LANKASIGN CERTIFICATION SERVICE PROVIDER

CERTIFICATION PRACTICE STATEMENT

Version 3.3

Issue Date: 08th April 2024

Issued By: LankaPay Private Limited

Your Trusted
Payment Network

TABLE OF CONTENTS

CONTENTS PAGE

Document Revision Information

VERSION	CHANGES	DATE
1.0	Created by Chandana Gamage & Thilina Wijewicrema	09th May 2009
2.0	Updated by Dileepa Lathsara & Duleep Liyanage	01st Nov 2012
3.0	Updated by Viraj Premaratne & Manoj Fernando	01st May 2019
3.1	Updated by Manoj Fernando	01st Aug 2021
3.2	Updated by Manoj Fernando	27th Jul 2023
3.3	Updated by Manoj Fernando & Sajith Bandara	08th Apr 2024

DOCUMENT APPROVERS		
Name	**Designation**	**Signature**
Channa de Silva	CEO	Digitally signed by Channa de Silva Date: 2024.04.09 12:36:27 +05'30'

Submitted By

Name : Manoj Fernando

Designation : Chief Manager IT Security Solutions

Signature : Manoj Fernando Digitally signed by Manoj Fernando Date: 2024.04.08 09:00:26 +05'30'

Trademark Notices

The LankaSign logo and service trademarks are the properties of LankaPay (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 LankaPay (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 LankaPay (Pvt.) Ltd.) must be addressed to LankaSign, LankaPay (Pvt.) Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, Bank of Ceylon Mawatha, Colombo 00100. LankaSign Helpdesk. Tel: +9411 2356900 Fax: +94 11 2544346 E-mail: helpdesk@lankapay.net

1. Definitions

1. CA - Certification Authority is an entity appointed in terms of Chapter IV of the Electronic Transaction Act, No. 19 of 2006
2. CSP - Certification Service Provider is an entity which is approved to issue digital certificates under the Electronic Transaction Act, No.19 of 2006.
3. OCSP - Online Certificate Status Protocol
4. 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)
5. 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
6. Decryption - Refers to algorithmic schemes that decode non-readable or cipher text in to readable or plain text.
7. Encryption - Refers to algorithmic schemes that encode plain text into non-readable form or cipher text.
8. PKCS #10 -Public key standard which defines syntax for issuing server certificate requests.
9. PKCS#12- A file format for storing an encrypted key, certificate, and optionally the certificate chain. Private Key is required.
10. X.509 - Public key infrastructure certificate and CRL profile
11. NDES – Network Device Enrollment Service
12. 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.
13. 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.
14. Registrant/Applicant - The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate.
15. Signature Verifier is an entity or person that validates a certificate.
16. Policy Authority - Body established to oversee the creation and update of certificate policies, review certification practice statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.

17. Registration Authority (RA) - An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).
18. Repository - A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
19. Object identifiers - identifies the purpose to which the certificate is used. Email signing, client authentication, etc.

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 LankaPay (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.

2.1 Overview

- This CPS is applicable to all products and services provided through LankaSign CSP.

2.2 Role of the LankaSign CPS and Other Practices Documents

The CPS describes at a general level the overall business, legal, and technical infrastructure of LankaSign. This CPS then applies all standards from the CPS to LankaSign participants, and explains specific practices of LankaSign in response to the CPS. More specifically, the CPS describes, among other things:

1. Obligations of Certification Authorities, Registration Authorities, Subscribers within LankaSign domain.
2. Legal matters that are covered in LankaSign Digital Certificate Subscriber Agreement.
3. Audit practices & related security practices related to LankaSign
4. Methods used within LankaSign domain to confirm the identity of certificate applicants for each type of certificate.

5. Operational procedures for certificate lifecycle services undertaken in LankaSign Domain: Certificate applications, issuance, acceptance, revocation, and renewal.
6. Operational security procedures for audit logging, records retention, and disaster recovery used within LankaSign domain.
7. Physical, personnel, key management, and logical security practices of LankaSign domain.
8. Certificate and Certificate Revocation List content within LankaSign domain, and
9. Administration of the CPS, including methods of amending it. LankaSign may publish Certification Practice Statements that are supplemental to this CPS in order to comply with the specific policy requirements of Government, or other industry standards requirements.
10. These supplemental Certification Practice Statements shall be made available to subscribers and their Relying Parties for the certificates issued under the supplemental practice statements.
11. The CPS, however, is only one of a set of documents relevant to LankaSign domain and the other documents include:
    I. The Security and Audit Requirements Guide, which describes detailed requirements for LankaSign and Affiliates/Outsourced partners concerning personnel, physical, telecommunications, logical, and cryptographic key management security.
    II. Ancillary agreements imposed by LankaSign. These agreements would bind Subscribers, and Relying Parties of LankaSign. Among other things, the agreements may flow down to LankaSign CPS and, in some cases, state specific practices for how they must meet LankaSign Standards. In many instances, the CPS refers to these ancillary documents for specific, detailed practices implementing LankaSign Standards where including the specifics in the CPS could compromise the security of LankaSign domain.

Table 1: Provides relevant LankaSign practices documents and indicates the availability status.

Document	Status	Availability to the public
LankaSign Certificate Policy (CP)	Not Restricted	Yes
LankaSign Certification Practice Statement (CPS)	Not Restricted	Yes
Security and Audit Requirements Guide	Restricted	No

Documents available to the public can be obtained by writing to helpdesk@lankapay.net or referring to the LPPL website. Table 1: Types and Availability of Practices Documents

2.3 Specification of Administration Organization

The organization administering this CPS is the LankaSign Policy Authority (PA). Policy Authority is the body established to oversee the creation and update of certificate policies, review certification practice statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.

Composition of the Policy Authority (PA) would be as follows.

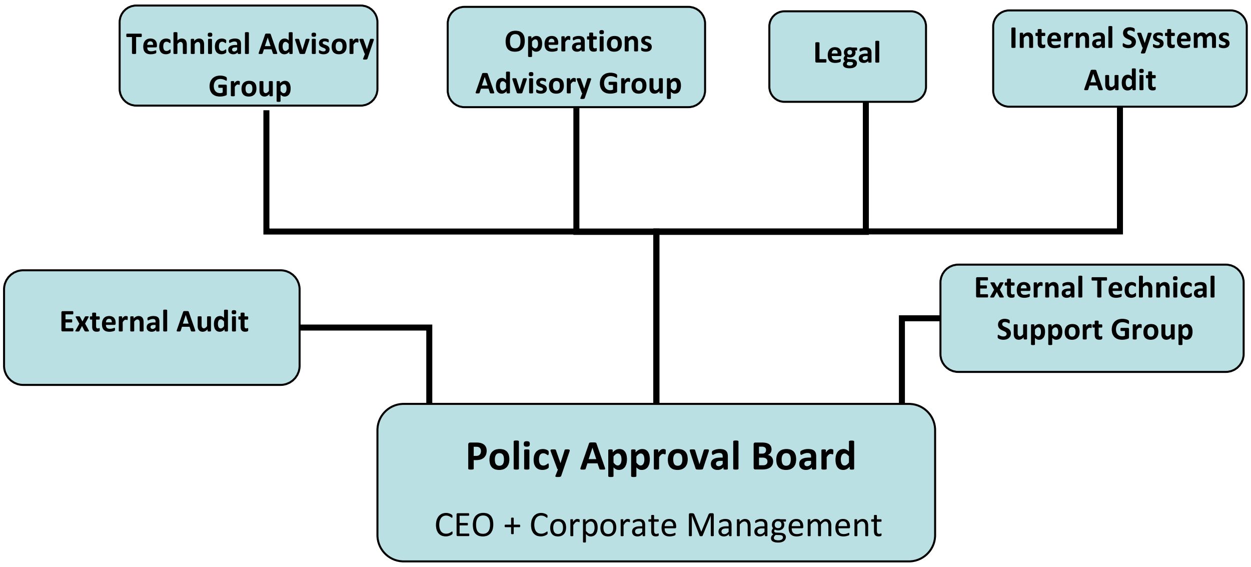

Figure 1: Composition of the Policy Authority (PA)

Obligations of Policy Authority

The Policy Authority shall make the determination that a CPS complies with the policy. The Policy Authority shall

- Approve the CPS for each CA that issues certificates under this policy;
- Review periodic self-assessments to ensure that CAs are operating in compliance with their approved CPSs;
- Revise this CP/CPS to maintain the level of assurance and operational practicality at least on an annual basis;
- Publicly distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs.

Inquiries to LankaSign Practices Development Group should be addressed as follows:

Chief Manager IT Security Solutions
LankaPay (Pvt.) Ltd.
Level 18, Bank of Ceylon Head Office
“BOC Square”, No. 01, Bank of Ceylon Mawatha

Colombo 00100
Sri Lanka
(+94) 11 2356900

2.4 Contact Person

Address inquiries about the CPS to helpdesk@lankapay.net or to the following address:

Chief Manager IT Security Solutions
LankaPay (Pvt.) Ltd.
Level 18, Bank of Ceylon Head Office,
“BOC Square”, No. 01, Bank of Ceylon Mawatha
Colombo 00100
Sri Lanka
(94) 11 2356900

3. Procedures and Practices

3.1 Certificate Application Procedure

All Certificate applicants must complete the application process, which includes

1. Completion of the LankaSign Digital Certificate Subscriber Agreement/Terms & Conditions. This is a service agreement that enrolls an individual or an organization to the LANKASIGN-CSP service and must be completed per individual/organization.
2. Completion of the appropriate LANKASIGN-CSP digital certificate application forms. This is a product request that must be completed per certificate request.
3. Provision of proof of identity and other authenticated/official documentation as requested by LANKASIGN-CSP during the certificate issuance process.
4. 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:
   a. 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.
   b. 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.
   c. 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.
5. 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.
   a. Certificate applications must be submitted to either LANKASIGN-CSP, LANKASIGN-CSP approved RA or LankaSign approved outsourced entity.
   b. 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 Certificate Application Validation

LANKASIGN-CSP or LankaSign CSP approved entity shall review the information provided by the applicant to determine that it is an accountable legal entity, whether an organization or an individual. This validation activity shall be done by requesting individual's or official company documentation.

LANKASIGN-CSP may modify the requirements related to application information for individuals or organizations from time to time, to respond to CSP operational requirements, the business context of the usage of a digital certificate, or as prescribed by law in Sri Lanka. LANKASIGN- CSP may accept or reject at its discretion documentation supporting an application. For issuance of certificates that involve Internet domain names, LANKASIGN-CSP shall verify the applicant's right to use the domain name indicated in the application form. The verification shall be done by reviewing domain name ownership records available publicly through Internet or approved local and global domain name registrars.

Verification may be supplemented through the use of the administrator contact associated with the domain name register record. On the issuance of a digital certificate, LANKASIGN-CSP shall assign a unique serial number to the certificate. For any type of digital certificate issued by LANKASIGN-CSP, the owner/user of the certificate has a continuous obligation to monitor the accuracy of the submitted information and notify LANKASIGN-CSP of any changes that would have an impact on the validity of the certificate. Failure to comply with the obligations as set out in the LankaSign Digital Certificate Subscriber Agreement will result in the revocation of the owner's/user's digital certificate without further notice to the owner/user and the owner shall pay any charges payable but that have not yet been paid under the agreement.

3.3 Certificate Application Rejection

If the verification of information pertaining to a certificate request application fails, LANKASIGN-CSP will reject the certificate application. Furthermore LANKASIGN-CSP reserves its right to reject applications to issue a certificate to applicants if, on its own assessment, by issuing a certificate to such parties the good and trusted name of LANKASIGN-CSP may be tarnished, diminished or have its value reduced and under such circumstances may reject the application without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal. However, applicants whose applications have been rejected may subsequently reapply with suitable rectification of noted failings as determined by LANKASIGN-CSP.

3.4 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:

1. 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.
2. 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:

   a. The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate.
   b. 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.
   c. 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 reasonable under the provisions made for the relying party under this CPS and within the LankaSign Digital Certificate Subscriber Agreement.

3.5 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:

There has been loss, theft, modification, unauthorized disclosure, change of authorized user /owner or other compromise of the private key associated with the certificate.

The owner/user of the certificate or LANKASIGN-CSP has breached a material obligation under this CPS.

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.

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.

There has been a modification of the information pertaining to the certificate owner/user that is contained within the certificate.

LANKASIGN-CSP has authority to revoke issued certificates immediately upon termination of agreement.

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 Prior to the revocation of a certificate, LANKASIGN-CSP will verify that the revocation request has been:

Made by the organization or individual entity that has made the certificate application.

Made by the RA on behalf of the organization or individual entity that used the RA to make the certificate application.

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.

3.6 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 digital certificate is with the certificate owner/user. The renewal request should be accompanied by the relevant digital certificate application form.

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 CSP Root Signing Key Protection and Recovery

Protection of the LANKASIGN-CSP root signing key pairs is ensured with the use of Thales nShield Edge Hardware Security Module (HSM) which is certified to FIPS-140-2 Level 3 (Federal Information Processing Standard) used to certify cryptographic modules. The LANKASIGN-CSP root signing key pairs are 4096-bit and were generated within the HSM. The HSM is protected by Admin Card (Smart Card) set created when installing Security World (THALES Software Agent). For LANKASIGN-CSP root key recovery purposes, the HSM configuration data is encrypted and stored in a physical media within a secure environment. The decryption password is maintained on a printed media and stored in a physically secure environment access to which requires two or more authorized officials of the LANKASIGN.

4.3 CSP Root Signing Key Generation Process

Generation of the LANKASIGN-CSP root signing key is ensured with the use of HSM which are certified to FIPS-140-2 Level 3. The LANKASIGN-CSP takes necessary precautions to prevent compromise or unauthorized usage of the key.

The LANKASIGN-CSP root key was generated in accordance with guidelines provided in the CPS and the entire process including the activities and the personnel involved were recorded for audit purposes.

4.4 CSP Root Signing Key Archival

When any LANKASIGN-CSP root signing certificate expires, key will be archived for at least 10 years. The keys will be archived in a secure physical media and stored in a physically secure environment access to which requires two or more authorized officials of the LANKASIGN. All key transfers will be done in encrypted format only.

4.5 Procedure for CSP Root Signing Key Changeover

The lifetime of LANKASIGN-CSP root signing keys is defined below. Towards the end of lifetime for each key, a new LANKASIGN-CSP signing key pair is created and all subsequently issued certificates and CRLs are signed with the new signing key. Therefore, both keys may be concurrently active for a period of time termed the changeover period.

4.6 Description Usage Lifetime Size

The defined lifetime of each certificate type is as below:

1. CSP Self signed Root Certificate for LankaPay Root Certificate Authority 15 years 4096 bit
2. CSP signed Intermediate Certificate for LankaPay Certificate Authority 12 years 2048 bit
3. Document Signing Certificate 05 years 2048 bit
4. Application Certificate 05 years 2048 bit
5. Mobile Certificates life time is set based on requirement

4.7 Description Usage Lifetime Size

All the LANKASIGN-CSP Root CA and Issuing CA certificates will be distributed along with the crypto tokens, email, and storage media or over the LankaSign official web site or SDK by LANKASIGN-CSP. LANKASIGN-CSP will provide technical assistance to its clients for embedding the CSP Root CA and Issuing CA certificates in applications.

4.8 Physical Security of CSP Operations

Access to the CSP operations center operated and managed by LANKASIGN-CSP is physically secured through a multi-layer access control mechanism including perimeter security external to facility, internal access to facilities, video monitoring, two-factor authenticated access to compartmentalized facilities using biometrics, etc. Access to the secure sections of the CSP operations center is only allowed for authorized personnel selected and verified through a documented process. All access to the secure sections of the CSP operations center are controlled with two-factor authentication using biometrics and all activities are monitored and logged. LANKASIGN-CSP has made reasonable efforts to ensure that the CSP operations center is protected from the incidents listed below with the help of LankaPay Data Center Protection System:

1. Fire and smoke damage
2. Flood and water damage
3. Malicious physical damage by intruders

LANKASIGN-CSP has made reasonable efforts to ensure that the CSP operations center is provided with primary and secondary power supplies, air conditioning and ventilation systems for reliable operation of its systems. LANKASIGN-CSP asserts that it makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities. LankaSign Security Clearances provide authorizations and security clearances related to LankaSign CSP.

4.9 Digital Certificate Management

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

1. Verification of the identity and other relevant details of an applicant (individual or organization) for issuance of a certificate
2. Authorizing the issuance of certificates
3. Issuance of certificates
4. Verification of the identity and other relevant details of an applicant (individual or organization) for revocation of a certificate
5. Revocation of certificates
6. Listing, distributing and publishing of certificates
7. Listing, distributing and publishing of CRLs
8. 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.

4.10 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 Document Signing and Application certificates.. LANKASIGN-CSP may update or extend its list of digital certificate products, including the types of certificates it issues, as it sees fit.

1. Document Signing Certificate - These are Document Signing 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.
2. Application Certificate – These are Digital Signature Certificates which allow to use signing through Application or Software. Developer or owner can user certificate without violate rules and regulations of LankaSign-CSP

4.11 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.

4.12 LANKASIGN-CSP Certificate Usage Profiles

LANKASIGN-CSP certificates include key usage extension fields to specify the purposes for which the certificate may be used and to technically limit the functionality of the certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of LANKASIGN-CSP. The possible key purposes identified by the X.509v3 standard are the following:

1. Digital signature, for verifying digital signatures that have purposes other than those identified in (2), (6) or (7), that is, for entity authentication and data origin authentication with integrity.
2. Non-repudiation, for verifying digital signatures used in providing a none-repudiation service which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in (6) or (7) below)
3. Key encipherment, for enciphering keys or other security information, e.g. For key transport.
4. Data encipherment, for enciphering user data, but not keys or other security information as in (c) above.
5. Key agreement is used when the sender and receiver of the public key need to derive the key without using encryption.
6. Key certificate signing, for verifying a CA's signature on certificates, used in CA certificates only
7. CRL signing, for verifying a CA's signature on CRLs.
8. Encipher only, public key agreement key for use only in enciphering data when used with key agreement.
9. Decipher only, public key agreement key for use only in deciphering data when used with key agreement

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, as described below. 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:

1. Terms and conditions of the digital certificate.
2. Any other applicable certificate policy as may be stated on an issued LANKASIGNCSP certificate, including the location of this CPS.
3. The mandatory elements of the standard X.509v3.
4. Any non-mandatory but customized elements of the standard X.509v3.
5. Content of extensions and enhanced naming that are not fully expressed within a certificate.
6. 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 & 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.

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 to the certificate owner/user. Failure to comply with this as a relying party will result in the termination of the agreement with the relying party, the removal of permission to use or access the LANKASIGN-CSP repositories and any digital certificates or services provided by LANKASIGN-CSP.

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 adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository as indicated under section 4.29 on Notices.

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:

1. To minimize internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
2. Provide correct and accurate information in its communications with LANKASIGN- CSP
3. 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.
4. 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.
5. 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.
6. Use LANKASIGN-CSP certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.
7. Cease using a LANKASIGN-CSP certificate if any information in it becomes misleading obsolete or invalid.
8. 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.
9. 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.
10. 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.
11. Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a LANKASIGN-CSP certificate.
12. 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:

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.

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

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

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.

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

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.

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.

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

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 Indemnity by Certificate Owner/User

The certificate owner/user agrees to indemnify and hold LANKASIGN-CSP and its certificate owners/users harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind that LANKASIGN-CSP, and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from:

1. Any false or misrepresented data supplied by the certificate owner/user.
2. Any failure of the certificate owner/user to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CSP, LANKASIGN-CSP, or any person receiving or relying on the certificate.
3. Failure to protect the certificate owner's/user's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the certificate owner's/user's confidential data.
4. Breach of any 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.

5.13 Obligations of LANKASIGN-CSP Registration Authorities

A LANKASIGN-CSP RA operates under the policies and practices detailed in this CPS and shall:

1. Receive applications for LANKASIGN-CSP certificates in accordance with this CPS.
2. Perform all verification actions prescribed by the LANKASIGN-CSP validation procedures and this CPS.
3. Receive, verify and relay to LANKASIGN-CSP all requests for revocation of a LANKASIGN-CSP certificate in accordance with the LANKASIGN-CSP revocation procedures and the CPS.
4. Comply with applicable laws and regulations.
5. Forward validated and verified certificate requests to CA for validation and issuance

5.14 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:

1. 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.
2. Study the limitations to the usage of digital certificates.
3. Read and agree with the terms of the LANKASIGN-CSP CPS and relying party Terms and Conditions.
4. 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.
5. Trust a LANKASIGN-CSP certificate only if it is valid and has not been revoked or has expired.
6. Rely on a LANKASIGN-CSP certificate, only as may be reasonable under the circumstances listed in this clause and other relevant clauses of this CPS.
7. Relying Party cannot hold LPPL liable for any certificate related matter including validation.

5.15 Legality of Information

Certificate owners/users shall solely be responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed. Without limiting other certificate owner/user obligations stated in this CPS, certificate owners/users are liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein..

5.16 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. LANKASIGN-CSP, however, cannot accept any liability beyond the limits set in this CPS under section 4.18 on 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.

5.17 Obligations of LANKASIGN-CSP

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

1. Comply with this CPS and its internal or published policies and procedures.
2. Comply with applicable laws and regulations.
3. 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.
4. Provide trust mechanisms, including a key generation mechanism and key protection regarding its own infrastructure.
5. Provide prompt notice in case of compromise of its private key(s).
6. Provide and validate application procedures for the various types of certificates that it may make publicly available.
7. Issue digital certificates in accordance with this CPS and fulfill its obligations presented herein.
8. Publish accepted certificates in accordance with this CPS.
9. Provide support to certificate owners /users and relying parties as described in this CPS.
10. Revoke certificates according to this CPS.
11. Provide for the expiration and renewal of certificates according to this CPS.
12. Make available a supplemental copy of this CPS and applicable policies to requesting

5.18 Damage and Limitations

LANKASIGN - CSP disclaims all warranties and obligations of any type, including any parties. warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and cannot be excluded

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 non-performance of certificates or digital signatures. LANKASIGN-CSP does not limit or exclude liability for death or personal injury.

5.19 Conflict of Rules

When this CPS conflicts with other rules, guidelines, or contracts, the latest version of this CPS as made available under section 4.29 on Notices, shall prevail and bind the certificate owner/user and other parties except as to other contracts either:

1. Predating the first public release of the present version of this CPS.
2. Expressly superseding this CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

5.20 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.

5.21 Infringement and Other Damaging Material

LANKASIGN-CSP clients represent and warrant that when submitting to LANKASIGNCSP 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.

5.22 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 LANKASIGNCSP 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.

5.23 Governing Law and Jurisdiction

This CPS is governed by, and construed in accordance with the law of the Democratic Socialist Republic of Sri Lanka. The provision of the law shall apply to all LANKASIGNCSP commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to LANKASIGN-CSP products and services where LANKASIGNCSP acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including LANKASIGN-CSP relying parties, irrevocably agrees that the courts of the Democratic Socialist Republic of Sri Lanka have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CPS or the provision of LANKASIGN-CSP PKI services.

5.24 Dispute Resolution

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution, parties agree to notify LANKASIGN- CSP of the dispute with a view to seek dispute resolution.

5.25 Successors and Assigns

This CPS shall be binding upon the successors and assigns, whether express or implied of the parties.

5.26 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.

5.27 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.

5.28 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.

5.29 No Waiver

This CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this CPS shall not be deemed a waiver of future enforcement of that or any other provision.

5.30 Notices

LANKASIGN-CSP accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from LANKASIGN-CSP, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within seven (7) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via registered mail addressed as follows:

Chief Manager IT Security Solutions
LankaPay (Pvt.) Ltd.
Level 18, Bank of Ceylon Head Office,
“BOC Square”, No. 01, Bank of Ceylon Mawatha
Colombo 00100
Sri Lanka
(94) 11 2356900
http://www.lankapay.net
Email: helpdesk@lankapay.net

5.31 Fees

LANKASIGN-CSP charges fees for the certificate services provided to its clients for issuance, renewal and reissue of certificates. LANKASIGN-CSP shall not charge fees for the revocation of certificates or for the provision of certificate status verification services for LANKASIGN- CSP issued certificates including OCSP Responder Systems and CRLs. Upon the issuance or renew al of a certificate, LANKASIGN-CSP shall not refund the payments made.

5.32 Reissue

During a 14 day period beginning from the time a certificate is issued, certificate owners may request to reissue their certificates without incurring additional charges. The reissue may be requested for the purpose of amendment of information provided in the certificate application procedure and LANKASIGN-CSP shall strictly follow the certificate application validation procedure for the certificate reissue. If the reissue request does not pass the validation process, LANKASIGN-CSP reserves the right to refuse the reissue of certificate and revoke the original certificate without a refund.