Macao Post and Telecommunications eSignTrust Certification Services

Relying Party Agreement

Macao Post and Telecommunications eSignTrust Certification Services Relying Party Agreement

YOU MUST READ THIS RELYING PARTY AGREEMENT ("AGREEMENT") BEFORE VALIDATING AN ELECTRONIC CERTIFICATE ("CERTIFICATE") OF MACAO POST AND TELECOMMUNICATIONS (“CTT”) ESIGNTRUST CERTIFICATION SERVICES (“ESIGNTRUST”), USING ESIGNTRUST'S ONLINE CERTIFICATE STATUS PROTOCOL ("OCSP") SERVICES, OR OTHERWISE ACCESSING OR USING ESIGNTRUST'S DATABASE OF CERTIFICATE REVOCATIONS AND OTHER INFORMATION ("REPOSITORY") OR ANY CERTIFICATE REVOCATION LIST ISSUED BY ESIGNTRUST. ("ESIGNTRUST CRL"). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT SUBMIT A QUERY AND DO NOT DOWNLOAD, ACCESS, OR USE ANY ESIGNTRUST CRL BECAUSE YOU ARE NOT AUTHORIZED TO USE ESIGNTRUST'S REPOSITORY OR ANY ESIGNTRUST CRL.

1. Background. This Agreement becomes effective when you submit a query to search for a certificate, or to verify an electronic signature created with a private key corresponding to a public key contained in a Certificate, by downloading a eSignTrust CRL, or when you otherwise use or rely upon any information or services provided by eSignTrust's Repository, eSignTrust's website, or any eSignTrust CRL, or when you use eSignTrust's OCSP services. Relying Party Agreements in force within eSignTrust's certificate subdomain of “CTT eSignTrust Services” (“eSignTrust Certificates Net” or “ECN”) appear at:

   https://www.esigntrust.com/en/repos_rpa.html.

2. Definitions. The capitalized terms used in this Agreement shall have the following meanings unless otherwise specified:

   “Accredited Certification Authority” means a Certification Authority accredited by government of Macao SAR.

   “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.

   "Certificate" shall mean a digitally signed message that contains a Subscriber's public key and associates it with information authenticated by eSignTrust or an eSignTrust authorized entity.

   "Certificate Applicant" shall mean an individual or organisation that requests the issuance of a Certificate by a Certification Authority.

   "Certificate Chain" shall mean an ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.

   "Certification Authority" or "CA" or “Certification Entity” shall mean an entity authorized to issue, manage, revoke, and renew Certificates in the ECN.

   “Electronic Document” means the result of relating data being processed electronically for the purpose of reproducing or representing a person, a thing or a fact.

   "Non-verified Subscriber Information" means any information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.

"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. A Qualified Certificate must only be issued by a legally Accredited Certification Authority through a rigorous authentication process.

"Registration Authority" shall mean an entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.

"Relying Party" shall mean an individual or organisation that acts in reliance on a Certificate or a digital signature.

"Repository" shall mean a portion of the eSignTrust website where Relying Parties, Subscribers, and the general public can obtain soft copies of eSignTrust literature, including but not limited to, the eSignTrust CPS, Subscriber Agreements, whitepapers, and CRLs.

"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.

"Subscriber" shall mean a person who is the subject of and has been issued a Certificate ("Certificate Holder").

"Subscriber Agreement" shall mean an agreement used by a CA or RA setting forth the terms and conditions under which an individual or organisation acts as a Subscriber.

"Subscriber Organisation" shall mean the sponsoring organisation of a Subscriber and it contracts with a Certification Authority for the issuance of a Certificate to the Subscriber and bears responsibility towards the CA for the use of the private key associated with the public key of the Subscriber's Certificate.

"eSignTrust CPS" shall mean the eSignTrust Certification Practice Statement, as amended from time to time, which may be accessed from https://www.esigntrust.com/en/repos_cps.html.

3. Sufficient Information. You acknowledge and agree that you have access to sufficient information to ensure that you can make an informed decision as to the extent to which you will choose to rely on the information in a Certificate. You acknowledge and agree that your use of the Repository, your use of any eSignTrust CRL, and your use of eSignTrust's OCSP services are governed by this Agreement and the eSignTrust CPS. For more educational material, see the tutorial contained in eSignTrust's Customer Support at http://www.eSignTrust.com. YOU ARE SOLELY RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A CERTIFICATE. You also acknowledge and agree that you shall bear the legal consequences of your failure to comply with the Relying Party obligations set forth in this Agreement.

4. ECN Certificates. The Certificates relied upon in accordance with this Agreement are issued within the ECN. The ECN is a public key infrastructure that provides Certificates for internet and data network applications. eSignTrust is the only service provider within the ECN. The ECN and eSignTrust under this Agreement offer several distinct types ("Types") of certification services, for both the Internet and other networks. Each Type, or level, of Certificate provides specific functionality and security features and corresponds to a specific level of trust. The following subsections state the appropriate uses and authentication procedures for each Type of Certificate. For more detailed information about eSignTrust's certification services, see the eSignTrust CPS.

(i) eSignTrust Qualified Certificates. This Type of Certificates offers the highest level of assurances within the ECN. The Certificates are issued to natural persons, authorised personnel of organisations or government agencies, and authentication procedures are based on the assurances that the identity and, if applicable, any specific qualifications of the Subscriber is verified requiring personal (physical) presence of the Subscriber before an officer of eSignTrust that confirms the identity and, if applicable, any specific qualifications of the Subscriber using, at minimum, a well-recognised form of government-issued identification with photo and the written confirmation of email address of the Subscriber. If the applicants are outside Macao, the Registration Authority will provide online Identification and Authentication service to those who are eligible. In addition, when the Subscriber representing a Subscriber Organisation the Certificate provides assurances based on a confirmation that the Subscriber Organisation does in fact exist, that the organisation has authorised the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorised to do so. This Type of Certificates provides very high degree of assurance for the identity of a Subscriber and is suitable for high value transaction, extremely sensitive information and the need of the verification of the lawful authenticity and validity of Qualified Electronic Signature.

(ii) eSignTrust Normalised Certificates. This Type of Certificates offers the medium level of assurances in comparison with the other two Types (i and iii) within the ECN. The Certificates are issued to natural persons, authorised personnel of organisations or government agencies, and authentication procedures are based on the assurances that the identity of the Subscriber is verified requiring personal (physical) presence of the Subscriber before an officer of eSignTrust that confirms the identity of the Subscriber using, at minimum, a well-recognised form of government-issued identification with photo and the written confirmation of email address of the Subscriber. If the applicants are outside Macao, the Registration Authority will provide online Identification and Authentication service to those who are eligible. In addition, when the Subscriber representing a Subscriber Organisation the Certificate provides assurances based on a confirmation that the Subscriber Organisation does in fact exist, that the organisation has authorised the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorised to do so. This Type of Certificates provides medium degree of assurance for the identity of a Subscriber and is suitable for medium-value transaction, sensitive information and legally valid Advanced Electronic Signature.

(iii) eSignTrust Encipherment Certificates. This Type of Certificates offers medium level of assurances within the ECN. The Certificates are issued to natural persons, authorised personnel and units of organisations or government agencies, and authentication procedures are based on the assurances that the identity of the Subscriber is verified 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. In addition, when the Subscriber representing a Subscriber Organisation the Certificate provides assurances based on a confirmation that the Subscriber Organisation does in fact exist, that the organisation has authorised the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorised to do so. This Type of Certificates is suitable for the uses of information confidentiality/encryption, of sending encrypted electronic message to the Subscriber/Subscriber Organisation; of permitting the Subscriber/Subscriber Organisation to decrypt messages; of permitting the Subscriber/Subscriber Organisation to acknowledge receipt of the encrypted message by sending an acknowledgement with a digital signature added to it to confirm the identity of the receiving Subscriber/Subscriber Organisation.

(iv) eSignTrust Personal Secure Email Certificates. This Type of Certificates offers the lowest level of assurances within the ECN. The Certificates are issued to individual Subscribers

only, and authentication procedures are based on assurances that the Subscriber's distinguished name is unique and unambiguous within the domain of a particular CA and that a certain e-mail address is associated with a public key. This Type of Certificates is appropriate for securing e-mail communications with digital signatures and/or encryption, and access control for non-commercial or low-value transactions where proof of identity is unnecessary.

5. Your Obligations. As a Relying Party, you are obligated to:

   (i) 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;

   (ii) utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations you wish to perform, as a condition of relying on a Certificate in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain. You agree that you will not rely on a Certificate unless these verification procedures are successful;

   (iii) check the status of a Certificate on which you wish to rely, as well as all the Certificates in its Certificate Chain. If any of the Certificates in the Certificate Chain have been revoked, you agree that that you will not rely on the end-user Subscriber Certificate or other revoked Certificate in the Certificate Chain; and

   (iv) rely on the Certificate, if all of the checks described in the previous paragraphs are successful, provided that reliance upon the Certificate is reasonable under the circumstances and in light of Section 3 of this Agreement. If the circumstances indicate a need for additional assurances, it is your responsibility to obtain such assurances for such reliance to be deemed reasonable.

6. Limitations on Use. Certificates issued under the ECN are not designed, intended, or authorized 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 weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. The private key of an eSignTrust Qualified Certificate shall only be used, according to the conditions specified in the Certificate, to create Qualified Electronic Signature using eSignTrust's SSCD. The private key of an eSignTrust Normalised Certificate shall only be used, according to the conditions specified in the Certificate, to create Advanced Electronic Signature using means that the signatory can maintain under his sole control. eSignTrust Encipherment Certificates and eSignTrust Personal Secure Email Certificates shall not be used as proof of identity or as support of non-repudiation of identity or authority. eSignTrust, and its CAs and RAs are not responsible for assessing the appropriateness of the use of a Certificate. You agree as a Relying Party that Certificates will not be used or relied upon by you beyond the limitations set forth in this Agreement.

7. Compromise of ECN Security. You agree that you shall not monitor, interfere with, or reverse engineer the technical implementation of the ECN, except upon prior written approval from eSignTrust, and shall not otherwise intentionally compromise the security of the ECN.

8. Effect of a Certificate. You acknowledge and agree, to the extent permitted by the applicable law, that an Electronic Document susceptible of representation as written declaration and bearing a Qualified Electronic Signature verifiable with reference to a Qualified Certificate has full evidentiary value of the declarations attributed to its signatory. Subject to the applicable law, an electronic signature or transaction entered into with reference to a Certificate shall be effective regardless of the geographic location where the Certificate is issued or the electronic signature

created or used, and regardless of the geographic location of the place of business of the CA or Subscriber.

9. eSignTrust Warranties. eSignTrust warrants to Relying Parties who reasonably rely on a Certificate

   (i) that all information in or incorporated by reference in the Certificate, except for Nonverified Subscriber Information, is accurate;

   (ii) that Certificates appearing in the Repository have been issued to the individual or organisation named in the Certificate as the Subscriber, and the Subscriber has accepted the Certificate by receiving the Certificate contained in a storage media and signing a receipt of acknowledgement, or by downloading it from a website or via an email message sent to the Subscriber containing the Certificate; and

   (iii) the entities that approved the Certificate Application and issued the Certificate have substantially complied with the eSignTrust CPS when issuing the Certificate.

10. Disclaimers. YOU AGREE THAT YOUR USE OF ESIGNTRUST'S SERVICE(S) IS SOLELY AT YOUR OWN RISK. YOU AGREE THAT ALL SUCH SERVICES ARE PROVIDED ON AN "AS IS" AND AS AVAILABLE BASIS, EXCEPT AS OTHERWISE NOTED IN THIS AGREEMENT. ESIGNTRUST EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. OTHER THAN THE WARRANTIES AS SET FORTH IN SECTION 9, ESIGNTRUST DOES NOT MAKE ANY WARRANTY THAT THE SERVICE WILL MEET YOUR REQUIRMENTS, OR THAT THE SERVICE WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR FREE; NOR DOES ESIGNTRUST MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE SERVICE OR TO THE ACCURACY OR RELIABILITY OF ANY INFORMATION OBTAINED THROUGH THE SERVICE. YOU UNDERSTAND AND AGREE THAT ANY MATERIAL AND/OR DATA DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF ESIGNTRUST'S SERVICES IS DONE AT YOUR OWN DISCRETION AND RISK. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM ESIGNTRUST OR THROUGH ESIGNTRUST'S SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY MADE HEREIN. ESIGNTRUST IS NOT RESPONSIBLE FOR AND SHALL HAVE NO LIABILITY WITH RESPECT TO ANY PRODUCTS AND/OR SERVICES PURCHASED BY YOU FROM A THIRD PARTY.

11. Indemnification. You agree to release, indemnify, defend and hold harmless eSignTrust and any non-eSignTrust CAs or RAs, and any of their respective contractors, agents, employees, officers, directors, shareholders, affiliates and assigns from all liabilities, claims, damages, costs and expenses, including reasonable attorney's fees and expenses, of third parties relating to or arising out of

   (i) your failure to perform the obligations of a Relying Party,

   (ii) your reliance on a Certificate that is not reasonable under the circumstances, or

   (iii) your failure to check the status of a Certificate to determine if the Certificate is expired or revoked. When eSignTrust is threatened with suit or sued by a third party, eSignTrust may seek written assurances from you concerning your promise to indemnify eSignTrust, your failure to provide those assurances may be considered by eSignTrust to be a material breach of this Agreement. eSignTrust shall have the right to participate in any defense by you of a third-party claim related to your use of any eSignTrust services, with counsel of

our choice at your own expense. You shall have sole responsibility to defend eSignTrust against any claim, but you must receive eSignTrust's prior written consent regarding any related settlement, otherwise such settlement will not be binding on eSignTrust. The terms of this Section 11 will survive any termination or cancellation of this Agreement.

12. Limitations of Liability. THIS SECTION 12 APPLIES TO LIABILITY UNDER CONTRACT (INCLUDING BREACH OF WARRANTY), OR (INCLUDING NEGLIGENCE AND/OR STRICT LIABILITY), AND ANY OTHER LEGAL OR EQUITABLE FORM OF CLAIM. IF YOU INITIATE ANY CLAIM, ACTION, SUIT, ARBITRATION, OR OTHER PROCEEDING RELATING TO SERVICES PROVIDED UNDER THIS SECTION AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, eSignTrust's TOTAL LIABILITY FOR DAMAGES SUSTAINED BY YOU AND ANY THIRD PARTY FOR ANY USE OR RELIANCE ON A SPECIFIC CERTIFICATE SHALL BE LIMITED, IN THE AGGREGATE, TO THE AMOUNTS SET FORTH BELOW.

Type	Liability Caps
eSignTrust Qualified Certificate	MOP 200,000.00
eSignTrust Normalised Certificate	MOP 50,000.00
eSignTrust Encipherment Certificate	MOP 50,000.00
eSignTrust Personal Secure Email Certificate	MOP 1,000.00

The liability limitations provided in this Section 12 shall be the same regardless of the number of digital signatures, transactions, or claims related to such Certificate. eSignTrust SHALL NOT be obligated to pay more than the total liability limitation for each Certificate that is relied upon.

13. Protection of Private Key. YOU ARE HEREBY NOTIFIED OF THE POSSIBILITY OF THEFT OR OTHER FORM OF COMPROMISE OF A PRIVATE KEY CORRESPONDING TO A PUBLIC KEY CONTAINED IN A CERTIFICATE, WHICH MAY OR MAY NOT BE DETECTED, AND OF THE POSSIBILITY OF USE OF A STOLEN OR COMPROMISED KEY TO FORGE A DIGITAL SIGNATURE TO A DOCUMENT.

14. Governing Law. The parties agree that any disputes related to the services provided under this Agreement shall be governed in all respects by and construed in accordance with the laws of Macao Special Administrative Region (“MSAR”), excluding its conflict of laws rules.

15. Dispute Resolution. To the extent permitted by law, before you may invoke any dispute resolution mechanism with respect to a dispute involving any aspect of this Agreement, you shall notify eSignTrust, and any other party to the dispute for the purpose of seeking dispute resolution. If the dispute is not resolved within thirty (30) calendar days after the initial notice, then a party may proceed in accordance with corresponding stipulation in eSignTrust CPS.

16. Severability. If any provision of this Agreement, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this Agreement (and the application of the invalid or unenforceable provision to other persons or circumstances) shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.

17. Force Majeure. Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire,

storm, natural disaster, act of God, war, armed conflict, terrorist action, labor strike, lockout, boycott, provided that the party relying upon this Section 17 shall (i) have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (ii) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event a force majeure event described in this Section 17 extends for a period in excess of thirty (30) days in aggregate, the other party may immediately terminate this Agreement.

18. Survival. This Agreement shall be applicable for as long as you rely on a Certificate, use the OCSP service, access or use the eSignTrust database of CRL information and in any matter of respect concerning the subject matter of this Agreement.

19. Non-Assignment. Except as otherwise set forth herein, your rights under this Agreement are not assignable or transferable. Any attempt by your creditors to obtain an interest in your rights under this Agreement, whether by attachment, levy, garnishment or otherwise, renders this Agreement voidable at eSignTrust's option.

20. Independent Contractors. The parties to this Agreement are independent contractors. Neither party is an agent, representative, or partner of the other party. Neither party shall have any right, power or authority to enter into any agreement for or on behalf of, or incur any obligation or liability of, or to otherwise bind, the other party. This Agreement shall not be interpreted or construed to create an association, joint venture or partnership between the parties or to impose any partnership obligation or liability upon either party. Each party shall bear its own costs and expenses in performing this Agreement.

21. Notices. You will make all notices, demands or requests to eSignTrust with respect to this Agreement in writing to:

    Attn: eSignTrust Policy Management Group,
    eSignTrust Certification Services,
    Macao Post and Telecommunications, Largo do Senado,
    Macao.

22. Entire Agreement. This Agreement constitutes the entire understanding and agreement between eSignTrust and you with respect to the transactions contemplated, and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement or communication between eSignTrust and you concerning the subject matter hereof. Neither party is relying upon any warranties, representations, assurances or inducements not expressly set forth herein. Section headings are inserted for convenience of reference only and are not intended to be part of or to affect the meaning of this Agreement. Terms and conditions that conflict with this Agreement are null and void.