the Certificates must identify the Subjects to which they are assigned in a meaningful way. RAs will not issue Certificates for Subjects that contain domain names, IP Addresses, DN, URL, and/or e-mail addresses that the Subscribers do not legitimately own or control. Examples of fields and extensions where these names appear include subject DN and subject alternative names.

TLS Certificates and Client Authentication Certificates: The value of the Common Name to be used in the Certificate is the Subscriber's fully qualified hostname or path that is used in the DNS of the

secure server on which the Subscriber is intending to install the Certificate. Notwithstanding the preceding sentence, the Common Name may include wildcard characters (i.e., an asterisk character).

3.1.3 Anonymity or Pseudonymity of Subscribers
International Domain Names (IDNs) will be verified and represented in the commonName and subjectAltName using Punycode.

3.1.4 Rules for Interpreting Various Name Forms
The CA interprets X.500 Distinguished Names in accordance with X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names
Names SHALL be defined unambiguously for each Subject in a Repository. The Distinguished Name attribute is to be unique and SHALL accurately identify the Subject to which it is issued.

3.1.6 Recognition, Authentication, and Role of Trademarks
Subscribers must not request Certificates with any content that infringes on the intellectual property rights of another entity. Entrust verifies trade names when they are submitted as part of the Organization Name in accordance with the applicable validation requirements. Except as otherwise specifically stated in this CP/CPS, Entrust does not verify an Applicant's right to use a trademark outside of the Organization Name and does not resolve trademark disputes. Entrust may reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key
For Key Pairs generated by the Applicant, the CA performs proof of possession tests for CSRs created using reversible asymmetric algorithms (such as RSA) by validating the signature on the CSR submitted by the Applicant with the Certificate Application.

3.2.2 Authentication of Organization Identity
The RA performs verification of any organizational identities that are submitted by an Applicant or Subscriber in accordance with the practices mandated by the Policy Authority. The RA determines whether the organizational identity and address provided with a Certificate Application are consistent with information contained in third-party databases and/or governmental sources. The information and sources used for the verification of Certificate Applications may vary depending on the jurisdiction of the Applicant or Subscriber.

In the case of organizational identities that are not registered with any governmental sources, the RA uses commercially reasonable efforts to confirm the existence of the organization. Such commercially reasonable efforts may include site visits or third-party attestation letters.

3.2.3 DBA/Tradename
If the Subject identity information includes a DBA or tradename, the RA SHALL verify the Applicant's right to use that name through a Reliable Data Source prior to requesting Certificate

issuance. For purposes of verifying a DBA or trade name, the Reliable Data Source must demonstrate the Applicant's legal right to use the name. Examples include, as applicable:

(i) Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
(ii) Communication with a government agency responsible for the management of such DBAs or trade names;
(iii) A third-party attestation letter accompanied by documentary support; or
(iv) A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

The RA uses a Reliable Data Source to verify that the registration of the DBA or tradename is valid.

3.2.4 Verification of Country

Verification of country will be done in accordance with the methods of §3.1.4.

3.2.5 Validation of Domain Authorization or Control

3.2.5.1 Fully Qualified Domain Names

TLS Certificates

The RA will confirm that prior to issuance, the RA validated each Fully Qualified Domain Name (FQDN) listed in the TLS Certificate using at least one of the methods listed below.

Completed validations of Applicant authority may be used for the issuance of multiple Certificates over time. For purposes of domain validation, the term Applicant includes the Applicant's Affiliate.

The RA maintains a record of which domain validation method was used to validate every domain:

(i) **Constructed Email to Domain Contact:** the RA confirms the Applicant's control over the FQDN by sending a verification email containing a CA-generated Random Value to a constructed domain contact email address and validating the Applicant's response.

The RA checks that the Applicant controls the domain by sending a unique Random Value to a constructed email address such as:

- admin@domain
- administrator@domain
- webmaster@domain
- hostmaster@domain
- postmaster@domain

The Applicant proves control by replying with the same Random Value.

- The value must be unique for each email and valid for up to 30 days.
- One email can be used to validate multiple FQDNs if the ADN used applies to all of them.

This confirms that the Applicant has control of the domain by showing they can access the designated constructed email address.

(ii) **Email to DNS TXT Contact**: the RA confirms the Applicant's control over the FQDN by emailing a unique Random Value to the email address listed in the domain's DNS TXT record. The Applicant proves control by replying with that same value.

- The email must go to an address published as the DNS TXT Record Email Contact.
- The value must be unique for each email and valid for up to 30 days.
- One email can validate multiple FQDNs provided the email address applies to all of them.

This confirms the Applicant has access to the email address defined in DNS for the domain.

(iii) **DNS TXT Change:** the RA confirms the Applicant's control over the FQDN by verifying the presence of a CA-generated Random Value in a DNS TXT record corresponding to an Applicable Domain Name (ADN).

The ADN may be used directly or with a prefixed Domain Label beginning with an underscore ("_").

- Random Value MUST be unique to the Certificate Request.
- The CA MUST NOT reuse the same Random Value after:
  - 30 days from its creation, or
  - If the Applicant submitted the Certificate Request, the expiration of the permitted reuse period for domain validation data applicable to that Certificate.

The RA MUST verify that the Random Value contained in the DNS TXT record matches the value provided by the CA, demonstrating the Applicant's control of the ADN and the corresponding FQDN.

(iv) **Agreed Upon Change to Website v2**: The RA confirms the Applicant's control over the FQDN or IP Address by verifying that the Applicant has published a Request Token or Random Value in a file that is retrievable over HTTP/HTTPS.

- The entire Request Token or Random Value MUST NOT appear in the HTTP request used to retrieve the file.
- The RA retrieves the file over HTTP or HTTPS and must receive a 2xx response code.
- The file must be located at: /. well-known/pki-validation/
- The file must be hosted on the Authorization Domain Name and accessed over an Authorized Port.

Redirects Handling: May be followed only if:

- Redirects are initiated at the HTTP protocol layer.
- Redirects result from HTTP 301, 302, 307, or 308 status codes as defined in RFC 7231 and RFC 7538.
- The CA follows redirects only to the final Location header value.
- Redirect targets use only the http or https scheme.

- Redirect targets are accessed over Authorized Ports.
- Redirects do not change the Authorization Domain Name being validated.

This confirms that the Applicant has control of the domain by proving they can modify content at a required location on the site.

(v) **Agreed Upon Change to Website – ACME**: Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in §8.3 of RFC 8555.

- The CA receives a successful HTTP response from the request (meaning a 2xx HTTP status code is received).
- The token (as defined in RFC 8555, §8.3) is not used for more than 30 days from its creation.

If CA follows redirects, the following apply:

- Redirects are initiated at the HTTP protocol layer.
- Redirects will be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, §6.4, or a 308 HTTP status code response, as defined in RFC 7538, §3.
- Redirects must be to the final value of the Location HTTP response header, as defined in RFC 7231, §7.1.2.
- Redirects must be to resource URLs with either the "http" or "https" scheme.
- Redirects must be to resource URLs accessed via Authorized Ports.

Note: The CAs will not issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is not used for validating Wildcard Domain Names.

(vi) **DNS TXT Change – ACME (DNS Labeled with Account ID – ACME):** Domain validation using the ACME DNS-01 challenge through the placement of a DNS TXT record at a domain name prescribed by the ACME protocol.

For this method, the validation token SHALL be cryptographically bound to the requesting ACME Account ID and uniquely associated with the Fully Qualified Domain Name (FQDN) or wildcard domain for which certification is requested. The DNS TXT record must be published by the Applicant within the authoritative DNS zone for the domain and must remain accessible for the duration of the validation process. Successful validation requires demonstration of effective control over the domain namespace by proving the Applicant's ability to create or modify DNS records under that domain. The CA SHALL only issue certificates when validation responses are verified as correct, complete, timely, and bound to the authenticated ACME account initiating the request.

The RA performs DNS-based domain validation by issuing an ACME DNS-01 challenge containing a nonce-based validation token derived from and bound to the Applicant's authenticated ACME Account ID.

The Applicant is instructed to publish the provided token value as a DNS TXT record at the designated challenge label (e.g., acme-challenge. <domain>).

Validation systems query authoritative DNS servers to confirm the presence and correctness of the TXT record and validate that the response corresponds to the expected account-bound token.

Once the challenge is successfully verified, the CA records evidence of validation, including the domain name, challenge type, validation timestamp, and ACME Account ID, and fulfills certificate issuance. Failed or expired challenges require revalidation prior to issuance.

3.2.5.2 Non-Fully Qualified Domain Names

RAs allow non-FQDN to be used. Non-FQDNs must be multi-label name or reserved IP Address. Each non-FQDN is reserved for one Subscriber for each CA used to issue TLS Certificates.

3.2.5.3 Authentication of an IP Address

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of an IP Address listed in a Certificate.

The RA will confirm that prior to issuance, the RA has validated each IP Address listed in the Certificate in support of Agreed Upon Change to Website v2 verification.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in §4.2.1.2 prior to Certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's Affiliate.

RAs will maintain a record of which IP Address validation method was used to validate every IP Address.

3.2.6 Wildcard Validation

The RAs follow a documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the Certificate "registry-controlled" label or is a "public suffix" (e.g. ".com, .co, .uk"), see RFC 6454 §8.2 for further explanation). If the FQDN portion of any Wildcard Domain Name is registry-controlled or is a "public suffix", the RA will refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace.

3.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the RA evaluates the source for its reliability, accuracy, and resistance to alteration or falsification.

3.2.8 CAA Records

No additional requirements beyond those defined in this CP/CPS.

3.2.9 Authentication of Email Address

No additional requirements beyond those defined in this CP/CPS.

3.2.10 Authentication of Registered Trademark

No additional requirements beyond those defined in this CP/CPS.

3.2.11 Authentication of Individual Identity

The CA does not issue Certificates to individual human Subscribers, where the name of the individual would be included in the Subject field, except in the case where the individual's name is part of an organization identity, in which case it is verified only in accordance with §3.2.2.

3.2.12 Non-verified Subscriber Information

All Certificate request information provided by the Subscriber is verified in accordance using an independent source of information or an alternative communication channel before it is included in the Certificate.

3.2.13 Validation of Authority

The CA allows a Subscriber to specify the individuals who may request Certificates and will not accept any Certificate requests that are outside this specification.

Entrust RAs will verify the authority of a Subscriber Representative by either checking or using a Reliable Data Source to confirm the individual's employment within the Subscriber's Enterprise.

Entrust RAs will verify the authority of a proposed Enterprise RA by using a reliable method of communication (which may be via email) to contact the Subscriber Representative and obtaining the Subscriber Representative's confirmation (which may be by clicking an "I agree" button) of the Enterprise RA's authority to act on behalf of an Enterprise.

The CA will provide the Subscriber with a list of its Subscriber Representative, Enterprise RA, and other authorized individuals upon the Subscriber's verified written request.

3.2.14 Criteria for Interoperation

No additional requirements beyond those defined in this CP/CPS.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Each Certificate includes an expiration date. Certificate expiration limits the period during which the associated Key Pair may be exposed or compromised. Accordingly, when submitting a new Certificate Application, Entrust recommends generating a new Key Pair and including the new Public Key in the application.

If a Subscriber wishes to continue using a Certificate beyond its expiration date, the Subscriber must obtain a new Certificate and replace the one that is expiring. Subscribers submitting a new Certificate Application are required to complete the initial application process as described in §4.1. The RA may reuse documents and data previously provided under §3.2 to verify Certificate information in accordance with §4.2.1.

The RA that processes a Subscriber's Certificate Application will make a commercially reasonable effort to notify the Subscriber of the Certificate's upcoming expiration by sending an email to the technical contact identified in the Certificate Application. Upon expiration, the Subscriber must immediately discontinue use of the Certificate and remove it from any Devices and/or software in which it has been installed.

The Subscriber may request a replacement Certificate using an existing Key Pair.

3.3.2 Identification and Authentication for Re-key after Revocation

The CA does not renew Certificates that have been Revoked. If a Subscriber wishes to continue using a Certificate after it has been Revoked, the Subscriber must submit a new application and obtain a replacement Certificate. To receive a new Certificate, the Subscriber is required to complete the full initial application process, as described in §4.1. Upon revocation, the Subscriber must immediately discontinue use of the Certificate and remove it from all Devices and software where it has been installed.

3.3.3 Identification and Authentication for Revocation Requests

A Subscriber may request revocation of their Certificate at any time provided that the Enterprise RA can validate the Subscriber is the person, organization, or entity to whom the Certificate was issued. The Enterprise RA will authenticate a request from a Subscriber for revocation of their Certificate by authenticating the Subscriber or confirming authorization of the Subscriber through a reliable method of communication. Upon receipt and confirmation of such information, the RA will then process the revocation request as stipulated in §4.9.

An Enterprise RA may use multi-factor authentication to request revocation of a Certificate.

4.0 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

To obtain a Certificate, an Applicant must:

(i) Generate a secure and cryptographically sound Key Pair, if not generated by a CA
(ii) Agree to the terms and conditions of this CP/CPS and the Subscriber Agreement, and
(iii) Complete and submit a Certificate Application, providing all information requested by an RA without any errors, misrepresentation, or omissions.

Upon completion of the Certificate Application and acceptance of the terms and conditions of this CP/CPS and the Subscriber Agreement, an RA follows the procedures described in §3.2 to perform verification of the information contained in the Certificate Application. If the verification performed by an RA is successful, the RA may, in its sole discretion, request the issuance to the Applicant of a Certificate from a CA.

4.1.1 Who Can Submit a Certificate Application

Either the Applicant or an individual authorized to request Certificates on behalf of the Applicant may submit Certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to the RA.

4.1.2 Enrollment Process and Responsibilities

The CA requires that each Applicant submit a Certificate request and application information prior to issuing a Certificate. The CA or RA authenticates all communication from an Applicant and protects against modification.

Applicants request a Certificate by completing the request forms online. Applicants are solely responsible for submitting a complete and accurate Certificate request for each Certificate.

The enrollment process includes:

i. Submitting a complete Certificate application,
ii. Generating a Key Pair, and
iii. Delivering the Public Key of the Key Pair to the CA.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The CAs and RAs may use the documents and data provided under §3.2 to verify Certificate information. They may also reuse previous validations, provided that the data or documentation was originally obtained from a source specified in §3.2, and CA or the RA performed the initial validation no more than 398 days prior to the reuse.

4.2.2 Approval or Rejection of Certificate Applications

No additional requirements beyond those defined in this CP/CPS.

4.2.3 Time to Process Certificate Applications
No additional requirements beyond those defined in this CP/CPS.

4.2.4 Certification Authority Authorization Records
No additional requirements beyond those defined in this CP/CPS.

4.3 Certificate Issuance
After performing verification of the information provided by an Applicant in a Certificate Application, a Registration Authority (RA) may request that the CA issue a Certificate. Upon receipt of a valid and authorized request from an RA, the CA may generate and digitally sign the Certificate in accordance with the Certificate profile described in §7.

An Enterprise Registration Authority (Enterprise RA) if approved by the PA, may operate within an approved Enterprise environment and is responsible for performing identity and authorization verification in accordance with Enterprise-specific policies and procedures. An Enterprise RA may authorize Certificate issuance on behalf of the Enterprise and submit a Certificate request to the CA.

4.3.1 CA Actions During Certificate Issuance
The CA is responsible for the final decision to approve and issue Certificates, based on information provided by the RA.

The CA enforces multi-factor authentication for all accounts capable of causing Certificate issuance or performing Registration Authority functions.

4.3.2 Manual Authorization of Certificate Issuance for Root CAs
Certificate issuance by the Root CA SHALL require at least two individuals authorized by the CA.

Root CA Private Keys will not sign Subscriber Certificates.

4.3.3 Issuance of Subscriber Certificate
The CA will not issue Certificates with a validity period that exceeds that of the corresponding issuing CA Certificate with the following exception:

- For Certificate types where no well-defined expiration date exists in applicable standards (e.g., Device Identity Certificates), the notAfter value SHALL be set to 99991231235959Z.

4.3.4 Linting of To-be-signed Certificate Content
Entrust MAY use pre-issuance Linting to validate issued Certificates against applicable standards and requirements, including RFC 5280 and relevant certificate policies and profiles.

4.3.5 Linting of Issued Certificates
Entrust uses post-issuance Linting to validate issued Certificates against applicable standards and requirements, including RFC 5280 and relevant certificate policies and profiles.

4.3.6 Notification to Subscriber by the CA of Issuance of Certificate
Once a Certificate has been generated and placed in a Repository, the CA that issued the Certificate uses commercially reasonable efforts to notify the Applicant that the Applicant’s Certificate is

available. The communication may contain a URL for use by the Applicant to retrieve the Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance
No additional requirements beyond those defined in this CP/CPS.

4.4.2 Publication of the Certificate by the CA
No additional requirements beyond those defined in this CP/CPS.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities
No additional requirements beyond those defined in this CP/CPS.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage
Subscribers SHALL conform to §9.6.3.

4.5.2 Relying Party Public Key and Certificate Usage
Relying Parties SHALL conform to §9.6.4.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal
CAs or RAs may provide a Certificate lifecycle monitoring service which will support Certificate renewal.

4.6.2 Who May Request Renewal
Subjects, Subscribers or Subscriber agents may request renewal of Certificates.

4.6.3 Processing Certificate Renewal Requests
CAs or RAs will process Certificate renewal requests with validated verification data. Previous verification data may be used as specified in §4.2.1.

Certificates may be renewed using the previously accepted Public Key, if the Public Key meets the key size requirements of §6.1.5.

4.6.4 Notification of New Certificate Issuance to Subscriber
CAs or RAs will provide Certificate renewal notification to the Subscriber or Subscriber agents through an Internet link or by email.

Subscribers or Subscriber agents may request that email renewal notices are not sent for their expiring Certificates.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate
No additional requirements beyond those defined in this CP/CPS.

4.6.6 Publication of the Renewal Certificate by the CA
CAs or RAs will provide the Subscriber with a Certificate through an Internet link.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities
No additional requirements beyond those defined in this CP/CPS.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key
No additional requirements beyond those defined in this CP/CPS.

4.7.2 Who May Request Certification of a New Public Key
No additional requirements beyond those defined in this CP/CPS.

4.7.3 Processing Certificate Re-keying Requests
No additional requirements beyond those defined in this CP/CPS.

4.7.4 Notification of New Certificate Issuance to Subscriber
No additional requirements beyond those defined in this CP/CPS.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate
No additional requirements beyond those defined in this CP/CPS.

4.7.6 Publication of the Re-keyed Certificate by the CA
No additional requirements beyond those defined in this CP/CPS.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities
No additional requirements beyond those defined in this CP/CPS.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification
No additional requirements beyond those defined in this CP/CPS.

4.8.2 Who May Request Certificate Modification
No additional requirements beyond those defined in this CP/CPS.

4.8.3 Processing Certificate Modification Requests
No additional requirements beyond those defined in this CP/CPS.

4.8.4 Notification of New Certificate Issuance to Subscriber
No additional requirements beyond those defined in this CP/CPS.

4.8.5 Conduct Constituting Acceptance of Modified Certificate
No additional requirements beyond those defined in this CP/CPS.

4.8.6 Publication of the Modified Certificate by the CA
No additional requirements beyond those defined in this CP/CPS.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities
No additional requirements beyond those defined in this CP/CPS.

4.9 Certificate Revocation and Suspension
The CA Revokes a Certificate upon receiving a valid Revocation request from an authorized RA. An RA may request Revocation after receiving a valid Revocation request from the Subscriber. An RA must request Revocation if it becomes aware of any event requiring the Subscriber to stop using the Certificate.

CAs do not support the suspension of Certificates.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate
The CA may Revoke a Subscriber's Certificate—and an RA must request Revocation—if the CA or RA knows, or has reasonable grounds to believe, that any of these events have occurred:

(i)	The Subscriber requests in writing that the CA Revoke the Certificate.
(ii)	The Subscriber notifies the CA that the original Certificate request was not authorized and does not retroactively grant authorization.
(iii)	The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise.
(iv)	The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).
(v)	The CA obtains evidence that the validation of the domain authorization or control for any FQDN or IP Address in the Certificate should not be relied upon.
(vi)	The Certificate no longer complies with the requirements of §6.1.5 and §6.1.6.
(vii)	The CA obtains evidence that the Certificate was misused.
(viii)	The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement.
(ix)	The CA is made aware of any circumstance indicating that use of a FQDN or IP Address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name).

(x)	The CA is made aware that a Certificate with a Wildcard Domain Name has been used to authenticate a fraudulently misleading subordinate FQDN.
(xi)	The CA is made aware of a material change in the information contained in the Certificate.
(xii)	The CA is made aware that the Certificate was not issued in accordance with this CP/CPS.
(xiii)	The CA determines that any of the information appearing in the Certificate is inaccurate.
(xiv)	Revocation is required by any other section in this CP/CPS.
(xv)	The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.
(xvi)	The technical content or format of the Certificate presents an unacceptable risk to Relying Parties.
(xiv)	A Certificate is used to digitally sign hostile code, including spyware or other malicious software (malware).
(xv)	Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of a Certificate or CA.

4.9.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA may Revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

(i) Subordinate CA requests Revocation in writing.
(ii) The Subordinate CA notifies the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization.
(iii) The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of §6.1.5 and §6.1.6.
(iv) The Issuing CA obtains evidence that the Certificate was misused.
(v) The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP/CPS.
(vi) The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading.
(vii) The Issuing CA or Subordinate CA ceases operations for any reason and has not planned for another CA to provide Revocation support for the Certificate.
(viii) Revocation is required by the Issuing CA's CP/CPS.

4.9.2.1 Who Can Request Revocation

Certificate Authorities (CAs), Registration Authorities (RAs), and Enterprise Registration Authorities (Enterprise RAs) may initiate revocation.

An RA, or Enterprise RA may authorize revocation of a Subscriber's Certificate at any time and for any reason, including in response to a Subscriber's request to Revoke their own Certificate. When requesting Revocation authorization, the Subscriber shall validate their identity to the RA. Neither the CA nor the RA is required to act on a Revocation request until the RA has completed the required authorization.

Subscribers may submit Certificate Problem Reports to inform the CA or RA of a reasonable cause to Revoke the Certificate.

4.9.3 Procedure for Revocation Request

A Subscriber must request Revocation of their Certificate if they suspect, know, or have reasonable grounds to believe that any of the following have occurred:

- Key compromise of the Subscriber's Private Key.
- Knowledge that the original Certificate request was unauthorized and will not be retroactively authorized.
- A change in the information contained in the Certificate.
- A change in circumstances causing Certificate information to become inaccurate, incomplete, or misleading.

A Subscriber's Revocation request is verified by the RA.

If a Certificate is Revoked for any reason, the Subscriber will be notified by email sent to the Enterprise RA. Revocation does not alter the Subscriber's contractual obligations under this CP/CPS and the Subscriber Agreement.

Subscribers may submit a CPR using the contact information provided in §1.5.2.

4.9.4 Revocation Request Grace Period

In the case of Private Key Compromise, or suspected Private Key Compromise, a Subscriber SHALL request the Revocation of the corresponding Certificate immediately upon detection of the Key Compromise or suspected Key Compromise. Revocation requests for other required reasons should be made as soon as reasonably practicable.

4.9.5 Time within Which CA Must Process the Revocation Request

The CA will process the request to Revoke the Certificate immediately and post the Revocation in the next CRL update.

4.9.6 Revocation Checking Requirement for Relying Parties

A Relying Party is expected to verify whether a Certificate on which it intends to rely has been Revoked. Such verification should be performed by consulting the applicable Certificate Revocation Lists maintained in the appropriate Repository or by conducting an online Revocation status check using OCSP. Under no circumstances SHALL Entrust Group be liable for damages arising from (i) a Relying Party's failure to verify the Revocation or expiration status of a Certificate, or (ii) any reliance placed on a Certificate that has been Revoked or has expired.

4.9.7 CRL Issuance Frequency

The CA issues Certificate Revocation Lists (CRLs) as follows:

(i) CRLs for Certificates issued to Subordinate CAs are published at least once every twelve months, and within 24 hours following the Revocation of a Subordinate CA Certificate.
(ii) CRLs for Subscriber Certificates are published at least once every 24 hours.

4.9.8 Maximum Latency for CRLs

No additional requirements beyond those defined in this CP/CPS.

4.9.9 On-line Revocation/Status Checking Availability

If specified in the Certificate, the CA provides OCSP response information for issued Certificates.

4.9.10 On-line Revocation Checking Requirements

The CAs support OCSP capability using the GET method as described in RFC6960 and/or RFC 5019 for Certificates issued in accordance with this CP/CPS.

The CAs sign and make available OCSP as follows:

- OCSP responses for Certificates issued to Subordinate CAs are issued at least once every twelve months or within 24 hours after Revoking a Subordinate CA Certificate.
- OCSP responses for Subscriber Certificates are issued at least once every 24 hours.

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

No additional requirements beyond those defined in this CP/CPS.

4.9.12 Special Requirements Re Key Compromise

If a Subscriber suspects or becomes aware that the Private Key corresponding to the Public Key contained in their Certificate has been Compromised, the Subscriber SHALL immediately notify the RA that processed the Certificate Application, using the procedures set forth in §3.4. Upon such suspicion or knowledge, the Subscriber SHALL immediately cease using the Certificate and SHALL remove it from all Devices and software in which it has been installed. The Subscriber is responsible for investigating the circumstances of the actual or suspected Compromise and for notifying any Relying Parties that may have been affected.

Subscribers may report a Private Key Compromise to the CA using one of the following demonstration methods:

- Submission of a signed CSR with a common name of “Proof of Key Compromise for Entrust”.
- Submission of the Private Key.

4.9.13 Circumstances for Suspension

The Repository will not include entries that indicate that a Certificate has been suspended.

4.9.14 Who Can Request Suspension
Not applicable**.**

4.9.15 Procedure for Suspension Request
Not applicable.

4.9.16 Limits on Suspension Period
Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics
Certificate status information may be available via CRL and OCSP responder. The Repository is available via HTTP. The serial number of a Revoked Certificate remains on the CRL for at least one CRL issuance after the validity period of the Certificate expires.

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.

The CA maintains an online 24x7 Repository for application software to automatically check the status of all unexpired Certificates issued by the CA.

4.10.3 Optional Features
No additional requirements beyond those defined in this CP/CPS.

4.11 End of Subscription
No additional requirements beyond those defined in this CP/CPS.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy Practices
No additional requirements beyond those defined in this CP/CPS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices
No additional requirements beyond those defined in this CP/CPS.

5.0 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Security Controls

5.1.1 Site Location and Construction

Entrust hosts and operates the CAs from secure facilities. The CA equipment is located inside a security zone that is physically separated from Entrust's corporate systems with access restricted to personnel in Trusted Roles. The security zone is protected by electronic control access systems, alarmed doors and is monitored via a 24x7 recorded security camera and motion detector system.

5.1.2 Physical Access

Entrust operates the CAs within data centers that provide physical protection for systems that process high-value, sensitive information. The buildings are located outside flood and known earthquake zones. The physical protection mechanisms provided at these sites include:

- Badge access to facility;
- Access verification controls (badge and biometric required to access data center floor);
- Security (alarm) systems for both the facility and cages;
- 24x7x365 security guard staffing and monitoring;
- Video surveillance and recording via closed circuit TV;

5.1.3 Power and Air Conditioning

Entrust operates the CAs within secure data centers that are equipped with the following:

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

These environmental controls conform to local standards and are appropriately secured to prevent unauthorized access and/or tampering with the equipment.

5.1.4 Water Exposures

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 on the activation of multiple fire alarms.

5.1.5 Fire Prevention and Protection

The CA facilities are protected by fire detection, alarm, and suppression systems and comply with applicable local commercial building codes for fire prevention and protection. Periodic inspections, testing and maintenance of all systems are performed by facility personnel and/or system providers to ensure proper function.

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. Archived material is stored in a room separate from the CA equipment until it is transferred to the archive storage facility.

5.1.7 Waste Disposal
Waste is removed or destroyed in accordance with industry best practice. Media used to store sensitive data is destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-site Backup
As stipulated in §5.5.

5.2 Procedural Controls

5.2.1 Trusted Roles
The CAs have a number of Trusted Roles appointed by the PA and authorized for sensitive operation of the CA software. The controls detailed in this CP/CPS are implemented and maintained by authorized personnel in Trusted Roles.

5.2.2 Number of Persons Required per Task
CA Private Key management operations, including key generation, backup, and destruction, shall be performed under dual control. At least two authorized individuals must be present and participate in each operation. These activities shall be conducted within a physically secured environment with appropriate access controls to prevent unauthorized access.

5.2.3 Identification and Authentication for Each Role
Personnel in Trusted Roles must undergo background investigations, must be trained for their specific role, and are appointed by the PA.

5.2.4 Roles Requiring Separation of Duties
Roles requiring a separation of duties include those performing:

(i) Authorization functions including verification of information in Certificate Applications and approvals of Certificate Applications and Revocation requests;
(ii) CA systems management and cryptographic key life cycle management;
(iii) CA systems development;
(iv) Compliance management: overall responsibility for administering the implementation of the CA's security practices, maintenance of policy and practices; and
(v) Security operations: continuous monitoring, detection, analysis, and response to security threats affecting an organization's information systems and data

5.3 Personnel Controls
Operational personnel for a CA will not be assigned other responsibilities that conflict with their operational responsibilities for the CA. The privileges assigned to operational personnel for a CA will be limited to the minimum required to carry out their assigned duties.

5.3.1 Qualifications, Experience and Clearance Requirements
Prior to the engagement of any person in the Certificate management process, the CA or RA will verify the identity and trustworthiness of such person.

5.3.2 Background Check Procedures
No additional requirements beyond those defined in this CP/CPS.

5.3.3 Training Requirements
Personnel in Trusted Roles and validation specialist roles complete skills-training based on industry requirements.

Validation specialists who perform information verification duties complete skills-training that covers basic PKI knowledge, authentication and vetting policies and procedures (including this CP/CPS), and common threats to the information verification process (including phishing and other social engineering tactics).

Validation specialists receive skills-training prior to commencing their job role and are required to pass an examination on the applicable information verification requirements. The CA maintains records of such training and ensures that personnel entrusted with validation specialist duties maintain an appropriate skill level.

5.3.4 Retraining Frequency and Requirements
CAs and RAs provide refresher training and informational updates sufficient to ensure that all personnel in Trusted Roles retain the requisite degree of expertise.

5.3.5 Job Rotation Frequency and Sequence
No additional requirements beyond those defined in this CP/CPS.

5.3.6 Sanctions for Unauthorized Actions
No additional requirements beyond those defined in this CP/CPS.

5.3.7 Independent Contractor Requirements
No additional requirements beyond those defined in this CP/CPS.

5.3.8 Documentation Supplied to Personnel
No additional requirements beyond those defined in this CP/CPS.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded
The CAs and all RAs operating under a CA record in detail every action taken to process a Certificate request and to issue a Certificate, including all information generated or received in connection with a Certificate request, and every action taken to process the Request, including time, date, and personnel involved in the action.

The foregoing record requirements include, but are not limited to, an obligation to record the following CA Certificate key lifecycle events, including:

a. Key generation, backup, storage, recovery, archival, and destruction;
b. Certificate requests, renewal and re-key requests, and Revocation;
c. Approval and rejection of Certificate requests;
d. Cryptographic device lifecycle management events;

e. Generation of CRLs
f. Signing of OCSP responses; and
g. Introduction of new Certificate profiles and retirement of existing Certificate profiles.

Subscriber Certificate lifecycle management events, including:

h. Certificate requests, renewal and re-key requests, and Revocation;
i. All verification activities required by this CP/CPS;
j. Approval and rejection of Certificate requests;
k. Issuance of Certificates; and
l. Generation of CRLs
m. Signing of OCSP responses.

Security events, including:

n. Successful and unsuccessful PKI system access attempts;
o. PKI and security system actions performed;
p. Security profile changes;
q. System crashes, hardware failures, and other anomalies;
r. Firewall and router activities; and
s. Entries to and exits from the CA facility.

Log entries include the following elements:

t. Date and time of event;
u. Identity of the person making the journal record; and
v. Description of event.

5.4.2 Frequency of Processing Log

No additional requirements beyond those defined in this CP/CPS

5.4.3 Retention Period for Audit Log

The CA will retain for at least two years:

(i) CA Certificate and key lifecycle management event records, as set forth in §5.4.1(i), after either: the destruction of the CA Private Key, or the revocation or expiration of the CA Certificate, whichever occurs later;
(ii) Subscriber Certificate lifecycle management event records, as set forth in §5.4.1(ii), after the expiration of the Subscriber Certificate; and
(iii) Any security event records, as set forth in §5.4.1(iii), after the event occurred.

5.4.4 Protection of Audit Log

No additional requirements beyond those defined in this CP/CPS.

5.4.5 Audit Log Backup Procedures

No additional requirements beyond those defined in this CP/CPS.

5.4.6 Audit Collection System

No additional requirements beyond those defined in this CP/CPS.

5.4.7 Notification to Event-causing Subject

No additional requirements beyond those defined in this CP/CPS.

5.4.8 Vulnerability Assessments

Risk is managed through automated monitoring and periodic reviews conducted at the discretion of the Policy Authority. This process supports ongoing identification of foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of Certificate data or Certificate management processes. Based on the results of these activities, a security plan may be established, maintained, and updated as necessary under the direction of the PA and OA to manage and control identified risks.

Entrust regularly assesses Certificate management systems and the supporting infrastructure for vulnerabilities. Assessments are performed on a regular basis and after significant changes, security incidents, or newly disclosed vulnerabilities that may affect CA operations. Vulnerabilities are risk-ranked, remediated, or formally accepted within severity-based timeframes, and tracked to closure. Assessment results, remediation actions, exceptions, and risk acceptance decisions are documented and retained as audit records. Results are considered as input to the CA's broader security plan.

5.5 Records Archival

5.5.1 Types of Records Archived

The audit trail files, databases and revocation information for the CAs are archived.

5.5.2 Retention Period of for Archive

The CA will retain all documentation relating to Certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least two years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

Archived records are stored in a manner that protects them from unauthorized deletion or destruction for the duration of the required retention period, except where transfer to replacement media is required.

Entrust ensures that archive storage preserves the integrity, authenticity, and confidentiality of archived data, and that only authorized roles may perform archive management operations.

If the original storage media cannot reliably retain data for the required retention period, archived records shall be migrated to replacement media or storage systems that provide equivalent protection.

5.5.4 Archive Backup Procedures

No additional requirements beyond those defined in this CP/CPS.

5.5.5 Requirements for Time-stamping of Records

The time for the CA systems is synchronized with a recognized UTC(k) laboratory or National Measurement Institute to ensure accurate time stamps (non-cryptographic) on archived records.

5.5.6 Archive Collection System

No additional requirements beyond those defined in this CP/CPS.

5.5.7 Procedures to Obtain and Verify Archive Information
No additional requirements beyond those defined in this CP/CPS.

5.6 Key Changeover
CAs' Key Pairs will be retired from service at the end of their respective lifetimes as defined in §6.3. 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. The CA key changeover process will be performed such that it causes minimal disruption to Subscribers and Relying Parties.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures
CAs have a security incident response plan, a disaster recovery plan, and a business continuity plan to provide for timely recovery of services in the event of a security incident, breach of security, loss of system integrity, or system outage. Incidents and compromises are handled in accordance with documented procedures defined for the service.

They address the following:

(i) the conditions for activating the plans;
(ii) resumption procedures;
(iii) a maintenance schedule for the plan;
(iv) awareness and education requirements;
(v) the responsibilities of the individuals;
(vi) testing of recovery plans.

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

(vii) secure on-site and off-site storage of backup HSMs containing copies of all CA Private Keys
(viii) secure on-site and off-site storage of all requisite activation materials
(ix) regular synchronization of critical data to the disaster recovery site
(x) regular incremental and daily backups of critical data within the primary site
(xi) environmental controls as described in §5.1
(xii) High availability architecture for critical systems

Entrust has policies and procedures that will be employed in the event of CA Key Compromise. At a minimum, all Subscribers will be informed as soon as practicable of such a Key Compromise and information will be posted in the Repository.

5.7.2 Computing Resources, Software and/or Data are Corrupted
No additional requirements beyond those defined in this CP/CPS.

5.7.3 Entity Private Key Compromise Procedures
No additional requirements beyond those defined in this CP/CPS.

5.7.4 Business Continuity Capabilities after a Disaster

No additional requirements beyond those defined in this CP/CPS.

5.8 CA or RA Termination

When termination of a CA becomes necessary, the CA will take reasonable steps to minimize disruption to Subscribers, Relying Parties, and dependent systems and will provide advance notice of termination to affected Customers where commercially and operationally feasible.

Upon termination of CA operations, the CA Revokes all unexpired Certificates issued under the CA and publishes final CRLs unless one or more of the following conditions apply:

(i) A qualified successor CA assumes responsibility for certificate lifecycle management and validation services;

(ii) The Certificate is a Device Identity Certificate or other constrained-use Certificate and is governed by an approved lifecycle or trust model that does not require Revocation at CA termination;

(iii) It is determined by the PA that Revocation is technically infeasible or would introduce greater operational or security risk than continued validity, provided that compensating controls are documented and approved.

The CA ensures that Certificate status information services are maintained or transferred to a qualified successor for an appropriate duration necessary to support Relying Party validation, unless an alternative trust or lifecycle model is defined for a specific certificate class.

Upon completion of termination activities, the CA SHALL securely archive required records and destroy CA Private Keys in accordance with §6.2.10.

6.0 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

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

(i) Prepare and follow a Key Pair generation script;
(ii) Have a qualified auditor witness the CA Key Pair generation process;
(iii) Have a qualified auditor issue a report opining that the CA followed its CA Key Pair generation ceremony during its key generation process and the controls to ensure the integrity and confidentiality of the CA Key Pair;
(iv) Generate the CA Key Pair in a physically secured environment;
(v) Generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
(vi) Generate the CA Key Pair within cryptographic modules meeting the applicable requirements of §6.2.11;
(vii) Log its CA Key Pair generation activities; and
(viii) Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CP/CPS and (if applicable) its CA Key Pair generation script.

6.1.1.2 RA Key Pair Generation

No additional requirements beyond those defined in this CP/CPS.

6.1.1.3 Subscriber Key Pair Generation

The Applicant or Subscriber is required to generate or initiate a new, secure, and cryptographically sound Key Pair to be used in association with the Subscriber's Certificate or Applicant's Certificate Application. The CAs will reject a Certificate request if one or more of the following conditions are met:

(i) The Key Pair does not meet the requirements set forth in §6.1.5 and/or §6.1.6;

(ii) There is clear evidence that the specific method used to generate the Private Key was flawed;

(iii) The CA is aware of a demonstrated or proven method that exposes the Private Key to compromise;
(iv) The CA has previously been notified that the Private Key has suffered a Key Compromise, using the procedure for Revocation request as described in §4.9.3 and §4.9.12;
(v) The CA is aware of a demonstrated or proven method to easily compute the Private Key based on the Public Key.

6.1.2 Private Key Delivery to Subscriber

CAs do not generate, archive or deliver the Key Pair on behalf of the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

The Public Key to be included in a Certificate is delivered to the CA in a signed Certificate Signing Request (CSR) as part of the Certificate Application process. The signature on the CSR will be verified by the CA prior to issuing the Certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The Certification Authority Certificate(s) containing the Root CAs Public Key are made available to Subscribers with the Certificate or may be obtained from the Entrust support team. The Subordinate CA Certificate is provided to the Subscriber with the Certificate.

The Subordinate CA Certificate for the CA is provided to the Relying Parties by the Subscriber.

6.1.5 Key Sizes

Supported key sizes for CA and Subscriber Certificates include:

(i) RSA-4096, RSA-3072, RSA-2048
(ii) ECC NIST P-384 and P-256 ML-DSA-87,
(iii)ML-DSA-65, ML-DSA-44

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA Public Keys, CAs will confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent will be in the range between $2^{16}+1$ and $2^{256}-1$. The modulus will also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752.

For ECC Public Keys, CAs will confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

6.1.7 Key Usage Purposes

Root CA Private Keys must not be used to sign Certificates except in the following cases:

(i) Self-signed CA Certificates to represent the Root CA itself;

(ii) CA Certificates for Subordinate CAs and Cross Certificates;

(iii) delegated OCSP certificates; and

(iv) Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CAs have implemented physical and logical safeguards to prevent unauthorized Certificate issuance. Protection of the CA Private Key outside the validated system consists of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. The CA encrypts its Private Key with an algorithm and key-length that are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key.

6.2.1 Cryptographic Module Standards and Controls

CA Private Keys must be stored and protected on cryptographic modules that meet or exceed the requirements as defined in §6.2.11. Private Keys on cryptographic modules are held in secure facilities under two-person control.

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

A minimum of two-person control will be established on any CA Private Key for all purposes including activation and backup and may be implemented as a combination of technical and procedural controls. Persons involved in management and use of the CA Private Keys will be designated as authorized by the CA for this purpose. The names of the parties used for two-person control will be maintained on a controlled list.

6.2.3 Private Key Escrow

Entrust does not escrow the CAs' Private Keys.

6.2.4 Private Key Backup

CA Private Keys are backed up under the two-person control used to create the original version of the Private Keys. All copies of the CA Private Key are securely protected. Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's Certificate.

6.2.5 Private Key Archival

No additional requirements beyond those defined in this CP/CPS.

6.2.6 Private Key Transfer into or from Cryptographic Module

CA Private Keys are generated by and secured in a cryptographic module. In the event that a Private Key is to be transported from one cryptographic module to another, the Private Key must be migrated using the secure methodology supported by the cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

CA Private Keys are stored on a cryptographic module and are secured in the cryptographic module as defined in §6.2.11.

6.2.8 Method of Activating Private Key

CA Private Keys are activated under two-person control using the methodology provided with the cryptographic module.

Subscriber Private Keys are activated by the Subscriber to meet the requirements of the security software used for their applications. Subscribers are responsible for the protection of their Private Keys in accordance with applicable requirements in this CP/CPS and SHALL meet the requirements in §9.6.3.

6.2.9 Method of Deactivating Private Key

CA Private Keys will be deactivated when the CA is not required for active use. Deactivation of the Private Keys will be done in accordance with the methodology provided with the cryptographic module.

6.2.10 Method of Destroying Private Key

CA Private Keys SHALL be destroyed under dual control. Destruction MAY be performed by one of the following methods:

- Execution of a zeroization command within the cryptographic module;
- Cryptographic deletion of the Private Key from the cryptographic module; or
- Physical destruction of the cryptographic module.

All destruction of CA Private Keys SHALL be authorized by the Operational Authority.

If a cryptographic module is removed from service, all Private Keys SHALL be removed from the module prior to its decommissioning.

6.2.11 Cryptographic Module Rating

CA Key Pairs must be generated and protected on a cryptographic module that is compliant to at least FIPS 140-2 Level 3, FIPS 140-3 Level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No additional requirements beyond those defined in this CP/CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificate	Operational Periods
CA Key Pairs	Maximum validity of 25 years
TPM Root CA Key Pairs	Maximum validity of 41 years
TLS Certificates	Maximum validity of 39 months
Mobile Device Certificates	Maximum validity of 60 months
Device Identity Certificates	no stipulation

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No additional requirements beyond those defined in this CP/CPS.

6.4.2 Activation Data Protection

No additional requirements beyond those defined in this CP/CPS.

6.4.3 Other Aspects of Activation Data

No additional requirements beyond those defined in this CP/CPS.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The systems on which the CAs operate are physically secured as described in 5.1. The operating systems on which the CAs operate are hardened and enforce identification and authentication of users. Access to CA software, databases and audit trails is restricted to authorized Trusted Roles.

The CA enforces multi-factor authentication for all RA and Enterprise RA accounts capable of directly causing Subscriber Certificate issuance.

6.5.2 Computer Security Rating

No additional requirements beyond those defined in this CP/CPS.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

No additional requirements beyond those defined in this CP/CPS.

6.6.2 Security Management Controls

The configuration of the CA system as well as any modifications and upgrades are documented and controlled. Methods of detecting unauthorized modifications to the CA equipment and configuration are in place to ensure the integrity of the security software, firmware, and hardware for correct operation. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system.

6.6.3 Life Cycle Security Controls

No additional requirements beyond those defined in this CP/CPS.

6.7 Network Security Controls

CA and RA systems are connected to a private network that is segmented and protected by multiple layers of firewalls from the internet and corporate networks. Flows between network segments are restricted to necessary ports and protocols to perform CA, RA or management functions under the Principle of Least Privilege. Systems are hardened with services, ports and accounts not used removed and/or disabled. Changes are documented and approved via a change management process and executed by Trusted Roles. Only Trusted Roles have access to CA and RA systems or the network components that restrict access to CA systems.

6.8 Time-stamping

No additional requirements beyond those defined in this CP/CPS.

7.0 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

CAs issue Certificates in accordance with X.509 Recommendations. Certificate profiles for Root CA, Subordinate CA, and Subscriber Certificates are described in the sections below.

Certificates have a serial number greater than zero (0) that contains at least 64 unpredictable bits.

Subscriber Certificates are issued from dedicated Subordinate CAs based on the policy identifiers listed in §7.1.6.4.

7.1.1 Version Number

All Certificates issued by the CAs are X.509 version 3 certificates.

7.1.2 Certificate Extensions

Certificate extensions are set as stipulated in IETF RFC 5280 and are applied as appropriate to the certificate type being issued.

7.1.2.1 Root CA Certificate

Extension	Critical	Description
basicConstraints	Yes	CA field is set to be true pathLenConstraint field not present
keyUsage	Yes	Bit positions for keyCertSign, cRLSign and digitalSignature are set
certificatePolicies		Not present
extendedKeyUsage		Not present

7.1.2.2 Subordinate CA Certificate

Extension	Critical	Description
basicConstraints	Yes	CA field is set to be true pathLenConstraint field not present
keyUsage	Yes	Bit positions for keyCertSign, cRLSign and digitalSignature
certificatePolicies	No	Policy Identifier, Qualifier ID of CP/CPS and URI for CP/CPS are required
extendedKeyUsage	No	As applicable from the following: None present Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
cRLDistributionPoints	No	HTTP URL of the CA's CRL service

authorityInformationAccess	No	As applicable from the following: HTTP URL of the Issuing CA's OCSP responder HTTP URL of the Issuing CA's Certificate

7.1.2.3 Subscriber Certificate

Extension	Critical	Description
basicConstraints		Not present
keyUsage	Yes	As applicable from the following: Digital Signature Key Encipherment
certificatePolicies	No	Policy Identifier, Qualifier ID of CP/CPS and URI for CP/CPS are required
extendedKeyUsage	No	As applicable from the following: None present Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
cRLDistributionPoints	No	HTTP URL of the CA's CRL service
authorityInformationAccess	No	As applicable from the following: HTTP URL of the Issuing CA's OCSP responder HTTP URL of the Issuing CA's Certificate

7.1.2.4 All Certificates

Except as indicated in this CP/CPS, all other fields and extensions are set in accordance with RFC 5280.

7.1.2.5 Application of RFC 5280

No additional requirements beyond those defined in RFC 5280 and this CP/CPS.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP/CPS shall be signed using an algorithm corresponding to one of the following object identifiers (OIDs):

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}

Signature Algorithm ID	OID
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
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)}
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)}

7.1.4 Name Forms

7.1.4.1 Issuer Information

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, §4.1.2.4.

7.1.4.2 Subject Information – Subscriber Certificates

Name forms for Subscriber Certificates are as stipulated in §3.1.1. All other optional attributes must contain information that has been verified by the CA or RA. Optional attributes will not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.3 Subject Information – Root CA Certificates and Subordinate CA Certificates

No additional requirements beyond those defined in RFC 5280 and this CP/CPS.

7.1.5 Name Constraints

No additional requirements beyond those defined in RFC 5280 and this CP/CPS.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers
No additional requirements beyond those defined in RFC 5280 and this CP/CPS.

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

7.1.6.3 Subordinate CA Certificates
Subordinate CA Certificates must include either the "any policy" certificate policy object identifier or one or more explicit certificate policy object identifiers that indicates compliance with a specific certificate policy, as in §1.2.

7.1.6.4 Subscriber Certificates
Certificates may include one of the certificate policy object identifiers as in §1.2

7.1.7 Usage of Policy Constraints Extension
No additional requirements beyond those defined in RFC 5280 and this CP/CPS.

7.1.8 Policy Qualifiers Syntax and Semantics
No additional requirements beyond those defined in RFC 5280 and this CP/CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies 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:

- 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 Number
CRLs issued by the CAs are X.509 version 2.

7.2.2 CRL and CRL Entry Extensions
reasonCode (OID 2.5.29.21): The CRLReason code extension may be used for revoked Certificates and will not be marked critical. The CRLReason indicated must not be unspecified (0) and if reasonCode unspecified (0) is used, the CA will omit the reasonCode entry in the CRL.

This extension must not be marked critical. The most appropriate reason must be selected by the Subscriber or the CA from one the following:

(i) keyCompromise (1), if the key to the certificate has been or is suspected to be compromised or has signed Suspect Code;

(ii) cACompromise (2), if the CA has been or is suspected to be compromised;

(iii) affiliationChanged (3), if verified information in the Certificate has changed and as such the Relying Parties should no longer trust the Certificate

(iv) superseded (4), if the Certificate has been reissued, rekeyed or renewed by another Certificate, the CA has evidence the validation of domain or IP address should not be relied upon or the Certificate was not issued in accordance with this CP/CPS;

(v) cessationOfOperation (5), if the website or Device is no longer in service or the Subscriber no longer controls the domain or IP address; or

(vi) privilegeWithdrawn (9), if the CA determines the privilege of the Certificate issued the Subscriber no longer exists.

The default revocation reason is unspecified (0) which results in no reasonCode being provided in the CRL. The CA will not use reasonCode certificateHold (6). The priviledgeWithdrawn (9) reasonCode is not made available to the Subscriber.

7.3 OCSP Profile

The profile for the Online Certificate Status Protocol (OCSP) messages issued by a CA conform to the specifications contained in the IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP) Profile.

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been rRevoked, then the revocationReason field within the RevokedInfo of the CertStatus will be present.

The CRLReason indicated contains a value permitted for CRLs, as specified in §7.2.2.

7.3.1 Version Number

No additional requirements beyond those defined in RFC 5280 and this CP/CPS.

7.3.2 OCSP Extensions

No additional requirements beyond those defined in RFC 5280 and this CP/CPS.

8.0 COMPLIANCE AUDIT AND OTHER ASSESSMENT

8.1 Frequency or Circumstances of Assessment

Compliance audits are conducted for CAs issuing Certificates and for RAs within the scope of this CP/CPS, excluding Enterprise RAs.

The period during which the CA issues Certificates will be divided into an unbroken sequence of audit periods. Audit periods are established in accordance with applicable audit criteria and generally cover a duration of up to one year.

8.2 Identity/Qualifications of Assessor

The compliance audit of the CAs is performed by an auditor which possesses the following qualifications and skills:

(i) Independence from the subject of the audit.
(ii) Ability to conduct an audit that addresses the criteria of the audit schemes specified in §8.4.
(iii) Assigns individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function.
(iv) Bound by law, government regulation, or professional code of ethics.

8.3 Assessor's Relationship to Assessed Entity

The firm selected to perform the compliance audit for the CAs and RAs will be independent from the entity being audited.

8.4 Topics Covered by Assessment

The compliance audit will test compliance of the CAs and RAs against the policies and procedures set forth as applicable in:

i. This CP/CPS; and
ii. WebTrust for Certification Authorities.

8.5 Actions Taken as a Result of Deficiency

Upon receipt of a compliance audit that identifies any deficiencies, the audited CA or RA will use commercially reasonable efforts to correct any such deficiencies in an expeditious manner.

8.6 Communication of Results

The results of all compliance audits will be communicated to the Policy Authority and to any third-party entities which are entitled by law or regulation to receive a copy of the audit results.

8.7 Self-audits

Self-audit activities include periodic automated and/or manual processes designed to assess compliance with applicable requirements.All Subscriber Certificates are self-audited using Linting software to monitor adherence to the applicable items of this CP/CPS, limited to the scope of coverage provided by the Linter.

9.0 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees
No stipulation.

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

9.3 Confidentiality of Business Information
Confidentiality obligations between Entrust and Subscriber are governed by the Verified PKIaaS Agreement. Otherwise, no stipulation.

9.4 Privacy of Personal Information
Obligations between Entrust and Subscriber are governed by the Verified PKIaaS Agreement. Otherwise, no stipulation.

9.4.1 Privacy Plan
Entrust follows the policies, statements and practices available at https://www.entrust.com/legal-compliance/privacy ("Privacy Plan") when handling personal information.

9.4.2 Notice and Consent to Use Private Information
Personal information contained in a Certificate may be published in online public repositories and all Subscribers consent to the global transfer of any personal data contained in the Certificate.

9.5 Intellectual Property Rights
Entrust retains all rights, title, and interest (including all intellectual property rights), in, to and under the CP/CPS and all Certificates and CA Certificates, except for any information that is supplied by an Applicant or a Subscriber and that is included in a Certificate, which information SHALL remain the property of the Applicant or Subscriber. No right is or SHALL be deemed to be granted under this CP/CPS, whether by implication, estoppel, inference or otherwise.

9.6 Representation and Warranties

9.6.1 CA Representations and Warranties
No stipulation.

9.6.2 RA Representations and Warranties
No stipulation.

9.6.3 Subscriber Representations and Warranties
As a condition of having any Certificate issued to or for Subscriber, each Subscriber (in this section, "Subscriber" includes "Applicant" when referring to any time prior to issuance of the Certificate)

makes, on its own behalf and if applicable on behalf of its principal or agent under a subcontractor or hosting service relationship, the representations, commitments, affirmations and warranties set out in each applicable Subscriber Agreement.

9.6.4 Relying Parties Representations and Warranties

Each Relying Party makes the following representations, commitments, affirmations and warranties:

(i)	The Relying Party SHALL understand and, if necessary, receive proper education in the use of Public-Key cryptography, including the use and validation of Certificates
(ii)	The Relying Party SHALL read and accepts all terms and conditions of the CP/CPS.
(iii)	The Relying Party SHALL verify Certificates, including use of CRLs, in accordance with the certification path validation procedure specified in ITU-T Rec. X.509:2005 | ISO/IEC 9594-8 (2005), taking into account any critical extensions and approved technical corrigenda as appropriate.
(iv)	The Relying Party SHALL trust and make use of a Certificate only if the Certificate has not expired or been revoked and if a proper chain of trust can be established to a trustworthy Root CA.
(v)	The Relying Party SHALL properly validate a Certificate before deciding whether to rely on such Certificate, including confirmation that the Certificate has not expired or been Revoked and that a proper chain of trust can be established to a trustworthy Root CA.
(vi)	The Relying Party SHALL not rely on a Certificate that cannot be validated back to a trustworthy Root CA.
(vii)	The Relying Party SHALL exercise its own judgment in determining whether it is reasonable under the circumstances to rely on a Certificate, including determining whether such reliance is reasonable given the nature of the security and trust provided by a Certificate and the value of any transaction that may involve the use of a Certificate.
(viii)	The Relying Party SHALL not use a Certificate for any hazardous or unlawful (including tortious) activities.
(ix)	The Relying Party SHALL not rely on a Revoked or expired Certificate.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

ENTRUST GROUP EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CP/CPS OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF QUALITY, MERCHANTABILITY, NON-INFRINGEMENT, TITLE AND FITNESS FOR A PARTICULAR PURPOSE, AND ALL WARRANTIES, REPRESENTATIONS,

CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. ENTRUST GROUP FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT (A) THE SUBSCRIBER TO WHICH IT HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (B) A SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CERTIFICATE, OR (C) THAT THE INFORMATION CONTAINED IN THE CERTIFICATES OR IN ANY CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY ENTRUST, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

IT IS AGREED AND ACKNOWLEDGED THAT APPLICANTS AND SUBSCRIBERS ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO ENTRUST AND RELIED UPON BY A RELYING PARTY. ENTRUST GROUP DOES NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION ENTERED INTO BY THE SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE.

IT IS UNDERSTOOD AND AGREED UPON BY SUBSCRIBERS AND RELYING PARTIES THAT IN USING AND/OR RELYING UPON A CERTIFICATE THEY ARE SOLELY RESPONSIBLE FOR THEIR RELIANCE UPON THAT CERTIFICATE AND THAT SUCH PARTIES MUST CONSIDER THE FACTS, CIRCUMSTANCES AND CONTEXT SURROUNDING THE TRANSACTION IN WHICH THE CERTIFICATE IS USED IN DETERMINING SUCH RELIANCE.

9.8 Limitations of Liability

Limitations of liability between Entrust Group and a Customer are as set out in the Verified PKIaaS Agreement.

Limitations of liability between a CA and a Subscriber are as set out in the applicable Subscriber Agreement.

SUBJECT TO THE FOREGOING AND IF ABOVE DOES NOT APPLY:

IN NO EVENT WILL ENTRUST GROUP BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR EXEMPLARY DAMAGES OR FOR ANY LOSS OF BUSINESS, OPPORTUNITIES, CONTRACTS, REVENUES, PROFITS, SAVINGS, GOODWILL, REPUTATION, USE, OR DATA, OR COSTS OF REPROCUREMENT OR BUSINESS INTERRUPTION, OR ANY LOSS OR DAMAGE THAT IS NOT DIRECTLY ATTRIBUTABLE TO THE ENTRUST'S SERVICES PROVIDED UNDER THIS CP/CPS INCLUDING ANY LOSS OR DAMAGE RESULTING FROM THE COMBINATION OR

INTEGRATION OF THE CERTIFICATE OR SERVICES WITH ANY SOFTWARE OR HARDWARE NOT PROVIDED BY ENTRUST IF THE LOSS OR DAMAGE WOULD NOT HAVE OCCURRED AS A RESULT OF USE OF THE CERTIFICATE OR CERTIFICATE SERVICES ALONE.

IN NO EVENT WILL ENTRUST GROUP'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS CP/CPS AND THE USE AND PERFORMANCE OF ANY PRODUCTS AND SERVICES PROVIDED HEREUNDER EXCEED ONE THOUSAND UNITED STATES DOLLARS ($1,000.00 U.S.).

THE EXCLUSIONS AND LIMITS IN THIS SECTION (LIMITATIONS OF LIABILITY) APPLY: (A) REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE), WARRANTY, BREACH OF STATUTORY DUTY, MISREPRESENTATION, STRICT LIABILITY, STRICT PRODUCT LIABILITY, OR OTHERWISE; (B) ON AN AGGREGATE BASIS, REGARDLESS OF THE NUMBER OF CLAIMS, TRANSACTIONS, DIGITAL SIGNATURES OR CERTIFICATES; (C) EVEN IF THE POSSIBILITY OF THE DAMAGES IN QUESTION WAS KNOWN OR COMMUNICATED IN ADVANCE AND EVEN IF SUCH DAMAGES WERE FORESEEABLE; AND (D) EVEN IF THE REMEDIES FAIL OF THEIR ESSENTIAL PURPOSE. ENTRUST HAS SET ITS PRICES AND PROVIDES CERTIFICATES IN RELIANCE ON THE EXCLUSIONS AND LIMITS IN THIS SECTION (LIMITATIONS OF LIABILITY), WHICH FORM AN ESSENTIAL BASIS OF THE PROVISION OF THE SERVICES DESCRIBED IN THIS CP/CPS.

Notwithstanding anything to the contrary in this Section (Limitation of Liability), to the extent required by applicable law Entrust neither excludes nor limits its liability for: (i) death or bodily injury caused by its own negligence; (ii) its own fraud or fraudulent misrepresentation; or (iii) other matters for which liability cannot be excluded or limited under applicable law.

9.9 Indemnities

9.9.1 Indemnification by CAs

No stipulation.

9.9.2 Indemnification by Relying Parties

RELYING PARTIES SHALL INDEMNIFY AND HOLD ENTRUST GROUP (COLLECTIVELY, THE "INDEMNIFIED PARTIES") HARMLESS FROM AND AGAINST ANY AND ALL LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISING OUT OF OR RELATING TO ANY USE OR RELIANCE BY A RELYING PARTY ON ANY CERTIFICATE OR ANY SERVICE PROVIDED IN RESPECT TO CERTIFICATES, INCLUDING (I) LACK OF PROPER VALIDATION OF A CERTIFICATE BY A RELYING PARTY, (II) RELIANCE BY THE RELYING PARTY ON AN EXPIRED OR REVOKED CERTIFICATE, (III) USE OF A CERTIFICATE OTHER THAN AS PERMITTED BY THE CP/CPS, (IV) FAILURE BY A RELYING PARTY TO EXERCISE REASONABLE JUDGMENT IN THE CIRCUMSTANCES IN RELYING ON A CERTIFICATE, OR (V) ANY CLAIM OR ALLEGATION THAT THE RELIANCE BY A RELYING PARTY ON A

CERTIFICATE OR THE INFORMATION CONTAINED IN A CERTIFICATE INFRINGES, MISAPPROPRIATES, DILUTES, UNFAIRLY COMPETES WITH, OR OTHERWISE VIOLATES THE RIGHTS INCLUDING INTELLECTUAL PROPERTY RIGHTS OR ANY OTHER RIGHTS OF ANYONE IN ANY JURISDICTION. NOTWITHSTANDING THE FOREGOING, RELYING PARTIES SHALL NOT BE OBLIGATED TO PROVIDE ANY INDEMNIFICATION TO AN INDEMNIFIED PARTY IN RESPECT TO ANY LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS AND EXPERT'S FEES) TO THE EXTENT THAT SUCH LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISE OUT OF OR RELATE TO ANY WILLFUL MISCONDUCT BY SUCH INDEMNIFIED PARTY.

9.9.3 Indemnification by Subscribers
No stipulation.

9.10 Term and Termination
No stipulation.

9.11 Individual Notices and Communications with Participants
No additional requirements beyond those defined in this CP/CPS.

9.12 Amendments

9.12.1 Procedure for Amendment
Entrust may, in its discretion, modify the CP/CPS and the terms and conditions contained herein from time to time.

9.12.2 Notification Mechanism and Period
Modifications to the CP/CPS SHALL be published in the Repository and SHALL become effective fifteen (15) days after publication in the Repository unless Entrust withdraws such modified CP/CPS prior to such effective date. In the event that Entrust makes a significant modification to CP/CPS, the version number of the CP/CPS SHALL be updated accordingly. Unless a Subscriber ceases to use, removes, and requests revocation of such Subscriber's Certificate(s) prior to the date on which an updated version of the CP/CPS becomes effective, such Subscriber SHALL be deemed to have consented to the terms and conditions of such updated version of the CP/CPS and SHALL be bound by the terms and conditions of such updated version of the CP/CPS.

9.12.3 Circumstances Under which OID must be Changed
No additional requirements beyond those defined in this CP/CPS.

9.13 Dispute Resolution Provisions
Dispute resolution between Entrust Group and a Customer SHALL be governed by the Verified PKIaaS Agreement.

Dispute resolution between a CA and a Subscriber SHALL be governed by the applicable Subscriber Agreement.

9.14 Governing Law

As between Entrust Group and a Customer, the construction, validity, interpretation, enforceability and performance of this CP/CPS SHALL be governed by the law indicated in the Verified PKIaaS Agreement.

As between a CA and a Subscriber, the construction, validity, interpretation, enforceability and performance of this CP/CPS SHALL be governed by the law indicated in the applicable Subscriber Agreement.

Subject to the foregoing, the laws of the Province of Ontario, Canada, excluding its conflict of laws rules, SHALL govern the construction, validity, interpretation, enforceability and performance of the CP/CPS. The application of the United Nations Convention on Contracts for the International Sale of Goods to the CP/CPS is expressly excluded. Any dispute arising out of or in respect to the CP/CPS, or in respect to any Certificates or any services provided in respect to any Certificates that is not resolved by alternative dispute resolution, SHALL be brought in the provincial or federal courts sitting in Ottawa, Ontario, and each person, entity, or organization hereby agrees that such courts SHALL have personal and exclusive jurisdiction over such disputes. In the event that any matter is brought in a provincial or federal court, any claimants waive any right that such claimants may have to a jury trial.

9.14.1 Compliance with Applicable Law

Certificates and related information may be subject to export, import, and/or use restrictions. Subscribers and Relying Parties will comply in all respects with any and all applicable laws, rules and regulations and obtain all permits, licenses and authorizations or certificates that may be required in connection with their exercise of their rights and obligations under any part of the CP/CPS and/or Subscriber Agreement, including use or access by any of Subscriber or Relying Party's users. Without limiting the foregoing, Subscribers and Relying Parties will comply with all applicable trade control laws, including but not limited to any sanctions or trade controls of the European Union ("E.U."), Canada, the United Kingdom ("U.K."), and United Nations ("U.N."); the Export Administration Regulations administered by the U.S. Department of Commerce's Bureau of Industry and Security; U.S. sanctions regulations administered by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"); or on the U.S. Department of Commerce Entities List ("Entities List"); and any import or export licenses required pursuant to any of the foregoing; and all applicable anti-money laundering laws, including the U.S. Bank Secrecy Act, Money Laundering Control Act, and Patriot Act, the Canadian Proceeds of Crime (Money Laundering) and Terrorist Financing Act, the U.K. Proceeds of Crime Act, and legislation implementing the International Convention on the Suppression of the Financing of Terrorism or the money laundering provisions of the U.N. transnational Organized Crime Convention. Each Subscriber and Relying Party represents and warrants that: (a) neither it nor any of its users is located in, under the control of, or a national or resident of any country to which the export of any software or technology, or related information, would be prohibited by the applicable laws, rules or regulations of the U.S., Canada, U.K., E.U., or other applicable jurisdiction; (b) neither it nor any of its users is a Person to whom the export of any software or technology licensed under the Agreement, or related information, would be prohibited

by the laws of the U.S., Canada, U.K., E.U., or other applicable jurisdiction; (c) it and each of its users has and will comply with applicable laws, rules and regulations of the U.S., Canada, U.K., E.U., or other applicable jurisdiction(s) and of any state, province, or locality or applicable jurisdiction governing exports of any product or service provided by or through Entrust; (d) it and all its users will not use any product or service for any purposes prohibited by applicable laws, rules or regulations on trade controls, including related to nuclear, chemical, or biological weapons proliferation, arms trading, or in furtherance of terrorist financing; (e) neither it nor any of its users nor any of its affiliates, officers, directors, or employees is (i) an individual listed on, or directly or indirectly owned or controlled by, a Person (whether legal or natural) listed on, or acting on behalf of a Person listed on, any U.S, Canadian, E.U., U.K., or U.N. sanctions list, including OFAC's list of Specially Designated Nationals or the Entities List; or (ii) located in, incorporated under the laws of, or owned (meaning 50% or greater ownership interest) or otherwise, directly or indirectly, controlled by, or acting on behalf of, a person located in, residing in, or organized under the laws of any of the countries listed as Restricted Countries at https://www.entrust.com/legal-compliance/sanctioned-countries (each of (i) and (ii), a "Denied Party"); and (f) it and each of its users is legally distinct from, and not an agent of any Denied Party. In the event any of the above representations and warranties is incorrect or the Subscriber, Relying Party or any their users engages in any conduct that is contrary to sanctions or trade controls or other applicable laws, regulations, or rules, any agreements, purchase orders, performance of services, or other contractual obligations of Entrust are immediately terminated.

9.15 Miscellaneous Provisions

9.15.1 Entire Agreement

No additional requirements beyond those defined in this CP/CPS.

9.15.2 Assignment

Entrust may assign, sell, transfer, or otherwise dispose of the CP/CPS and any Subscriber Agreement, together with all of its rights and obligations under the CP/CPS and any Subscriber Agreement (i) to an Affiliate, or (ii) as part of a sale, merger, or other transfer of all or substantially all the assets or stock of the business of Entrust to which the CP/CPS and/or the Subscriber Agreement relates.

9.15.3 Severability

To the extent permitted by applicable law, any provision of law is waived that would render any provision of the CP/CPS invalid or otherwise unenforceable in any respect. In the event that any provision of the CP/CPS is held to be invalid or otherwise unenforceable in application to particular facts or circumstances: (a) such provision will be interpreted and amended to the extent necessary to fulfill its intended purpose to the maximum extent permitted by applicable law and its validity and enforceability as applied to any other facts or circumstances will not be affected or impaired; and (b) the remaining provisions of the CP/CPS will continue in full force and effect. For greater certainty, it is expressly understood and intended that each provision that deals with limitations and exclusions of liability, disclaimers of representations, warranties and conditions, or indemnification is severable from any other provisions.

9.15.4 Force Majeure

"Force Majeure Event" means any event or circumstance beyond Entrust Group's reasonable control, including but not limited to, floods, fires, hurricanes, earthquakes, tornados, epidemics, pandemics, other acts of God or nature, strikes and other labor disputes, failure of utility, transportation or communications infrastructures, riots or other acts of civil disorder, acts of war, terrorism (including cyber terrorism), malicious damage, judicial action, lack of or inability to obtain export permits or approvals, acts of government such as expropriation, condemnation, embargo, changes in applicable laws or regulations, and shelter-in-place or similar orders, and acts or defaults of third party suppliers or service providers. In the event that a Force Majeure Event directly or indirectly causes a failure or delay in Entrust Group's performance of its obligations under the CP/CPS, Entrust Group SHALL not be in default or liable for any loss or damages where performance is impossible or commercially impracticable.

9.16 Other Provisions

9.16.1 Conflict of Provisions

In the event of any conflict between the provisions of this CP/CPS and the provisions of any Subscriber Agreement, the terms and conditions of this CP/CPS SHALL govern.

9.16.2 Waiver

The failure of Entrust to enforce, at any time, any of the provisions of this CP/CPS, or the failure of Entrust to require, at any time, performance by any Applicant, Subscriber, Relying Party or any other person, entity, or organization of any of the provisions of this CP/CPS, SHALL in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of Entrust to enforce each and every such provision thereafter. The express waiver by Entrust of any provision, condition, or requirement of this CP/CPS SHALL not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

9.16.3 Interpretation

All references in this CP/CPS to "section" or "§" refer to the sections of this CP/CPS unless otherwise stated. As used in this CP/CPS, neutral pronouns and any variations thereof SHALL be deemed to include the feminine and masculine and all terms used in the singular SHALL be deemed to include the plural, and vice versa, as the context may require. The words "hereof", "herein", and "hereunder" and other words of similar import refer to this CP/CPS as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this CP/CPS. The words "including", "include" and "includes" will each be deemed to be followed by the phrase "without limitation".

10.0 APPENDIX A - DEFINITIONS AND ACRONYMS

10.1 Definitions

Term	Definition
Affiliate	With respect to any organizational party, a person or entity that directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with that party. In this context, a party "controls" a corporation or another entity if it directly or indirectly owns or controls fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of control or, in the case of a non-corporate entity, an equivalent interest.
Applicant	A person, entity, or organization applying for a Certificate, but which has not yet been issued a Certificate, or a person, entity, or organization that currently has a Certificate or Certificates and that is applying for renewal of such Certificate or Certificates or for an additional Certificate or Certificates.
Certificate	A digital document issued by the CA that, at a minimum: (a) identifies the CA issuing it, (b) names or otherwise identifies a Subject, (c) contains a Public Key of a Key Pair, (d) identifies its Operational Period, and (e) contains a serial number and is digitally signed by a CA. In this CP/CPS, "Certificate" means end entity TLS Certificates, Device Identity Certificates, Mobile Device Certificates, and Client Authentication Certificates issued as part of Verified PKIaaS; and "CA Certificate" means a certificate issued to a CA operated by Entrust as part of Verified PKIaaS.
Certificate Application	The form and application information requested by an RA and submitted by an Applicant when applying for the issuance of a Certificate.
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Revocation List	A time-stamped list of the serial numbers of Revoked Certificates that have been digitally signed by a CA
Certification Authority	A certification authority operated by or on behalf of Entrust for the purpose of issuing, managing, Revoking, renewing, and providing access to Certificates. The CA (i) creates and digitally signs Certificates (ii) makes Certificates available, and (iii) creates and digitally signs Certificate Revocation Lists containing information about Certificates that have been Revoked and which should no longer be used or relied upon.

Certification Authority Authorization	Has the meaning given in RFC 8659.
Certification Practice Statement	A statement of the practices that the CA uses in issuing, managing, Revoking, renewing, and providing access to Certificates (this document).
Client Authentication Certificate:	A Certificate issued to authenticate clients to servers and does not include the serverAuth extended key usage.
Cross Certificate(s)	A Certificate(s) that (i) includes the Public Key of a Key Pair generated by a Certification Authority; and (ii) includes the digital signature of a Root CA.
Customer	The entity that has entered into a Verified PKIaaS Agreement with Entrust.
Dedicated CA	A CA that is established for use by a specific Enterprise.
Device	An electronic endpoint in a network, system, or application, such as a computer, laptop, terminal, workstation, server, pager, telephone, smartphone, tablet, virtual workload, or other physical object enabled through embedded technology to execute functions and collect and exchange data.
Device Identity Certificate	A Certificate issued by a Certification Authority to identify a Device for which no good expiration date can be assigned, for example, a Certificate which binds the Device's model and serial number to its Public Key, sometimes referred to as a "birth Certificate".
Domain Contact	The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.
Enterprise	A group of organizations (legal persons) each of which is an Affiliate of all the others.
Enterprise Registration Authority	An employee or agent of an Enterprise organization who acts as a type of constrained RA, verifying Certificate Applications from that Enterprise.
Entrust	Means Entrust Corporation.
Entrust Group	Collectively Entrust Corporation, its Affiliates, its licensors suppliers, and subcontractors, and the directors, officers, employees, agents and independent contractors of any of them.
FIPS	Federal Information Processing Standards. These are U.S. Federal standards that prescribe specific performance requirements, practices, formats, communication protocols, and other requirements for hardware, software, data, and telecommunications operation

Fully Qualified Domain Name	A domain name that includes the domain labels of all superior nodes in the Internet domain name system.
IETF	The Internet Engineering Task Force, an international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the efficient operation of the Internet.
IP Address	A 32-bit or 128-bit number assigned to a Device that uses the Internet Protocol for communication.
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Key Pair	Two mathematically related cryptographic keys, having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is believed to be computationally infeasible to discover the other key.
Linting	A process in which the content of digitally signed data such as a Certificate, Certificate Revocation List, or OCSP response, or data-to-be signed object such as a tbsCertificate (as described in RFC 5280, §4.1.1.1) is checked for conformance with the profiles and requirements.
Mobile Device Certificate	A Certificate issued by a Certification Authority to identify a Device, but which is not a Device Identity Certificate.
Object Identifier	A specially-formatted sequence of numbers that is registered in accordance with internationally-recognized procedures for object identifier registration.
Operational Period	With respect to a Certificate, the period of its validity. The Operational Period would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate) and ends on the date and time it expires as noted in the Certificate or earlier if the Certificate is Revoked.
Policy Authority	Personnel who work for or on behalf of Entrust and who are responsible for determining the policies and procedures that govern the operation of the PKI.

Private Key	The key of a Key Pair used to decrypt an encrypted message. This key must be kept secret.
Public Key	The key of a Key Pair used to encrypt a message. The Public Key can be made freely available to anyone who may want to send encrypted messages to the holder of the Private Key of the Key Pair. The Public Key is usually made publicly available in a Certificate and is often obtained by accessing a repository or database. A Public Key is used to encrypt a message that can only be decrypted by the holder of the corresponding Private Key.
Registration Authority	An entity that: (1) receives Certificate Applications from Applicants applying for the issuance of a Certificate, and (2) verifies information in and about the Certificate Application, Subject, and/or Applicant following the procedures prescribed by the PA and CAs. In the event that the Certificate Application satisfies the criteria defined by the PA and CAs, an RA may send a request to a CA requesting that the CA generate, digitally sign, and issue a Certificate containing the information verified by the RA.
Reliable Data Source	An authoritative, verifiable, identification document, record, or source of data that demonstrates or provides evidence of identity and other information (such as legal rights and employment) that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
Relying Party	A person, entity, or organization that relies on or uses a Certificate and/or any other information provided in a Repository under a CA to obtain and confirm the Public Key and identity of a Subscriber.
Repository	A collection of databases and web sites that contain information about Certificates issued by a CA including among other things, the types of Certificates and services provided by the CA, Certificate Revocation Lists, OCSP responses, descriptions of the practices and procedures of the CA, and other information and documents that are intended to govern the use of Certificates issued by the CA.
Reserved IP Address	An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-specialregistry.xhtml

	https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-specialregistry.xhtml
Revoke, Revoked or Revocation	With respect to a Certificate, to prematurely end the Operational Period of that Certificate from a specified time forward.
Root CA	A CA that is self-signed and serves as the trust anchor at the top of a certificate chain.
Secure Socket Layer (SSL)	The predecessor to TLS. SSL is deprecated and insecure.
Shared CA	A CA which issues Certificates to one or more Subscribers who may be unrelated to each other.
Subordinate CA	A CA whose CA Certificate is issued by another CA.
Subordinate CA Certificate	A Certificate that (i) includes the Public Key of a Key Pair generated by a certification authority; and (ii) includes the digital signature of a Root CA or Subordinate CA.
Subject	The person, entity, organization or Device identified in the "Subject" field in a Certificate.
Subscriber	A person, entity, or organization that has applied for and has been issued a Certificate.
Subscriber Agreement	The agreement posted in Entrust's Repository applicable to a particular Certificate type, between the CA who issues such Certificate and the Subscriber.
Subscriber Representative	An individual who is authorized to represent a Subscriber.
TLS Certificate (and Private TLS Certificate)	A TLS Certificate issued by a Certification Authority for use on secure servers. The Certification Authority Root CA Certificate is not distributed to any application software vendor for public trust. The Private TLS Certificate may contain domain names which are not publicly registered.
Trusted Role	An employee or contractor of a CA who has authorized access to any component of CA Infrastructure.

Verified PKIaaS Agreement	A legal agreement with Entrust or one of its Affiliates for the provision of Verified PKIaaS.
Wildcard Domain Name	A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

10.2 Acronyms

CA	Certification Authority
CPR	Certificate Problem Report
CP/CPS	Combined Certificate Practice and Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
ECC	Elliptic Curve Cryptography
EKU	Extended Key Usage
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
RA	Registration Authority
RFC	Request for Comment

RSA	Rivest–Shamir–Adleman cryptosystem
SAN	Subject Alternative Name
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Universal Resource Locator

END

fRemainder of his page intentionally left blank.