LANKASIGN CERTIFICATION SERVICE PROVIDER

CERTIFICATE POLICY

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	UPDATES	DATE
1.0	Created by Chandana Gamage & Thilina Wijewicrema	09th May 2009
2.0	Updated by Dileepa Lathsara & Duleep Liyanage	01st Nov 2012
2.1	Updated by Dileepa Lathsara & Duleep Liyanage	01st Apr 2013
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 April 2024

DOCUMENT APPROVERS		
Name	**Designation**	**Signature**
Channa de Silva	CEO	Digitally signed by Channa de Silva Date: 2024.04.09 12:36:51 +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 08:59:43 +05'30'

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.
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. 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.
9. Registrant/Applicant - The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate.
10. Signature Verifier - is an entity or person that validates a certificate.
11. 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. The Policy Authority shall make the determination that a CPS complies with the policy.
12. 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).
13. Repository - A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
14. Object identifiers - identifies the purpose to which the certificate is used. Email signing, client authentication, etc.

2. Introduction

This document describes the Certificate Policy (CP) of the LankaPay (Pvt) Ltd Certification Service Provider (LANKASIGN-CSP). This includes the policy requirements related to the life cycles of the data handled at each stage which consists of user applications, certificates, physical and environment security controls, certification revocation lists, audits and securing personal and confidential information of organizations and users.

3. Registrants

Registrants are entities / users requesting to register with LANKASIGN-CSP by signing LankaSign Digital Certificate Subscriber Agreement/Terms & Conditions in order to obtain digital certificates. The approved subscribers should be able to prove their identity with the additional information requested by LANKASIGN-CSP and LANKASIGN-CSP should be able to verify such information with the relevant organizations.

3.1 Responsibilities of the Registrants (prior to issuing certificates)

1. Key pair generation should be done using a trustworthy system
2. Accurate information should be provided to the LANKASIGN-CSP Registration Authority.
3. LANKASIGN-CSP should be informed immediately in case of private key loss / compromise or in the event of a change of the authorized user, if issued to an organization

3.2 Responsibilities of the certificate owners

1. Registrants should not share the private keys with other parties
2. Registrants should take reasonable mechanisms to protect their private keys
3. Registrants should use the LANKASIGN-CSP certificates for the acceptable use only.
4. Certificates issued by LANKASIGN-CSP should be used in accordance with all applicable laws and should not be used for illegal or purposes which includes but is not limited to:
    - Control equipment in hazardous circumstances
    - For uses requiring highly reliable performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems
    - Weapons control systems, where failure could lead directly to death, personal injury
    - Which will cause severe environmental damage
    - Malicious activities like distribution of viruses, etc
    - Obtain the identity of other individuals or entities
    - Publish discriminating material
5. Registrants should adhere to LANKASIGN-CSP rules and policy guidelines

3.3 Responsibility of the Relying Parties

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.

Relying parties should;

1. Read and follow the guidelines in the LANKASIGN-CSP Certificate Policy (CP) and Certificate Practice Statement (CPS)
2. Use the certificates for acceptable use only
3. Not accept authorization attributes based solely on LANKASIGN-CSP issued certificates
4. Verify the validity of the certificates using expiry date, up to date certificate revocation list (CRL) and from the OCSP (Online Certificate Status Protocol) service
5. Not rely on the certificate or other revoked certificates in the certificate chain if a certificate is revoked

4. Certificate Application Rejection

The Certificate Application should be rejected if RA (Registration Authority) confirms that;

1. The applicant does not have the private key corresponding to the public key to be included in the certificate. Or
2. The information provided by the subscriber is not verifiable or incorrect.
3. The applicant has filed for insolvency or winding up of the organization, found guilty of a civil or criminal offence in a court of law, of unsound mind or a minor.

5. Certificate Revocation

LANKASIGN-CSP shall revoke the certificates if;

1. A valid request for revocation is submitted.
2. The information supplied is misleading.
3. The owner/user has failed to comply with the rules in the CP and CPS or misuse of the digital certificate by the subscriber.
4. The entity to which the certificate has been issued has ceased to exist.
5. The signature algorithm needs to be changed because the old algorithm is less secure.
6. Compromise of the CSP security system or the root key occurs.
7. The key size needs to be increased to protect against advances in cryptanalysis and the increasing amount of computer power available to an attacker.
8. If the CSP thinks that the digital certificate should be suspended in public interest.

9. A legal or government demand is received.

6. Certificate Information Dissemination by CSP

1. Ensure that the CSP certificates (public keys of LANKASIGN-CSP) are distributed by the below means;
    a) Publish on the LANKASIGN-CSP official web site.
    b) Include in third-party software which has agreements with LANKASIGN-CSP
2. The information related to the LANKASIGN-CSP should be updated regularly.
3. A new certificate revocation list (CRL) should be published every 8 hours. (CRL Publish Interval 8hrs)
4. LANKASIGN-CSP OCSP service should be up-to-date and accurate.
5. CRLs and OCSP Servers should be updated immediately in case of a serious key compromise.

7. Privacy of Personal/Business Information collected by CSP

1. Minimum amount of personal information should be collected by LANKASIGN-CSP that is necessary for the purposes and not more than that.
2. The information provided by the subscribers should be shared if requested by the governmental agencies.
3. All the information should be collected by fair and lawful means.
4. Security safeguards should be in place to protect the subscribers' personal and business related information in a manner appropriate to its sensitivity.
5. All the customer information should be stored securely.
6. All the confidential personal/business information should be communicated if necessary using secure encryption methodologies.
7. Subscribers personal/business information should not be used for any purpose other than the purposes specified at time of collection, or without the prior consent from the owner.
8. Subscribers' personal/business information should not be sold or otherwise distributed to any third party.
9. Accuracy of subscribers' personal/business information should be maintained in a highly accurate manner, and at any time subscribers have the right to inform LANKASIGN-CSP and update personal/business information.

8. Maintaining Security

CSP needs to be well secured and it should follow firm policies and procedures to maintain its security. CSP infrastructure should be capable of maintaining the Confidentiality, Integrity and Availability (CIA) features and it should be operated in a physically well-secured environment as described below.

8.1 Physical Security

1. All the critical systems of the LANKASIGN-CSP should be kept inside the CSP server room with dual layer access control system.
2. All the staff should use their biometric authentication to enter in to the LANKASIGN-CSP server room.
3. No outside personnel will be allowed to enter in to the LANKASIGN-CSP server room without being accompanied by an authorized person from LPPL.
4. Guidelines on LankaSign Security Clearances should be followed.
5. All the access to the LANKASIGN-CSP server room should be logged.
6. Paper based documents with confidential information like application forms, documents provided by the subscribers and the other documents containing confidential information of the CSP should be kept in a well secured place at LANKASIGN-CSP.

8.2 Technical Security

1. The root certificate key of the CSP should be used only for the signing of intermediate CSP certificates.
2. It should be performed under the supervision of CIO and DCEO or CEO.
3. The intermediate CA certificate should be used to sign subscriber certificates or revocation lists.
4. No removable media or devices should exist on the operating online systems.
5. Removals of any device from the LANKASIGN-CSP systems are strictly prohibited and must be authorized by the LPPL CEO.
6. All the systems should be monitored regularly for intrusion and compromise of the system.

9. Vulnerability Assessment

Comprehensive vulnerability assessments which include all the systems in the LANKASIGN-CSP network should be performed on a quarterly basis

10. Backups

1. The CSP private signing key generation data should be backed up and stored in a well secured environment.
2. Root signing key should be recovered only by at least three key custodian holders in the presence of CEO and DCEO with the approval of LPPL director Board in a physically secured environment.
3. Backup copies of the CSP private signing key generation data should be subject to the same or greater level of security controls as keys currently in use.
4. When the keys are stored in a dedicated key processing hardware module, access controls should be in place to ensure that the keys are not accessible outside the hardware module.
5. All the CSP systems should be replicated to a high availability system real time.
6. At least one set of backup should be kept in an offsite location before a major change in addition to the real time replication.
7. All the backup data should have the same level of security as the main operational systems.

11. Disposal

1. Paper bases documents should be disposed using a shredder.
2. Any removed device should be fully wiped out of data before disposal.

12. Power

1. All the systems in the LANKASIGN-CSP network should have UPS power backup, and
2. the critical systems which need 24X7 availability like information dissemination system or the OCSP Responder should be connected to external, electricity power generator in case of power breakdown.

13. Maintenance

Any of the systems handed over to the service providers for maintenance work should be fully wiped out of data before such hand over.