

Macao Post and Telecommunications eSignTrust Certification Services Privacy Statement

As part of the eSignTrust pledge to our customers, we recognize and respect your right to privacy. This Privacy Statement (or “Statement”) informs our customers of the privacy practices employed in the provision of eSignTrust solutions, services and website. Questions relating to this policy statement should be directed towards the following link www.esigntrust.com.

CPS and Associated Agreements

This Privacy Statement supplements the practices and policies relating to privacy protection stated within the Subscriber Agreement, Relying Party Agreement and eSignTrust Certification Practice Statement (CPS). Please refer to these documents for the practices employed by eSignTrust for the issuance, management and revocation of certificate-based solutions.

Informational Collection and Use

eSignTrust does not collect any information on its customers without prior consent. As part of the service offerings, customers will be prompted for information when enrolling for a certificate, downloading a solution or requesting further information. No information is collected about a customer if just browsing the website.

Certificate Enrolment

When enrolling for a certificate, customers will be required to provide certain information as per the requirements for the certificate type. The exact informational requirements are set out in the relevant Subscriber Agreement and associated schedules and listed in the eSignTrust CPS. Some of the submitted details will be displayed within the certificate and as a result will be publicly available. Details that will become public are clearly stated as 'public' in the enrollment process, Subscriber Agreement and associated schedules.

Solution Download

When requesting support service, you will be required to submit personal information as specified on the support page. This information will be used by eSignTrust to

contact the customer about the services on our site for which they have expressed interest, including solution updates and associated promotional material. It also aids eSignTrust in providing improved services by collating general demographic information.

Information Request

eSignTrust provides the ability to request further information or ask questions to the support team by displaying email links throughout the website. If a customer elects to use such links they may be requested to provide additional information depending on the nature of the contact. Typically, such additional information may include further contact details, and in the case of technical support, additional information about the customer's PC configuration may be required to aid a prompt and accurate response to the query.

External Links

The eSignTrust website contains links to external websites. eSignTrust is not responsible for the privacy practices of such other sites. This Statement applies solely to information collected by this website. eSignTrust has no control over the accuracy of information displayed by such websites.

Security

This website takes every precaution to protect our customer's information. When customers submit sensitive information via the website, such information is protected both online and off-line. During certificate registration, where sensitive information is required, the transmission of information is encrypted and protected using Secure Sockets Layer (SSL). eSignTrust shall use SSL encryption to protect sensitive information online and do everything in our power to protect user-information off-line. All of our customer's information, not just the sensitive information mentioned above, is restricted in our offices. Only employees who need the information to perform a specific job (for example billing administration or the development team) are granted access to personally identifiable information. ALL employees are kept up-to-date on our security and privacy practices. Every quarter, as well as any time new policies are added, our employees are notified and/or reminded about the importance we place on privacy, and what they can do to ensure the protection of our customers' information. The servers that we store personally identifiable information on are kept in a secure

environment, behind a locked cage.

Supplementation of Information (validation of submitted details)

In order for eSignTrust to properly fulfill its obligation to our customers, it is necessary for us to supplement the information we receive with information from 3rd party sources. For example, prior to the issuance of some certificate types eSignTrust may use Government sourced database or information to validate the accuracy of supplied data. This is an integral aspect of the service provided by eSignTrust.

Service Updates

Established customers will occasionally receive information on solutions, services, special deals, and a newsletter. Out of respect for the privacy of our customers we present the option not to receive these types of communications. We also send the user service announcement updates. Customers are not able to unsubscribe from service announcements, which may contain important security information about the service.

Certificate Revocation & Expiry

Access to all issued certificates is provided through the eSignTrust public repository. Because of the nature of the service provided, there may be circumstances under which a certificate is revoked (cancelled). Furthermore, as the lifetime of all certificates is finite (lasting usually 3 year), certificates will expire. eSignTrust still provides public access to both revoked and expired certificates to ensure a party relying on the certificate may still be able to retrieve the certificate and verify a signature made with the certificate. Such certificates are flagged as revoked or expired within the repository.

Customer Consent

By using our Web site, customers consent to the collection and use of this information by eSignTrust. If any subsequent changes are made to our privacy practices, we will post those changes on relevant pages so that customers are always aware of what information is changed, how it is used and under what circumstances it may be disclosed.