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

Macao Post eSignTrust Certification Services

Certificate Policies of Macao Post eSignTrust Certification Services

Version: 1.0
Document Release Date: 23 January 2006

This document contains proprietary information furnished for evaluation purposes only; except with the express written permission of Direcção dos Serviços de Correios ("DSC"), such information may not be published, disclosed, or used for any other purpose. You acknowledge and agree that this document and all portions thereof, including, but not limited to, any copyright, trade secret and other intellectual property rights relating thereto, are and at all times shall remain the sole property of DSC and that title and full ownership rights in the information contained herein and all portions thereof are reserved to and at all times shall remain with DSC. You acknowledge and agree that the information contained herein constitutes a valuable trade secret of DSC. You agree to use utmost care in protecting the proprietary and confidential nature of the information contained herein.

1. Policy Outline

Macao Post eSignTrust Certification Services (“eSignTrust") is the first accredited Certification Authority ("CA") established in Macao SAR, providing Macao-wide PKI services. Certificates issued by eSignTrust within the sub-domain of “Macao Post eSignTrust Services” are classified as under “eSignTrust Certificates Net” (ECN).

This Certificate Policy (“CP”) is a named set of rules that indicates the applicability of a certificate within “eSignTrust Certificates Net” (ECN) to a particular community and/ or class of application with common security requirements, and is further supported by the eSignTrust Certification Practice Statement (“CPS”).

When eSignTrust issues a certificate within ECN, it is providing a statement that a particular certificate is associated with the Subscriber uniquely and unambiguously named within the domain of Issuing CA, and that the public key on that certificate is bound to that Subscriber. However, the extent to which the certificate user (relying party) should rely on this CP needs to be assessed by the certificate user, taking into consideration the eSignTrust CPS.

This document is targeted at:

- ECN certificate Subscribers who need to understand how they are authenticated and what their obligations are as ECN Subscribers and how they are protected under ECN;
- Relying parties who need to understand how much trust to place in an ECN certificate, or an electronic signature using that certificate.

This CP is not a legal agreement between eSignTrust and ECN participants; rather, contractual obligations between eSignTrust and ECN participants are established by means of agreements with such participants. This CP is the principal statement of policy governing the ECN. However, it does not govern any services outside the ECN.

1.1. Overview

A summary of Types of Certificates within the ECN is as follows:

a) Qualified Certificate
b) Normalised Certificates
c) Encipherment Certificates
d) Secure Email Certificates

This CP is applicable to the above Types of Certificates.

1.2. Document name and Identification

This document is the Macao Post eSignTrust Certification Services Certificate Policy (CP). eSignTrust, acting as the policy-defining authority, has assigned an object identifier value extension for each Type of Certificates issued under eSignTrust Certificates Net (ECN). The object identifier values used for the Types of Individual Subscriber Certificates are:

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) id-normalised-certtype (2) id-personal-scope (1)	eSignTrust Personal Normalised Identity Certificate;
		OID: 1.3.6.1.4.1.15108.2.1.2.1
		eSignTrust Personal Normalised Encipherment 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
		eSignTrust Corporate Normalised Encipherment 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-normalised -certtype (2) id-government-scope (3)	eSignTrust Government Normalised Identity Certificate;
		OID: 1.3.6.1.4.1.15108.2.1.2.3
		eSignTrust Government Normalised Encipherment Certificate;
		OID: 1.3.6.1.4.1.15108.2.1.2.3

Encipherment Certificate for	iso(1) org (3) dod (6) internet(1) private (4) enterprise (1) id-esigntrust (15108)	eSignTrust Personal Encipherment Certificate;

Personal	id-pki (2) id-certificate-policy (1) id-encipherment -certtype (4) id-personal-scope (1)	OID: 1.3.6.1.4.1.15108.2.1.4.1
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 (4) id-corporate-scope (2)	eSignTrust Corporate Encipherment Certificate; OID: 1.3.6.1.4.1.15108.2.1.4.2
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 (4) id-government-scope (3)	eSignTrust Government Encipherment Certificate; OID: 1.3.6.1.4.1.15108.2.1.4.3
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

1.3. Types of Certificates

eSignTrust Issuing CA's upon issuance of a certificate to a Subscriber confirms the identity of the Subscriber or the credibility of other data, such as Subscriber's name, organisation and organisational unit. It also confirms the public key possessed by that Subscriber is the property of this very subscriber. Due to above, the relying party upon reception of signed message is able to verify the ownership of the certificate, which signed the message and, optionally, account him/her action being performed or obligations he/she made.

eSignTrust issues certificates in three levels of distinctive credibility. Credibility of the certificate depends on enforcement of subscriber's identity verification procedure and the effort used by eSignTrust to verify the data submitted by the requester in his/her/its registration application. The more complicated and strengthen such level of the security, the higher level of credibility is assigned.

1.3.1. Qualified Certificate for Personal, Corporate and Government

Qualified Certificate provides a very high degree of assurance of the Subscriber's personal identity/working identity and, where applicable, professional qualification, procuration information or other information relevant for the use of the Certificate.

For a Certificate of this type to be issued, the individual applying for a Certificate must present himself in person during the registration process. The enrolment of this type of certificate is allowed only in eSignTrust Registration Authority or authorised premises designated for registration purpose. For Qualified Certificate for Corporate and Government, certificate usage scope is limited and according to sponsoring organisation's power and will.

A Public Key certified in this manner may be used solely in the context of Qualified Electronic Signature purpose. In addition, Qualified Certificate issued requiring use of Secure Signature-Creation Devices (SSCD).

Qualified Certificate is used to support legally valid Qualified Electronic Signatures in accordance with the Macao S.A.R. Electronic Documents and Signatures Law (Law no. 5/2005). It provides a very high level of Personal/Professional/commercial/ official electronic identity assurance. Qualified Electronic Signature could be generated by use of a SSCD containing a Qualified Certificate.

The maximum accumulated civil liability of eSignTrust for the data in the certificates issued is MOP$200,000.00 (two hundred thousand Patacas) per certificate/year. Qualified Certificates issued have limited guarantees and responsibilities.

1.3.2. Normalised Certificate for Personal, Corporate and Government

Normalised Identity Certificate and Encipherment Certificate are issued by eSignTrust Issuing CA’s for a single certificate signing request (CSR). The enrolment of this type of certificate is allowed only in eSignTrust Registration Authority or authorised premises designated for registration purpose.

eSignTrust verifies the information provided by a Subscriber in person (physical presence) during certificate registration. Email address and subscriber name and surname, sponsoring organisation name and organisation unit of private entity or the representative of the legal entity are subjected to verification. Certificate usage scope is limited and according to individual’s/organisational power and will.

Corporate Normalised Certificate is issued to organisations that hold a valid business registration certificate issued by the Government of Macao Special Administrative Region (Macao S.A.R.). It identifies a member or employee of the Subscriber Organisation (the "Authorised Users") who has been duly authorised to use that certificate.

Government Normalised Certificate is issued to Bureau, Departments and Agencies of the Government of Macao S.A.R. and statutory bodies of Macao whose existence is recognised by the laws of Macao S.A.R. It identifies a member of a Subscriber Organisation (the "Authorised Users") who has been duly authorised to use that certificate.

Normalised Certificates are intended mainly for securing electronic correspondence, encrypting/decrypting binary objects and protecting data transmission for individual. A Normalised Identity Certificate is for signing purposes, while Normalised Encipherment Certificate is for encipherment purpose. An Advance Electronic Signature could be generated by use of the Personal Normalised Identity Certificate.

The maximum accumulated civil liability of eSignTrust for the data in the certificates issued is MOP$50,000.00 (fifty thousand Patacas) per certificate/year. Normalised Certificates issued have limited guarantees and responsibilities.

1.3.3. Personal Encipherment Certificate

Personal Encipherment Certificate is issued by eSignTrust Issuing CA's for a single Certificate Signing Request (CSR). The enrolment of this type of certificate is allowed only in eSignTrust Registration Authority or authorised premises designated for registration purpose.

eSignTrust verifies the data provided by the Subscriber in person during certification enrolment process. Email address, Subscriber name and surname, sponsoring organisation name and organisation unit of private entity or the representative of the legal entity are subjected to verification. Certificate usage scope is limited and according to sponsoring organisation's power and will.

Personal Encipherment Certificates are issued to individuals. These certificates may be used to encrypt/decrypt binary objects and protecting data transmission. Key usage of Government Encipherment Certificate is designed for encipherment purpose.

The maximum accumulated civil liability of eSignTrust for the data in the certificates issued according with the above policy is MOP$50,000.00 (fifty thousand Patacas) per certificate/year. Certificates issued within this policy have limited guarantees and responsibilities.

1.3.4. Corporate Encipherment Certificate

Corporate Encipherment Certificate is issued by eSignTrust Issuing CA's for a single Certificate Signing Request (CSR). The enrolment of this type of certificate is allowed only in eSignTrust Registration Authority or authorised Remote Registration Authority approved by eSignTrust.

eSignTrust verifies the data provided by the Subscriber in person during certification enrolment process. Email address, Subscriber name and surname, sponsoring organisation name and organisation unit of private entity or the representative of the legal entity are subjected to verification. Certificate usage scope is limited and according to sponsoring organisation's power and will.

Corporate Encipherment Certificate is issued to organisations that hold a valid business registration certificate issued by the Government of Macao S.A.R., It identifies a member of a Subscriber Organisation (the "Authorised Users") who has been duly authorised to use that certificate. These certificates may be used to encrypt/decrypt binary objects and protecting data transmission.

Corporate Encipherment Certificates are intended mainly for encrypting/ decrypting binary objects and protecting data transmission for corporate organisation or authorised corporate representatives. Key usage of Corporate Encipherment Certificate is designed for encipherment purpose.

The maximum accumulated civil liability of eSignTrust for the data in the certificates issued according with the above policy is MOP$50,000.00 (fifty thousand Patacas) per certificate/year. Certificates issued within this policy have limited guarantees and responsibilities.

1.3.5. Government Encipherment Certificate

Government Encipherment Certificate is issued by eSignTrust Issuing CA's for a single Certificate Signing Request (CSR). The enrolment of this type of certificate is allowed only in eSignTrust Registration Authority or authorised Remote Registration Authority approved by eSignTrust.

eSignTrust verifies the data provided by the Subscriber in person during certification enrolment process. Email address, Subscriber name and surname, sponsoring organisation name and organisation unit of private entity or the representative of the legal entity are subjected to verification. Certificate usage scope is limited and according to sponsoring organisation's power and will.

Government Encipherment Certificate is issued to Bureau, Departments and Agencies of the Government of Macao S.A.R. and statutory bodies of Macao whose existence is recognised by the laws of Macao S.A.R.. It identifies a member of a Subscriber Organisation (the "Authorised Users") who has been duly authorised to use that certificate. These certificates may be used to encrypt/decrypt binary objects and protecting data transmission.

Government Encipherment Certificates are intended mainly for encrypting/decrypting binary objects and protecting data transmission for Government organisation or authorised Government representatives. Key usage of Government Encipherment Certificate is designed for encipherment purpose.

The maximum accumulated civil liability of eSignTrust for the data in the certificates issued according with the above policy is MOP$50,000.00 (fifty thousand Patacas) per certificate/year. Certificates issued within this policy have limited guarantees and responsibilities.

1.3.6. Secure Email Certificate for Personal

Email Certificates are intended mainly for the casual application that does not require any legal binding protection and gets a low and limited warranty and financial liability from eSignTrust. An Email Certificate key usage is designed for signing and encipherment purpose, and it is technically capable of ensuring security of email communications.

Other than the e-mail address of Subscriber, all other information and identity of Subscriber included in the certificate is non-verified (Nonverified Subscriber Information). Also, it includes a limited confirmation of the Subscriber's e-mail address.

The maximum accumulated civil liability of eSignTrust for the data in the certificates issued according with the above policy is MOP$1,000.00 (one thousand Patacas) per certificate/year. Certificates issued within this policy have limited guarantees and responsibilities.

2. Community and Applicability

2.1. Policy Management Authority

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

2.2. Certification Authorities

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

- Root CA; and
- Personal Secure Email CA, Personal CA, Government CA, Corporate CA, Personal QC CA, Government QC CA and Corporate QC CA (i.e., Issuing CA's).

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

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

2.3. Registration Authorities

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

a) To process applications for certificates and requests for certificate suspension and revocation;
b) To perform Identification and Authentication ("I&A") of natural persons in accordance with the eSignTrust CPS, and this CP; and
c) To submit request to the Issuing CA for certificate issuance, suspension or revocation;
d) To recover Subscriber's encryption key upon request and consensus of the Subscriber

RA's will also perform other obligations set forth in this CP, the eSignTrust CPS, and the applicable RA Agreement.

Registration Authority is considered to be part of eSignTrust, only those organisations that have been authorised by the Macao Post Policy Management Authority and that agree to be bound by an appropriate RA Agreement, this CP, and the eSignTrust CPS will be permitted to act as Remote Registration Authority.

2.4. Repositories

Each Issuing CA shall publish Certificates, Certificate status information, and CRL's to a Repository. Such Repository shall be publicly accessible.

The Macao Post Policy Management Authority has authorised eSignTrust to operate and manage the Repository. Other entities or organisations may perform Repository functions provided that such entities are authorised by the Macao Post Policy Management Authority and agree to be bounded by the terms of this CP, the eSignTrust CPS, applicable PKI Documents, and such other requirements as the Macao Post Policy Management Authority may establish.

2.5. Subscribers

eSignTrust issues certificates to natural persons who are individuals, or affiliated individuals of government agencies or departments, 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, eSignTrust also issues identity certificate to hardware device such as Virtual Private Network (VPN) devices.

2.6. Sponsoring organisation

Sponsoring organisations 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 the eSignTrust CPS.

2.7. Relying parties

A Relying Party may be a natural person, government agency or department, or organisation that reasonably relies on a certificate in accordance with the eSignTrust CPS and this CP.

2.8. Applicability

The following types of certificates are intended for use with applications requiring authentication, message integrity, and digital signature features:

- eSignTrust Personal Email Certificate;
- eSignTrust Personal Normalised Identity Certificate;
- eSignTrust Personal Qualified Certificate;
- eSignTrust Government Normalised Identity Certificate;
- eSignTrust Government Qualified Certificate;
- eSignTrust Corporate Normalised Identity Certificate;

- eSignTrust Corporate Qualified Certificate;

The following types of certificates are intended for use with applications requiring confidentiality, and encipherment features:

- eSignTrust Personal Email Certificate;
- eSignTrust Personal Normalised Encipherment Certificate;
- eSignTrust Personal Encipherment Certificate;
- eSignTrust Government Normalised Encipherment Certificate;
- eSignTrust Government Encipherment Certificate;
- eSignTrust Corporate Normalised Encipherment Certificate;
- eSignTrust Corporate Encipherment Certificate.

3. Rights, Obligations and Liabilities

The eSignTrust CPS sets out the rights, obligations, and liabilities of CA's, RA's, Subscribers, and Relying Parties, and all such provisions must be read and accepted by all parties and shall be deemed to be incorporated herein by reference.

4. Identification and Authentication

Registration of the following types of certificates will be based on RA's adopting a in person registration process of certificate applicants together with the relevant identification documents stated in the eSignTrust CPS:

- eSignTrust Personal Normalised Identity Certificate;
- eSignTrust Personal Normalised Encipherment Certificate;
- eSignTrust Personal Qualified Certificate;
- eSignTrust Government Normalised Identity Certificate;
- eSignTrust Government Normalised Encipherment Certificate;
- eSignTrust Government Qualified Certificate;
- eSignTrust Government Encipherment Certificate;
- eSignTrust Corporate Normalised Identity Certificate;
- eSignTrust Corporate Normalised Encipherment Certificate;
- eSignTrust Corporate Qualified Certificate;
- eSignTrust Corporate Encipherment Certificate.

5. Operational Requirements

The eSignTrust CPS sets out the operational requirements for certificate application, registration, issuance, acceptance, suspension, revocation, and renewal, and all such provisions must be read and accepted by all parties and shall be deemed to be incorporated herein by reference.

6. Technical Security Control

The eSignTrust CPS sets out the technical security controls for key-pair generation and installation, private key protection, other aspects of key-pair management, activation data, computer security controls, certificate life-cycle technical controls, network security controls, and cryptographic module engineering controls.

7. Certificate Profiles

The eSignTrust CPS sets out the various certificates, reference to CPS for details definition of the certificate profiles.

8. Certificate Policy Administration

This Certificate Policy is published in the eSignTrust Issuing CA web site at http://www.esigntrust.com/en/repository/ and is administered in accordance with the eSignTrust Certification Practice Statement (CPS).

[END OF DOCUMENT]