eSignTrust
澳門郵政 CORREIOS DE MACAU
電子認證服務 SERVIÇOS DE CERTIFICAÇÃO

Macao Post and Telecommunications eSignTrust Certification Services

Certification Practice Statement of Macao Post and Telecommunications eSignTrust Certification Services

Copyright © Correios e Telecomunicações de Macau, 2019. All rights reserved.

Version: 5.0
Document Release Date: 11 February 2019

eSignTrust and the eSignTrust logo are the registered trademarks of Correios e Telecomunicações de Macau ("CTT"). No part of this publication may be reproduced, in whole or in part without prior permission of CTT.

1. INTRODUCTION 8

1.1. Overview 8
1.2. Document Name and Identification 8
1.3. PKI Participants 9
  1.3.1. Policy Management Authority 9
  1.3.2. Certification Authorities 9
  1.3.3. Registration Authorities 9
  1.3.4. Repositories 10
  1.3.5. Subscribers 10
  1.3.6. Relying Parties 10
1.4. Certificate Usage 11
  1.4.1. Identity Certificate (Signing Certificate) Usage 11
  1.4.2. Encipherment Certificate Usage 11
  1.4.3. Email Certificate Usage 12
1.5. Policy Administration 12
  1.5.1. Specification of administrative organisation 12
  1.5.2. Contact person 12
  1.5.3. Person determining CPS suitability for the policy 13
1.6. Definitions and Acronyms 13

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 22

2.1. Repository 22
2.2. Publication of certification information 22
2.3. Time or frequency of publication 22
2.4. Access controls on repositories 22

3. IDENTIFICATION AND AUTHENTICATION (I&A) 23

3.1. Naming 23
  3.1.1. Type of Names 23
  3.1.2. Need for Names to be Meaningful 23
  3.1.3. Anonymity or Pseudonymity of Subscribers 23
  3.1.4. Rules for Interpreting Various Name Forms 23
  3.1.5. Uniqueness of Names 26
  3.1.6. Recognition, Authentication, and Role of Trademarks 26
3.2. Initial Identity Validation 27
  3.2.1. Method to Prove Possession of Private Key 27
  3.2.2. Authentication of Organisation Identity 28
  3.2.3. Authentication of Individual Identity 28
  3.2.4. Nonverified Subscriber Information 29
  3.2.5. Validation of Authority 29
  3.2.6. Criteria for interoperation 30
3.3. Identification and Authentication for Re-key Requests 30
  3.3.1. Identification and Authentication for routine re-key requests 30
  3.3.2. Identification and Authentication for re-key After Revocation 31
3.4. Identification and Authentication for Revocation Requests 31

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 33

4.1. Certificate Application 33
  4.1.1. Who can submit a certificate application 33
  4.1.2. Enrollment process and responsibilities 33
4.2. Certificate Application Processing 35
  4.2.1. Performing identification and authentication functions 35
  4.2.2. Approval or rejection of certificate application 35
  4.2.3. Time to process certificate applications 35
4.3. Certificate Issuance 36
  4.3.1. CA actions during certificate issuance 36
  4.3.2. Notification to subscriber by the CA of issuance of certificate 36

4.4. CERTIFICATE ACCEPTANCE 36
  4.4.1. *Conduct constituting certificate acceptance* *37*
  4.4.2. *Publication of the certificate by CA* *37*
  4.4.3. *Notification of certificate issuance by the CA to other entities* *37*
4.5. KEY PAIR AND CERTIFICATE USAGE 37
  4.5.1. *Subscriber private key and certificate usage* *37*
  4.5.2. *Relying party public key and certificate usage* *37*
4.6. CERTIFICATE RENEWAL 38
  4.6.1. *Circumstance for certificate renewal* *38*
  4.6.2. *Who may request renewal* *38*
  4.6.3. *Processing certificate renewal requests* *38*
  4.6.4. *Notification of new certificate issuance to subscriber* *38*
  4.6.5. *Conduct constituting acceptance of a renewal certificate* *38*
  4.6.6. *Publication of the renewal certificate by CA* *38*
  4.6.7. *Notification of certificate issuance by the CA to other entities* *38*
4.7. CERTIFICATE RE-KEY 39
  4.7.1. *Circumstance for certificate re-key* *39*
  4.7.2. *Who may request certification of a new public key* *39*
  4.7.3. *Processing certificate re-keying requests* *39*
  4.7.4. *Notification of new certificate issuance to subscriber* *39*
  4.7.5. *Conduct constituting acceptance of a re-keyed certificate* *39*
  4.7.6. *Publication of the re-keyed certificate by the CA* *39*
  4.7.7. *Notification of certificate issuance by the CA to other entities* *39*
4.8. CERTIFICATE MODIFICATION 39
  4.8.1. *Circumstance for certificate modification* *39*
  4.8.2. *Who may request certificate modification* *40*
  4.8.3. *Processing certificate modification requests* *40*
  4.8.4. *Notification of new certificate issuance to subscriber* *40*
  4.8.5. *Conduct constituting acceptance of modified certificate* *40*
  4.8.6. *Publication of the modified certificate by the CA* *40*
  4.8.7. *Notification of certificate issuance by the CA to other entities* *40*
4.9. CERTIFICATE REVOCATION AND SUSPENSION 40
  4.9.1. *Circumstances for revocation* *40*
  4.9.2. *Who can request revocation* *41*
  4.9.3. *Procedure for revocation request* *41*
  4.9.4. *Revocation request grace period* *42*
  4.9.5. *Time within which CA must process the revocation request* *42*
  4.9.6. *Revocation checking requirement for relying parties* *42*
  4.9.7. *CRL issuance frequency* *42*
  4.9.8. *Maximum latency for CRLs* *43*
  4.9.9. *On-line revocation/status checking availability* *43*
  4.9.10. *On-line revocation checking requirements* *43*
  4.9.11. *Other forms of revocation advertisements available* *43*
  4.9.12. *Special requirement re-key compromise* *43*
  4.9.13. *Circumstance for suspension* *43*
  4.9.14. *Who can request suspension* *43*
  4.9.15. *Procedure for suspension request* *44*
  4.9.16. *Limit on suspension period* *44*
4.10. CERTIFICATE STATUS SERVICES 44
  4.10.1. *Operational characteristics* *44*
  4.10.2. *Services availability* *45*
  4.10.3. *Optional features* *45*
4.11. END OF SUBSCRIPTION 45
4.12. KEY ESCROW AND RECOVERY 45
  4.12.1. *Key Escrow and recovery policy and practices* *45*
  4.12.2. *Session key encapsulation and recovery policy and practices* *45*

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 46
5.1. PHYSICAL CONTROLS 46
5.1.1. Site Location and Construction 46
5.1.2. Physical Access 46
5.1.3. Power and Air Conditioning 46
5.1.4. Water Exposure 46
5.1.5. Fire Prevention and Protection 47
5.1.6. Media Storage 47
5.1.7. Waste Disposal 47
5.1.8. Off-site backup 47
5.2. PROCEDURAL CONTROL 47
5.2.1. Trusted Roles 47
5.2.2. Number of persons required per task 48
5.2.3. Identification and authentication of each role 48
5.3. PERSONNEL CONTROL 48
5.3.1. Background, qualifications, experience, and clearance requirements 48
5.3.2. Background check procedures 49
5.3.3. Training requirements 49
5.3.4. Retraining frequency and requirements 49
5.3.5. Job rotation frequency and sequence 49
5.3.6. Sanctions for unauthorised actions 49
5.3.7. Independent Contractor requirements 50
5.3.8. Documentation supplied to personnel 50
5.4. AUDIT LOGGING PROCEDURES 50
5.4.1. Types of event recorded 50
5.4.2. Frequency of processing log 50
5.4.3. Retention period for audit log 50
5.4.4. Protection of audit log 51
5.4.5. Audit log backup procedures 51
5.4.6. Audit collection system (internal or external) 51
5.4.7. Notification to event-causing subject 51
5.4.8. Vulnerability assessments 51
5.5. RECORDS ARCHIVAL 51
5.5.1. Types of records archived 51
5.5.2. Retention period for archive 52
5.5.3. Protection of archive 52
5.5.4. Archive backup procedures 52
5.5.5. Requirements for time-stamping of records 52
5.5.6. Archive collection system (internal or external) 52
5.5.7. Procedures to obtain and verify archived information 52
5.6. KEY CHANGEOVER 52
5.7. COMPROMISE AND DISASTER RECOVERY 53
5.7.1. Incident and Compromise handling procedures 53
5.7.2. Computing resources, software, and/or data are corrupted 53
5.7.3. Entity private key compromise procedures 54
5.7.4. Business continuity capabilities after a disaster 54
5.7.5. CA or RA Termination 54
6. TECHNICAL SECURITY CONTROLS 55
6.1. KEY PAIR GENERATION AND INSTALLATION 55
6.1.1. Key pair generation 55
6.1.2. Private key delivery to Subscriber 55
6.1.3. Public key delivery to certificate issuer 55
6.1.4. CA public key delivery to users 55
6.1.5. Key sizes 56
6.1.6. Public key parameters generation and quality checking 56

6.1.7. *Key usage purposes* ... 56
6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROL ... 56
6.2.1. *Cryptographic module Standards and control* ... 56
6.2.2. *Private Key (m out of n) multiperson control* ... 57
6.2.3. *Private Key Escrow* ... 57
6.2.4. *Private Key backup* ... 57
6.2.5. *Private key archival* ... 57
6.2.6. *Private Key transfer into or from a cryptographic module* ... 57
6.2.7. *Private Key storage on cryptographic module* ... 57
6.2.8. *Method of activating private key* ... 58
6.2.9. *Method of deactivating private key* ... 58
6.2.10. *Method of destroying private key* ... 58
6.2.11. *Cryptographic module rating* ... 58
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT ... 58
6.3.1. *Public key archival* ... 58
6.3.2. *Certificate operational periods and key pair usage period* ... 59
6.4. ACTIVATION DATA ... 59
6.4.1. *Activation data generation and installation* ... 59
6.4.2. *Activation data protection* ... 59
6.4.3. *Other aspects of activation data* ... 59
6.5. COMPUTER SECURITY CONTROLS ... 59
6.5.1. *Specific computer security technical requirements.* ... 59
6.5.2. *Computer security rating* ... 60
6.6. CERTIFICATE LIFE CYCLE TECHNICAL CONTROLS ... 60
6.6.1. *System development controls* ... 60
6.6.2. *Security management controls.* ... 60
6.6.3. *Life cycle security ratings* ... 60
6.7. NETWORK SECURITY CONTROLS ... 60

7. CERTIFICATE, CRL, AND OCSP PROFILES ... 62

7.1. CERTIFICATE PROFILE ... 62
7.1.1. *Version number(s)* ... 62
7.1.2. *Certificate Extensions* ... 62
7.1.3. *Algorithm Object Identifier* ... 62
7.1.4. *Name Forms* ... 63
7.1.5. *Name Constrains* ... 63
7.1.6. *Certificate Policy Object Identifier* ... 63
7.1.7. *Usage of Policy Constraints extension* ... 64
7.1.8. *Policy qualifiers syntax and semantics* ... 64
7.1.9. *Processing semantics for the critical certificate policies extension* ... 64
7.2. CRL PROFILE ... 64
7.2.1. *Version number(s)* ... 65
7.2.2. *CRL and CRL entry extensions* ... 65
7.3. OCSP PROFILE ... 65
7.3.1. *Version Number* ... 66
7.3.2. *OCSP extensions* ... 66

8. COMPLIANCE AUDIT AND OTHER ASSESSMENT ... 67

8.1. FREQUENCY OF ENTITY COMPLIANCE AUDIT ... 67
8.2. IDENTITY/QUALIFICATIONS OF THE AUDITOR ... 67
8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED PARTY ... 67
8.4. TOPICS COVERED BY AUDIT ... 67
8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY ... 67
8.6. COMMUNICATION OF RESULTS ... 67

9. OTHER BUSINESS AND LEGAL MATTERS ... 68

9.1. FEES 68
  9.1.1. Certificate issuance or renewal fees *68*
  9.1.2. Certificate access fees *68*
  9.1.3. Revocation or status information access fees *68*
  9.1.4. Fees for other services *68*
  9.1.5. Refund policy *68*
9.2. FINANCIAL RESPONSIBILITY 68
  9.2.1. Insurance coverage *68*
  9.2.2. Other assets *69*
  9.2.3. Insurance or warranty coverage for end-entities *69*
9.3. CONFIDENTIALITY OF BUSINESS INFORMATION 69
  9.3.1. Scope of confidential information *69*
  9.3.2. Information not within the scope of confidential information *69*
  9.3.3. Responsibility to protect confidential information *69*
9.4. PRIVACY OF PERSONAL INFORMATION 69
  9.4.1. Privacy plan *69*
  9.4.2. Information treated as private *69*
  9.4.3. Information not deemed private *70*
  9.4.4. Responsibility to protect private information *70*
  9.4.5. Notice and consent to use private information *70*
  9.4.6. Disclosure pursuant to judicial or administrative process *70*
  9.4.7. Other information disclosure circumstances *71*
9.5. INTELLECTUAL PROPERTY RIGHTS 71
9.6. REPRESENTATIONS AND WARRANTIES 71
  9.6.1. CA representations and warranties *71*
  9.6.2. RA representations and warranties *72*
  9.6.3. Subscriber representations and warranties *72*
  9.6.4. Relying Party representations and warranties *72*
  9.6.5. Representations and warranties of other participants *73*
9.7. DISCLAIMERS OF WARRANTIES 73
9.8. LIMITATIONS OF LIABILITY 74
9.9. INDEMNITIES 75
9.10. TERM AND TERMINATION 76
  9.10.1. Term *76*
  9.10.2. Termination *76*
  9.10.3. Effect of termination and survival *76*
9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 76
9.12. AMENDMENTS 76
  9.12.1. Procedure for amendment *76*
  9.12.2. Notification mechanism and period *77*
  9.12.3. Circumstances under which OID must be changed *77*
9.13. DISPUTE RESOLUTION PROVISIONS 77
9.14. GOVERNING LAW 78
9.15. COMPLIANCE WITH APPLICABLE LAW 78
9.16. MISCELLANEOUS PROVISIONS 78
  9.16.1. Entire agreement *78*
  9.16.2. Assignment *78*
  9.16.3. Severability *78*
  9.16.4. Enforcement (attorneys' fees and waiver of rights) *79*
  9.16.5. Force majeure *79*
9.17. OTHER PROVISIONS 79

10. APPENDIX A 80

10.1. QUALIFIED CERTIFICATE PROFILE FOR PERSONAL 80
10.2. QUALIFIED CERTIFICATE PROFILE FOR CORPORATE 83
10.3. QUALIFIED CERTIFICATE PROFILE FOR GOVERNMENT 86

10.4. ENCIPHERMENT CERTIFICATE PROFILE FOR PERSONAL 89
10.5. ENCIPHERMENT CERTIFICATE PROFILE FOR CORPORATE 91
10.6. ENCIPHERMENT CERTIFICATE PROFILE FOR GOVERNMENT 93
10.7. NORMALISED CERTIFICATE PROFILE FOR PERSONAL 95
10.8. NORMALISED CERTIFICATE PROFILE FOR CORPORATE 97
10.9. NORMALISED CERTIFICATE PROFILE FOR GOVERNMENT 99
10.10. SECURE EMAIL CERTIFICATE PROFILE 101

1. Introduction

1.1. Overview

The Government of the Macao Special Administrative Region (“MSAR”) is committed to promote the development of Information Technology and implementation of Electronic Governing and Administration in Macao. In order to support the present and future growing volume of e-governance and e-business, Macao Post and Telecommunications Bureau, hereafter “CTT”, deployed Public Key Infrastructure (PKI) to improve business processes and efficiencies. PKI technologies leverage electronic signing, encryption, and non-repudiation to allow Government agencies and businesses to migrate from manual processing to automated processing, especially around document processing/sharing, and communications.

Macao Post and Telecommunications eSignTrust Certification Authority (“Entidade Certificadora”, hereafter “eSignTrust") is the first accredited Certification Authority ("CA") established in MSAR, providing Macao-wide PKI services. eSignTrust is an operational unit that is managed by Macao Post and Telecommunications. In addition, eSignTrust is the first accredited Certification Authority issuing Qualified Certificates according to Electronic Documents and Signatures Law of MSAR (Law no. 5/2005). Qualified Certificate provides a very high degree of assurance of certificate holder’s identity for his/her private or professional electronic identity, in an organisation or in the Government of MSAR.

This Certification Practice Statement ("CPS") describes the practices followed by eSignTrust in generating, issuing, and revoking of certificates identified in this eSignTrust CPS. It also describes the terms and conditions to be abided by anyone who subscribes, uses, and relies on certificates issued by eSignTrust.

This eSignTrust CPS is developed with reference to RFC 3647 issued by Internet Engineering Task Force. For sections that are not applicable to the services offered by eSignTrust, they are maintained for completeness but without any stipulations.

1.2. Document Name and Identification

This eSignTrust CPS is referred to as the "Macao Post and Telecommunications eSignTrust Certification Practice Statement ".

For identification purposes, this eSignTrust CPS bears the Object Identifier ("OID"):

iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certification-practice-statement (2) id-cps-number (1) id-cps-version (5)

1.3.6.1.4.1.15108.2.2.1.5

1.3. PKI Participants

The following subcomponent describes the identity or type of entities that fill the roles of participants within PKI, additional explanation of each participant definition and responsibility are shown.

1.3.1. Policy Management Authority

A committee comprised of individuals appointed by the CTT Administration Board that advises eSignTrust on policy matters and resolves disputes between parties served by the eSignTrust Certificate Policy.

1.3.2. Certification Authorities

The eSignTrust PKI is a single root-hierarchical PKI that currently consists of two (2) levels of Certification Authority as follow:

a) Root CA; and
b) Personal Normalised Sub-CA, Government Normalised Sub-CA, and Corporate Normalised Sub-CA; Personal Qualified Sub-CA, Government Qualified Sub-CA, and Corporate Qualified Sub-CA; Secure Email Sub-CA (All subordinate CAs are Issuing CAs in the eSignTrust PKI hierarchy).

The eSignTrust PKI Root CA is the highest point of trust within the eSignTrust PKI hierarchy. The primary purpose of the Root CA is to certify Issuing CAs by digitally signing the Issuing CAs' Certificates. The Root CA self-signs its own certificate.

The primary purpose of the Issuing CAs operating under the eSignTrust PKI hierarchy is to provide certificate management services (i.e., generation, operational use, key compromise contingency, suspension, revocation, and expiry) for Subscribers.

Currently eSignTrust operates each of these two (2) levels. However, nothing in this eSignTrust CPS prevents eSignTrust from authorising other Organisations to act as Issuing CAs in the future, provided that such Organisations adhere to the requirements of this eSignTrust CPS, other applicable PKI documents, and such other requirements as eSignTrust may establish. Refer to CPS Section 9.6.1 for CA representations and warranties.

1.3.3. Registration Authorities

The primary purposes of a Registration Authority (RA) are:

- to process applications for certificates and requests for certificate suspension and revocation;

- to perform Identification and Authentication (I&A) of Applicants, Subscribing Customers, and/ or Subjects in accordance with this eSignTrust CPS, the applicable Certificate Policy, and the applicable authentication policy; and
- to make a request to the Issuing CA to issue, suspend, or revoke a certificate.

RAs will also perform other obligations set forth in this eSignTrust CPS and the applicable RA Agreement.

Only those organisations that have been authorised by eSignTrust and that agree to be bound by an appropriate RA Agreement, this eSignTrust CPS, the applicable Certificate Policies, and the applicable authentication policies will be permitted to act as RAs.

Initially, all RA functions will be performed by eSignTrust. However, nothing in this eSignTrust CPS prohibits eSignTrust from authorising other Entities or other organisations to perform RA functions in the future, subject to the provisions of this eSignTrust CPS, the applicable PKI documents, and such other requirements as eSignTrust may establish. Refer to CPS Section 9.6.2 for Registration Authority representations and warranties.

1.3.4. Repositories

Each Issuing CA shall publish certificates, certificate status information, and Certificate Revocation List (CRL) to a Repository. Such Repository shall be accessible to Relying Parties and Subscribers.

Other entities or other organisations may also perform Repository functions provided that such organisations are authorised by eSignTrust and agree to be bound by the terms of this eSignTrust CPS, the applicable PKI documents, and such other requirements as eSignTrust may establish.

1.3.5. Subscribers

eSignTrust issues certificates to individuals, and affiliated individuals of Government Departments and Agencies, and Organisations, provided that the responsibility and accountability is attributable to an individual or affiliated individual as custodian of the Public/ Private Key Pair. In addition, Sponsoring Organisation(s) of a Subscriber will be responsible for all payment obligations in relation to each Subscriber's certificate that they decide to sponsor. They shall be entitled to revoke these sponsored Subscriber's certificates as set out in this eSignTrust CPS. Refer to CPS Section 9.6.3 for Subscriber representations and warranties.

1.3.6. Relying Parties

A Relying Party may be an Individual, Government Department or Agency, or Organisation that Reasonably Relies on a certificate in accordance with this eSignTrust CPS. A Relying Party, before any act of reliance, must independently assess the appropriateness of the use of a certificate for any given purpose and determine that the certificate will, in fact, be used for an appropriate purpose. Refer to CPS Section 9.6.4 for Replying Party representations and warranties.

1.4. Certificate Usage

1.4.1. Identity Certificate (Signing Certificate) Usage

Certificate types	Personal Normalised Certificate, Government Normalised Certificate, Corporate Normalised Certificate, Personal Qualified Certificate, Government Qualified Certificate, Corporate Qualified Certificate
Suitable uses	The certificate with identification usage is suitable for authentication of Subscriber identity, and for creating Digital Signature to ensure security services of access control, integrity, authentication and non-repudiation. Different types of Electronic Signature have different level of legal effectiveness. Qualified Electronic Signature is created using a Qualified Certificate and a SSCD. An electronic document signed with a Qualified Electronic Signature shall have the full evidentiary value in accordance with EDS Law of MSAR. A Qualified Certificate provides very high degree of assurance for the identity of a certificate holder with whom an Individual or Organisation is associated. Qualified Certificates are suitable for high value transactions, extremely sensitive information and lawful authenticity of QES. (e.g. contracts, declarations, high value transactions, etc.) Advanced Electronic Signature is created using a Normalised Certificate. An electronic document signed with an Advanced Electronic Signature shall have legal effectiveness. Normalised Certificates are suitable for business transactions and moderately sensitive information. (e.g., electronic mail, retail transactions, contracts, travel order, etc.).
Restricted uses	No stipulation for Normalised Certificates. Qualified Electronic Signature is created using a Qualified Certificate with its corresponding Private Key contained in a SSCD.
Prohibited uses	The Private Key of Signing Certificate Key-Pair shall not be used outside the limitations and contexts set out in this CPS and shall not, in any case, be used in violation of applicable law.

1.4.2. Encipherment Certificate Usage

Certificate classes	Personal Encipherment Certificate, Government Encipherment Certificate, Corporate Encipherment Certificate, Encipherment Certificate for Unit

Suitable uses	The Certificate with Encipherment usage is suitable for encryption of information to ensure confidentiality.
Restricted uses	The Private Key of the Encipherment Key-Pair can be used merely for the acknowledgement of receiving an encrypted message by digitally signing an acknowledgement receipt to confirm the identity of the receiving Subscriber.
Prohibited uses	The Private Key of the Encipherment Key-Pair cannot be used for authentication of Subscriber identity and shall not, in any case, be used in violation of applicable law.

1.4.3. Email Certificate Usage

Certificate type	Personal Secure Email Certificate
Suitable uses	The certificate is suitable for authentication of an e-mail address of a Subscriber, and for digital signature, encryption, and access control for non-commercial, or low-value transactions, or low sensitive information where proof of identity in person is unnecessary.
Prohibited uses	The Private Key of the Email Certificate Key-Pair cannot be used to create Qualified Electronic Signatures nor Advanced Electronic Signature and shall not, in any case, be used in violation of applicable law.

1.5. Policy Administration

1.5.1. Specification of administrative organisation

This eSignTrust CPS is administered and published by Macao Post and Telecommunications eSignTrust Certification Authority.

1.5.2. Contact person

Enquiries or other communication about this eSignTrust CPS should be directed to the following address or as updated in eSignTrust website.

Macao Post and Telecommunications eSignTrust Certification Services
Attn: eSignTrust Customer Services
Edf. dos Correios 12 andar, Estrada de D. Maria II, 11 a 11-D
Macao

Phone: 853-2833 0338
Fax: 853-8299 5515

Email: enquiry@esigntrust.com

1.5.3. Person determining CPS suitability for the policy

The management of eSignTrust determines the suitability of this eSignTrust CPS.

1.6. Definitions and Acronyms

Capitalised terms and acronyms used herein and in related agreements and other documents incorporating this eSignTrust CPS have the following meanings.

Activation Data	Private data used or required to access or activate cryptographic modules (i.e., a PIN, pass phrase or a manually-held key share used to unlock Private Keys for signing or decryption events).
Advanced Electronic Signature	Advanced Electronic Signature (AES) shall mean an electronic signature which is uniquely linked to the signatory, is capable of identifying the signatory. It is created using means that the signatory can maintain under his sole control and it is linked to the data to which relates in such a manner that any subsequent change of the data is detectable.
Affiliated Individual	An individual who is authorised by a Government Agency or Department, or a Corporate/Company to hold a certificate as an employee, partner, member, officer, agent, licensee, permitted or other associate of the Government Agency or Department, or Corporate/Company containing the Government Agency's or Department's, or 'Corporate's/Company's name.
Applicant	An entity that requests a Certificate on behalf of the Subject. The Applicant may or may not be the Subject. For example, a physical person or the Applicant requests a Certificate on behalf of a legal person or the Subject, which can also be an organisation or a Government agency.
Authenticating Registration Authority ("RA")	A Registration Authority that has been authenticated by an Issuing CA, issued a Registration Authority Certificate by the Issuing CA, and entered into an agreement with the Issuing CA authorising the Authenticating RA to process applications for certificates, and conduct Identification & Authentication of applicants in accordance with all applicable laws and the Policy.
Authorised User	Refer to Affiliated Individual.

Certificate	A computer-based record or electronic message that at a minimum: Identifies the Issuing CA issuing it; Identifies a Subscriber; Contains the Public Key of the Subscriber; Identifies the certificate's operational period; and Is digitally signed by an Issuing CA.
Certification Authority	A certification authority (CA) is an entity responsible for issuing, managing and revoking certificates, In addition, certificate repository is also managed by the CA.
Certificate Export PIN	A secret code selected and entered by the Subscriber during the certificate exporting process. This code is only known to the Subscriber, and all eSignTrust personnel do not have access to this code.
Certificates Issuance	The acts performed by an Issuing CA in creating a certificate, listing itself as "Issuer", notifying the certificate applicant of its contents, and that the certificate is ready and available for acceptance.
Certificate Lifecycle Management Challenge Phase	A secret code selected and entered by the Subscriber during the certificate generation process. This code can be used to activate certificate revocation requests submitted on-line by Subscribers.
Certificate Policy ("CP")	A named set of rules that govern the generation, issuance, use of certificates and revocation, as well as indicate the applicability of certificates to particular communities and classes of applications with common security requirements.
Certificate Profile	The protocol used in Chapter 7 of this eSignTrust CPS to establish the allowed format and contents of data fields within certificates. Data fields within certificates usually identify the Issuing CA, the Subscriber, the Issuing CA's CPS, the certificate's validity period, and other information that identifies the Subscriber.
Certificate Revocation List ("CRL")	A list of certificates indicating certificates that have been revoked earlier than the end of their validity periods.
Certification Practice Statement ("CPS")	A statement of the practices that an Issuing CA employs in issuing and/or administering certificates in accordance with the Certificate Policy.

Crypto module	Hardware and/ or software that: • generates Key Pairs; • stores cryptographic material; and/or • performs cryptographic functions.
Digital Signature	The transformation of a message involving a certificate and Public Key Cryptography such that a Relying Party having the initial message and the Subscriber's certificate can accurately determine: • whether the transformation was created using the Private Key that corresponds to the Subscriber's Public Key; and • whether the message has been altered since the transformation was made. Digital Signature is a type of electronic signature.
Distinguished Name ("DN")	The unique identifier for a Subscriber so that he, she or it can be located in a directory. For example, the DN for a Subscriber might contain but not limited to the following attributes: • common name (CN); • e-mail address (E); • title (T) • organisation name (O); • organisational unit (OU); and • country/region (C).
Electronic Signature	An electronic record which is directly or logically link to an electronic document and it is co-related with a set of electronic data, such that these data can be used for various method of authentication.
Electronic Device	Computer software, or hardware, or other electronic or automated means configured and enabled by the Subscriber to act as its agent and to initiate or respond to electronic records or performances, in whole or in part, without review or intervention by the Subscriber.
Email Certificate	See Secure Email Certificate.
Encipherment Certificate	A certificate to be used only for encryption of information.
Expiration or Certificate Expiry	The natural cessation of the validity of a certificate by the elapse of its predetermined ending date.
Government Agency or Department	Bureaus, departments, and agencies of the Government of MSAR.

Hardware Token	A secure hardware device (e.g. smartcard, USB token or a hardware security module) used to store Subscriber's private key, public key and certificate.
Identification and Authentication ("I&A")	To ascertain and confirm through appropriate inquiry and investigation, with reasonable skill and care, the identity of a Subscriber, an Organisation, an Electronic Device, or other person.
Identity Certificate	A certificate to be used only for authenticating of Subscriber identity, and for Digital Signature, Advanced and Qualified Electronic Signatures.
Individual	A physical person and not a legal entity.
Issuing CA	An entity authorised by eSignTrust to issue and manages certificates asserting the eSignTrust CPS.
Issuing CA Certificate	The certificate at the immediately following the Root CA Certificate of a certification chain within the eSignTrust PKI hierarchy, issued by the Root CA in a secure and trustworthy manner. An Issuing CA Certificate is established as part of the set-up and activation of an Issuing CA. The Issuing CA Certificate contains the Public Key that corresponds to the Issuing CA Private Signing Key that the CA uses to create Subscriber certificates. The Issuing CA Certificate, and its corresponding Public Key, may be embedded in software or obtained or downloaded by the affirmative act of a Relying Party in order to establish a certification chain.
Issuing CA Private Key	The Private Key that corresponds to an Issuing CA's Public Key listed in the Issuing CA Certificate and that is used to sign Subscriber certificates.
Key Generation	The trustworthy process of creating a Public/ Private Key Pair.
Lightweight Directory Access Protocol ("LDAP")	A client-server protocol used for accessing an X.500 directory service over the Internet.
Normalised Certificate	A certificate which is not defined as Qualified Certificate, however still require face to face authentication or authentication mechanism of equivalent certainty during registration process.
Online Certificate Status Protocol ("OCSP")	A certificate checking protocol identified by RFC 6960 that enables an application to determine the suspension/ revocation state of an identified certificate by issuing a status request to an OCSP responder and suspending acceptance of the certificate in question until the responder has provided the application with a response.

Organisation	An entity that is legally recognised in its jurisdiction of origin (e.g., a company, corporation, partnership, sole proprietorship, government department ("Government Agencies"), non-government organisation, university, special interest group or non-profit corporation).
Encipherment Certificate	Encipherment Certificate issued to an Individual, a business subunit or an Organisation.
Policy	The eSignTrust Certificate Policy, used interchangeably with eSignTrust CP. eSignTrust CP is combined with this version of CPS.
Policy Management Authority	A working group established by the CTT Administration Board which is responsible for making recommendations to eSignTrust for setting, implementing, interpreting and administering policy decisions regarding the eSignTrust CPS and for resolving disputes between parties subject to the Policy.
Private Key	The key of a Public/ Private Key Pair kept secret by its holder, for use to create Digital Signatures and/ or to decrypt messages or files that were encrypted with the Subscriber's corresponding Public Key.
Public Key	The key of a Public/ Private Key Pair that is used to verify a Digital Signature created with its corresponding Private Key, that can be made publicly available in a certificate, and that can also be used to encrypt messages or files which can then be decrypted only with the intended recipient's corresponding Private Key. The Public Key is attached to the Subscriber certificate and signed by the Issuing CA's Private Key during the certificate generation process.
Public Key Cryptography	A type of cryptography known also as asymmetric cryptography that uses a unique Public/ Private Key Pair of mathematically related numbers. The Public Key can be made available to anyone who wishes to use it, while the Private Key is kept secret by its holder. The Public Key can be used to encrypt information or verify a Digital Signature, while the Private Key can be used to decrypt information or generate a Digital Signature.
Public Key Infrastructure ("PKI")	The architecture, organisation, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based Public Key Cryptography system.

Public/ Private Key Pair	A Public Key and its corresponding Private Key in Public Key Cryptography (also known as asymmetric cryptography): • keys that have the property that the Public Key can verify a Digital Signature that the corresponding Private Key creates; and/ or • keys that can encrypt and decrypt information for confidentiality purposes, in which the Public Key is used to encrypt data that can be decrypted only by using the intended recipient's corresponding Private Key.
Qualified Certificate	Qualified Certificate provides a very high degree of assurance of certificate holder's identity in an organisation and where applicable. Qualified Certificate contents meet the requirements as stipulated in Art.º9 of Macao Electronic Documents and Signatures Law. Moreover, as stipulated in Art.º10 of the same, Qualified Certificate needs to be issued by an accredited certification authority.
Qualified Electronic Signature	"Qualified Electronic Signature" (QES), according to the applicable law, is an Advanced Electronic Signature (AES) based on a Qualified Certificate and is created using a Secure Signature-Creation Device, which is in conformance to internationally recognised standards, capable of making effective protection against fraudulent signatures.
Reasonable Reliance	Reliance on a Digital Certificate is considered reasonable if the Relying Party has: a) verified that a Digital Signature in question was created by the Private Key corresponding to the Public Key in the certificate while the certificate was valid (i.e., confirmed that the document signed with the Digital Signature had not been altered and an online status check of the certificate confirmed that the certificate was valid); OR b) for the purposes of access control, verified that the certificate was valid and an online status check of the certificate was confirmed; AND c) validated the certificate chain from the Subscriber Certificate back to the Issuing CA and Root CA; AND/OR d) used the certificate for purposes appropriate under the eSignTrust CPS, without knowledge of any facts that would cause a person of ordinary business prudence to refrain from relying on the certificate, and under circumstances where reliance would be reasonable and otherwise in good faith in light of all the circumstances that were known or should have been known to the Relying Party prior to reliance.

Recommended Reliance Limit	A Recommended Reliance Limit is an Issuing CA's recommended maximum total amount which a Relying Party should risk in a transaction or communication depending upon a given certificate. Recommended Reliance Limits vary by certificate type. A Relying Party is advised to consider the Recommended Reliance Limit in electing to rely upon a certificate, but is not prohibited from using any certificate type for any purpose or transaction based upon the applicable Recommended Reliance Limit.
Registration	Registration is the process of receiving or obtaining a request for a certificate from a Subscriber, and collecting and entering the information needed from that Subscriber to include in and support I&A and issuance of a certificate.
Registration Authority ("RA")	Organisation or Individual who are authorised by an Issuing CA to locally collect Subscribers' identity information for purposes of entry into a certificate. No Organisation or Individual shall be authorised to act as an RA by an Issuing CA unless the Issuing CA has bound the Individual or Organisation to comply with the terms of the Policy.
Relying Party	A Relying Party is an Individual or Organisation who relies on a certificate issued under the terms of the eSignTrust Policy. A Relying Party's actions in reliance upon a certificate are reasonable when their actions constitute Reasonable Reliance as specified in the eSignTrust Policy.
Renewal or Renew a Certificate	The creation of a new certificate with the same Subscriber name, and/ or authorisations as the previous one where applicable, but referencing a new Key Pair, extended validity period, and a new serial number.
Repository	A publicly accessible online system maintained by or on behalf of an Issuing CA for storing and retrieving certificates and other information relevant to certificates and Digital Signatures.
Revocation or Revoke a Certificate	The act of making a certificate ineffective permanently from a specified time forward. Revocation is affected by notation or inclusion in a set of revoked certificates or other directory or database of revoked certificates.
Root CA	An entity authorised by eSignTrust to issue and manages Issuing CA Certificates asserting the eSignTrust CPS.

Root CA Certificate	The certificate at the beginning of a certification chain within the eSignTrust PKI hierarchy, self-issued in a secure and trustworthy manner. A Root CA Certificate is established as part of the set-up and activation of an Issuing CA. The Root CA Certificate contains the Public Key that corresponds to the Root CA Private Signing Key that the Root CA uses to create Issuing CA Certificates. The Root CA Certificate, and its corresponding Public Key, may be embedded in software or obtained or downloaded by the affirmative act of a Relying Party in order to establish a certification chain.
Root CA Private Key	The Private Key used by the Root CA to sign the Issuing CA Certificate and certify the Issuing CA's Public/ Private Key Pair.
Secure Email Certificate	A computer-based record or electronic message that is based on authentication of subscriber's email address.
Secure Signature-Creation Device (SSCD)	"Secure Signature-Creation Device" (SSCD) means a signature-creation device which is in conformance to internationally recognised standards, capable of making effective protection against fraudulent signatures.
Signature Key (Signature Creation Data)	The Private Key of a Key Pair used by the Subscriber for signing and to establish non-repudiation.
Smart Token PIN	A secret code selected and entered by the Subscriber during the Subscriber's Smart Token initialisation process. This code is only known to the Subscriber, and none of the eSignTrust personnel has access to it. This code is used to protect the Subscriber Private Key in a Smart Token media.
Sponsoring Organisation	A Government Agency or Department, or an Organisation that has authorised the issuance of a certificate identifying the Subscriber as having an affiliation with the Government Agency or Department, or Organisation (e.g., as an employee, partner, member, officer, agent, licensee, permitted or other associate). Sponsoring Organisation signs the "Subscriber Agreement" in the application process.
Strong PIN or Password	An alphanumeric code or Personal Identification Number (PIN) of at least eight (8) characters used to gain access to a locked system.

Subscriber	An Individual that: • is named or identified in a certificate as its subject; • holds the Private Key that corresponds to the Public Key listed in that certificate; and • is the holder of a certificate. For Encipherment Certificate, its subject can also be a business sub-unit, an Organisation or a Government Agency.
Suspension or Suspend a Certificate	The act of making a certificate ineffective temporarily from a specified time forward. Suspension is affected by notation or inclusion in a set of suspended certificates or other directory or database of suspended certificates.
Third Party Identity Proofing	The process by which an Issuing CA confirms Subscriber information provided in Registration, by verification through other organisations and agencies which serve as information or reference services.
Trustworthy System	Computer hardware and software that: • are reasonably secure from intrusion and misuse; and • conform to requirements established by the Government of the MSAR, when applicable.

2. Publication and Repository Responsibilities

2.1. Repository

eSignTrust operates a secure on-line Repository available to Relying Parties, that contains the information detailed in the next section.

The information contained in the Repository shall be publicly accessible from the Internet all days, 24 hours a day and 7 days a week, excluding necessary maintenance time and except in cases of force majeure. eSignTrust will do its best effort to obtain an uptime of 99% for this information in each calendar year.

eSignTrust reserves the right to publish the Repository's information by other means.

2.2. Publication of certification information

eSignTrust will make the following publicly available in its Repository:

- This CPS and its previous versions;
- The applicable CP(s) under which Certificates are issued according with this CPS;
- The eSignTrust Root CA(s) and Issuing CA(s) Certificates;
- All Certificates issued in accordance with this CPS;
- Latest CRL(s) issued by the eSignTrust Issuing CA(s);
- Other relevant information relating to eSignTrust Certificates.

An updated copy of this CPS is available in electronic form on the Internet at https://www.esigntrust.com/CPS.

2.3. Time or frequency of publication

Certificates are published in the Repository as soon as possible after issuance.

CRLs are published in accordance with Section 4.10.

New or modified versions of this CPS, Subscriber Agreements, or Relying Party Agreements are typically published within reasonable days after their approval.

2.4. Access controls on repositories

eSignTrust does not impose any access control for viewing the eSignTrust Root CA's and Issuing CA's Certificates, the CRL, the past and present versions of this CPS and the applicable CPs, except during reasonable maintenance periods, where access will be unavailable.

However, eSignTrust will implement access controls or security measures such that eSignTrust is the only entity that can have write or modification access to the Repository information.

3. Identification and Authentication (I&A)

3.1. Naming

3.1.1. Type of Names

Each Subscriber shall be represented by a clearly distinguishable and unique X.500 Distinguished Name ("DN") in the certificate "subject" field in accordance with PKIX Part 1.

The DN shall be in the form of a X.500 printableString, and shall not be blank.

3.1.2. Need for Names to be Meaningful

eSignTrust Qualified Certificates and Normalised Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual that is the Subject of the Certificate. eSignTrust Secure Email Certificates contain non-verified names providing no identity association of the Subject of the Certificate.

eSignTrust CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3. Anonymity or Pseudonymity of Subscribers

eSignTrust does not permit anonymity or pseudonymity of Subscriber except for Email Certificate where the identity of Subscriber is not authenticated.

3.1.4. Rules for Interpreting Various Name Forms

Type	Qualified Certificate
Description	For Government, Subscriber must be an Affiliated Individual of a government agency of Macao SAR. For Corporate, Subscriber must be an Affiliated Individual of a Sponsoring Organisation with valid registration in Macao. For Personal, Subscriber must be an individual with valid identification document.
Subject Name	This field contains an X.501 distinguished name and consists of the followings: • E-mail address of Subscriber • Name of Subscriber • A Title attribute reference professional qualification of Subscriber or category/position of Subscriber in

	Sponsoring Organisation where applicable • Holder Reference Number • An OU attribute referencing procuration information where applicable • An OU attribute referencing registration information of Sponsoring Organisation where applicable • An OU attribute referencing Subscriber belonging unit where applicable • An OU attribute referencing Sponsoring Organisation • An OU attribute referencing the terms of use of the Certificate • An OU attribute referencing the Type of Certificate • O=Macao Post and Telecommunications Bureau eSignTrust Services • A C attribute using ISO 3166-1 alpha-2 country code referencing the country/region where the identity document of Subscriber is issued
Key Usage	Digital Signature, Non-Repudiation

Type	Normalised Certificate
Description	For Government, Subscriber must be an Affiliated Individual of a government agency of Macao SAR. For Corporate, Subscriber must be an Affiliated Individual of a Sponsoring Organisation with valid registration in Macao. For Personal, Subscriber must be an individual with valid identification document.
Subject Name	This field contains an X.501 distinguished name and consists of the followings: • E-mail address of Subscriber • Name of Subscriber • Holder Reference Number • A Title attribute referencing category/position of Subscriber in Sponsoring Organisation where applicable • An OU attribute referencing registration information of Sponsoring Organisation where applicable • An OU attribute referencing Subscriber belonging unit where applicable • An OU attribute referencing Sponsoring Organisation • An OU attribute referencing the terms of use of the Certificate • An OU attribute referencing the Type of Certificate

	• O=Macao Post and Telecommunications Bureau eSignTrust Services • A C attribute using ISO 3166-1 alpha-2 country code referencing the country/region where the identity document of Subscriber is issued
Key Usage	Digital Signature, Non-Repudiation

Type	Encipherment Certificate
Description	For Government, Subscriber must be an Affiliated Individual of a government agency of Macao SAR. For Corporate, Subscriber must be an Affiliated Individual of a Sponsoring Organisation with valid registration in Macao. For Personal, Subscriber must be an individual with valid identification document.
Subject Name	This field contains an X.501 distinguished name and consists of the followings: • E-mail address of Subscriber • Name of Subscriber • Holder Reference Number • A Title attribute referencing category/position of Subscriber in Sponsoring Organisation where applicable • An OU attribute referencing registration information of Sponsoring Organisation where applicable • An OU attribute referencing Subscriber belonging unit where applicable • An OU attribute referencing Sponsoring Organisation • An OU attribute referencing the terms of use of the Certificate • An OU attribute referencing the Type of Certificate • O=Macao Post and Telecommunications Bureau eSignTrust Services • A C attribute using ISO 3166-1 alpha-2 country code referencing the country/region where the identity document of Subscriber is issued
Key Usage	Key Encipherment

Type	Email Certificate
Description	For Personal, Subscriber must be an individual with valid e-mail address.
Subject Name	This field contains an X.501 distinguished name and consists of the followings:

	• E-mail address of Subscriber • Name of Subscriber (which is Nonverified Subscriber Information) • An OU attribute referencing the terms of use of the Certificate • An OU attribute referencing the Type of Certificate • O=Macao Post and Telecommunications eSignTrust Services
Key Usage	Digital Signature, Key Encipherment

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. eSignTrust, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrates, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. eSignTrust is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

In the event of any dispute concerning name claim issues, eSignTrust reserves the right to make all decisions, and shall be the final arbiter of all such claims in relation to Subscriber names in all assigned certificates. A party requesting a certificate shall demonstrate its right to use a particular name. eSignTrust shall have the right to reject any name in its sole and absolute discretion.

3.1.5. Uniqueness of Names

The identification of every Subscriber Certificates issued by eSignTrust is performed on the basis of subject Distinguished Names (DN). A subject DN is composed of the name of Subscriber and attributes relevant for the identification of Subscriber.

If a composed DN violates other entity’s right to this name, eSignTrust shall add another attribute(s) to DN at its sole discretion, which ensures the uniqueness of this name within the subdomain of eSignTrust Issuing CA. A Subscriber is entitled to reject a composed Distinguished Name in the course specified in CPS Section 4.4. If any Subscriber resigns from eSignTrust service, the request of attributing his/her/its DN to another Subscriber must be rejected.

3.1.6. Recognition, Authentication, and Role of Trademarks

eSignTrust has its own registered trade mark consisting of graphic mark and inscription, which constitute the following logo:

This mark and inscription constitute the logo of eSignTrust. The logo is a registered trademark of eSignTrust and cannot be used by any party without a written approval of eSignTrust.

eSignTrust mark is an additional element of the logo of every Registration Authority operating on behalf of eSignTrust Certification Authority. The approval of the use of logo of the eSignTrust Certification Authority is automatically issued when a new Registration Authority is registered by eSignTrust.

No Subscriber is guaranteed that its name will contain a trademark, trade name, corporate name or other specific referential material. eSignTrust may attempt to accommodate such requests at its own discretion.

eSignTrust shall not knowingly allow an entity to hold a name that a civil court has determined it has no right to use; provided that eSignTrust has no obligation to make any inquiry or investigation into the existence or validity of such an order, or the status of any trademark and is not required to revoke and re-issue such a name to the rightful owner if it has already issued one sufficient for identification within the eSignTrust PKI.

3.2. Initial Identity Validation

eSignTrust may use any legal means of communication or investigation to ascertain the identity of an organisational or individual Applicant. eSignTrust may refuse to issue a Certificate in its sole discretion.

3.2.1. Method to Prove Possession of Private Key

eSignTrust verifies the Certificate Applicant's possession of a private key through the use of a digitally signed certificate request pursuant to PKCS #10, another cryptographically-equivalent demonstration, or another eSignTrust-approved method.

Where a key pair is generated by eSignTrust on behalf of a Subscriber, this requirement is not applicable.

The eSignTrust RA and designated RAs which are assigned and approved by eSignTrust, are solely responsible for Subscriber key generation process for Qualified Certificates, Normalised Certificates and Encipherment Certificates, and these are done in a controlled and secured environment appropriate for certificate registration purpose, to ensure that Subscriber Private Keys are not tampered with or subjected to unauthorised access. The Subscriber Private Key and Certificate will be generated on secure storage media and securely handed control over to the Subscriber.

3.2.2. Authentication of Organisation Identity

For eSignTrust Organisational Certificate applications, certificate requests are created, processed and approved by authorised eSignTrust personnel using a controlled process that requires the participation of multiple trusted eSignTrust employees. eSignTrust authenticates the identity of the organisation by checking its organisational documentation issued by a competent authority. The RAs within the eSignTrust Qualified and Normalised PKI segment are obliged to undertake the procedures set forth in this CPS and in the appropriate internal documents in order to authenticate the organisation identity.

For the eSignTrust Qualified Certificate and Normalised Certificate, the authentication of an organisation will require the appropriate documents as deemed necessary, including but not limited to the followings:

- Business Registration Certificate
- Photocopy of "Initial Activity Declaration" M/1 Form, M/2 Form, "Tax Payment" M/8 Form, or any government-issued declarations, where applicable
- Notarised copy of the articles of association, when required
- Original of Board or Shareholders meeting's minutes, or notarised copy, when required

3.2.3. Authentication of Individual Identity

When eSignTrust issues individual Certificates, it confirms that:

- The Certificate Applicant is the person identified in the Certificate Application
- The Certificate Applicant rightfully controls the private key corresponding to the public key to be listed in the Certificate in accordance with CPS Section 3.2.1, and
- All information in or incorporated by reference in the Certificate, except for Nonverified Subscriber Information, is accurate.

The following procedures correspond to authentication of individual identify for various certificate types issued by eSignTrust CAs:

- Qualified Certificate / Normalised Certificate

  When issuing a Qualified Certificate or Normalised Certificate, eSignTrust verifies, by appropriate means and in accordance with MSAR law, the identity and, if applicable, any specific attributes of the Subscriber. Verification of the identity of each applicant for Qualified and Normalised Certificate will be accomplished through one of the following processes appropriately determined by eSignTrust:

  a) By appearing before an authorised eSignTrust representative, a notary or an official with comparable authority within the jurisdiction of MSAR, that confirms the identity and, if applicable, any specific qualifications of the applicant using, at minimum, a well-recognised form of government-issued identification with photo and the written confirmation of email address of the applicant; or

b) By using government-issued electronic identification means, for which prior to the issuance of the certificate, a physical presence of the natural person was ensured and which provides a higher degree of confidence in the claimed or asserted identity of a person, when available; or

c) By secure remote videoconferencing, when available; or

d) By using other available identification methods recognised at MSAR government level which provide equivalent assurance in terms of reliability to physical presence.

◆ Encipherment Certificate

The authentication of eSignTrust Encipherment Certificate is based on the verification of the identity of the Subscriber using, at minimum, a well-recognised form of government-issued identification with photo when the Subscriber is a natural person and the written confirmation of email address of the Subscriber.

◆ Secure Email Certificate

The authentication of eSignTrust Secure Email Certificate Applications is based on a check to ensure the Subscriber's distinguished name is unique and unambiguous within the domain of Secure Email CA and that a certain e-mail address is associated with a public key. The authentication of this type of certificate does not provide assurances of identity (i.e., that a Subscriber is who he or she claims to be). The common name of the Subscriber is Nonverified Subscriber Information. Also, it includes a limited confirmation of the Certificate Applicant’s e-mail address.

3.2.4. Nonverified Subscriber Information

Secure Email Certificate contains Nonverified Subscriber Information. Refer to CPS Section 3.2.3.

3.2.5. Validation of Authority

eSignTrust Certification Authorities and Registration Authorities can confirm private entities authorisation to take actions on behalf of other entities, usually legal entities. Such authorisations are usually associated with a particular role in an institution.

Authentication of authorisations is a part of registration or certification authority processing an application for a certificate for a legal entity. An issued certificate is a confirmation that a legal entity is entitled to use a private key on behalf of a legal entity.

Authorisation is delegated by a legal entity to either its employees or agents (account offices). Procedure of authorisation authentication employed by eSignTrust comprise, apart from authorisation authentication, the authentication of a private entity to whom these authorisations where delegated. The authentication of a private entity's identity is performed in the way described in CPS Section 3.2.3.

3.2.6. Criteria for interoperation

In the case of applications by a CA wishing to operate within, or interoperate with, eSignTrust will enter into agreement with corresponding CA and finally approval of its status as interoperated CA by performing the check required for confirmation of the identity of organisation specified in Section 3.2.2. In addition, administrator and/or contact personal status will be confirmed by the procedure specified in Section 3.2.3.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for routine re-key requests

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of certificate usage. eSignTrust requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey").

Generally speaking, "Rekey" is commonly described as "Certificate Renewal," focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasising whether or not a new key pair is generated.

For all eSignTrust Certificates, this distinction is not important as a new key pair is always generated as part of eSignTrust Subscriber Certificate replacement process.

At least one (1) month prior to the scheduled expiration of the operational period of an issued Subscriber certificate, eSignTrust will send email to inform the Subscriber to apply for the renewal of the certificate and key-pair, provided that the original certificate has not been suspended or revoked. The renewal process has to be completed within the validity period of the existing certificate lapses.

Renewal of Qualified Certificates, Normalised Certificates and Encipherment Certificates shall follow the same identification and authentication procedures in Sections 3.2.2, 3.2.3, However, due to the fact that Email Certificate is generated online, renewal process does not involves physical presence of the Subscriber. A notification email will be sent one (1) month prior to the certificate expiration. Renewal ID and renewal URL will be included inside the email. Subscriber will be required to prove that he/she is the original requestor of the expiring certificate by signing a certificate generation request with Subscriber's expiring Email Certificate.

CA Certificates:

Renewal of CA Certificates is permitted as long as the cumulative certified lifetime of the CA key pair does not exceed the applicable maximum CA key pair lifetime specified.

3.3.2. Identification and Authentication for re-key After Revocation

In the event of any suspected or actual key compromise and hence the Subscriber certificate is revoked, under such circumstance, the Subscriber is required to apply for new certificate and key-pairs as per a new application. The identification and authentication procedures as per Section 3.2.2 and Section 3.2.3, shall be followed.

Furthermore, rekey after revocation is not permitted if:

- revocation occurred because the certificate was issued to a person other than the one named as the Subject of the certificate,
- the certificate was issued without the authorisation of the person named as the Subject of such certificate, or
- the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false. Subject to the proceeding paragraph, Subscriber Certificates, which have been revoked, may be replaced.

3.4. Identification and Authentication for Revocation Requests

Prior to the revocation of a Certificate, eSignTrust verifies that the revocation has been requested by the Certificate's Subscriber, the Sponsoring Organisation or a competent authority. Acceptable procedures for authenticating Subscriber revocation requests include:

- Having the Subscriber to submit the Subscriber's "Challenge Phrase" and revoking the Certificate automatically if it matches the Challenge Phrase on record. In case the Subscriber lost his or her certificate's Challenge Phrase, self-revocation will not be allowed and revocation of the certificate will be performed by eSignTrust's personnel upon the validation of a written request from the Subscriber.
- Communication with the Subscriber providing reasonable assurances that the person requesting revocation is, in fact, the Subscriber. Depending on the circumstances, such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

eSignTrust personnel is entitled to request the revocation of Subscriber Certificates and CA certificates. However, the requests for eSignTrust to revoke a CA Certificate need to be authenticated by eSignTrust Management to ensure that the revocation is sufficiently authorised.

All revocation requests will be verified by the eSignTrust with the relevant revocation reasons, before any revocation is submitted and committed by eSignTrust. A Subscriber or Sponsoring Organisation may request the revocation of own certificate or sponsoring certificate. In addition, eSignTrust reserves its right to revoke the private key and a Certificate where (i) eSignTrust suspects a compromise of the Subscriber private key or Certificate, or (ii) such compromise is proven, or (iii) eSignTrust is properly requested by a competent authority. In all cases, eSignTrust Issuing CA or RA will promptly notify the Subscriber of the revocation.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who can submit a certificate application

It is the responsibility of Individuals and Sponsoring Organisations who require certificates and key-pairs to complete a certificate application request to eSignTrust. The applicant for a certificate shall complete the relevant certificate application forms prescribed by eSignTrust, and enter into a Subscriber Agreement with the Issuing CA. The certificate application forms can either be obtained from designated eSignTrust RA locations, premises of other organisations designated by eSignTrust, or downloaded via the eSignTrust website. The Subscriber must have attained a minimum age of eighteen (18) years old. eSignTrust does not warrant to applicants of their successful application of certificates.

4.1.2. Enrollment process and responsibilities

Documents may be submitted in physical or electronic means. If signatures are required in the electronic documents, then valid Electronic Signatures are acceptable. eSignTrust has sole discretion to determine acceptable types of Electronic Signatures.

4.1.2.1. eSignTrust Email Certificate

The procedures to apply for an eSignTrust Email certificate are as follows:

- Subscriber is required to input enrollment information including a purchased authentication passcode and a Certificate Lifecycle Management Challenge Phase;
- Complete the prescribed online application form and accept the Subscriber Agreement.

4.1.2.2. Personal Encipherment Certificate, Personal Normalised Certificate and Personal Qualified Certificate

The procedures to apply for the above certificate are defined as follow:

- Complete and submit the prescribed application form and Subscriber Agreement to designated eSignTrust RA location(s) or premises of other organisations designated by eSignTrust;
- Attach and submit photocopy or electronic copy of official photo-ID (e.g., identity card, passport, etc.) and applicable document relevant for Certificate Application ; and
- Pay the subscription fees, where applicable.

4.1.2.3. Government Encipherment Certificate, Government Normalised Certificate and Government Qualified Certificate

The procedures to apply for the above certificates are defined as follow:

- Complete and submit the prescribed application form(s) and Subscriber Agreement to designated eSignTrust RA location(s) or premises of other organisations designated by eSignTrust;
- Attach and submit photocopy or electronic copy of official photo-ID (if applicable) of sponsored Subscriber and applicable document relevant for Certificate Application;
- Attach Letter of Authorisation by Sponsoring Organisation. eSignTrust will verify the authoritative signatory named in the Letter of Authorisation in support of the application; and
- Pay the subscription fees, where applicable.

4.1.2.4. Corporate Encipherment Certificate, Corporate Normalised Certificate and Corporate Qualified Certificate

The procedures to apply for the above certificates are defined as follow:

- Complete and submit the prescribed application form(s) and Subscriber Agreement to the eSignTrust RA location(s) or premises of other organisations designated by eSignTrust;
- Attach and submit photocopy or electronic copy of official photo-ID (e.g., identity card, passport, etc.) of sponsored Subscriber and applicable document relevant for Certificate Application;
- Attached Letter of Authorisation by Sponsoring Organisation or a notarised copy when required;
- Provide information of official company/ business/ organisation registration documents issued by Government of MSAR. When online database of official documents provided by Government of MSAR is not accessible by eSignTrust, then the original or the notarised copy of the documents is required; and
- Pay the subscription fees, where applicable.

4.1.2.5. eSignTrust Subordinate CA Certificate

The eSignTrust Root CA issues certificates only to subordinate CAs, the CA certificate request is approved by eSignTrust with management authorisation and generated by authorised personnel through a controlled process that requires the participation of multiple trusted individuals.

4.2. Certificate Application Processing

4.2.1. Performing identification and authentication functions

4.2.1.1. Secure Email Certificate

eSignTrust does not perform any identification check to verify the certificate application of this certificate type, certificate request submitted with a valid authentication passcode will be automatically approved.

4.2.1.2. Qualified Certificate, Normalised Certificate and Encipherment Certificate

Refer to CPS Section 3.2.1, 3.2.2 and 3.2.3 for Identification and Authentication procedures details. Identification and Authentication process must occur in the authorised RA premises or in a controlled and secured environment designated for certificate registration purpose; and, when applicable, payment needs to be made by Subscriber or Sponsoring Organisation prior submission of certificate request. Upon successful verification of I&A of Certificate Application, certificate request shall be submitted following authorised RA procedure together with Subscriber information. Qualified Certificate requests being submitted will normally require dual approval.

4.2.1.3. eSignTrust Subordinate CA Certificate

In the case when an organisation prefer to join the eSignTrust PKI hierarchy as a Subordinate CA, an eSignTrust Subordinate CA certificate can be issued by eSignTrust Root CA and the organisation possess of the Subordinate CA needs to ahere this CPS, applicable CP, RA agreement, Relying Party Agreement and related necessary documents. The above mentioned documents need to be conformed to corresponding eSignTrust documents.

4.2.2. Approval or rejection of certificate application

Approval or rejection of certificate application is made according to Identification and Authentication information accuracy and payment status of corresponding certificate request.

4.2.3. Time to process certificate applications

Application for Qualified Certificate, Normalised Certificate and Encipherment Certificate submitted to eSignTrust RA will be processed within a reasonable time frame after request submission and validation. Secure Email Certificate requests will be automatically approved when a valid authentication passcode is provided.

4.3. Certificate Issuance

4.3.1. CA actions during certificate issuance

A Certificate is created and issued following the approval of a Certificate Application by eSignTrust or following receipt of an eSignTrust RA's request to issue the Certificate. eSignTrust creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application. eSignTrust is not responsible for monitoring, investigating, or confirming the accuracy or completeness of certificate information after certificate acceptance. After certificate acceptance, the Subscriber and/ or the Sponsoring Organisation bear the sole obligation to report any material changes in certificate information that may necessitate certificate revocation.

4.3.2. Notification to subscriber by the CA of issuance of certificate

eSignTrust shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates shall be made available to Subscribers, either by allowing them to download from eSignTrust web site or via a message sent to the Subscriber containing the Certificate. If the Certificate is presented to the Subscriber immediately, no notification is required.

4.4. Certificate Acceptance

By accepting a Certificate, the Subscriber:

- Agrees to be bound by the continuing responsibilities, obligations and duties imposed by the eSignTrust CPS;
- Agrees to be bound by the eSignTrust Subscriber Agreement;
- Represents and warrants that to his knowledge no unauthorised person has had access to the private key associated with the Certificate;
- Represents and warrants that the Certificate information he has supplied during the registration process is truthful and accurate; and
- Represents and warrants that he is using his private key and the Certificate exclusively for authorised and legal purposes consistent with the eSignTrust CPS and Subscriber Agreement.

Upon receipt of a Certificate, the Subscriber is responsible for verifying that the information contained within the Certificate is accurate and complete and that the Certificate is not damaged or otherwise corrupted. In the event the Certificate is inaccurate, damaged or corrupted, the Subscriber should contact eSignTrust to have the Certificate replaced as determined by eSignTrust.

4.4.1. Conduct constituting certificate acceptance

eSignTrust registration authority procedures ensures that certificate issuance will only take place when the Subscriber is ready to pick-up/download and install the certificate. If the Subscriber does not reject the Certificate or its contents, the acceptance process is completed which constitutes Certificate acceptance, no further confirmation is required.

If the Certificate is presented immediately to the Subscriber at eSignTrust RA location(s) or premises of other organisations designated by eSignTrust, the Subscriber is required to sign an acceptance receipt.

4.4.2. Publication of the certificate by CA

eSignTrust publishes the Certificates it issues in a publicly accessible repository.

4.4.3. Notification of certificate issuance by the CA to other entities

No stipulation.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber private key and certificate usage

Certificates issued according to eSignTrust Email Certificate, eSignTrust Normalised Certificate, eSignTrust Encipherment Certificate, eSignTrust Qualified Certificate policies, the Subscriber has the responsibility to use his private key and certificate only for appropriate application as set forth in CPS Section 1.4 and in consistency with applicable certificate content. Use of a private key and certificate are also subject to the terms of the Subscriber Agreement. The use of a private key is permitted only after the Subscriber has accepted the corresponding certificate. The Subscriber must discontinue use of the private key following the expiration or revocation of the certificate.

4.5.2. Relying party public key and certificate usage

Regarding relying party responsibilities relating to the use of a Subscriber's public key and certificate, a relying party may be obligated to rely on certificates only for appropriate applications as set forth in CPS Section 1.4 and in consistency with applicable certificate content, successfully perform public key operations as a condition of relying on a certificate, assume responsibility to check the status of a certificate using one of the required or permitted mechanisms set forth in the CPS, and assent to the terms of the applicable Relying Party Agreement as a condition of relying on the certificate.

4.6. Certificate Renewal

Prior to the expiration of an existing subscriber’s certificate, it is necessary for the subscriber to obtain a new certificate to maintain continuity of certificate usage. eSignTrust requires that the Subscriber generate a new key pair to replace the expiring key pair(technically defined as “rekey”), while not permits subscribers to request a new certificate for an existing key pair(technically refined as “renewal”). Therefore, the following sections regarding renewal will have no stipulation.

4.6.1. Circumstance for certificate renewal

No stipulation.

4.6.2. Who may request renewal

No stipulation.

4.6.3. Processing certificate renewal requests

No stipulation.

4.6.4. Notification of new certificate issuance to subscriber

No stipulation.

4.6.5. Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6. Publication of the renewal certificate by CA

No stipulation.

4.6.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.7. Certificate Re-key

4.7.1. Circumstance for certificate re-key

Requested by Subscriber for generation of new key pairs and applying for the issuance of a new certificate that certifies the new public key, due to certificate revoked, key compromised or certificate validity.

4.7.2. Who may request certification of a new public key

Certificate re-keying requests shall be submitted by the Subscriber, or a delegate. Such requests can also be signed using the existing Subscriber’s certificate as long as the certificate is valid.

4.7.3. Processing certificate re-keying requests

Certificate re-keying request is processed by performing identification, authorisation, and validation checks specified in Section 3.2. However, subscriber personal information is updated upon request by the Subscriber. The procedures as specified in Section 3.2 may not be performed in its entirety if signed request or authorisation from the Subscriber is obtained using their existing and valid certificate.

4.7.4. Notification of new certificate issuance to subscriber

Same as Section 4.3.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

Same as Section 4.4.1.

4.7.6. Publication of the re-keyed certificate by the CA

Re-keyed certificate will be published on eSignTrust Repository; in addition, publication will be proceeded when re-key request is approved.

4.7.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.8. Certificate Modification

4.8.1. Circumstance for certificate modification

No stipulation.

4.8.2. Who may request certificate modification

No stipulation.

4.8.3. Processing certificate modification requests

No stipulation.

4.8.4. Notification of new certificate issuance to subscriber

No stipulation.

4.8.5. Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6. Publication of the modified certificate by the CA

No stipulation.

4.8.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for revocation

Certificate revocation request might be issued at anytime for a listed reason.

4.9.1.1. Revocation by Subscriber or Sponsoring Organisation

A Subscriber or Sponsoring Organisation where applicable, shall promptly request revocation of a certificate whenever:

a) The subject name on the certificate is no longer current, complete, or true;
b) The private key, or the media/secure device holding the private key associated with the certificate is known or suspected to of being damaged, lost disclosed, compromised, or subjected to unauthorised use in any way; or
c) The Subscriber is no longer affiliated with the Sponsoring Organisation.

4.9.1.2. Revocation by eSignTrust

The eSignTrust Issuing CA shall revoke a certificate:

a) Upon request by a Subscriber, a Sponsoring Organisation or a competent authority, where applicable;
b) Upon failure of a Subscriber (or a Sponsoring Organisation, where applicable) to meet its material obligations under this eSignTrust CPS and/ or Subscriber Agreement, any other regulation, or law applicable to the certificate that may be in force;
c) If knowledge or reasonable suspicion of compromise is obtained; or
d) If the eSignTrust Issuing CA determines that the certificate was not properly issued in accordance with this eSignTrust CPS.

4.9.2. Who can request revocation

Certificate revocation can be initiated by:

a) The Subscriber of the Certificate, Sponsoring Organisation or a competent authority, where applicable.
b) An authorised representative, or legal representative of the Subscriber, or Sponsoring Organisation where applicable.
c) An RA who informs eSignTrust of any information that came to its attention that may give rise to the need for revoking a certificate. It will be the responsibility of eSignTrust to review and act upon such information.
d) eSignTrust may summarily revoke certificates within its domain, provided that notice and cause are given.

4.9.3. Procedure for revocation request

Except for the revocation request generated stipulated below, eSignTrust accepts no other methods of revocation requests generation.

a) Online Revocation

For Subscribers who possess or are able to recall their Certificate Lifecycle Management Challenge Phase, they can instantly revoke their certificate via eSignTrust at www.esigntrust.com.

b) Offline Revocation

Alternatively, offline revocation request forms have been prescribed by eSignTrust and are available for download at its website. For circumstances where Subscriber does not recall his/her pass phrase, self-revocation feature will not be available to Subscriber and only eSignTrust system administrator can perform certificate revocation with request from Subscriber.

In addition, Revocation requests for Personal Certificates have to be submitted to eSignTrust and they will be authenticated using the Subscribers' relevant identity information according to Section 3.2.3.

Furthermore, duly completed certificate revocation request forms have to be submitted to the eSignTrust personnel, who are authorised to accept such requests on behalf of eSignTrust.

Revocation requests by Sponsoring Organisations via post will be verified with the requestor via the Sponsoring Organisations' telephone number on record.

Revocation requests by Sponsoring Organisations, via facsimile or other methods of communications, will similarly be verified as above. However, the original revocation requests must be received by eSignTrust within ten (10) working days time for the certificate revocation to take effect. For Qualified Certificate, during that period, the related certificate will be suspended, pending receipt of the original revocation request. If the original revocation requests are not received within the above ten (10) working days, eSignTrust personnel will follow-up with the Sponsoring Organisations. Failing to verify the legitimacy of the revocation request, the corresponding certificate may be reverted from suspension.

4.9.4. Revocation request grace period

No stipulation.

4.9.5. Time within which CA must process the revocation request

eSignTrust will process revocation requests as promptly as practicable upon receiving and validating the requests with the Subscriber or Sponsoring Organisation where applicable. eSignTrust will take all reasonable efforts to ensure that certificates are revoked and published onto the CRL in the Repository.

4.9.6. Revocation checking requirement for relying parties

Relying parties could perform revocation checking by comparing current certificate serial number against corresponding CRL. CRL can be downloaded from CRL distribution point extension of a certificate.

4.9.7. CRL issuance frequency

The CRL in the repository is updated at least every 24 hours, even if there are no changes or updates to be made, to ensure timeliness of information.

4.9.8. Maximum latency for CRLs

CRLs for Certificates issued to subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation.

4.9.9. On-line revocation/status checking availability

eSignTrust supports OCSP and its certificate database is updated upon on-line revocation. If the certificate has OCSP feature enabled, Relying Party application requires a compatible OCSP requester to use OCSP capabilities of the certificate database.

Subscribers should notify the Relying Parties if their certificates have OCSP feature enabled.

4.9.10. On-line revocation checking requirements

In accordance with Relying Party obligations, they must validate every certificate they receive in connection with a transaction with Reasonable Reliance as defined in Section 1.6 above.

4.9.11. Other forms of revocation advertisements available

No stipulation.

4.9.12. Special requirement re-key compromise

There are no variations from the certificate revocation procedures as per section above where the revocation is due to private key compromise.

4.9.13. Circumstance for suspension

Suspension is the placement of a certificate on-hold for a brief period without revocation in order for eSignTrust to carry out further investigation regarding the validity of the certificate. Suspension is only applicable to Qualified Certificates.

4.9.14. Who can request suspension

eSignTrust and RA **do accept** requests for suspension of certificates by Subscribers or Sponsoring Organisations.

Hence, eSignTrust may initiate a suspension of a certificate pending validation for:

a) A revocation request received by eSignTrust; or

b) Any information received by the eSignTrust which may necessitate the revocation of a certificate.

4.9.15. Procedure for suspension request

Offline suspension request forms have been prescribed by eSignTrust and are available for download at www.esigntrust.com. Duly completed certificate suspension request forms have to be submitted to eSignTrust.

Suspension requests for Personal Certificates might be submitted to eSignTrust Issuing CA or RA where they will be authenticated using the Subscriber's relevant identity information. Alternatively the verification of suspend request can be performed by other mean, such as via telephone, however, Identification & Authentication requirements still remain.

Suspension requests by Sponsoring Organisations via post, facsimile or other methods of communications will be verified with the requestor via the Sponsoring Organisations' telephone number on record and they will be authenticated using the Subscriber' relevant information stated in Section 3.2.2 above.

Within a ten (10) working days elapsed time, the related certificate will be suspended pending receipt of the original revocation request. If the original revocation requests are not received within the above ten (10) working days, eSignTrust personnel will follow-up with the Sponsoring Organisations or individual, failing to verify the legitimacy of the revocation request, the corresponding certificate may be reverted from suspension.

4.9.16. Limit on suspension period

The eSignTrust Issuing CA may suspend a certificate for up to ten (10) working days pending validation of the revocation requests. Following that, eSignTrust may either cancel the Suspension, or extend the Suspension for a maximum of one (1) further month if necessary. eSignTrust will not be liable for any loss or damage suffered by the Subscriber or any third party as a result of the suspension of a certificate.

4.10. Certificate Status Services

4.10.1. Operational characteristics

Certificate status checking services are available to the relying parties via CRL at eSignTrust Repository, LDAP directory and via an OCSP responder (where available). Checking can be performed using Subscriber email address, Subscriber common name, and the checking result will be returned.

4.10.2. Services availability

Certificate status checking services are available 24x7, except in case of planned maintenance or force majeure. CRL generation is scheduled to be executed daily, while OCSP service will be available 24 hours a day and 7 days a week, relying parties consulting this services need to agree the corresponding Relying Parties Agreements before engage with this service.

4.10.3. Optional features

No stipulation.

4.11. End of Subscription

End of Subscriber certification services can be due to revocation of certificates or expiration of the certificate, refer to Section 4.9 for details in revocation procedure.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and recovery policy and practices

eSignTrust provides an archival service for Subscriber’s Encipherment Private Key. If Subscribers should require retrieving a copy of their encipherment public key, encipherment private key and encipherment certificate, they have to apply personally at eSignTrust using a request form by eSignTrust.

4.12.2. Session key encapsulation and recovery policy and practices

No stipulation.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

The eSignTrust CA operations are housed in a secured data centre with multiple layers of perimeter protection to control normal physical access to the core of the CA operations.

The secured data centre is further equipped with physical intrusion detection system, closed circuit surveillance system, and 24-hours alarm monitoring by a security agency.

eSignTrust also maintains disaster recovery facilities for its CA operations. eSignTrust disaster recovery facilities are also protected by multiple tiers of physical security.

5.1.2. Physical Access

eSignTrust CA operation is located in a site that affords commercially reasonable physical security. The CA systems are protected by multiple layers of physical security, with access to the lower layer required before gaining access to the higher layers.

Progressively restrictive physical access privileges control access to each layer. Access to each layer requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional layers enforce individual access control through the use of two-factor authentication including biometrics. Unescorted personnel, including employees without proper authorisation or visitors, are normally not allowed into such secured areas.

5.1.3. Power and Air Conditioning

The critical components of the eSignTrust Issuing CA and RA systems are supported by Uninterruptible Power Supply ("UPS") systems and backup by power generators. Such UPS and backup power generator facilities are subjected to regular testing.

Air-conditioning is provided by a system of multiple, independent air handlers that continually monitor and adjust temperature and humidity for optimum operating conditions.

5.1.4. Water Exposure

The eSignTrust CA employs appropriate safeguards (such as moisture detectors and drainage pipes) to detect and protect its secure operating area against water exposure (e.g., from floods or pipe leakage).

5.1.5. Fire Prevention and Protection

The eSignTrust CA employs appropriate safeguards to protect its secure operating area against fire hazards.

In addition, eSignTrust premises are installed with fire and smoke detection systems, and both fixed and portable fire suppression systems for countering fire hazards. eSignTrust fire prevention and protection measures comply with local fire safety regulations.

5.1.6. Media Storage

Off-site backup media are stored in a fireproof vault in a secured storage facility. Access to the vault is restricted to minimal authorised personnel.

5.1.7. Waste Disposal

All confidential, private, and/ or sensitive information materials are shredded or otherwise destroyed on-site prior to disposal so that they are unreadable and irrecoverable. Cryptographic devices are physically destroyed or disposed in accordance the manufacturers' guidance.

5.1.8. Off-site backup

All backup (e.g., data, programs, full system) media are removed to the off-site storage location, which is geographically diverse from the primary CA operations site. Physical access to the off-site location is restricted to minimal authorised personnel.

5.2. Procedural Control

5.2.1. Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- The validation of information in Certificate Applications;
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrolment information;
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository; or
- The handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- Customer service personnel,

- Cryptographic business operations personnel,
- Security personnel,
- System administration personnel,
- Designated engineering personnel, and
- Executives that are designated to manage infrastructural trustworthiness.

5.2.2. Number of persons required per task

The eSignTrust CA utilises commercially reasonable practices to ensure that one individual acting alone cannot circumvent safeguards by segregating responsibilities into multiple roles and individuals. Each account on the CA systems has limited capabilities commensurate with the role of the account holder.

The eSignTrust CA ensures that no single individual may gain access to any archived/ escrowed Subscriber Encipherment Private Keys. At minimum, procedural or operational mechanisms is in place to perform a Key recovery, using a split-knowledge technique to prevent disclosure to an unauthorised individual. Multi-user control is also required for CA key generation.

The eSignTrust CA ensures that any verification process it employs provides for oversight of all activities performed by privileged eSignTrust Issuing CA role holders. To ensure the integrity of eSignTrust Issuing CA equipment and operation, wherever possible a separate individual will be identified for each trusted role. The separation provides a set of checks and balances over the eSignTrust Issuing CA and RA operation. Under no circumstances will the incumbent of an eSignTrust Issuing CA role perform its own auditor function.

5.2.3. Identification and authentication of each role

All eSignTrust Issuing CA and RAs personnel will have their identity and authorisation verified in accordance with Macao Post and Telecommunications Bureau policy and procedures before they are:

- Included in the access list for the eSignTrust Issuing CA and RAs site;
- Included in the access list for physical access to the eSignTrust Issuing CA and RAs system; and
- Given an account on the CA systems.

5.3. Personnel Control

5.3.1. Background, qualifications, experience, and clearance requirements

eSignTrust Issuing CA follows personnel and management policies sufficient to provide reasonable assurance of:

- The trustworthiness and competence of employees, including those at approved RAs; and
- The satisfactory performance of their duties in manners consistent with this eSignTrust CPS.

5.3.2. Background check procedures

eSignTrust Issuing CA conducts appropriate investigation of all personnel, including those at eSignTrust RAs, who serve in trusted roles, to verify their trustworthiness and competence in accordance with the requirements of this eSignTrust CPS. Personnel serving in trusted roles at designated RAs is to be checked by their corresponding entities in accordance with the requirements of this eSignTrust CPS. All personnel who fail any required investigation will not serve or continue to serve in a trusted role. Similar to Section 5.3.6 below, the eSignTrust Issuing CA will also promptly suspend his/ her access rights to CA systems.

5.3.3. Training requirements

eSignTrust Issuing CA ensures that all personnel performing CA related services, including those in approved RAs, receive relevant training in:

- The CA and/ or RA security principles and mechanisms;
- Security awareness;
- PKI software versions in use on the CA systems;
- All PKI duties they are expected to perform; and
- Disaster recovery and business continuity procedures.

5.3.4. Retraining frequency and requirements

The requirements of Section 5.3.3 above are kept current to accommodate changes in the CA systems. Refresher training will be conducted as required, and the eSignTrust reviews these requirements on appropriate regular basis.

5.3.5. Job rotation frequency and sequence

No stipulation.

5.3.6. Sanctions for unauthorised actions

In the event of actual or suspected unauthorised action by personnel performing duties with respect to the operation of a CA and/ or RA, the eSignTrust Issuing CA will promptly suspend his or her access to the CA systems and/or will be subjected to disciplinary actions which may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorised actions.

5.3.7. Independent Contractor requirements

eSignTrust Issuing CA and RAs may employ contract personnel to perform services associated with the operation and management of the eSignTrust PKI. Such contractors will enter into written agreements defining their roles and responsibilities, to ensure that they are bound to security and confidentiality requirements that are at least as restrictive as those applicable to employees.

5.3.8. Documentation supplied to personnel

Documentation sufficient to define duties and procedures for each role is provided to personnel filling respective roles.

5.4. Audit Logging procedures

5.4.1. Types of event recorded

The eSignTrust maintains system audit logs that provide adequate details to establish the validity of Subscribers' Digital Signature and of the proper operation of the eSignTrust PKI. At minimum, system audit logs relating to system events, CA application events and other key-pair and certificate related events will be maintained.

5.4.2. Frequency of processing log

eSignTrust Issuing CA personnel review the audit logs at least on a weekly basis, and all significant events are explained in an audit summary.

The reviews involve using reliable methods for verifying that audit logs have not been tampered with, brief inspection of audit log entries, and more thorough investigation of any alerts or irregularities in the audit logs. Supporting manual and electronic logs from the eSignTrust Issuing CA and RAs will be compared where any action is deemed suspicious. Actions taken following these reviews will be documented. When applicable, reliable automated tools will be used to complete the above task.

5.4.3. Retention period for audit log

The audit logs relevant to the CA operations recorded in CA audit trails will be retained for a minimum of fifteen (15) years.

5.4.4. Protection of audit log

Electronic and manual audit log files are reasonably protected from unauthorised viewing, modification, deletion, or other tampering through the use of physical and logical access controls.

5.4.5. Audit log backup procedures

Audit logs and audit summaries are backed-up on a regular basis.

5.4.6. Audit collection system (internal or external)

Audit processes will be invoked at system start-up, and will cease only at system shutdown. Should it become apparent that a critical automated audit system has failed, manually generated audit data will be recorded by eSignTrust personnel until the audit capability is restored.

5.4.7. Notification to event-causing subject

There is no notification requirement when an event is audited or real-time alerts given to an event-causing subject for any audited event.

5.4.8. Vulnerability assessments

eSignTrust conducts vulnerability assessments as required by their CA security procedures, over the Issuing CA operations. The assessment results will be reported to eSignTrust for review and approval of an improvement action plan.

5.5. Records Archival

5.5.1. Types of records archived

The eSignTrust Issuing CA maintains records that provide adequate details to establish the validity of Subscribers' Digital Signature and of the proper operation of the eSignTrust PKI. At minimum, records relating to system events, CA application events and other key-pair and certificate related events are maintained. Such records include:

- Certificates requests together with records of actions and information that are material to the certificate application;
- The certificate lifecycle events which include identity of the Subscriber named in the certificate, the identity of person requesting certificate revocation/suspension/unsuspension;
- Certificates and CRLs issued;
- CP and CPS issued;

- Subscriber agreements and/or contracts; and
- Audit results.

5.5.2. Retention period for archive

The archives of the CA operations will be retained for a minimum of fifteen (15) years or following retention schedules prescribes by MSAR Laws and Regulations.

5.5.3. Protection of archive

The archived records are protected at a level of physical security where only authorised eSignTrust Issuing CA personnel can access them. Electronic records are also environmentally protected and stored at a secured off-site location.

5.5.4. Archive backup procedures

All archived records are stored at a secured off-site location with similar protection as stated in the previous section.

5.5.5. Requirements for time-stamping of records

The records referred to in Section 5.5.1 above are time-stamped at the point of occurrence. eSignTrust Issuing CA ensures that time-stamp clocks and system clocks are not subject to unauthorised manipulation.

5.5.6. Archive collection system (internal or external)

No stipulation.

5.5.7. Procedures to obtain and verify archived information

During any audits required by this eSignTrust CPS, the auditor shall assess the controls for preserving the integrity of the archived information.

5.6. Key changeover

The life span of the eSignTrust Root and Issuing CAs' certificates and Key-Pairs are twenty five (25) years and fifteen (15) years respectively. New eSignTrust Root and Key-Pairs will be generated at every twenty-second (22th) year of the life span of the current eSignTrust Root and Key-Pairs, and be used for subsequent signing of certificates till the twenty-second (22th) year of the new set's life span.

Therefore, at any one time between the twenty-second (22th) year and twenty-fifth (25th) year of the life span of the eSignTrust Root and Key-Pairs, there will exist two (2) sets of valid eSignTrust Root and Issuing CAs' Certificates and Key-Pairs. Both sets of eSignTrust Root and Issuing CAs' Certificates will be made available in the eSignTrust Repository for validation of the certificate chain from the Subscriber certificates back to their corresponding set of eSignTrust Root and Issuing CAs' Certificates.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise handling procedures

The eSignTrust Issuing CA maintains detailed documentation covering Business Continuity Plan as well as Incident Response Plan. The purpose of this plan is to restore core business operations as quickly as practicable when systems and/or operations have been significantly and adversely impacted by security incidents, natural disasters and unplanned events.

In addition, the eSignTrust Issuing CA tests its disaster recovery, and business resumption plans at least once every twelve (12) months. The test results and findings will be fully documented. The disaster recovery and business resumption plan will at minimum cover:

Repository Services

The set up of an operational facility located in a geographically diverse area that is capable of providing Repository services in accordance with this eSignTrust CPS within twenty-four (24) hours of an unanticipated emergency.

Certificate Issuance Services

The set up of an operational facility located in a geographically diverse area that is capable of providing certificate issuance services in accordance with this eSignTrust CPS within a reasonable timeframe.

5.7.2. Computing resources, software, and/or data are corrupted

eSignTrust makes regular system backups on at least a weekly basis and maintains backup copies of its CA Private Keys, which are stored in a secure, off-site location. If eSignTrust discovers that any of its computing resources, software, or data operations have been compromised, eSignTrust assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If eSignTrust determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, eSignTrust suspends such operation until it determines that the risk is mitigated.

5.7.3. Entity private key compromise procedures

In the event that the certificates of the eSignTrust Root CA and/ or Issuing CA containing the Public Keys that correspond to the Private Key used by the eSignTrust Root CA and/ or Issuing CA to issue certificates are compromised, the eSignTrust Issuing CA will firstly:

- Publish the serial number of the revoked certificate to an appropriate ARL;
- Notify all certificate holders of the revocation through all reasonable means.

After addressing the above, the eSignTrust Issuing CA will then proceed to:

- Generate new Root CA and/ or Issuing CA Key-Pairs where applicable;
- Re-issue all certificates and CRLs using the new signing Key-Pairs; and
- Notify all RAs, Subscribers, Sponsoring Organisation, and Relying Parties of the new Issuance of certificates.

5.7.4. Business continuity capabilities after a disaster

eSignTrust has implemented a disaster recovery site which is geographically diverse from the primary CA operations site. In the event of disaster requiring temporary or permanent cessation of operations from eSignTrust primary site, eSignTrust disaster recovery plan is initiated and will restore essential operations at the disaster recovery site within twenty four (24) hours following the disaster.

Building security or contracted security personnel will monitor the CA operations facility after a disaster to protect against loss, additional damage to, and theft of sensitive materials and information.

5.7.5. CA or RA Termination

When it is necessary to terminate the CA operations of eSignTrust, the following procedures will be carry out to minimise disruption to subscribers and relying parties:

- Providing a minimum of ninety (90) days of reasonable notice to all RAs, certificate holders, Sponsoring Organisations, and Relying Parties;
- Transfer of service and operational records to a successor CA by the end of the notice period; and
- Preserving any records not transferred to a successor CA.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. *Key pair generation*

eSignTrust Root and Issuing CA Key-Pairs Generation

Private Keys of Key-Pairs for the eSignTrust Root and Issuing CA are directly generated in hardware cryptographic module validated as per Section 6.2.1 below and are not extractable. The Key-Pairs generation is performed by multiple pre-selected, trained and trusted individuals using controlled system and processes that provide for the security and required cryptographic strength for the generated keys. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. The Key-Pairs generation will also be witnessed.

Subscriber Key-Pairs Generation

Generation of any eSignTrust Subscriber Key-Pair are distributed at the respective RA premises, or designated locations, using trustworthy system. The Private Keys are generated using native features provided by the systems/devices themselves. Subsequent to Key-Pair generation, Certificate Signing Requests ("CSR") are created and sent to the eSignTrust Issuing CA for creation and signing of the corresponding certificate. The eSignTrust Issuing CA signed certificate is then returned to the RA/ Subscriber.

6.1.2. *Private key delivery to Subscriber*

After key-pair generation at the RA location, the Subscriber private key will be stored in a storage media, of the type indicated by the Subscriber in the certificate application form. The access to the storage media will be immediately handed over to the Subscriber upon the completion of the Identification & Authentication process of the Subscriber.

6.1.3. *Public key delivery to certificate issuer*

A PKCS#10 Certificate Signing Requests ("CSR") is being sent to the eSignTrust Issuing CA for creation and signing of a corresponding certificate, copy of the Subscriber Public Key is bound to the CSR, delivered to the eSignTrust Issuing CA, and finally bound to the Subscriber certificate that is signed by the eSignTrust Issuing CA.

6.1.4. *CA public key delivery to users*

The Public Keys of the eSignTrust Root and Issuing CAs are published at the eSignTrust website at <www.esigntrust.com>.

Those keys are distributed solely in a form of X.509 v.3 certificate.

6.1.5. Key sizes

eSignTrust Root is at a minimum of 4096-bit RSA. Issuing CAs key-pairs is at a minimum of 2048-bit RSA. eSignTrust administrator certificate key-pair and Subscriber key-pair are at a minimum of 1024-bit RSA.

6.1.6. Public key parameters generation and quality checking

The parameters used to create eSignTrust Root CA and Issuing CA Public Keys are generated using state of the art technology by the eSignTrust Root CA’s and Issuing CA's CA systems respectively.

The parameters used to create administrator and Subscriber Public Keys are generated using eSignTrust PKI system.

The quality of eSignTrust Root CA and Issuing CAs Public Key parameters are automatically checked by the eSignTrust Root CA’s and Issuing CA's CA systems that generate the Public Key.

The quality of administrator and Subscriber Public Key parameters is automatically checked by eSignTrust PKI system that generates the Public Key.

6.1.7. Key usage purposes

The X.509 v.3 certificates issued by the eSignTrust Issuing CA contain the Key Usage certificate extension, restricting the purpose to which the certificate can be applied. Details of appropriate usage of certificates issued by eSignTrust are listed in CPS Section 1.4.

The public / private key pair is used to provide encryption, decryption, authentication, integrity and support for non-repudiation services if allowed in the Key Usage certificate extension.

Additional extensions can be added to allow or restrict key usage to some applications.

6.2. Private Key protection and cryptographic module engineering control

6.2.1. Cryptographic module Standards and control

The hardware cryptographic modules used by the eSignTrust for Root and Issuing CAs Key-Pairs generation and protection are certified to meet the requirement of FIPS 140-2 Level 3. The software cryptographic modules used by the administrator and Subscriber Key-Pairs generation are validated to at least FIPS 140-1 Level 1.

6.2.2. Private Key (m out of n) multiperson control

eSignTrust uses technical procedures that require the participation of multiple trusted individuals to perform highly sensitive CA cryptographic operations. eSignTrust uses “Secret Sharing” to split the activation data needed to make use of a CA private key into separate parts called “Secret Shares” which are held by trained and trusted individuals called “Shareholders.” A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module. The threshold number of shares needed to sign a CA certificate is three (3). Shareholders are comprised of eSignTrust senior management in trusted roles.

6.2.3. Private Key Escrow

eSignTrust does not escrow Root, Issuing CAs or Subscriber Signing private keys with any third party.

6.2.4. Private Key backup

Backup of the eSignTrust Root and Issuing CAs Private Keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices in a secured off-site location, and their restoration is split-controlled between eSignTrust senior management in trusted roles.

eSignTrust may provide backup services for Encipherment Private Keys that are not required to be kept on a hardware device.

6.2.5. Private key archival

eSignTrust does not archive copies of Root, Issuing CAs or Subscriber private keys except the Subscriber Encipherment Certificate Private Keys that can be recovered upon request by the Subscribers, see Section 6.2.3, 6.2.4 for details.

6.2.6. Private Key transfer into or from a cryptographic module

As per Section 6.1.1 above, Private Keys of Key-Pairs for the eSignTrust Root and Issuing CAs are directly generated in hardware cryptographic module validated as per Section 6.2.1 of this CPS and are not extractable.

6.2.7. Private Key storage on cryptographic module

eSignTrust generates CA key pairs on the hardware cryptographic modules in which the keys will be used. The private key remains stored in encrypted form within hardware cryptographic modules and associated key storage devices validated as per Section 6.2.1 of this CPS.

6.2.8. Method of activating private key

The eSignTrust Root and Issuing CAs Private Keys are activated by tokens and activation Data is split-controlled between eSignTrust senior management in trusted roles.

6.2.9. Method of deactivating private key

eSignTrust CA private keys are deactivated upon system log off or disconnection. eSignTrust administration certificate private keys (used for authentication to the RA application) are deactivated upon system log off. eSignTrust RAs are required to log off their workstations when leaving their work area.

Administrator and Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card / hardware token from the smart card reader or depending upon the authentication mechanism employed by the user. End-user Subscribers have an obligation to adequately protect their private key(s).

6.2.10. Method of destroying private key

When necessary, eSignTrust destroys CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key.

eSignTrust utilises the zeroisation function of its hardware cryptographic modules according to the specifications of the hardware manufacturer and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged. CA key destruction activities require the participation of multiple trusted individuals.

6.2.11. Cryptographic module rating

For eSignTrust Root and Issuing CA key pair generation and CA private key storage, eSignTrust uses hardware cryptographic modules that are certified at or at least meet the requirements of FIPS 140-2 Level 2 and Level 3.

The software cryptographic modules used by the administrator and Subscriber Key-Pairs generation are validated to at least FIPS 140-1 Level 1.

6.3. Other aspects of key pair management

6.3.1. Public key archival

The eSignTrust Issuing CA archives all public keys and certificates upon their expiry or revocation.

6.3.2. Certificate operational periods and key pair usage period

The validity period of eSignTrust Root are twenty-five (25) years and Issuing CAs' Certificates and Key-Pairs are fifteen (15) years. The validity period of all other entity and Subscriber certificate and key-pairs is three (3) years.

6.4. Activation Data

6.4.1. Activation data generation and installation

The Activation data (Secret Shares) used for protecting tokens containing eSignTrust CA private keys is generated in accordance with the requirements outlined in Section 6.2.2 of this CPS. The creation and distribution of Secret Shares is logged.

6.4.2. Activation data protection

The Activation data used for eSignTrust Root and Issuing CA private key activation is protected by means of cryptographic controls and physical access controls.

6.4.3. Other aspects of activation data

If there is a need to transmit the activation data of CA private keys, this transmission will be protected against information loss, theft, data change and unauthorised release.

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements.

All CA system servers include the following functionalities, either provided by the operating system, or through a combination of operating system, PKI application, and physical safeguards:

- Access control to CA services and PKI roles;
- Enforced separation of duties for PKI roles;
- Identification and authentication of PKI roles and associated identities;
- Use of cryptography for session communication security;
- Archival of CA-related history and audit data;
- Audit of CA-related security events; and
- Recovery mechanisms for keys and the Issuing CA system.

6.5.2. Computer security rating

The eSignTrust Issuing CA has implemented an appropriate Information Security Management System in conformance with industry best practice such as AICPA/CICA WebTrust for Authorities Principles and Criteria.

6.6. Certificate Life Cycle Technical Controls

6.6.1. System development controls

System development is implemented in a controlled and secure environment segregated from the CA production environment. All process, hardware and software are firstly tested within eSignTrust controlled and secure Test/Staging Environment before deployment to the CA production environment.

eSignTrust operational policy requires fully documented change management and configuration management for system development control.

6.6.2. Security management controls.

A formal configuration management methodology is used for installation and ongoing maintenance of the CA systems.

The CA software, when first loaded, provides for the verification that the software:

- Originated from the software developer;
- Has not been modified prior to installation; and
- Is the version intended for use.

The eSignTrust Issuing CA has procedures to periodically verify the integrity of the CA software. In addition, there are also procedures and policies in place to control, monitor and validate the configuration of the CA systems.

6.6.3. Life cycle security ratings

No stipulation.

6.7. Network Security Controls

The eSignTrust Issuing CA implemented a three-tiered network infrastructure comprised of firewalls and intrusion detection systems which are configured to allow access only to addresses, ports, protocols, and commands required for the trustworthy provision of PKI services by eSignTrust 's CA systems.

The eSignTrust Root CA equipment is stand-alone and shut-down after signing of the eSignTrust Issuing CA Certificates.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

CPS Section 7.1 defines eSignTrust Certificate Profile and Certificate content requirements for Certificates issued under this CPS. eSignTrust Certificates conform to

- The Electronic Documents and Signatures Law of MSAR (Law no. 5/2005)
- ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008
- RFC 3739: Internet X.509 Public Key Infrastructure : Qualified Certificate Profile, March 2004

Refer to Appendix A for details in certificate profiles being implemented by eSignTrust.

7.1.1. Version number(s)

eSignTrust CA and end-user Subscriber Certificates are X.509 Version 3 Certificates.

7.1.2. Certificate Extensions

eSignTrust populates certificates with extensions specified in Appendix A. Other extensions may be supported in the future.

7.1.3. Algorithm Object Identifier

The eSignTrust PKI supports the following algorithm:

- RSA 1024/ 2048/ 4096 Digital Signature in accordance with PKCS#1;
- SHA-1/SHA256 in accordance with US FIPS PUB 180-4 and ANSIX9.30 (OID: 1.2.840.113549.1.1.5 / 2.16.840.1.101.3.4.2.1)
- Triple-DES in accordance with ANSI X9.52;
- Message Authentication Code (MAC) in accordance with US FIPS PUB 113, ANSI X9.9 and X.19; and
- MD5 Message-Digest Algorithm in accordance with Internet RFC 1321 (OID: 1.2.840.113549.1.1.4)

7.1.4. Name Forms

Certificate issued by eSignTrust Issuing CA contain the full X.500 Distinguished Name of the eSignTrust Issuing CA as the issuer in the issuer name field and Certificate Subject in the subject name field.

eSignTrust populates Certificates with an Issuer and Subject Distinguished Name in accordance with Section 3.1.

7.1.5. Name Constrains

No stipulation.

7.1.6. Certificate Policy Object Identifier

Each certificate issued by the eSignTrust Issuing CA contains the OID of the eSignTrust CP under which the certificate is issued.

Certificate Policy	Description	OID
Qualified Certificate for Personal	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certificate-policy (1) id-qualified-certtype (3) id-personal-scope (1)	eSignTrust Personal Qualified Identity Certificate; OID: 1.3.6.1.4.1.15108.2.1.3.1
Qualified Certificate for Corporate	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certificate-policy (1) id-qualified-certtype (3) id-corporate-scope (2)	eSignTrust Corporate Qualified Identity Certificate; OID: 1.3.6.1.4.1.15108.2.1.3.2
Qualified Certificate for Government	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certificate-policy (1) id-qualified-certtype (3) id-government-scope (3)	eSignTrust Government Qualified Identity Certificate; OID: 1.3.6.1.4.1.15108.2.1.3.3
Normalised Certificate for Personal	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certificate-policy (1) idnormalised-certtype (2) id-personal-scope (1)	eSignTrust Personal Normalised Identity Certificate; OID: 1.3.6.1.4.1.15108.2.1.2.1
Normalised Certificate for Corporate	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certificate-policy (1) id-normalised-certtype (2) id-corporate-scope (2)	eSignTrust Corporate Normalised Identity Certificate; OID: 1.3.6.1.4.1.15108.2.1.2.2
Normalised Certificate for Government	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certificate-policy (1) id-	eSignTrust Government Normalised Identity Certificate; OID: 1.3.6.1.4.1.15108.2.1.2.3

	normalised-certtype (2) id-government-scope (3)	
Encipherment Certificate for Personal	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certificate-policy (1) id-encipherment-certtype (5) id-personal-scope (1)	eSignTrust Personal Encipherment Certificate; OID: 1.3.6.1.4.1.15108.2.1.5.1
Encipherment Certificate for Corporate	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certificate-policy (1) id-encipherment-certtype (5) id-corporate-scope (2)	eSignTrust Corporate Encipherment Certificate; OID: 1.3.6.1.4.1.15108.2.1.5.2
Encipherment Certificate for Government	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certificate-policy (1) id-encipherment-certtype (5) id-government-scope (3)	eSignTrust Government Encipherment Certificate; OID: 1.3.6.1.4.1.15108.2.1.5.3
Personal Secure Email Certificate	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108) id-pki (2) id-certificate-policy (1) id-email-certtype (1) id-personal-scope (1)	eSignTrust Personal Email Identity and Encipherment Certificate; OID: 1.3.6.1.4.1.15108.2.1.1.1

7.1.7. *Usage of Policy Constraints extension*

No stipulation.

7.1.8. *Policy qualifiers syntax and semantics*

eSignTrust includes brief statements in Certificates about the limitations of liability and other terms associated with the use of a Certificate in the Policy Qualifier field of the Certificates Policy extension.

7.1.9. *Processing semantics for the critical certificate policies extension*

No stipulation

7.2. CRL Profile

Field	Value or Value Constraint
Version	V2
Issuer	Entity that has signed and issued the CRL. The CRL issuer Name is in accordance with the Issuer Distinguished Name requirements specified in CPS Section 3.1.1
Effective Date	Issue date of CRL. eSignTrust CRLs are effective

	upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with requirements of CPS Section 4.9.7.
Signature Algorithm	Algorithm used to sign the CRL. eSignTrust CRLs are signed using sha1RSA in accordance with RFC3280

7.2.1. Version number(s)

eSignTrust Issuing CA issues X.509 version 2 CRL.

7.2.2. CRL and CRL entry extensions

Extension	Value or Value Constraint
Authority Key Identifier	Provides a means of identifying the public key corresponding to the private key used to sign a CRL. The identification can be based on either the key identifier or on the issuer name and serial number.
Issuer Alternative Name	Domain name of the issuing CA
CRL Number	It is a number which conveys a monotonically increasing sequence number for a given CRL scope and CRL issuer.
Issuing Distribution Point	It identifies the CRL distribution point and scope for a particular CRL, and it indicates whether the CRL covers revocation for end entity certificates only, CA certificates only, attribute certificates only, or a limited set of reason codes.

7.3. OCSP Profile

The protocol of on-line certificate status verification (OCSP) is used by certification authentication and allows certificate status evaluation. The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a signed positive response.

Information concerning OCSP responder operation information is presented on (www.esigntrust.com/en/repository.html).

OCSP certificate may contain information about the means of contact with OCSP server. This information is included in the field of AuthorityInfoAccessSyntax extension indicates how to access CA information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and CA policy data.

7.3.1. Version Number

eSignTrust OCSP profile follows IETF PKIX RFC2560 OCSP Version 1.0.

7.3.2. OCSP extensions

No OCSP extensions are supported.

8. Compliance Audit and Other Assessment

To ensure that all eSignTrust's procedures and practices are by the Issuing CA and/ or RAs operated in accordance with this eSignTrust CPS, compliance assessment will be conducted on a regular basis.

8.1. Frequency of entity compliance audit

Compliance audits / assessment against this eSignTrust CPS shall be conducted at least on an annual basis.

8.2. Identity/qualifications of the auditor

The auditors performing the compliance audit / assessment shall be suitably qualified (e.g., Certified Information Systems Auditor qualification) and demonstrates proficiency in public key infrastructure technology, information security tools and techniques and security auditing.

8.3. Assessor's relationship to assessed party

Compliance audits / assessment of eSignTrust operations are performed by a reputable auditor firm that is independent of eSignTrust.

8.4. Topics covered by audit

The compliance audit / assessment will evaluate compliance of the Issuing CA and / or RAs against this eSignTrust CPS.

8.5. Actions taken as a result of deficiency

If a compliance audit / assessment reports any material non-compliance, the Issuing CA and/ or RAs shall develop a remedial plan for such non-compliance.

If eSignTrust determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the eSignTrust CA, a corrective action plan will be developed and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, eSignTrust management will evaluate the significance of such issues and determine the appropriate course of action.

8.6. Communication of results

The results of any compliance audit / assessment of the Issuing CA and/ or RAs shall be reported to the Issuing CA and/ or RAs and filed with the eSignTrust management.

9. Other Business and Legal Matters

9.1. Fees

A regularly updated pricing sheet of eSignTrust services is publicly available on its website at www.eSignTrust.com.

eSignTrust reserves the right to change its fees from time to time and to publish its pricing sheet by other means.

9.1.1. Certificate issuance or renewal fees

Such fees, where applicable, are published in the pricing sheet in accordance with the previous section.

9.1.2. Certificate access fees

Such fees, where applicable, are published in the schedule of fees in accordance with Section 9.1.

9.1.3. Revocation or status information access fees

Such fees, where applicable, are published in the pricing sheet in accordance with Section 9.1.

9.1.4. Fees for other services

Such fees, where applicable, are published in the schedule of fees in accordance with Section 9.1.

9.1.5. Refund policy

No stipulation.

9.2. Financial responsibility

9.2.1. Insurance coverage

eSignTrust activity is dully covered by civil liability insurance, in accordance with the applicable laws of MSAR.

9.2.2. Other assets

Being part of Macao Post and Telecommunications Bureau, which, in turn, is a body of MSAR Administration, eSignTrust does not suffer from the risks commonly associated to private companies' activity, therefore being able to provide a stable, risk-free and long-lasting service to its valuable costumers.

9.2.3. Insurance or warranty coverage for end-entities

Not applicable.

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

It is recommended that a Certificate does not contain any sensitive business information that is not necessary for its effective use.

eSignTrust may request business information for archiving purposes or for any other reason, such as imposed by law. This information will be kept confidential.

Audit information shall be considered sensitive and shall not be disclosed to anyone for any purpose other than for auditing or mandatory reporting purposes, or where otherwise required by MSAR laws.

9.3.2. Information not within the scope of confidential information

Certificates, CRLs and personal, corporate, governmental or other organisational information appearing on them and in the Repository are not considered confidential and are disclosed.

9.3.3. Responsibility to protect confidential information

As stated in Section 9.3.1.

9.4. Privacy of personal information

9.4.1. Privacy plan

eSignTrust shall comply with privacy plans that apply to specific Subscribers' activities, if required by applicable laws or policies.

9.4.2. Information treated as private

It is recommended that a Certificate does not contain any sensitive personal information that is not necessary for its effective use.

eSignTrust may request not-to-be-certified personal information to be used in managing of Certificates, or for billing or archiving purposes, or for any other reason, such as imposed by law. This information will be kept confidential.

eSignTrust protects private information using appropriate safeguards and a reasonable degree of care.

Digital Signature Private Keys shall be kept confidential.

9.4.3. Information not deemed private

As stated in Section 9.3.2.

9.4.4. Responsibility to protect private information

Information collected that is considered private or confidential, or personally identifiable, will not be sold, rented, leased or disclosed in any manner to any third party without prior express written consent of the Subscriber, unless required by law or MSAR court order.

eSignTrust employees and contractors are expected to handle personal information in strict confidence and meet the requirements of MSAR law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

The CRL shall provide information via the Repository, indicating the fact of Certificate revocation, but not the reason for the revocation status.

9.4.5. Notice and consent to use private information

As stated in the previous section.

9.4.6. Disclosure pursuant to judicial or administrative process

No information shall be released to the MSAR judicial or administrative authorities by eSignTrust, the Issuing CAs, RAs, and their employees or agents, except where:

- A properly constituted warrant or such other legally enforceable document in MSAR is produced; and
- The law enforcement official is duly authorised by the competent authorities of the MSAR and is properly identified.

9.4.7. Other information disclosure circumstances

No information shall be released to any person by eSignTrust, the Issuing CAs, RAs, and their employees or agents, except where:

- A properly constituted instrument recognised by the laws of MSAR requiring production of the information is produced; and
- The person requiring production is a person authorised to do so and is properly identified.

The subject of a registration record has full access to that record and is empowered to authorise release of that record to another person. No release of information is permitted without formal authorisation.

9.5. Intellectual property rights

eSignTrust warrants that it is in possession of, or holds licences for the use of hardware and software in support of this eSignTrust CPS.

Private Keys are the sole property of the Individual or Sponsoring Organisation names in the «Subject» field of the Certificates containing the corresponding Public Keys. eSignTrust hereby grants to Subscribers a limited revocable license to use such Certificates as are provided to them in accordance with this eSignTrust CPS and the Subscriber Agreement, for their exclusive use, only for the limited purposes set forth in this eSignTrust CPS, and only during the validity period of the Certificates. Any other use of the above is expressly prohibited.

This eSignTrust CPS, its OIDs and all eSignTrust trademarks used or embedded in or in connection with any and all Certificates issued and all software developed by eSignTrust pursuant to this eSignTrust CPS, including all documentation and manuals relating thereto, are the intellectual property of eSignTrust and are protected by copyright, trademark or other laws regarding intellectual property, and may be used only by permission from eSignTrust, and only in accordance with the provisions of such permission and this eSignTrust CPS. Any other use of the above without the express written permission of eSignTrust is expressly prohibited.

9.6. Representations and warranties

9.6.1. CA representations and warranties

eSignTrust warrants only that its makes reasonable efforts to ensure its procedures are implemented in accordance with this eSignTrust CPS, as well as with the applicable laws of MSAR. Namely, when issuing a Certificate, eSignTrust warrants that:

- It will use reasonable care in the creation of the Certificate to ensure no errors introduced by itself in the certificate information;
- The Certificate complies in all material aspects with the CPS; and

- Its revocation services and use of a Repository conform to the CPS in all material aspects.

9.6.2. RA representations and warranties

Where an eSignTrust Issuing CA appoints a Remote RA, the Issuing CA may enter into an indemnification agreement with the Remote RA in accordance with Section 9.9, but the Issuing CA remains responsible to Subscribers, Relying Parties and the governmental regulatory bodies of MSAR, where applicable.

9.6.3. Subscriber representations and warranties

Subscribers/Sponsoring Organisations are responsible for:

- The provision of complete, true, updated and non-misleading information, as appropriately required by the Issuing CA or RA, in order to meet Subscriber registration requirements or Certificate renewal requirements;
- The payment of the fees for Certificate issuance or renewal, where applicable; and
- The requesting of the revocation of the Certificate if the Certificate information is no longer valid or the sponsored Subscriber is no longer affiliated with the Sponsoring Organisation.

9.6.4. Relying Party representations and warranties

Prior to relying or using a Certificate issued by eSignTrust, Relying Parties are responsible for:

- Understanding, agreeing to, and accepting the terms of this eSignTrust CPS;
- Ensuring that the Certificate and its intended use is in accordance with the applicable provisions of this eSignTrust CPS;
- Checking the validation of the Certificate (*i.e.*, confirm that it has not expired, or been revoked or suspended), by consulting the Repository of the Issuing CA as detailed in Section 4.10;
- Trusting and making use of the Certificate only if a valid Certificate chain is established between the Relying Party and the subject in the Certificate. A valid Certificate chain means that Certificate signatures have been validated back to the Issuing CA and Root CA, and the Repository has been checked to determine the validity of the Certificate;
- Verifying that the Digital Signature in question was created by the Private Key corresponding to the Public Key in the Certificate during the Certificate's validity period;
- Confirming that any document signed with a Digital Signature has not been altered; and

- Acting in good faith, in light of all circumstances that were known or should have reasonably been known to the Relying Party prior to and at the time of Reasonable Reliance.

9.6.5. Representations and warranties of other participants

Not applicable.

9.7. Disclaimers of warranties

eSignTrust shall assume duty of care and liabilities to the extent stipulated in this CPS, as well as in applicable MSAR laws, and no further. eSignTrust makes no other expressed or implied warranties, and has no further obligations.

Unless otherwise stated in the Subscriber Agreement, in this eSignTrust CPS, the Issuing CA and the RA:

- Have no obligations to monitor the Subscribers in their use of the Certificate and its corresponding Private Key, and do not provide any warranties on their fitness of use;
- Undertake no responsibility to notify Relying Parties of any changes in the circumstances relating Subscribers, or suspension or revocation of the Certificates since the use of the Private Keys or Certificates by the Subscribers, other than via the publishing of CRL at the Repository; and
- Are committed only to reasonable care and skill in performing its certification services.

eSignTrust employees or other entities acting for or on behalf of eSignTrust are not parties to any Subscriber Agreement or Relying Party Agreement, and none of them shall accept any responsibility in their own rights in any legal action, claims or forms of redress initiated by a Subscriber or a Relying Party.

eSignTrust warranty, liability or obligations shall lapse upon any attempt by the Subscriber or Relying Party of the Certificate to circumvent duty, or any failure to observe obligations in the Subscriber Agreement or Relying Party Agreement, where applicable, and in this eSignTrust CPS. Upon any of such occurrences, the right of the Subscriber and Relying Parties to make claims shall also lapse.

eSignTrust PKI is not designed, intended or authorised for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems or weapon control systems, where failure could lead directly to death, personal injury or severe environmental damage.

Where a Certificate issued by an eSignTrust Issuing CA expires, or is revoked in accordance with this eSignTrust CPS, eSignTrust obligations and duties to the Subscriber and Relying Parties under any Subscriber Agreement or Relying Party Agreement and under this eSignTrust CPS shall lapse without notice.

eSignTrust, the Issuing CAs and the RAs disclaim any liability to a Subscriber, or a Relying Party, who fails to make any legal claims arising from, or in connection with, the issuance, suspension or revocation of a Certificate within two (2) years from the date upon which the Subscriber or the Relying Party, as the case may be, becomes aware of the facts or circumstances giving rise to such claim. Where the Subscriber or the Relying Party, upon reasonable care and diligence, should have been aware of such facts or circumstances at an earlier date, the above period of two (2) years shall commence from such earlier date.

9.8. Limitations of liability

To the extent permitted by law, Parties that choose to rely on any Certificate issued under this eSignTrust CPS consent that, regardless the place of performance, the domicile of the parties or other related locations, neither an Issuing CA nor a RA shall be liable for:

- Any loss caused by reliance on a false or forged Certificate, provided the Issuing CA or RA has complied with all requirements of this eSignTrust CPS;
- Any loss in excess of the Liability Cap caused by reliance upon a misrepresentation of a fact in a Certificate that an Issuing CA or any RA is required to confirm;
- Any damages for personal injury, pain and suffering, or emotional distress;
- Any indirect, incidental or consequential damages, or any loss of profits or data.

eSignTrust shall only incur liability upon:

- Proof of loss by the Relying Party;
- Proof of negligence or fault on the part of eSignTrust, its employees or its agents; and
- Proof that the cause of such loss or damage is due to Reasonable Reliance on the inaccurate, misleading or misrepresented information, subject to the limitations herein.

In the event any information contained in a Certificate issued by an eSignTrust Issuing CA is inaccurate, or any information contained therein or otherwise disclosed by eSignTrust is misrepresented owing to the negligence or fault of eSignTrust, its employees or its agents, eSignTrust shall in any event not be liable to the Subscriber or Relying Parties for loss or damage in excess of a Liability Cap stated in below table in respect of one Certificate and regardless the number of Digital Signatures, transactions or claims related to that Certificate.

Type	Liability Caps
Macao Post and Telecommunications Bureau eSignTrust Qualified Certificate	MOP 200,000.00
Macao Post and Telecommunications Bureau eSignTrust Normalised Certificate	MOP 50,000.00
Macao Post and Telecommunications Bureau eSignTrust Encipherment Certificate	MOP 50,000.00
Macao Post and Telecommunications Bureau eSignTrust Personal Secure Email Certificate	MOP 1,000.00

In case the Liability Cap is exceeded, the available Liability Cap shall be apportioned first to the earliest claims that achieve final dispute resolution, unless otherwise ordered by a court. In no event shall eSignTrust be obliged to pay more than the aggregate Liability Cap for each Certificate, regardless of the method of apportionment among claimants to the amount of the Liability Cap.

9.9. Indemnities

By accepting a Certificate, the Subscriber agrees to indemnify and hold eSignTrust and its RAs, agents and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable legal fees, that eSignTrust and its RAs, agents and contractors may incur, that are caused by the use or publication of a Certificate by eSignTrust and that arise from:

- Falsehood or misrepresentation of a fact by the Subscriber (or a person acting upon instructions from anyone authorised by the Subscriber);
- Failure by the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive eSignTrust, its RAs, agents and contractors, or any other person receiving or relying on the certificate; or
- Failure to protect the Subscriber's Private Key, or otherwise failure to take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's Private Key.

Any RA shall indemnify, hold harmless and defend the Issuing CA against any claims arising from or pertaining to wrongful or negligent acts or omissions of the RA.

An RA may enter into contracts, or include provisions in its contracts with Subscribers, under which Subscribers agree to indemnify, hold harmless and defend the RA against any claims arising from or pertaining to wrongful or negligent acts or omissions of the Subscriber.

9.10. Term and termination

9.10.1. Term

The eSignTrust CPS is effective since 11 February 2019.

9.10.2. Termination

Not applicable.

9.10.3. Effect of termination and survival

Not applicable.

9.11. Individual notices and communications with participants

Whenever any person hereto desires or is required to give any notice, demand or request with respect to this eSignTrust CPS, such communication shall be made either using digitally signed messages consistent with the requirements of this eSignTrust CPS or in writing.

Electronic communications shall be effective upon the sender's receiving a valid, digitally signed acknowledgement of receipt from the recipient. Such acknowledgement must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

To eSignTrust:

Macao Post and Telecommunications eSignTrust Certification Services
Attn: eSignTrust Customer Services
Edf. Dos Correios 12 andar, Estrada de D. Maria II, 11 a 11-D
Macao

From eSignTrust:

For an Individual, Government Agency or Department, or Organisation: the most recent address on file with eSignTrust.

9.12. Amendments

9.12.1. Procedure for amendment

This eSignTrust CPS is reviewed annually. Amendments are made by posting an updated version of the CPS to the online repository.

According with MSAR law, any amendments to this eSignTrust CPS shall also be submitted to MSAR accreditation authority for approval.

9.12.2. Notification mechanism and period

Editorial and typographical corrections, changes to contact details and other minor changes that do not materially impact Subscribers or Relying Parties may be changed without notice.

Major changes affecting Certificates are announced and approved by the accreditation authority prior to becoming effective.

9.12.3. Circumstances under which OID must be changed

Any new OID issued for an eSignTrust CPS change differs from the previous OID only in the version number.

9.13. Dispute resolution provisions

If a dispute arises in connection with this eSignTrust CPS, any Subscriber Agreement or any Relying Party Agreement, the aggrieved party shall provide written notification in accordance to Section 9.11 to the relevant parties regarding the dispute matter, and all parties shall agree to undertake in good faith to firstly use all reasonable endeavours to settle the dispute by negotiation or mediation.

If the parties are unable to resolve the dispute within thirty calendar days from the date the dispute first arose, then the parties agree to jointly appoint an independent arbitrator, having appropriate qualifications and practical experience, for the purpose of resolving the dispute, and agree to be bound by the decision of that arbitrator.

The parties shall promptly furnish to the arbitrator (imposing appropriate obligations of confidentiality) all information reasonably requested by him relating to the dispute.

The arbitrator shall use all reasonable endeavours to render his decision within ninety (90) calendar days following receipt of the information requested or, if this is not possible, as soon as practicable thereafter. The parties must fully co-operate with the arbitrator to achieve this objective. The arbitrator's decision shall be final and binding upon the parties, and shall provide the sole and exclusive remedies of the parties.

The arbitration shall take place in MSAR and be conducted in one of the official languages of MSAR or, alternatively and upon agreement of all parties, in English. The parties shall equally share the fees and expenses of the arbitrator.

All issues concerning the arbitration procedures that are not addressed above shall be regulated by Decree-Law n. 29/96/M, from June 11.

9.14. Governing law

The laws of the MSAR shall govern the validity, interpretation, construction and enforceability of this eSignTrust CPS, the Subscriber Agreements and the Relying Party Agreements.

Subscribers and Relying Parties agree to submit to the exclusive jurisdiction of MSAR courts.

9.15. Compliance with applicable law

Not applicable.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

Each and all provisions in this eSignTrust CPS shall be binding to all parties and their respective executors, administrators or personal representatives.

No term or provision of this eSignTrust CPS directly affecting the respective rights and obligations of eSignTrust, any Issuing CA or any RA may be orally amended, waived, supplemented, modified or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

Sections governing confidentiality of information, indemnification, eSignTrust warranties, disclaimer of warranties, limitation of liability, governing law and dispute resolution will survive any termination or expiration of any Subscriber Agreement or Relying Party Agreement.

9.16.2. Assignment

The rights and obligations of eSignTrust, the Issuing CAs and the RAs detailed in this eSignTrust CPS are assignable by the parties, by operation of law, provided such assignment undertaken is consistent with Section 5.7.5 on CA termination, and provided further that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.3. Severability

In the event that any, or any part, of the terms, conditions or provisions contained in this eSignTrust CPS are determined to be invalid, unlawful or unenforceable to any extent, such term, condition or provision shall be severed from the remaining terms, conditions or provisions, which shall continue to be valid and enforceable to the fullest extent permitted by law.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5. Force majeure

As stated in Section 2.1.

9.17. Other provisions

Not applicable.

10. Appendix A

For the fields supporting UTF-8 Unicode, the language selection preference will be English, Portuguese, Chinese if the information is provided in more than one acceptable language. English is recommended.

10.1. Qualified Certificate Profile for Personal

Field Name	Critical		Field Content
Standard fields			
Version			X.509 v3
Serial Number			(Set by Macao Post and Telecommunications CA System)
Signature Algorithm ID			Sha256RSA
Issuer Name			CN = eSignTrust Personal Qualified Certificate CA (G##)[1] OU = Terms of use at https://www.esigntrust.com/CPS OU = CTT eSignTrust Services O = Macao Post and Telecommunications Bureau C = MO
Validity		Not before	(UTC time set by Macao Post and Telecommunications CA System]
		Not after	(UTC time set by Macao Post and Telecommunications CA System)
Subject Name			E = [Holder's email address][2] CN = [Name of individual][3] T = [Title][4] Serial Number = [Holder Reference Number][5] OU = PORCUR - [Procuration information][6] OU = Terms of use at www.esigntrust.com/CPS[7] OU = Personal Qualified Certificate G##[8] O = Macao Post and Telecommunications Bureau C = [Holder's country/region as represented in Holder's identity document using ISO 3166-1 alpha-2 country code]

---

[1] ##: 2 digits to represent the current generation for this type of certificate.

[2] Holder's email address.

[3] Holder name format: [First name]+[Last name]. The [Last name] will be in all capital letters if it is in English or Portuguese.
This attribute supports UTF-8 Unicode.

[4] Holder's professional title. (if applicable)
This attribute supports UTF-8 Unicode.

[5] [Holder Reference Number]: 10-digit number assigned by eSignTrust.

[6] Holder's procuration information, max. 64 characters (see Remarks), following the format "PROCUR - " followed by the semantics of procuration information. (if applicable)
This attribute supports UTF-8 Unicode.

Remarks: The syntax "PROCUR – " consumes 9 characters .

[7] The year of emission, in four-digit format: yyyy.

[8] ##: 2 digits to represent the current generation for this type of certificate.

Subject Public Key Info			RSA (2048 Bits)
Issuer Unique ID			(Not used)
Subject Unique ID			(Not used)
CA Signature			(produced by Macao Post and Telecommunications CA System)
Standard extensions			
Authority Key Identifier		Key Identifier	(hash of authority public key)
Subject Key Identifier		Key Identifier	(hash of subject public key)
Key Usage	Set		Digital Signature, nonRepudiation
Extended Key Usage			(Not used)
Private Key Usage Period			(Not used)
Certificate Policies			[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15108.2.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esigntrust.com/CPS [2]Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=THIS POLICY ENSURES THAT THIS IS A QUALIFIED CERTIFICATE AND THE SUBJECT'S PRIVATE KEY IS CONTAINED IN SSCD ACCORDING TO THE ELECTRONIC DOCUMENTS AND SIGNATURES LAW OF MACAO SAR.
Policy Mappings			(Not used)
Subject Alternative Name		otherName	[Encoded Holder's identity information][9]
		rfc822	[Holder's email address]
Issuer Alternative Name			(Not used)
Subject Directory Attributes		countryOfCitizenship	[Holder's country/region of citizenship/residency] [10]
Basic constraints		Subject type	End Entity
		Path length constraint	None
Name Constraints			(Not used)
Policy Constraints			(Not used)
CRL Distribution Points			Distribution Point Name=[URL of CRL Distribution Point]
Private extension			
Authority Info Access			[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.gov.esigntrust.com
Netscape Cert Type			SSL Client Authentication
Qualified Certificate Statements (1.3.6.1.5.5.7.1.3)		id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	
		id-etsi-qcs-QcCompliance	

---

[9] The Holder's identity information means either MSAR BIR no if the Holder is a Macao resident; or the passport/other traveling document number of the Holder authenticated at the time of certificate registration.

[10] Holder's country/region of citizenship/residency: ISO 3166 code of country of citizenship of Holder who is non-Macao resident and is holding passport or other travel document, while Macao resident should use "MO"

		(0.4.0.1862.1.1)	
		id-etsi-qcs-QcLimitValue (0.4.0.1862.1.2)	QcEuLimitValue: [11] currency=[currency] amount=[value] exponent=[exp value]
		id-etsi-qcs-QcRetentionPeriod (0.4.0.1862.1.3)	QcEuRetentionPeriod: 15
		id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)	

---

[11] QC Limit Value: Transaction limit defined by the sponsoring organisation for the certificate holder, the value is stored according to the following formula:

[Currency] of [Amount value] * Exp ^ [Exponent value]

10.2. Qualified Certificate Profile for Corporate

Field Name	Critical		Field Content
Standard fields			
Version			X.509 v3
Serial Number			(Set by Macao Post and Telecommunications CA System)
Signature Algorithm ID			Sha256RSA
Issuer Name			CN = eSignTrust Corporate Qualified Certificate CA (G##)[12] OU = Terms of use at https://www.esigntrust.com/CPS OU = CTT eSignTrust Services O = Macao Post and Telecommunications Bureau C = MO
Validity		Not before	(UTC time set by Macao Post and Telecommunications CA System]
		Not after	(UTC time set by Macao Post and Telecommunications CA System)
Subject Name			E = [email address][13] CN = [Name of authorised delegate of Corporate][14] T = [Title][15] Serial Number = [Holder Reference Number][16] OU = PORCUR - [Procuration information][17] OU = BRN/TIN – [Corporate Registration Information][18] OU = UNIT - [Holder's Corporate branch/dept][19]

---

[12] ##: 2 digits to represent the current generation for this type of certificate.

[13] Holder's email address.

[14] Holder name format: [First name]+[Last name]. The [Last name] will be in all capital letters if it is in English or Portuguese.
This attribute supports UTF-8 Unicode.

[15] Holder's title in the Corporate, qualifications of the Holder will be in bracket. (if applicable)
This attribute supports UTF-8 Unicode.

[16] [Holder Reference Number]: 10-digit number assigned by eSignTrust.

[17] Holder's procuration information, max. 64 characters (see Remarks), following the format "PROCUR - " followed by the semantics of procuration information. (if applicable)
This attribute supports UTF-8 Unicode.

Remarks: The syntax "PROCUR – " consumes 9 characters .

[18] Registration information of the Corporate follows the format "BRN/TIN – ", followed by the corresponding information of [BRN] and [TIN], where:
BRN=Business Registration Number (商業企業登記編號/Número Registo Comercial)
BRN will be filled with one "0" if null.

TIN=Tax Identification Number(營業稅檔案編號/No. de Cadastro de Contribuição Industrial ou No. Fiscal)
TIN will be filled with one "0" if null.

[19] Belonging branch/department of the Holder, max. 64 characters (see Remarks), following the format "UNIT – " followed by the branch/department name. (if applicable)
This attribute supports UTF-8 Unicode.

Remarks: The syntax "UNIT – " consumes 7 characters .

			OU = COMP - [Holder's Corporate Name][20] OU = Terms of use at www.esigntrust.com/CPS[21] OU = Corporate Qualified Certificate G##[22] O = Macao Post and Telecommunications Bureau C = [Holder's country/region as represented in Holder's identity document using ISO 3166-1 alpha-2 country code]
Subject Public Key Info			RSA (2048 Bits)
Issuer Unique ID			(Not used)
Subject Unique ID			(Not used)
CA Signature			(produced by Macao Post and Telecommunications CA System)
Standard extensions			
Authority Key Identifier		Key Identifier	(hash of authority public key)
Subject Key Identifier		Key Identifier	(hash of subject public key)
Key Usage	Set		Digital Signature, nonRepudiation
Extended Key Usage			(Not used)
Private Key Usage Period			(Not used)
Certificate Policies			[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15108.2.1.3.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esigntrust.com/CPS [2]Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=THIS POLICY ENSURES THAT THIS IS A QUALIFIED CERTIFICATE AND THE SUBJECT'S PRIVATE KEY IS CONTAINED IN SSCD ACCORDING TO THE ELECTRONIC DOCUMENTS AND SIGNATURES LAW OF MACAO SAR.
Policy Mappings			(Not used)
Subject Alternative Name		otherName	[Encoded Holder's identity information][23]
		rfc822	[Holder's email address][24]
Issuer Alternative Name			(Not used)
Subject Directory Attributes		countryOfCitizenship	(Not used)
Basic constraints		Subject type	End Entity
		Path length constraint	None
Name Constraints			(Not used)

---

[20] Registered name of the Holder's belonging Corporate, max. 64 characters (see Remarks), following the format "COMP – " followed by the name of the Corporate.
This attribute supports UTF-8 Unicode.

Remarks: The syntax "COMP – " consumes 7 characters .

[21] The year of emission, in four-digit format: yyyy. (not used in G03)

[22] ##: 2 digits to represent the current generation for this type of certificate.

[23] The Holder's identity information means either MSAR BIR no if the Holder is a Macao resident; or the passport/other traveling document number of the Holder authenticated at the time of certificate registration.

[24] Holder's email address.

Policy Constraints			(Not used)
CRL Distribution Points			Distribution Point Name=[URL of CRL Distribution Point]
Private extension			
Authority Info Access			[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.corp.esigntrust.com
Netscape Cert Type			SSL Client Authentication
Qualified Certificate Statements (1.3.6.1.5.5.7.1.3)		id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	
		id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	
		id-etsi-qcs-QcLimitValue (0.4.0.1862.1.2)	QcEuLimitValue: [25] currency=[currency] amount=[value] exponent=[exp value]
		id-etsi-qcs-QcRetentionPeriod (0.4.0.1862.1.3)	QcEuRetentionPeriod: 15
		id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)	

---

[25] QC Limit Value: Transaction limit defined by the sponsoring organisation for the certificate holder, the value is stored according to the following formula:

[Currency] of [Amount value] * Exp ^ [Exponent value]

10.3. Qualified Certificate Profile for Government

Field Name	Critical		Field Content
Standard fields			
Version			X.509 v3
Serial Number			(Set by Macao Post and Telecommunications CA System)
Signature Algorithm ID			Sha256RSA
Issuer Name			CN = eSignTrust Government Qualified Certificate CA (G##)[26] OU = Terms of use at https://www.esigntrust.com/CPS[27] OU = CTT eSignTrust Services O = Macao Post and Telecommunications Bureau C = MO
Validity		Not before	(UTC time set by Macao Post and Telecommunications CA System]
		Not after	(UTC time set by Macao Post and Telecommunications CA System)
Subject Name			E = [Holder's email address][28] CN = [Name of authorised delegate][29] T = [Title][30] Serial Number = [Holder Reference Number][31] OU = PORCUR - [Procuration information][32] OU = UNIT - [Holder's Department/Division][33] OU = DEPT/ORG - [Holder's Government Agency Name][34]

---

[26] ##: 2 digits to represent the current generation for this type of certificate.

[27] The year of emission, in four-digit format: yyyy. (not used in G03)

[28] Holder's email address.

[29] Holder name format: [First name]+[Last name]. The [Last name] will be in all capital letters if it is in English or Portuguese.
This attribute supports UTF-8 Unicode.

[30] Holder's position in the Government Agency, qualifications of the Holder will be in bracket. (if applicable)
This attribute supports UTF-8 Unicode.

[31] [Holder Reference Number]: 10-digit number assigned by eSignTrust.

[32] Holder's procuration information, max. 64 characters (see Remarks), following the format "PROCUR - " followed by the semantics of procuration information. (if applicable)
This attribute supports UTF-8 Unicode.

Remarks: The syntax "PROCUR – " consumes 9 characters .

[33] Belonging department/division of the Holder, max. 64 characters (see Remarks), following the format "UNIT – " followed by the department/division name. (if applicable)
This attribute supports UTF-8 Unicode.

Remarks: The syntax "UNIT – " consumes 7 characters .

[34] Name of the Holder's belonging Government Agency, max. 64 characters (see Remarks), following the format "DEPT/ORG – " followed by the name of Government Agency.
This attribute supports UTF-8 Unicode.

Remarks: The syntax "DEPT/ORG –" consumes 11 characters.

			OU = Terms of use at www.esigntrust.com/CPS[35] OU = Government Qualified Certificate G##[36] O = Macao Post and Telecommunications Bureau C = [Holder's country/region as represented in Holder's identity document using ISO 3166-1 alpha-2 country code]
Subject Public Key Info			RSA (2048 Bits)
Issuer Unique ID			(Not used)
Subject Unique ID			(Not used)
CA Signature			(produced by Macao Post and Telecommunications CA System)
Standard extensions			
Authority Key Identifier		Key Identifier	(hash of authority public key)
Subject Key Identifier		Key Identifier	(hash of subject public key)
Key Usage	Set		Digital Signature, nonRepudiation
Extended Key Usage			(Not used)
Private Key Usage Period			(Not used)
Certificate Policies			[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15108.2.1.3.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esigntrust.com/CPS [2]Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=THIS POLICY ENSURES THAT THIS IS A QUALIFIED CERTIFICATE AND THE SUBJECT'S PRIVATE KEY IS CONTAINED IN SSCD ACCORDING TO THE ELECTRONIC DOCUMENTS AND SIGNATURES LAW OF MACAO SAR.
Policy Mappings			(Not used)
Subject Alternative Name		otherName	[Encoded Holder's identity information][37]
		rfc822	[Holder's email address]
Issuer Alternative Name			(Not used)
Subject Directory Attributes		countryOfCitizenship	(Not used)
Basic constraints		Subject type	End Entity
		Path length constraint	None
Name Constraints			(Not used)
Policy Constraints			(Not used)
CRL Distribution Points			Distribution Point Name=[URL of CRL Distribution Point]
Private extension			
Authority Info Access			[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.gov.esigntrust.com
Netscape Cert Type			SSL Client Authentication
Qualified Certificate		id-qcs-	

---

[35] The year of emission, in four-digit format: yyyy. (not used in G03)

[36] ##: 2 digits to represent the current generation for this type of certificate.

[37] The Holder's identity information means either MSAR BIR no if the Holder is a Macao resident; or the passport/other traveling document number of the Holder authenticated at the time of certificate registration.

Statements (1.3.6.1.5.5.7.1.3)		pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)	
		id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	
		id-etsi-qcs-QcLimitValue (0.4.0.1862.1.2)	QcEuLimitValue: [38] currency=[currency] amount=[value] exponent=[exp value]
		id-etsi-qcs-QcRetentionPeriod (0.4.0.1862.1.3)	QcEuRetentionPeriod: 15
		id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)	

---

[38] QC Limit Value: Transaction limit defined by the sponsoring organisation for the certificate holder, the value is stored according to the following formula:

[Currency] of [Amount value] * Exp ^ [Exponent value]

10.4. Encipherment Certificate Profile for Personal

Field Name	Critical		Field Content
Standard fields			
Version			X.509 v3
Serial Number			(Set by Macao Post and Telecommunications CA System)
Signature Algorithm ID			sha256RSA
Issuer Name			CN = eSignTrust Personal Certification Authority (G##)[39] OU = Terms of use at https://www.esigntrust.com/CPS OU = CTT eSignTrust Services O = Macao Post and Telecommunications Bureau C = MO
Validity		Not before	(UTC time set by Macao Post and Telecommunications CA System)
		Not after	(UTC time set by Macao Post and Telecommunications CA System)
Subject Name			E = [Holder's email address][40] CN = [Name of authorised delegate][41] Serial Number = [Holder Reference Number][42] OU = Terms of use at www.esigntrust.com/CPS[43] OU = Personal Encipherment Certificate G##[44] O = Macao Post and Telecommunications Bureau C = [Holder's country/area as represented in Holder's identity document using ISO 3166-1 alpha-2 country code]
Subject Public Key Info			RSA (2048 Bits)
Issuer Unique ID			(Not used)
Subject Unique ID			(Not used)
CA Signature			(produced by Macao Post and Telecommunications CA System)
Standard extensions			
Authority Key Identifier		Key Identifier	(hash of authority public key)
Subject Key Identifier		Key Identifier	(hash of subject public key)
Key Usage	Set		Key Encipherment
Extended Key Usage			(Not used)
Private Key Usage Period			(Not used)
Certificate Policies			[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.15108.2.1.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esigntrust.com/CPS
Policy Mappings			(Not used)
Subject Alternative Name		otherName	(Not used)
		rfc822	(Not used)

---

[39] ##: 2 digits to represent the current generation for this type of certificate.

[40] Holder's email address.

[41] Holder name format: [First name]+[Last name]. The [Last name] will be in all capital letters if it is in English or Portuguese.
This attribute supports UTF-8 Unicode.

[42] [Holder Reference Number]: 10-digit number assigned by eSignTrust.

[43] The year of emission, in four-digit format: yyyy. (not used in G03)

[44] ##: 2 digits to represent the current generation for this type of certificate.

Issuer Alternative Name			(Not used)
Subject Directory Attributes		countryOfCitizenship	(Not used)
Basic constraints		Subject type	End Entity
		Path length constraint	None
Name Constraints			(Not used)
Policy Constraints			(Not used)
CRL Distribution Points			Distribution Point Name=[URL of CRL Distribution Point]
Private extension			
Authority Info Access			[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.gov.esigntrust.com
Netscape Cert Type			(Not used)

10.5. Encipherment Certificate Profile for Corporate

Field Name	Critical		Field Content
Standard fields			
Version			X.509 v3
Serial Number			(Set by Macao Post and Telecommunications CA System)
Signature Algorithm ID			sha256RSA
Issuer Name			CN = eSignTrust Corporate Certification Authority (G##)[45] OU = Terms of use at https://www.esigntrust.com/CPS OU = CTT eSignTrust Services O = Macao Post and Telecommunications Bureau C = MO
Validity		Not before	(UTC time set by Macao Post and Telecommunications CA System)
		Not after	(UTC time set by Macao Post and Telecommunications CA System)
Subject Name			E = [Holder's email address][46] CN = [Name of authorised delegate][47] T = [Title][48] Serial Number = [Holder Reference Number][49] OU = UNIT - [Corporate Registration Information][50] OU = COMP - [Holder's Corporate Agency Name][51] OU = Terms of use at www.esigntrust.com/CPS[52] OU = Corporate Encipherment Certificate G##[53] O = Macao Post and Telecommunications Bureau C = [Holder's country/area as represented in Holder's identity document using ISO 3166-1 alpha-2 country code]
Subject Public Key Info			RSA (2048 Bits)

---

[45] ##: 2 digits to represent the current generation for this type of certificate.

[46] Holder’s email address.

[47] Holder name format: [First name]+[Last name]. The [Last name] will be in all capital letters if it is in English or Portuguese.
This attribute supports UTF-8 Unicode.

[48] Holder’s title in the Corporate, qualifications of the Holder will be in bracket. (if applicable)
This attribute supports UTF-8 Unicode.

[49] [Holder Reference Number]: 10-digit number assigned by eSignTrust.

[50] Belonging branch/department of the Holder, max. 64 characters (see Remarks), following the format “UNIT – ” followed by the department/division name. (if applicable)
This attribute supports UTF-8 Unicode.

Remarks: The syntax “UNIT – ” consumes 7 characters .

[51] Registered name of the Holder’s belonging Corporate, max. 64 characters (see Remarks), following the format “COMP – ” followed by the name of Corporate Agency.
This attribute supports UTF-8 Unicode.

Remarks: The syntax “COMP – ” consumes 7 characters.

[52] The year of emission, in four-digit format: yyyy. (not used in G03)

[53] ##: 2 digits to represent the current generation for this type of certificate.

Issuer Unique ID			(Not used)
Subject Unique ID			(Not used)
CA Signature			(produced by Macao Post and Telecommunications CA System)
Standard extensions			
Authority Key Identifier		Key Identifier	(hash of authority public key)
Subject Key Identifier		Key Identifier	(hash of subject public key)
Key Usage	Set		Key Encipherment
Extended Key Usage			(Not used)
Private Key Usage Period			(Not used)
Certificate Policies			[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.15108.2.1.5.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esigntrust.com/CPS
Policy Mappings			(Not used)
Subject Alternative Name		otherName	(Not used)
		rfc822	(Not used)
Issuer Alternative Name			(Not used)
Subject Directory Attributes		countryOfCitizenship	(Not used)
Basic constraints		Subject type	End Entity
		Path length constraint	None
Name Constraints			(Not used)
Policy Constraints			(Not used)
CRL Distribution Points			Distribution Point Name=[URL of CRL Distribution Point]
Private extension			
Authority Info Access			[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.corp.esigntrust.com
Netscape Cert Type			(Not used)

10.6. Encipherment Certificate Profile for Government

Field Name	Critical		Field Content
Standard fields			
Version			X.509 v3
Serial Number			(Set by Macao Post and Telecommunications CA System)
Signature Algorithm ID			sha256RSA
Issuer Name			CN = eSignTrust Government Certification Authority (G##)[54] OU = Terms of use at https://www.esigntrust.com/CPS OU = CTT eSignTrust Services O = Macao Post and Telecommunications Bureau C = MO
Validity		Not before	(UTC time set by Macao Post and Telecommunications CA System)
		Not after	(UTC time set by Macao Post and Telecommunications CA System)
Subject Name			E = [Holder's email address][55] CN = [Name of authorised delegate][56] T = [Title][57] Serial Number = [Holder Reference Number][58] OU = UNIT - [Holder's Department/Division][59] OU = DEPT/ORG - [Holder's Government Agency Name][60] OU = Terms of use at www.esigntrust.com/CPS[61] OU = Government Encipherment Certificate G##[62] O = Macao Post and Telecommunications Bureau C = [Holder's country/area as represented in Holder's identity

---

[54] ##: 2 digits to represent the current generation for this type of certificate.

[55] Holder's email address.

[56] Holder name format: [First name]+[Last name]. The [Last name] will be in all capital letters if it is in English or Portuguese.
This attribute supports UTF-8 Unicode.

[57] Holder's position in the Government Agency, qualifications of the Holder will be in bracket. (if applicable)
This attribute supports UTF-8 Unicode.

[58] [Holder Reference Number]: 10-digit number assigned by eSignTrust.

[59] Belonging department/division of the Holder, max. 64 characters (see Remarks), following the format "UNIT – " followed by the department/division name. (if applicable)
This attribute supports UTF-8 Unicode.

Remarks: The syntax "UNIT – " consumes 7 characters .

[60] Name of the Holder's belonging Government Agency, max. 64 characters (see Remarks), following the format "DEPT/ORG – " followed by the name of Government Agency.
This attribute supports UTF-8 Unicode.

Remarks: The syntax "DEPT/ORG –" consumes 11 characters.

[61] The year of emission, in four-digit format: yyyy. (not used in G03)

[62] ##: 2 digits to represent the current generation for this type of certificate.

			document using ISO 3166-1 alpha-2 country code]
Subject Public Key Info			RSA (2048 Bits)
Issuer Unique ID			(Not used)
Subject Unique ID			(Not used)
CA Signature			(produced by Macao Post and Telecommunications CA System)
Standard extensions			
Authority Key Identifier		Key Identifier	(hash of authority public key)
Subject Key Identifier		Key Identifier	(hash of subject public key)
Key Usage	Set		Key Encipherment (20)
Extended Key Usage			(Not used)
Private Key Usage Period			(Not used)
Certificate Policies			[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15108.2.1.5.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esigntrust.com/CPS
Policy Mappings			(Not used)
Issuer Alternative Name			(Not used)
Subject Directory Attributes		countryOfCitizenship	(Not used)
Basic constraints		Subject type	End Entity
		Path length constraint	None
Name Constraints			(Not used)
Policy Constraints			(Not used)
CRL Distribution Points			Distribution Point Name=[URL of CRL Distribution Point]
Private extension			
Authority Info Access			[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.gov.esigntrust.com
Netscape Cert Type			SSL Client Authentication

10.7. Normalised Certificate Profile for Personal

Field Name	Critical		Field Content
Standard fields			
Version			X.509 v3
Serial Number			(Set by Macao Post and Telecommunications CA System)
Signature Algorithm ID			sha256RSA
Issuer Name			CN = eSignTrust Personal Certification Authority (G##)[63] OU = Terms of use at https://www.esigntrust.com/CPS OU = CTT eSignTrust Services O = Macao Post and Telecommunications Bureau C = MO
Validity		Not before	(UTC time set by Macao Post and Telecommunications CA System)
		Not after	(UTC time set by Macao Post and Telecommunications CA System)
Subject Name			E = [Holder's email address][64] CN = [Name of authorised delegate][65] Serial Number = [Holder Reference Number][66] OU = Terms of use at www.esigntrust.com/CPS[67] OU = Personal Digital Certificate G##[68] O = Macao Post and Telecommunications Bureau C = [Holder's country/area as represented in Holder's identity document using ISO 3166-1 alpha-2 country code]
Subject Public Key Info			RSA (2048 Bits)
Issuer Unique ID			(Not used)
Subject Unique ID			(Not used)
CA Signature			(produced by Macao Post and Telecommunications CA System)
Standard extensions			
Authority Key Identifier		Key Identifier	(hash of authority public key)
Subject Key Identifier		Key Identifier	(hash of subject public key)
Key Usage	Set		Digital Signature, nonRepudiation
Extended Key Usage			(Not used)
Private Key Usage Period			(Not used)
Certificate Policies			[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.15108.2.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esigntrust.com/CPS
Policy Mappings			(Not used)
Subject Alternative Name		otherName	[Encoded Holder's identity information][69]

---

[63] ##: 2 digits to represent the current generation for this type of certificate.

[64] Holder's email address.

[65] Holder name format: [First name]+[Last name]. The [Last name] will be in all capital letters if it is in English or Portuguese.
This attribute supports UTF-8 Unicode.

[66] [Holder Reference Number]: 10-digit number assigned by eSignTrust.

[67] The year of emission, in four-digit format: yyyy. (not used in G03)

[68] ##: 2 digits to represent the current generation for this type of certificate.

		rfc822	[Holder's email address] [70]
Issuer Alternative Name			(Not used)
Subject Directory Attributes		countryOfCitizenship	(Not used)
Basic constraints		Subject type	End Entity
		Path length constraint	None
Name Constraints			(Not used)
Policy Constraints			(Not used)
CRL Distribution Points			Distribution Point Name=[URL of CRL Distribution Point]
Private extension			
Authority Info Access			[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.gov.esigntrust.com
Netscape Cert Type			(Not used)

---

[69] The Holder's identity information means either MSAR BIR no if the Holder is a Macao resident; or the passport/other traveling document number of the Holder authenticated at the time of certificate registration.

[70] Holder's email address.

10.8. Normalised Certificate Profile for Corporate

Field Name	Critical		Field Content
Standard fields			
Version			X.509 v3
Serial Number			(Set by Macao Post and Telecommunications CA System)
Signature Algorithm ID			sha256RSA
Issuer Name			CN = eSignTrust Corporate Certification Authority (G##)[71] OU = Terms of use at https://www.esigntrust.com/CPS OU = CTT eSignTrust Services O = Macao Post and Telecommunications Bureau C = MO
Validity		Not before	(UTC time set by Macao Post and Telecommunications CA System)
		Not after	(UTC time set by Macao Post and Telecommunications CA System)
Subject Name			E = [Holder's email address][72] CN = [Name of authorised delegate][73] T = [Title][74] Serial Number = [Holder Reference Number][75] OU = BRN/TIN [Corporate Registration Information] [76] OU = UNIT - [Corporate Registration Information][77] OU = COMP - [Holder's Corporate Agency Name][78]

---

[71] ##: 2 digits to represent the current generation for this type of certificate.

[72] Holder's email address.

[73] Holder name format: [First name]+[Last name]. The [Last name] will be in all capital letters if it is in English or Portuguese.
This attribute supports UTF-8 Unicode.

[74] Holder's title in the Corporate, qualifications of the Holder will be in bracket. (if applicable)
This attribute supports UTF-8 Unicode.

[75] [Holder Reference Number]: 10-digit number assigned by eSignTrust.

[76] Registration information of the Corporate follows the format ″BRN/TIN – ″, followed by the corresponding information of [BRN] and [TIN], where:

BRN=Business Registration Number (商業企業登記編號/Número Registo Comercial) BRN will be filled with one ″0″ if null.

TIN=Tax Identification Number(營業稅檔案編號/No. de Cadastro de Contribuição Industrial ou No. Fiscal) TIN will be filled with one ″0″ if null.

[77] Belonging branch/department of the Holder, max. 64 characters (see Remarks), following the format "UNIT – " followed by the department/division name. (if applicable)
This attribute supports UTF-8 Unicode.

Remarks: The syntax "UNIT – " consumes 7 characters .

[78] Registered name of the Holder's belonging Corporate, max. 64 characters (see Remarks), following the format "COMP – " followed by the name of Corporate Agency.

			OU = Terms of use at www.esigntrust.com/CPS[79] OU = Corporate Digital Certificate G##[80] O = Macao Post and Telecommunications Bureau C = [Holder's country/area as represented in Holder's identity document using ISO 3166-1 alpha-2 country code]
Subject Public Key Info			RSA (2048 Bits)
Issuer Unique ID			(Not used)
Subject Unique ID			(Not used)
CA Signature			(produced by Macao Post and Telecommunications CA System)
Standard extensions			
Authority Key Identifier		Key Identifier	(hash of authority public key)
Subject Key Identifier		Key Identifier	(hash of subject public key)
Key Usage	Set		Digital Signature, nonRepudiation
Extended Key Usage			(Not used)
Private Key Usage Period			(Not used)
Certificate Policies			[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.15108.2.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esigntrust.com/CPS
Policy Mappings			(Not used)
Subject Alternative Name		otherName	[Encoded Holder's identity information][81]
		rfc822	[Holder's email address] [82]
Issuer Alternative Name			(Not used)
Subject Directory Attributes		countryOfCitizenship	(Not used)
Basic constraints		Subject type	End Entity
		Path length constraint	None
Name Constraints			(Not used)
Policy Constraints			(Not used)
CRL Distribution Points			Distribution Point Name=[URL of CRL Distribution Point]
Private extension			
Authority Info Access			[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.corp.esigntrust.com
Netscape Cert Type			(Not used)

This attribute supports UTF-8 Unicode.

Remarks: The syntax "COMP – " consumes 7 characters.

[79] The year of emission, in four-digit format: yyyy. (not used in G03)

[80] ##: 2 digits to represent the current generation for this type of certificate.

[81] The Holder's identity information means either MSAR BIR no if the Holder is a Macao resident; or the passport/other traveling document number of the Holder authenticated at the time of certificate registration.

[82] Holder's email address.

10.9. Normalised Certificate Profile for Government

Field Name	Critical		Field Content
Standard fields			
Version			X.509 v3
Serial Number			(Set by Macao Post and Telecommunications CA System)
Signature Algorithm ID			sha256RSA
Issuer Name			OU = Terms of use at https://www.esigntrust.com/CPS OU = CTT eSignTrust Services O = Macao Post and Telecommunications Bureau C = MO CN = eSignTrust Government Certification Authority (G##)[83]
Validity		Not before	(UTC time set by Macao Post and Telecommunications CA System)
		Not after	(UTC time set by Macao Post and Telecommunications CA System)
Subject Name			E = [Holder's email address][84] CN = [Name of authorised delegate][85] T = [Title][86] Serial Number = [Holder Reference Number][87] OU = UNIT - [Holder's Department/Division][88] OU = DEPT/ORG - [Holder's Government Agency Name][89] OU = Terms of use at www.esigntrust.com/CPS[90] OU = Government Digital Certificate G##[91] O = Macao Post and Telecommunications Bureau

---

[83] ##: 2 digits to represent the current generation for this type of certificate.

[84] Holder's email address.

[85] Holder name format: [First name]+[Last name]. The [Last name] will be in all capital letters if it is in English or Portuguese.
This attribute supports UTF-8 Unicode.

[86] Holder's position in the Government Agency, qualifications of the Holder will be in bracket. (if applicable)
This attribute supports UTF-8 Unicode.

[87] [Holder Reference Number]: 10-digit number assigned by eSignTrust.

[88] Belonging department/division of the Holder, max. 64 characters (see Remarks), following the format "UNIT – " followed by the department/division name. (if applicable)
This attribute supports UTF-8 Unicode.

Remarks: The syntax "UNIT – " consumes 7 characters .

[89] Name of the Holder's belonging Government Agency, max. 64 characters (see Remarks), following the format "DEPT/ORG – " followed by the name of Government Agency.
This attribute supports UTF-8 Unicode.

Remarks: The syntax "DEPT/ORG –" consumes 11 characters.

[90] The year of emission, in four-digit format: yyyy. (not used in G03)

[91] ##: 2 digits to represent the current generation for this type of certificate.

			C = [Holder’s country/area as represented in Holder’s identity document using ISO 3166-1 alpha-2 country code]
Subject Public Key Info			RSA (2048 Bits)
Issuer Unique ID			(Not used)
Subject Unique ID			(Not used)
CA Signature			(produced by Macao Post and Telecommunications CA System)
Standard extensions			
Authority Key Identifier		Key Identifier	(hash of authority public key)
Subject Key Identifier		Key Identifier	(hash of subject public key)
Key Usage	Set		Digital Signature, nonRepudiation
Extended Key Usage			(Not used)
Private Key Usage Period			(Not used)
Certificate Policies			[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.15108.2.1.2.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esigntrust.com/CPS
Policy Mappings			(Not used)
Subject Alternative Name		otherName	[Encoded Holder’s identity information][92]
		rfc822	[Holder’s email address]
Issuer Alternative Name			(Not used)
Subject Directory Attributes		countryOfCitizenship	(Not used)
Basic constraints		Subject type	End Entity
		Path length constraint	None

---

[92] The Holder’s identity information means either MSAR BIR no if the Holder is a Macao resident; or the passport/other traveling document number of the Holder authenticated at the time of certificate registration.

10.10. Secure Email Certificate Profile

Field Name	Critical		Field Content
Standard fields			
Version			X.509 v3
Serial Number			(Set by Macao Post and Telecommunications CA System)
Signature Algorithm ID			sha256RSA
Issuer Name			CN = eSignTrust Secure Email CA-Persona Not Validated(G##)[93] OU = Terms of use at https://www.esigntrust.com/CPS OU = CTT eSignTrust Services O = Macao Post and Telecommunications Bureau C = MO
Validity		Not before	(UTC time set by Macao Post and Telecommunications CA System)
		Not after	(UTC time set by Macao Post and Telecommunications CA System)
Subject Name			E = [Holder's email address][94] CN = [Name of authorised delegate][95] OU = Terms of use at www.esigntrust.com/CPS[96] OU = Personal Secure Email Certificate G##[97] O = Macao Post and Telecommunications Bureau
Subject Public Key Info			RSA (2048 Bits)
Issuer Unique ID			(Not used)
Subject Unique ID			(Not used)
CA Signature			(produced by Macao Post and Telecommunications CA System)
Standard extensions			
Authority Key Identifier		Key Identifier	(hash of authority public key)
Subject Key Identifier		Key Identifier	(hash of subject public key)
Key Usage	Set		Digital Signature, Key Encipherment
Extended Key Usage			(Not used)
Private Key Usage Period			(Not used)
Certificate Policies			[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.15108.2.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.esigntrust.com/CPS
Policy Mappings			(Not used)
Subject Alternative Name		otherName	(Not used)
		rfc822	(Not used)
Issuer Alternative Name			(Not used)
Subject Directory Attributes		countryOfCitizenship	(Not used)
Basic constraints		Subject type	End Entity

---

[93] ##: 2 digits to represent the current generation for this type of certificate.

[94] Holder's email address.

[95] Holder name format: [First name]+[Last name]. The [Last name] will be in all capital letters if it is in English or Portuguese.
This attribute supports UTF-8 Unicode.

[96] The year of emission, in four-digit format: yyyy. (not used in G03)

[97] ##: 2 digits to represent the current generation for this type of certificate.

		Path length constraint	None
Name Constraints			(Not used)
Policy Constraints			(Not used)
CRL Distribution Points			Distribution Point Name=[URL of CRL Distribution Point]
Private extension			
Authority Info Access			(Not used)
Netscape Cert Type			(Not used)

[END OF DOCUMENT]