LANKACLEAR

Certification Service Provider

Summary Certification Practice Statement

Version 3.1

Lankasign

LankaClear (Pvt.) Ltd

Document Control

1.	Document Title	LANKACLEAR Certification Service Provider Summary Certification Practice Statement
2.	Date of Release	9th May 2009
3.	Document Superseded	V3.0
4.	Version No.	V3.1
5.	Document Owner	GM / CEO
6.	Document Authors	Senior Manager – Information Security Solutions

Document Approvers

S. No.	Approver	Designation	Signature
01	Channa de Silva	GM / CEO	Digitally signed by Channa de Silva Date: 2021.08.11 07:53:54 +05'30'

Document History

Version #	Date Applicable	Author / Owner	Notes (If any)
1.0			

2.0		Viraj Premaratne & Dulip Liyanage	
3.0	01st of May 2019	Viraj Premaratne & Manoj Fernando	Reviewed by Policy Authority
3.1	01st of Aug 2021	Manoj Fernando	Reviewed by Policy Authority

Trademark Notices

The LankaSign logo and service trademarks are the properties of LankaClear (Pvt.) Ltd. Other trademarks and service marks in this document are the property of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of LankaClear (Pvt.) Ltd.

Notwithstanding the above, permission is granted to reproduce and distribute this LankaSign Certification Practice Statement on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to LankaSign.

Requests for any other permission to reproduce this LankaSign Certification Practice Statement (as well as requests for copies from LankaClear (Pvt.) Ltd.) must be addressed to LankaSign, LankaClear (Pvt.) Ltd, Level 18, Bank of Ceylon Head Office, BOC Square , Bank of Ceylon Mawatha, Colombo 00100. LankaSign Helpdesk. Tel: +94 11 2356900 Fax: +94 11 2544346 Email: helpdesk@lankaclear.com

LankaSign

Contents

Trademark Notices 4
1 Definitions 7
2 Introduction 8
3 Procedures and Practices 8
3.1 Certificate Application Procedure 8
3.2 Practices for Reliance on Digital Certificates 9
3.3 Certificate Revocation 10
3.4 Certificate Renewal 10
4 Technology 11
Introduction 11
4.2 Digital Certificate Management 11
4.3 Types of LANKASIGN-CSP Certificates 12
4.4 Private Key Generation Process for a Certificate Owner 12
5 LankaSign Requirements and Legal Conditions 13
5.1 LANKASIGN-CSP Representations 13
5.2 Information Incorporated into a LANKASIGN-CSP Digital Certificate 13
5.3 Publication of Certificate Revocation Data 13
5.4 Duty to Monitor the Accuracy of Submitted Information 13
5.5 Publication of Information 13
5.6 Interference with LANKASIGN-CSP Implementation 14
5.7 Standards and Technologies 14
5.8 Reliance on Unverified Digital Signatures 14
5.9 Refusal to Issue a Certificate 14
5.10 Obligations of a Certificate Owner/User 14
5.11 Representations by Certificate Owner/User upon Acceptance 15
5.12 Obligations of a Relying Party 16
5.13 Accuracy of Information 16
5.14 Obligations of LANKASIGN-CSP 16
5.15 Damage and Limitations 17
5.16 Conflict of Rules 18
5.17 Intellectual Property Rights 18
5.18 Infringement and Other Damaging Material 18
5.19 Certificate Ownership 18

5.20 Severability 18
5.21 Interpretation.....19
5.22 Confidential Information 19

1 Definitions

a) **CA** - Certification Authority is an entity appointed in terms of Chapter IV of the Electronic Transaction Act, No. 19 of 2006

b) **CSP** - Certification Service Provider is an entity which is approved to issue digital certificates under the Electronic Transaction Act, No.19 of 2006.

c) **OCSP** - Online Certificate Status Protocol

d) **CRL** - Certificate Revocation List. A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date.

e) **Digital Certificate** - In cryptography, a public key certificate (or identity certificate) is an electronic document which uses a digital signature to bind together a public key with an identity

f) **Encryption** - Refers to algorithmic schemes that encode plain text into non-readable form or cipher text.

g) **NDES** – Network Device Enrollment Service

h) **Subscriber** - Once the Certificate issues, the Legal Entity is referred to as the Subscriber. A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

i) **Relying Party -** Any natural person or Legal Entity that relies on a Valid Certificate. Relying party is any service, site or entity that depends on LankaSign certificates to identify and authenticate a user who is requesting access to a digital resource including subscriber and digital signature verifier. A Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate to determine the suitability of the certificate for a particular use.

j) **Registrant/Applicant -** The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate.

k) **Signature Verifier** is an entity or person that validates a certificate.

s) **Repository -** A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.

t) **Object identifiers -** identifies the purpose to which the certificate is used. Email signing, client authentication, etc.

LankaSign

2 Introduction

This document is the LankaSign Certification Practice Statement (CPS). It states the practices that LankaSign Certification Service Provider (CSP) employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the LankaSign through LankaClear (Pvt) Ltd. LankaSign CSP is a provider of trusted infrastructure services to web sites, enterprises, electronic commerce service providers, and individuals. The company's domain name, digital certificate, and payment services provide the critical web identity, authentication, and transaction infrastructure that online businesses require to conduct secure e-commerce and communications.

The CPS is the principal statement of policy governing the LankaSign operations. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital certificates R and providing associated trust services. This applies to all stakeholders of LankaSign and thereby provides assurances of uniform trust throughout LankaSign trusted network.

3 Procedures and Practices

3.1 Certificate Application Procedure

All Certificate applicants must complete the application process, which includes:

a) Completion of the LankaSign Digital Certificate Subscriber Agreement. This is a service agreement that enrolls an individual or an organization to the LANKASIGN-CSP service and must be completed per individual/organization.

b) Completion of the appropriate LANKASIGN-CSP digital certificate application forms. This is a product request that must be completed per certificate request.

   i. Form_CA_01_Clearing_Application_Certificate. for LankaClear Clearing application Certificate requests ii. Form_CA_02_SSL_Certificates for SSL Certificate

   iii. Form_CA_03_User Certificate for individual users who requests for email / document signing certificates.

   iv. Form_CA_04 _3rd_Party_User_Certificatefor organizations who provides email / document signing certificates for their customers.

   v. Form_CA_05_Revocation to be used in the event of Loss / Theft / Compromised / Change of existing authorized user, this application revocation form should be promptly completed and submitted to LankaSign CSP. vi. Official_request_letter to be used in the event of requesting for a new certificate / renewal / revocation in the specified format.

   vii. Code Signing Form

c) Provision of proof of identity and other authenticated/official documentation as requested by LANKASIGN-CSP during the certificate issuance process.

LankaSign

d) Generation of key pair through a process determined by LANKASIGN-CSP. The process for generation of the key pair shall be determined solely by LANKASIGN-CSP at its discretion based on operational, technical and regulatory requirements and may take one of the following modes:
   i. Secure generation of the key pair at LANKASIGN-CSP operations center using secure hardware and issuance of the password protected private key using a secure hardware module.
   ii. Secure generation of the key pair at a client location using secure hardware and issuance of the password protected private key using a secure hardware module or installation on to a secure hardware module.
   iii. Secure generation of a key pair by the client and verifiable demonstration of ownership of the private key half of the key pair to LANKASIGN-CSP through the submission of a valid PKCS#10 CSR.

e) Demonstration to LANKASIGN-CSP by the certificate requester, of its capability to take all reasonable efforts to protect the integrity of the private key half out of the key pair.
   i. Certificate applications must be submitted to either LANKASIGN-CSP, LANKASIGN- CSP approved RA or LankaSign approved outsourced entity.
   ii. LANKASIGN-CSP shall process LankaSign certificate requests and issue certificates regardless of the applications accepting entity.

For SDK, the request is made via Microsoft Network Device Enrollment Service (NDES) method.

3.2 Practices for Reliance on Digital Certificates

The verification of a digital signature on a digitally signed object (a document file, any mode of digital communication, a program file, an IP packet, transaction etc) is used to determine that:

a) The private key corresponding to the public key listed in the signer's certificate has created the digital signature with respect to the signed object.
b) The signed object associated with this digital signature has not been altered since the digital signature was created. The final decision by the signature verifier concerning whether or not to rely on a verified digital signature is exclusively that of the signature verifier. The reliance on a digital signature should only occur if:

   i. The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate.
   ii. The relying party has checked the revocation status of the certificate by referring to the relevant CRLs or via the OCSP Server mentioned in the certificate and the certificate has not been revoked.
   iii. The relying party understands that a digital certificate is issued to a certificate owner/user for a specific purpose and that the private key associated with the digital certificate may only be used in accordance with the usages suggested in the CPS and named as Object Identifiers in the certificate profile. Reliance is accepted as

LankaSign

reasonable under the provisions made for the relying party under this CPS and within the LankaSign Digital Certificate Subscriber Agreement.

3.3 Certificate Revocation

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. LANKASIGN-CSP will revoke a digital certificate if:

a) There has been loss, theft, modification, unauthorized disclosure, change of authorized user /owner or other compromise of the private key associated with the certificate.
b) The owner/user of the certificate or LANKASIGN-CSP has breached a material obligation under this CPS.
c) The obligations of the certificate user/owner under this CPS are delayed or prevented by a natural disaster, digital user device or communications failure, or other cause beyond the reasonable control of owner/user, and as a result information owned/controlled by another individual or organization is materially threatened or compromised.
d) The obligations of the LANKASIGN-CSP under this CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the reasonable control of LANKASIGN-CSP, and as a result information owned/controlled by another individual or organization is materially threatened or compromised.
e) There has been a modification of the information pertaining to the certificate owner/user that is contained within the certificate.

The certificate owner or other appropriately authorized parties such as relevant organization / RAs can request revocation of a digital certificate using the LANKASIGN-CSP Certificate Revocation Request Form (Form_CA_05). Prior to the revocation of a certificate, LANKASIGN-CSP will verify that the revocation request has been:

a) Made by the organization or individual entity that has made the certificate application.
b) Made by the RA on behalf of the organization or individual entity that used the RA to make the certificate application.
c) Upon receipt of a certification revocation request, LANKASIGN-CSP will request confirmation from the certificate owner or from appropriately authorized parties either by telephone, email or by fax.

LankaSign CSP authorizes revocation automation for SDK using a program run on RA server with the relevant certificate serial numbers.

3.4 Certificate Renewal

The validity period of LANKASIGN-CSP digital certificates is detailed in the relevant field within the X.509v3 compliant certificate. LANKASIGN-CSP shall make reasonable efforts to notify certificate owners of approaching certificate expiration date and the requirement for certificate renewal. Notice shall ordinarily be provided within a 7 -day period prior to the expiry of the certificate. Notwithstanding notification by LANKASIGN-CSP, the sole responsibility for proper renewal of a

LankaSign

digital certificate is with the certificate owner/user. The renewal application requirements and procedures are the same as certificate application procedure followed by a request letter indicating the requirement in the formats specified in Official Request Letter format.

4 Technology

4.1 CSP Infrastructure

Introduction

The LANKASIGN-CSP infrastructure uses trustworthy systems to provide certificate services. These trustworthy systems include hardware, software and procedures to provide a high degree of resilience against computer security risks and physical security risks. The trustworthy systems are used to provide high level of availability, reliability, correctness of operation and for the enforcement of a security policy.

4.2 Digital Certificate Management

LANKASIGN-CSP certificate management refers to following main functions performed by LANKASIGN-CSP for the purpose of providing CSP services:

a) Verification of the identity and other relevant details of an applicant (individual or organization) for issuance of a certificate
b) Authorizing the issuance of certificates
c) Issuance of certificates
d) Verification of the identity and other relevant details of an applicant (individual or organization) for revocation of a certificate
e) Revocation of certificates
f) listing, distributing and publishing of certificates
g) Listing, distributing and publishing of CRLs
h) Storing and archiving of certificate details

LANKASIGN-CSP conducts the overall certification management within the LANKASIGN PKI. LANKASIGN-CSP is not involved in functions associated with the management of key by its clients including decommissioning or destruction of a certificate owner's/user's secret key.

LANKASIGN-CSP manages and makes publicly available list of revoked certificates using CRLs and OCSP Servers. All certificates and CRLs issued by LANKASIGN-CSP are compliant to X.509v3. Users of LANKASIGN-CSP issued certificates are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate. LANKASIGN-CSP updates and publishes a new CRL every 8 hours or more frequently under special circumstances.

LankaSign

4.3 Types of LANKASIGN-CSP Certificates

LANKASIGN-CSP currently offers a set of digital certificate products that can be used to provide secure personal and business communications including but not limited to secure e-mail /document signing and encryption, protection of online transactions, authenticity of executable code, identification of persons and identification of servers/devices on a network. LANKASIGN-CSP may update or extend its list of digital certificate products, including the types of certificates it issues, as it sees fit.

a) LANKASIGN-CSP Secure Server Certificates - These are Secure Server Certificates bound to a domain or IP address that in combination with SSL Web Server attest the public server's identity, providing full authentication and enabling secure communication with customers and business partners. The term public server can be used in the context of public Internet or in the context of private intranet with respect to the intended client base.

b) LANKASIGN-CSP Secure Email Certificates - These are Secure Email Certificates bound to an email address that is in combination with an S/MIME compliant email application allowing the owners/users of the certificates to digitally sign and email, or the relying parties to encrypt the email communication with the certificate owners/users.

c) LANKASIGN-CSP Digital Signature Certificates - These are Digital Signature Certificates bound to an identity of an individual or an organization entity/role that allow owners/users of the certificates to digitally sign digital objects for relying parties.

d) LANKASIGN-CSP Public Key Encryption Certificates - These are Public Key Encryption Certificates bound to an identity of an individual or an organization entity/role that allow relying parties to encrypt digital objects for the certificate owners/users.

e) LANKASIGN-CSP Code Signing Certificates – These are digital signature certificates which signs executables and scripts in order to verify the author's identity & ensure that the code has not been changed or corrupted since it was signed by the author.

4.4 Private Key Generation Process for a Certificate Owner

The certificate owner is solely responsible for the management of the private key associated with a certificate including protection, recovery and backup of keys. LANKASIGN-CSP will assist its clients upon request in the generation and secure storage of keys on an appropriate HSM or security token.

LankaSign

5 LankaSign Requirements and Legal Conditions

5.1 LANKASIGN-CSP Representations

LANKASIGN-CSP makes to all certificate applicants, certificate owners/users and relying parties certain representations regarding its public service. LANKASIGN-CSP reserves its right to modify such representations as it sees fit or required by law.

5.2 Information Incorporated into a LANKASIGN-CSP Digital Certificate

LANKASIGN-CSP incorporates by reference the following information in every digital certificate it issues:

a) Terms and conditions of the digital certificate.

b) Certificate policy as may be stated on an issued LANKASIGN-CSP certificate, including the location of this CPS.

c) The mandatory elements of the standard X.509v3.

d) Any non-mandatory but customized elements of the standard X.509v3.

e) Content of extensions and enhanced naming that are not fully expressed within a certificate.

f) Any other information that is indicated to be so in a field of a certificate.

LANKASIGN-CSP certificates may include a brief statement describing limitations of liability, validation period, and intended purpose of the certificate and disclaimers of warranty that may apply. Certificate applicants must agree to LANKASIGN-CSP Terms and Conditions before obtaining a certificate.

5.3 Publication of Certificate Revocation Data

LANKASIGN-CSP reserves its right to publish a Certificate Revocation List (CRL) or use OCSP services to publish CRLs as may be indicated.

5.4 Duty to Monitor the Accuracy of Submitted Information

In all cases and for all types of LANKASIGN-CSP certificates, the certificate owner/user has a continuous obligation to monitor the accuracy of the submitted information and notify LANKASIGN-CSP of any such changes.

5.5 Publication of Information

Published critical information may be updated from time to time as prescribed in this CPS. Such updates shall be indicated through appropriate version numbering and publication date on any new version.

LankaSign

5.6 Interference with LANKASIGN-CSP Implementation

Certificate applicants, certificate owners/users, relying parties and any other parties shall not interfere with, or reverse engineer the technical implementation of LANKASIGN-CSP PKI services including the key generation process, the LANKASIGN-CSP public repositories and web sites except as explicitly permitted by this CPS or upon prior written approval of LANKASIGN-CSP. Failure to comply with this as a certificate owner/user will result in the revocation of the owner's/user's digital certificate without further notice.

5.7 Standards and Technologies

LANKASIGN-CSP assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards enforces the requirements set out in this CPS. LANKASIGN-CSP cannot warrant that such user software will support and enforce controls required by LANKASIGN-CSP. Certificate applicants, certificate owners/users, relying parties and any other parties are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

5.8 Reliance on Unverified Digital Signatures

Parties relying on a LankaSign digital certificate must verify the digital signature at all times by checking the validity of a digital certificate against the relevant CRL published by LANKASIGN- CSP. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the certificate owner/user. Relying on an unverifiable digital signature may result in risks that the relying party, and not LANKASIGN-CSP, assumes in whole. By means of this CPS, LANKASIGN-CSP has informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public.

5.9 Refusal to Issue a Certificate

LANKASIGN-CSP reserves its right to refuse to issue a certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. LANKASIGN-CSP reserves the right not to disclose reasons for such a refusal.

5.10 Obligations of a Certificate Owner/User

Unless otherwise stated in this CPS, certificate owners/users shall exclusively be responsible:

a) To minimize internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
b) Provide correct and accurate information in its communications with LANKASIGN-CSP

c) Alert LANKASIGN-CSP if at any stage whilst the certificate is valid, any information originally submitted has changed since it had been submitted to LANKASIGN-CSP.

d) Read, understand and agree with all terms and conditions in this LANKASIGN-CSP CPS and associated policies published in the LANKASIGN-CSP Repositories as provided under section 4.29 in Notices.

e) Refrain from tampering with a LANKASIGN-CSP certificate. If a certificate is found to be tampered with based on the opinion of LankaSign CSP, it is considered null and void and shall be revoked.

f) Use LANKASIGN-CSP certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.

g) Cease using a LANKASIGN-CSP certificate if any information in it becomes misleading obsolete or invalid.

h) Cease using a LANKASIGN-CSP certificate if such certificate is expired and remove it from any applications and/or devices it has been installed on.

i) Refrain from using the certificate owner's/user's private key corresponding to the public key in a LANKASIGN-CSP issued certificate to issue end-entity digital certificates or subordinate CAs.

j) Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in a LANKASIGN-CSP certificate.

k) Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a LANKASIGN-CSP certificate.

l) Initiate renewal request of certificate prior to expiry by submitting relevant documents

5.11 Representations by Certificate Owner/User upon Acceptance

Upon accepting a certificate, the certificate owner/user represents to LANKASIGN-CSP and to relying parties that at the time of acceptance and until further notice:

a) Digital signatures created using the private key corresponding to the public key included in the certificate is the digital signature of the certificate owner/user and the certificate has been accepted and is properly operational at the time the digital Signature is created.

b) No unauthorized person has ever had access to the certificate owner/user's private key.

c) All representations made by the certificate owner/user to LANKASIGN-CSP regarding the information contained in the certificate are accurate and true.

d) All information contained in the certificate is accurate and true to the best of the Certificate Owner's/Users knowledge or to the extent that the certificate owner/user had notice of such information whilst the certificate owner/user shall act promptly to notify LANKASIGN-CSP of any material inaccuracies in such information.

e) The certificate is used exclusively for authorized and legal purposes, consistent with this CPS.

f) The certificate owner/user retains control of the private key, use a trustworthy system, and take reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.

g) The certificate owner/user will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as a CSP or otherwise, unless expressly agreed in writing between certificate owner/user and LANKASIGN-CSP.

LankaSign

h) The certificate owner/user agrees with the terms and conditions of this CPS and other agreements and policy statements of LANKASIGN-CSP.

i) The certificate owner/user abides by the laws applicable in Sri Lanka and in the country or territory in which activities related to the use of LANKASIGN-CSP issued digital certificates are being used including those related to intellectual property protection, viruses, accessing computer systems etc.

5.12 Obligations of a Relying Party

A party relying on a LANKASIGN-CSP certificate accepts that in order to reasonably rely on a LANKASIGN-CSP certificate they must:

a) Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate; the relying party must have reasonably made the effort to acquire sufficient knowledge on using digital certificates and PKI.

b) Study the limitations to the usage of digital certificates.

c) Read and agree with the terms of the LANKASIGN-CSP CPS and relying party Terms and Conditions.

d) Verify a LANKASIGN-CSP certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA or verify them through LANKASIGN-CSP's OCSP servers.

e) Trust a LANKASIGN-CSP certificate only if it is valid and has not been revoked or has expired.

f) Rely on a LANKASIGN-CSP certificate, only as may be reasonable under the circumstances listed in this CPS.

g) Relying Party can not hold LCPL liable for any certificate related matter including validation.

5.13 Accuracy of Information

LANKASIGN-CSP, recognizing its trusted position, makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated and correct information. LANKASIGNCSP, however, cannot accept any liability beyond the limits set in this CPS under Damage and Loss Limitations. All parties accessing the LANKASIGN-CSP Repositories and official web sites shall agree with the provisions of this CPS and any other conditions of usage that LANKASIGN-CSP may make available. The demonstration of the acceptance of the conditions of usage of the CPS shall be through the use of LANKASIGN-CSP issued certificates. Failure to comply with the conditions of usage of the LANKASIGN-CSP Repositories and web site may result in terminating the relationship between LANKASIGN-CSP and the party accessing these resources.

5.14 Obligations of LANKASIGN-CSP

To the extent specified in this CPS, LANKASIGN-CSP promises to:

a) Comply with this CPS and its internal or published policies and procedures.

LankaSign

b) Comply with applicable laws and regulations.

c) Provide infrastructure and certification services, including but not limited to the establishment and operation of the LANKASIGN-CSP OCSP Servers and web sites for the operation of PKI services.

d) Provide trust mechanisms, including a key generation mechanism and key protection regarding its own infrastructure.

e) Provide prompt notice in case of compromise of its private key(s).

f) Provide and validate application procedures for the various types of certificates that it may make publicly available.

g) Issue digital certificates in accordance with this CPS and fulfill its obligations presented herein.

h) Publish accepted certificates in accordance with this CPS.

i) Provide support to certificate owners/users and relying parties as described in this CPS.

j) Revoke certificates according to this CPS.

k) Provide for the expiration and renewal of certificates according to this CPS.

l) Make available a supplemental copy of this CPS and applicable policies to requesting parties.

5.15 Damage and Limitations

LANKASIGN-CSP disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein

LANKASIGN-CSP does not warrant the quality, functions or performance of any software or hardware device. Also, although LANKASIGN-CSP is responsible for the revocation of a certificate, it cannot be held liable if it cannot execute it for reasons outside its own control. Except to the extent of willful misconduct, the cumulative maximum liability accepted by LANKASIGN-CSP for the issuance of a certificate containing invalid information pertaining to the certificate owner/user that has been validated using the methods appropriate for the certificate class and/or type shall not exceed the fee charged by LANKASIGN-CSP for the issuance of the said certificate. In no event (except for fraud or willful misconduct) will the aggregate liability of LANKASIGN-CSP to all parties including without any limitation; a certificate owner, an applicant, a recipient, or a relying party; for all digital signatures and transactions related to such certificate exceeds the fee charged by LANKASIGN-CSP for the issuance of the said certificate.

In no event (except for fraud or willful misconduct) shall LANKASIGN-CSP be liable for any indirect, incidental or consequential damages; any loss of income or profits; any loss of data; any liability that arises from compromise of a certificate owner's private key; any liability that arises from the usage of a certificate that is not valid; any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CPS; any liability incurred due to reliance on verified information contained in the certificate if the faults in this verified information are due to fraud or willful misconduct of the certificate owner\user or any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or nonperformance of certificates or digital signatures. LANKASIGN-CSP does not limit or exclude liability for death or personal injury.

LankaSign

5.16 Conflict of Rules

When this CPS conflicts with other rules, guidelines, or contracts, the latest version of this CPS, shall prevail and bind the certificate owner/user and other parties except as to other contracts either:

a) Predating the first public release of the present version of this CPS.

b) Expressly superseding this CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

5.17 Intellectual Property Rights

LANKASIGN-CSP owns all intellectual property rights associated with its databases, web sites, and the LANKASIGN-CSP digital certificates and related documents.

5.18 Infringement and Other Damaging Material

LANKASIGN-CSP clients represent and warrant that when submitting to LANKASIGN-CSP and using a domain and distinguished name (and all other certificate application information) they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortuous interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated. Although LANKASIGN-CSP will provide all reasonable assistance, certificate owners\users shall defend, indemnify, and hold LANKASIGN-CSP harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of LANKASIGN-CSP.

5.19 Certificate Ownership

The digital certificates are the property of LANKASIGN-CSP. LANKASIGN-CSP gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. The party to which LANKASIGN-CSP issues a certificate shall be known as the "certificate user" for the said certificate in the context of the use of that certificate and all its copies.

The party with whom the agreement is signed shall be known as the “certificate owner”.

LANKASIGN-CSP reserves the right to revoke the certificate at any time. Private and public keys are property of the certificate owners who rightfully issue and hold them.

5.20 Severability

If any provision of this CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted in such manner as to affect the original intention of the parties. Each and every provision of this CPS that provides for a

LankaSign

limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

5.21 Interpretation

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service. In interpreting this CPS, parties shall also take into account the international scope and application of the services and products of LANKASIGN-CSP as well as the principle of good faith as it is applied in commercial transactions. The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS. Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

5.22 Confidential Information

It is agreed that information, material and any other confidential data coming to the knowledge of either party or its employees, agent, nominee either by disclosure by the Customer or otherwise, shall not be divulged or disclosed by either party and or its management, directors, officers, staff, employees, workers, representatives and agents to any person without the prior written consent of the Customer. This clause shall survive the termination of this Agreement.