Entrust PKIaaS

Certification Practice Statement (CPS)

May 20, 2021

Version 1.1

THIS DOCUMENT IS DESIGNATED FOR PUBLIC RELEASE AND MAY BE FREELY DISTRIBUTED

TABLE OF CONTENTS

RECORD OF CHANGES

Version	Date	Author(s)	Description
1.0	24-Feb-21	Colin Tulloch Bruce Morton Charley Chell Alexandra Stockwell	Initial publication
1.1	20-May	Jonah Guo Bruce Morton Charley Chell Alexandra Stockwell	Updated using PKIaaS 1.1 specs

1. INTRODUCTION

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

1.1 OVERVIEW

This CPS describes the practices and procedures of the Certificate Authorities (CAs) and other PKI participants, and forms part of the PKIaaS Agreement under which Entrust makes the PKIaaS available.

This CPS is applicable to the Certificate types issued by a Customer's Root CA or Issuing CA operated by Entrust as part of the PKIaaS as identified and listed in Appendix A.

This CPS is applicable to all persons, entities, and organizations, including, without limitation, all Applicants, Subscribers, Relying Parties, resellers, co-marketers and any other persons, entities, or organizations that have a relationship with Entrust in respect to Certificates issued as part of PKIaaS and/or any services provided by Entrust in connection with PKIaaS. This CPS is incorporated by reference into all Certificates issued by CAs created as part of PKIaaS.

This CPS provides Applicants, Subscribers, Relying Parties, resellers, co-marketers and other persons, entities, and organizations with a statement of the practices and policies of the CAs. This CPS also provides a statement of the rights and obligations of Entrust, any third parties that are operating RAs under the CAs, Applicants, Subscribers, Relying Parties, resellers, co-marketers and any other persons, entities, or organizations that may use or rely on Certificates or have a relationship with a CA or a RA operating under a CA in respect to Certificates and/or any services in respect to Certificates.

The CPS excludes PKI components and services deployed, hosted and operated by the Customer or its delegates, such as RA services, and subordinate or cross-certified CAs operated (by any party) outside of PKIaaS.

This CPS does not cover Entrust Digital Signing as a Service, Entrust Certificate Services, or any publicly-trusted Certificates issued by Entrust.

1.2 IDENTIFICATION

This document is the Entrust PKIaaS Certificate Practice Statement (PKIaaS CPS) and has been assigned the following Object Identifier (OID):

- 2.16.840.1.114027.200.6.10

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

The structure of the PKIaaS PKI environment is comprised of:

- Root CAs: The Root CAs serve as the Customer's PKI trust anchors. The Common Name (CN) of each root CA is defined by the Customer. The Customer's Root CAs issue Certificates to the Customer's Issuing CAs and OCSP services.
- Issuing CAs: The Issuing CAs are subordinate to the Root CAs. The Customer's Issuing CAs are hosted and operated by PKIaaS. The Issuing CAs issue Certificates to or for Subscribers.

1.3.2 Registration Authorities

The RA is the person or entity that makes the decision on whether or not a certificate should be issued in response to a Subscriber request. RAs verify the identity of Applicants and submit certificate issuance requests on their behalf. They are responsible for the Applicant registration, identification and authentication processes.

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

The Customer is the RA and is responsible for the identity verification of and certificate issuance to Subscribers.

1.3.3 Subscribers

Subscribers may use CA services, through an RA, to support transactions and communications.

The Customer is responsible for determining who may be a Subscriber and for determining which people, entities and devices may receive certificates.

1.3.4 Relying Parties

A Relying Party is an entity that relies on or uses a Certificate to verify the Subject's identity, the integrity of a digitally signed message, or to establish confidential communications with the Subject. The Relying Party is responsible for checking the validity of the Certificate using the appropriate Certificate Status Service §4.10.

The Customer is responsible for determining who may use issued certificates.

1.3.5 Entrust Policy Authority (Policy Authority)

Entrust is the Policy Authority, and is responsible for overseeing and setting policy and practices as applicable to this CPS.

1.3.6 Operational Authority.

Entrust is the Operational Authority (OA) and operates all Root and Issuing CA systems hosted and operated on behalf of Customers as part of PKIaaS. These systems issue and manage Certificates, Certificate Revocation Lists (CRLs) and OCSP responses issued in accordance with this CPS. The OA is responsible for:

- Developing and submitting to the Policy Authority for review and approval, the CPS;
- Responsible for all equipment and software, hosted by PKIaaS and required to operate the Customer's PKI; and

- Ensuring that the CAs, Repository, and other PKI-related components hosted by PKIaaS are operated in accordance with this CPS.

1.3.7 Other Participants

No stipulation.

1.4 CERTIFICATE USAGE

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

1.4.1 Appropriate Certificate Uses

The Customer may determine the appropriate uses of each Certificate type.

1.4.2 Prohibited Certificate Uses

The use of all Certificates issued shall be for lawful purposes and consistent with applicable laws, including without limitation, applicable export or import laws. It is prohibited to use Certificates in any manner that violates law. In addition, it is prohibited to use any Certificates in a manner that violates the PKIaaS Acceptable Use Policy.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administration of this Document

The CPS is administered by the Policy Authority; it is based on the policies established by Entrust.

1.5.2 Contact Information

Questions regarding this CPS shall be directed:

Entrust PKIaaS Policy Authority
support@entrust.com
1 (866) 267-9297

1.5.3 Person Determining CPS Suitability for the Policy

The Policy Authority determines the suitability and applicability of this CPS.

1.6 DEFINITIONS

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.

Activation Data: Data values, other than Keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held Key share).

Agreement: A legally binding contract for PKIaaS made up of the PKIaaS terms of use "PKIaaS Schedule", the Entrust General Terms and Conditions provided with the PKIaaS Schedule and which are also available at https://www.entrust.com/-/media/documentation/licensingandagreements/certificate-solutions-general-terms.pdf, and an Order for PKIaaS (as defined in the General Terms).

CA Certificate: A Certificate for one CA's Public Key issued by another CA.

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.

Certificate Revocation List (CRL): A time-stamped list of Certificate serial numbers revoked prior to the expiration of their Validity Periods.

Certification Authority (CA): Technology that creates, issues, manages and revokes Certificates.

Certification Practice Statement (CPS): A statement of the practices that a CA employs in issuing, managing, revoking, and renewing or Re-Keying Certificates.

Cryptographic Module: Either software, a device, or a utility that generates Key Pairs, stores cryptographic information, and/or performs cryptographic functions.

Customer: The entity that has entered into a PKIaaS Agreement with Entrust.

Digital Signature, Digitally Sign: The transformation of an electronic record by one person using a Private Key and Public Key Cryptography so that another person having the transformed record and the corresponding Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the Public Key and whether the record has been altered since the transformation was made.

Distinguished Name (DN): The unique identifier for a Subject so that s/he/it can be located in a directory based on the ITU/CCITT X.500 (e.g. the DN for a Subject might contain the following attributes: common name (cn), e-mail address (mail), Organization name (o), Organizational unit (ou), locality (l), state (st) and country (c)).

Issue Certificates, Issuance: The act performed by a CA in creating a Certificate listing with the CA as "Issuer"

Issuing Certification Authority (Issuing CA): In the context of a particular Certificate, the issuing CA is the CA that issued the Certificate.

Key Generation: The process of creating a Key Pair.

Key Pair: Two mathematically related cryptographic keys, 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.

Public Cloud: Computing services offered by third-party providers over the public internet.

Object Identifier (OID): The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In this CPS, they are used to uniquely identify Certificates issued under this CPS and the cryptographic algorithms supported.

Online Certificate Status Protocol (OCSP): A protocol that is used to provide real-time validation of a Certificate's status. An OCSP responder is used to respond to Certificate status requests and can issue one of three responses: Valid, Invalid, or Unknown. An OCSP responder replies to Certificate status requests on the basis of CRLs provided to it by CAs.

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.

PKI Certificate: A Certificate issued pursuant to this CPS.

Private Key: The sensitive Key in the Key Pair protected by the Subject (or individual or entity that controls the Subject) and kept secret. The Private Key creates Digital Signatures or decrypts data previously encrypted using the corresponding Public Key.

Public Key: The non-sensitive Key in the Key Pair submitted as part of a Certificate Signing Request by the Subscriber and disclosed in the subsequently-issued Certificate. The Public Key verifies Digital Signatures created using the corresponding Private Key, or encrypts data meant for decryption with the corresponding Private Key.

Public Key Cryptography: A type of cryptography also knows as asymmetric cryptography. This cryptography uses a Key Pair rather than a single Key to secure the authentication and/or confidentiality of data.

Public Key Infrastructure (PKI): The architecture, technology, practices, and procedures that support operation of a security system employing Certificates and Public Key Cryptography.

Registration Authority (RA): An individual or organization or process responsible for verifying the identity of a Subscriber.

Relying Party: An individual or legal entity that relies on a Certificate and/or any digital signatures verified using that Certificate.

Repository: An online system for storing and retrieving Certificates and other information relevant to Certificates, including information relating to Certificate validity or revocation.

Revoke (a Certificate): To invalidate a Certificate permanently from a specific time onward. Revocation includes listing the Certificate in a set of revoked Certificates or other directory or database of revoked Certificates (e.g. inclusion in a CRL). The system also prevents users from accessing revoked Certificates once connected to the central infrastructure.

Request For Comments (RFC): Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications such as Telnet and FTP.

Root CA: The top level CAs as described in §1.3.1.

Subject: The individual, legal entity, organization or device identified in a Certificate, who or which holds the Private Key corresponding to the Public Key given in the Certificate.

Subscriber: The person, legal entity, or organization that has applied for and has been issued a Certificate. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

Trusted Role: An employee or contractor who has authorized access to or control over PKIaaS.

Validity Period: The intended term of validity of a Certificate, beginning with the date of Issuance ("Valid From" or "Activation" date), and ending with the earlier of two dates: the expiration date indicated in the Certificate ("Valid To" or "Expiry" date) or the revocation date asserted in the revocation list specified as the CRL Distribution Point within the Certificate.

X.500: A series of computer networking standards covering electronic directory services. These services include Directory Access Protocol (DAP), Directory System Protocol (DSP), Directory Information Shadowing Protocol (DISP), and Directory Operational Bindings Management Protocol (DOP).

X.509: An International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) standard for Public Key Infrastructure which specifies standard formats for Public Key Certificates and certification path validation.

1.6.1 Acronyms

AES	Advanced Encryption Standard
CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSS	Certificate Status Server
DN	Distinguished Name
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
LRA	Local Registration Authority
PKIaaS	Public Key Infrastructure as a Service
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OTP	One-time Passcode
PA	Policy Authority
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request for Comment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
TLS	Transport Layer Security
URL	Uniform Resource Locator

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Entrust maintains the Repository to store various information related to Certificates and the operation of the CAs. This CPS and related information is published in the Repository.

2.1 REPOSITORY

Entrust maintains the Repository to allow access to Certificate-related and Certificate revocation information. The information in the Repository is accessible through a web interface, available on a 24x7 basis and is periodically updated as set forth in this CPS. The Repository is the only approved source for CRL and other information about Certificates.

PKIaaS will adhere to the latest version of the CPS published in the Repository.

The Repository can be accessed at https://www.entrust.net/CPS.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

PKIaaS publishes this CPS, CA Certificates, its form of Agreement, and CRLs in the Repositories.

2.3 TIME OR FREQUENCY OF PUBLICATION

The CPS will be re-issued and published at least once per year.

CRLs will be updated as per §4.9.7.

OCSP responses will be updated as per §4.9.10.

2.4 ACCESS CONTROLS ON REPOSITORIES

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

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

3.1.2 Need for Names to be Meaningful

CA Certificates must identify the subject as a CA and include the Customer organization name.

The RA is responsible to ensure the Subject names in Subscriber Certificates are meaningful to Relying Parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation

3.1.4 Rules for Interpreting Various Name Forms

No stipulation

3.1.5 Uniqueness of Names

CA distinguished names shall be unique.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of an Organization Identity

Responsibility of the RA.

3.2.3 Authentication of an Individual Identity

Responsibility of the RA.

3.2.4 Non-verified Subscriber Information

Responsibility of the RA.

3.2.5 Validation of Authority

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

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

3.2.6 Criteria for Interoperation

Responsibility of the RA.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Responsibility of the RA.

3.3.2 Identification and Authentication for Re-key after Certificate Revocation

Responsibility of the RA.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

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

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

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

4.1.1 Who Can Submit a Certificate Application

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

4.1.2 Enrollment Process and Responsibilities

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

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

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

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

The identification and authentication of the Subscriber is performed by the RA.

4.2.2 Approval or Rejection of Certificate Applications

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

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

4.2.3 Time to Process Certificate Applications

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

4.3 CERTIFICATE ISSUANCE

After performing verification of the information provided with a Certificate Application, an RA operating under a CA may request that a CA issue a Certificate. Upon receipt of a request from an RA operating under a CA, the CA will perform the verification described in §4.2.1, and then generate and digitally sign a Certificate in accordance with the Certificate profile described in §7.

4.3.1 CA Actions during Certificate Issuance

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

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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Notification to Subscriber is the responsibility of the RA.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

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

4.5.2 Relying Party Public key and Certificate Usage

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

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

Responsibility of the RA.

4.6.2 Who May Request Renewal

Responsibility of the RA.

4.6.3 Processing Certificate Renewal Requests

Certificate renewal is processed the same as Certificate issuance.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification to Subscriber is the responsibility of the RA.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

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

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Re-key

A Subscriber should request a Certificate with a new Public Key if the Private Key is compromised or at the end of the lifecycle of the Key Pair.

4.7.2 Who May Request Certification of a New Public Key

Responsibility of the RA.

4.7.3 Processing Certificate Re-keying Requests

Certificate re-key is processed the same as Certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification to Subscriber is the responsibility of the RA.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Rey-keyed Certificate by the CA

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

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.8 CERTIFICATE MODIFICATION

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

4.9 CERTIFICATE REVOCATION AND SUSPENSION

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

4.9.1 Circumstances for Revocation

Revocation of CA Certificates may be performed by Entrust in the following circumstances.

- The RA requests for an Issuing Certificate to be revoked;
- The RA can be shown to have violated, or is suspected of violating, the requirements of this CPS or the Agreement;
- There is a suspected compromise of the associated private key; or
- When the Agreement with Entrust is terminated.

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

4.9.2 Who can Request Revocation of a Certificate

The RA may request revocation of any Certificates issued.

It is the responsibility of the RA to handle Subscriber requests for Certificate revocation.

4.9.3 Procedure for Revocation Request

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

1. Compromise of the Certificates Private Key;
2. Knowledge that the original Certificate request was not authorized

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

4.9.4 Certificate Revocation Grace Period

CAs to not apply any grace period. Revocation requests are processed synchronously in sequence with the API request and response.

4.9.5 Time Within Which CA Must Process The Revocation Request

CAs will revoke Certificates upon receipt of a proper revocation request.

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 Revocation Lists Issuance Frequency

CRLs are generated at least every day with a next CRL update time of 2 days from the issuing date.

The revocation request of a certificate can set an instant CRL update flag. In this case a new CRL will be generated containing the revoked certificate in the requests as soon as possible,

depending on the service load. In a normal load the CRL will be generated in less than 15 minutes.

4.9.8 Maximum Latency for CRLs

CRLs are available within seconds of issuance. No delay is imposed between the issuance and publication of CRLs for caching or any other purpose.

4.9.9 On-line Revocation/Status Checking Availability

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

4.9.10 On-line Revocation Checking Requirements

CAs support an OCSP capability using the GET and POST methods for Certificates issued in accordance with this CPS.

The CAs shall sign and make available OCSP as follows:

1. OCSP responses for Issuing CA Certificates are issued upon request.
2. OCSP responses for Subscriber Certificates are issued upon request.

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

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

4.9.11 Other Forms of Revocation Advertisements Available

The CA does not provide any other forms of Certificate status.

4.9.12 Special Requirements re: Key Compromise

If an RA suspects, knows, or is informed of Private Key compromise, then the RA is required to take necessary steps to revoke the Certificate, immediately stop using such Certificate, and remove such Certificate from any devices and/or software in which such Certificate has been installed.

4.9.13 Circumstances for Suspension

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

4.9.14 Who Can Request Suspension

The RA may request suspension of any Certificates issued.

It is the responsibility of the RA to handle requests for Certificate suspension.

4.9.15 Procedure for Suspension Request

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

4.9.16 Limits on Suspension Period

There is no time limit on suspension.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

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

4.10.2 Service Availability

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

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

End of subscription is addressed in the Agreement.

4.12 KEY ESCROW AND RECOVERY

CA and Subscriber key escrow are not supported. Subscriber key recovery is not supported.

4.12.1 Key Escrow and Recovery Policy and Practices

CA Keys can be recovered from an database and HSM backup.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

5.1.1 Site Location and Construction

The computing facilities that host the HSM and Activation Data are located in Entrust Tier III, SSAE-18 datacenters. Access to these facilities is restricted to personnel in Trusted Roles.

The computing facilities that host the Certificate issuance, revocation and status service components are provided by one or more Public Clouds. The physical security controls imposed on components residing within a Public Cloud are outside the scope of this CPS.

5.1.2 Physical Access

The room containing the HSM is designated a two (2) person zone, and controls are used to prevent a person from being in the room alone. Alarm systems are used to notify security personnel of any violation of the rules for access to the HSM.

5.1.3 Power and Air Conditioning

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

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

The HSM is hosted in Tier III datacenters equipped with fire suppression mechanisms. The facility is fully wired for fire detection, alarm and suppression. Routine, frequent inspections of all systems are made to assure adequate operation.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-Site Backup

Backups of the CA key material and CA databases, sufficient to recover from system failure, shall be made on a periodic schedule in accordance with disaster recovery requirements in section 5.7.

5.2 PROCEDURAL CONTROLS FOR THE CA

5.2.1 Trusted Roles

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

5.2.2 Number of Persons Required Per Task

The CA Private Keys are backed up, stored, and recovered only by personnel in Trusted Roles using dual control in a physically secured environment.

5.2.3 Identification and Authentication for Each Role

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

5.2.4 Roles Requiring Separation of Duties

Personnel in Trusted Roles with the ability to deploy to or access the PKIaaS production systems do not have the ability to commit software code. Development team members with the ability to commit code do not have the ability to deploy to or access PKIaaS production systems.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel in Trusted Roles must undergo background investigations and must be trained for their specific role.

5.3.2 Background Check Procedures

Background checks are conducted as per the Entrust hiring processes.

5.3.3 Training Requirements

Personnel in Trusted Roles will receive training. Training will be conducted in the following areas:

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

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to the PKIaaS must meet applicable requirements as set forth in this CPS.

5.3.8 Documentation Supplied to Personnel

No stipulation.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

Significant security events in the CAs are automatically time-stamped and recorded as audit logs. Audit logs are archived periodically. Where these events cannot be electronically logged, the CA shall supplement electronic audit logs with physical logs as necessary.

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

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

5.4.2 Frequency of Processing Data

The audit logs are continuously monitored by a Security Information and Event Management (SIEM) system. Policy violations and other significant events generate alerts that are reviewed by operations and security teams for malicious activity.

5.4.3 Retention Period for Security Audit Data

The audit logs are retained on the PKI system for at least three months. Audit logs are periodically archived in accordance with section 5.5.

5.4.4 Protection of Security Audit Data

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

5.4.5 Audit Log Backup Procedures

Audit logs are periodically archived in accordance with section 5.5.

5.4.6 Audit Collection System

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

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Risk assessment is performed annually that:

1. (i) Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate data or Certificate management processes;
2. (ii) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate data and Certificate management processes; and
3. (iii) Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the risk assessment, a security plan is developed, implemented, and maintained consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate data and Certificate management processes. The security plan also takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

The audit logs, data and revocation information for the CAs are archived, as well as data necessary to access or verify archive contents.

5.5.2 Retention Period for Archive

Audit logs are retained by PKIaaS for a maximum of 6 years.

The data and revocation information of expired or deleted CAs are permanently deleted within 60 days.

5.5.3 Protection of Archive

The archive data is stored in a two-person controlled safe located in a facility to which only Entrust-authorized personnel have access.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System

Archive data will be collected as part of the routine system backup procedures, along with manual storage of physical materials such as cryptographic modules and datacenter access logs.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 KEY CHANGEOVER

CAs will not be re-keyed. CA key pairs will be retired from service at the end of their 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.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The disaster recovery plan addresses 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) recovery point objective (RPO) of fifteen minutes

(vii) recovery time objective (RTO) of 24 hours for essential CA operations which include Certificate revocation, and issuance of Certificate revocation status

(viii) testing of recovery plans

In order to mitigate the event of a disaster, the CAs have implemented the following:

(ix) two datacenters with highly-available HSMs and secure on-site and off-site storage of backup HSMs containing copies of all CA Private Keys

(x) secure on-site and off-site storage of all requisite activation materials

(xi) database replication between primary and secondary regions

(xii) daily database backups within both the primary and secondary regions

(xiii) weekly backup of critical data to a secure off-site storage facility

(xiv) secure off-site storage of disaster recovery plan and disaster recovery procedures

(xv) environmental controls as described in §5.1

Entrust has implemented physical datacenters near Dallas, TX and Denver, CO. Cloud-based components utilize multiple availability zones for high availability and a secondary region for disaster recovery.

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

5.7.2 Computing Resources, Software, and/or Data are Corrupted

No stipulation.

5.7.3 Entity Private Key Compromise Procedures

5.7.4 In the event of a compromised RA credential, the credential is revoked. Business Continuity Capabilities After a Disaster

No stipulation.

5.8 CA TERMINATION

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

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION

6.1.1 Key Pair Generation and Installation

6.1.1.1 CA Key Pair Generation

An API based, automated, documented process to generate CA key pairs is executed at the request of the RA.

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

(i) Generate the CA Key Pair in a physically secured environment;
(ii) Generate the CA Key Pair within hardware cryptographic modules meeting the applicable requirements of §6.2.11;
(iii) Log its CA Key Pair generation activities; and
(iv) Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CPS.

6.1.1.2 Subscriber Key Pair Generation

No stipulation, as the Subscriber Key Pair is generated by the Subscriber.

6.1.2 Key Delivery to Subscriber

Not applicable as the Subscriber Key Pair is generated by the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

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

RSA 4096
RSA 3072
RSA 2048
ECDSA P-521
ECDSA P-384
ECDSA P-256

6.1.6 Public Key Parameters Generation and Quality Checking

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

Subscriber Public Keys: no stipulation.

6.1.7 Key Usage Purposes

No stipulation.

6.2 PRIVATE KEY PROTECTION

6.2.1 Cryptographic Module Standards and Control

CA Private Keys must be used and protected on cryptographic modules that meet or exceed the requirements as defined in §6.2.11. The cryptographic modules are held in secure facilities.

6.2.2 CA Private Key Multi-Person Control

A minimum of two-person control will be established on the activation and backup of any CA Private Key, and may be implemented as a combination of technical and procedural controls. Persons involved in management and use of the CA Private Keys shall be Trusted Roles.

6.2.3 Private Key Escrow

CA Private Keys are not escrowed.

6.2.4 Private Key Backup

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

6.2.5 Private Key Archival

CA Private Keys are not archived.

6.2.6 Private Key Transfer into or from Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Keys

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

6.2.9 Private Key Deactivation Methods

CA Private Keys will be deactivated upon termination of service.

6.2.10 Private Signature Key Destruction Method

No stipulation.

6.2.11 Cryptographic Module Rating

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

6.3 OTHER ASPECTS OF KEY-PAIR MANAGEMENT

6.3.1 Public Key Archival

CA public keys are archived in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

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

Certificate operational (validity) periods are defined in Appendix A.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

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

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

6.4.2 Activation Data Protection

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

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

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The CA systems are physically secured as described in §5.1. The CA systems operate enforce identification and authentication of users. All Trusted Roles that are authorized to have access to

the CAs are required to use hardware tokens in conjunction with a PIN or biometric to gain access to the physical room that contains the CA key material being used for such CAs.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

Systems developed by Entrust are deployed in accordance with Entrust software lifecycle development standards.

6.6.2 Security Management Controls

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

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

A network firewall must protect network access to the CA system. The network firewall limits services allowed to and from the CA system to those required to perform CA functions.

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

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

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

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

6.8 TIME-STAMPING

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

7. CERTIFICATE AND CRL PROFILES

7.1 CERTIFICATE PROFILE

CAs issue Certificates in accordance with the X.509 version 3. Certificate profiles for Root CA Certificate, Subordinate CA Certificates, and Subscriber Certificates are described in sections below and in Appendix A.

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

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

7.1.3 Algorithm Object Identifiers

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

Signature Algorithm Identifier	OID
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
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}

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

Algorithm Identifier	OID
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
ecPublicKey	{iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) 1}

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

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

7.1.4 Name Forms

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

7.1.5 Name Constraints

The *nameConstraints* extension field is not used in CA Certificates.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

No stipulation.

7.1.6.2 Root CA Certificates

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

7.1.6.3 Issuing CA Certificates

No stipulation.

7.1.6.4 Subscriber Certificates

No stipulation.

7.1.7 Usage of Policy Constraints Extension

The *policyConstraints* extension is not used in CA Certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificate policies extension is marked Not Critical.

7.2 CRL PROFILE

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

- version: set to v2
- signature: identifier of the algorithm used to sign the CRL
- issuer: the full Distinguished Name of the CA issuing the CRL
- this update: time of CRL issuance
- next update: time of next expected CRL update
- revoked Certificates: list of revoked Certificate information

7.2.1 Version Numbers

No stipulation.

7.2.2 CRL Entry Extensions

CRLs issued support the Authority Key Identifier, crlNumber, invalidityDate, and expiredCertsOnCRL extensions.

7.3 OCSP PROFILE

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

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENT

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The Compliance Auditor shall perform an audit on an annual basis of all active CAs.

8.2 IDENTITY/QUALIFICATIONS OF COMPLIANCE AUDITOR

The compliance audit of the CAs will be performed by an auditor ("Compliance Auditor") which possesses the following qualifications and skills:

- Ability to conduct an audit that addresses the criteria of the audit schemes specified in §8.4;
- Bound by Entrust professional code of ethics.

8.3 COMPLIANCE AUDITOR'S RELATIONSHIP TO AUDITED PARTY

The Compliance Auditor is an internal employee on the Entrust Compliance and Audit team.

8.4 TOPICS COVERED BY COMPLIANCE AUDIT

Verify that all CAs comply with the requirements of the current version of this CPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Upon receipt of a compliance audit that identifies any deficiencies, the audited CA will correct any such deficiencies in an expeditious manner.

8.6 COMMUNICATION OF RESULT

The results of all compliance audits will be communicated to the Policy Authority.

9. OTHER BUSINESS AND LEGAL MATTERS

As per the applicable Agreement.

10. APPENDIX A – CERTIFICATE PROFILES

PKIaaS certificate issuance is always in the context of a Certificate Profile. These profiles are defined within the PKIaaS service and are referenced by name in certificate issuance requests.

Certificate profiles are listed below in "library sets" that are enabled as a set based on the applicability to Customer use cases.

10.1 CA CERTIFICATE PROFILES

Profile		**Root Certificate (ca-root)**	**Subordinate CA (ca-subord)**
Signature Algorithm		RSA 2048 -> sha256WithRSAEncryption RSA 3072 -> sha256WithRSAEncryption RSA 4096 -> sha512WithRSAEncryption ECDSA P-256 -> ecdsa-with-SHA256 ECDSA P-384 -> ecdsa-with-SHA384 ECDSA P-521 -> ecdsa-with-SHA512	RSA 2048 -> sha256WithRSAEncryption RSA 3072 -> sha256WithRSAEncryption RSA 4096 -> sha512WithRSAEncryption ECDSA P-256 -> ecdsa-with-SHA256 ECDSA P-384 -> ecdsa-with-SHA384 ECDSA P-521 -> ecdsa-with-SHA512
Issuer		Self-signed	Customer's root CA
Validity Period		Less than or equal to 20 years	Less than or equal to 10 years, subject to the constraint that the subordinate expiry cannot be beyond that of the root
Subject		No constraints	No constraints
Key Algorithm		RSA 2048, RSA 3072, RSA 4096 ECDSA P-256, ECDSA P-384, ECDSA P-521	RSA2048, RSA 3072, RSA 4096 ECDSA P-256, ECDSA P-384, ECDSA P-521
Extensions			
Basic Constraints	Critical	cA is True	cA is True, pathLenConstraint=0
Subject Key Identifier	Not critical	160-bit SHA-1 hash of subjectPublicKey	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	Not critical	Never present	Matches subjectKeyIdentifier of signing certificate
Key Usage	Critical	digitalSignature, keyCertSign, cRLSign	digitalSignature, keyCertSign, cRLSign
Extended Key Usage	Not critical	Never present	Never present
CRL Distribution Points	Not critical	Never present (not applicable)	Always present
AIA	Not critical	Never present	Supplied based on customer opt-in to OCSP

10.2 BASIC CERTIFICATE PROFILES (RSA)

Profile		**TLS Client Authentication (ee-auth)**	**TLS Server Authentication (webserver)**	**Validation Authority (ocsp)**
Signature Algorithm		RSA 2048 -> sha256WithRSAEncryption RSA 3072 -> sha256WithRSAEncryption RSA 4096 -> sha512WithRSAEncryption		
Issuer		Customer's subordinate issuing CA		
Validity Period		Less than or equal to 3 years, subject to the constraint that the subordinate expiry cannot be beyond that of the issuing CA	Less than or equal to 3 years, subject to the constraint that the subordinate expiry cannot be beyond that of the issuing CA	30 days
Subject		No constraints	No constraints	No constraints
Key Algorithm		RSA2048, RSA 3072, RSA 4096		
Extensions				
Basic Constraints	Critical	cA is False		
Subject Key Identifier	Not critical	160-bit SHA-1 hash of subjectPublicKey		
Authority Key Identifier	Not critical	Matches subjectKeyIdentifier of signing certificate		
Subject Alternative Name	Not critical	No constraints		
Key Usage	Critical	Digital Signature	Digital Signature, Key Encipherment	Digital Signature, Non-Repudiation
Extended Key Usage	Not critical	TLS Web Client Authentication	TLS Web Server Authentication, TLS Web Client Authentication	OCSP Signing
CRL Distribution Points	Not critical	Always present	Always present	Not applicable
AIA	Not critical	Supplied based on customer opt-in to OCSP	Supplied based on customer opt-in to OCSP	Not applicable
OCSP	Not critical	Never present	Never present	No check

10.3 BASIC CERTIFICATE PROFILES (ECDSA)

Profile		**TLS Client Authentication (ee-auth)**	**TLS Server Authentication (webserver)**	**Validation Authority (ocsp)**
Signature Algorithm		ECDSA P-256 -> ecdsa-with-SHA256 ECDSA P-384 -> ecdsa-with-SHA384 ECDSA P-521 -> ecdsa-with-SHA512		
Issuer		Customer's subordinate issuing CA		
Validity Period		Less than or equal to 3 years, subject to the constraint that the subordinate expiry cannot be beyond that of the issuing CA	Less than or equal to 3 years, subject to the constraint that the subordinate expiry cannot be beyond that of the issuing CA	30 days
Subject		No constraints	No constraints	No constraints
Key Algorithm		ECDSA P-256, ECDSA P-384, ECDSA P-521		
Extensions				
Basic Constraints	Critical	cA is False		
Subject Key Identifier	Not critical	160-bit SHA-1 hash of subjectPublicKey		
Authority Key Identifier	Not critical	Matches subjectKeyIdentifier of signing certificate		
Subject Alternative Name	Not critical	No constraints		
Key Usage	Critical	Digital Signature	Digital Signature	Digital Signature, Non-Repudiation
Extended Key Usage	Not critical	TLS Web Client Authentication	TLS Web Server Authentication, TLS Web Client Authentication	OCSP Signing
CRL Distribution Points	Not critical	Always present	Always present	Not applicable
AIA	Not critical	Supplied based on customer opt-in to OCSP	Supplied based on customer opt-in to OCSP	Not applicable
OCSP	Not critical	Never present	Never present	No check

10.4 ENTRUST CERTIFICATE ENROLLMENT GATEWAY WSTEP CERTIFICATE PROFILES

The Subscriber Certificate key algorithm / signature algorithm pair is at subscriber discretion.

Profile		**Digital Signature**	**Digital Signature with Key Encipherment**	**Key Encipherment**	**Non-Repudiation**
Issuer		Customers subordinate issuing CA			
Validity Period		Less than or equal to 3 years, subject to the constraint that the subordinate expiry cannot be beyond that of the issuing CA			
Subject		No constraints			
Extensions					
Basic Constraints	Critical	CA=False			
Subject Key Identifier	Not critical	160-bit SHA-1 hash of subjectPublicKey			
Authority Key Identifier	Not critical	Matches subjectKeyIdentifier of signing certificate			
Subject Alternative Name	Not critical	No constraints			
Key Usage	Critical	Digital Signature	Digital Signature, Key Encipherment	Key Encipherment	Non-Repudiation
Extended Key Usage	Not critical	No constraints			
CRL Distribution Points	Not critical	Always present			
AIA	Not critical	Supplied based on customer opt-in			
Other Extensions	Not critical	The following are allowed in requests. Other extensions are ignored • CertificatePolicies 2.5.29.32ApplicationPolicies 1.3.6.1.4.1.311.21.10 • SmimeCapabilities 1.2.840.113549.1.9.15 • MSTemplateOID 1.3.6.1.4.1.311.21.7 • MSTemplateName 1.3.6.1.4.1.311.20.2			

10.5 S/MIME SECURE EMAIL CERTIFICATE PROFILES

The Subscriber Certificate key algorithm / signature algorithm pair is at subscriber discretion.

Profile		**Digital Signature with Key Encipherment**	**Key Encipherment**	**Digital Signature, Non-Repudiation**
Issuer		Customers subordinate issuing CA		
Validity Period		Less than or equal to 3 years, subject to the constraint that the subordinate expiry cannot be beyond that of the issuing CA		
Subject		No constraints		
Extensions				
Basic Constraints	Critical	CA=False		
Subject Key Identifier	Not critical	160-bit SHA-1 hash of subjectPublicKey		
Authority Key Identifier	Not critical	Matches subjectKeyIdentifier of signing certificate		
Subject Alternative Name	Not critical	No constraints		
Key Usage	Critical	Digital Signature, Key Encipherment	Key Encipherment	Digital Signature, Non-Repudiation
Extended Key Usage	Not critical	TLS client authentication 1.3.6.1.5.5.7.3.2 Email Protection 1.3.6.1.5.5.7.3.4	Email Protection 1.3.6.1.5.5.7.3.4	Email Protection 1.3.6.1.5.5.7.3.4
CRL Distribution Points	Not critical	Always present		
AIA	Not critical	Supplied based on customer opt-in		