LANKACLEAR

Certification Service Provider

Summary Certificate Policy

Version 3.1

LankaClear (Pvt.) Ltd

Document Control

1.	Document Title	LANKACLEAR Certification Service Provider Summary Certificate Policy
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	Document Superseded	V3.0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: 2021.08.09 09:02:36 +05'30'

Document History

Version #	Date Applicable	Author / Owner	Notes (If any)
1.0	9th May 2009	Chandana Gamage & Thilina Wijewicrema	
2.0	1st Nov 2012	Dileepa Lathsara & Duleep Liyanage	Corrected by NOM and GM / CEO

2.1	1st April 2013	Dileepa Lathsara & Duleep Liyanage	Corrected by DGM and GM / CEO
3.0	01st May 2019	Viraj Premaratne & Manoj Fernando	Reviewed by Sanjeevani Seneviratne
3.1	01st Aug 2021	Manoj Fernando	Reviewed by Policy Authority

Table of Contents

1 Definitions 6
2 Introduction 8
3 Registrants 8
3.1 Responsibilities of the Registrants (prior to issuing certificates) 8
3.2 Responsibilities of the certificate owners 8
3.3 Responsibility of the Relying Parties 9
4 Certificate Application Rejection 9
5 Certificate Revocation 10
6 Certificate Information Dissemination by CSP 10
7 Privacy of Personal/Business Information collected by CSP 11
8 Maintaining Security 11
8.1 Physical Security 11
8.2 Technical Security 12

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) **Decryption** - Refers to algorithmic schemes that decode non-readable or cipher text in to readable or plain text.

g) **Encryption** - Refers to algorithmic schemes that encode plain text into nonreadable form or cipher text.

h) **PKCS #10** - Public key standard which defines syntax for issuing server certificate requests.

i) **PKCS#12** - A file format for storing an encrypted key, certificate, and optionally the certificate chain. Private Key is required.

j) **X.509** - Public key infrastructure certificate and CRL profile

k) **NDES** - Network Device Enrollment Service

l) **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.

m) **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.

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

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

p) **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.

r) **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).

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.

2 Introduction

This document describes the Certificate Policy (CP) of the LankaClear (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 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)

i. Key pair generation should be done using a trustworthy system

ii. Accurate information should be provided to the LANKASIGN-CSP Registration Authority

iii. 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

I. Registrants should not share the private keys with other parties

II. Registrants should take reasonable mechanisms to protect their private keys

III. Registrants should use the LANKASIGN-CSP certificates for the acceptable use only.

IV. 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

V. 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;

i. Read and follow the guidelines in the LANKASIGN-CSP Certificate Policy (CP) and Certificate Practice Statement (CPS)

ii. Use the certificates for acceptable use only

iii. Not accept authorization attributes based solely on LANKASIGN-CSP issued certificates

iv. 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

v. 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;

i. The applicant does not have the private key corresponding to the public key to be included in the certificate. Or

ii. The information provided by the subscriber is not verifiable or incorrect.

iii. The applicant has filed for insolvency or winding up of the organisation, 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;

i. A valid request for revocation is submitted.

ii. The information supplied is misleading.

iii. The owner/user has failed to comply with the rules in the CP and CPS or misuse of the digital certificate by the subscriber.

iv. The entity to which the certificate has been issued has ceased to exist.

v. The signature algorithm needs to be changed because the old algorithm is less secure.

vi. Compromise of the CSP security system or the root key occurs.

vii. The key size needs to be increased to protect against advances in cryptanalysis and the increasing amount of computer power available to an attacker. viii. If the CSP thinks that the digital certificate should be suspended in public interest.

ix. A legal or government demand is received.

6 Certificate Information Dissemination by CSP

i. 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

ii. The information related to the LANKASIGN-CSP should be updated regularly.

iii. A new certificate revocation list (CRL) should be published every 8 hours.

iv. LANKASIGN-CSP OCSP service should be up-to-date and accurate.

v. CRLs and OCSP Servers should be updated immediately in case of a serious key compromise.

7 Privacy of Personal/Business Information collected by CSP

i. Minimum amount of personal information should be collected by LANKASIGN-CSP that is necessary for the purposes and not more than that.
ii. The information provided by the subscribers should be shared if requested by the governmental agencies.
iii. All the information should be collected by fair and lawful means.
iv. Security safeguards should be in place to protect the subscribers' personal and business related information in a manner appropriate to its sensitivity.
v. All the customer information should be stored securely.
vi. All the confidential personal/business information should be communicated if necessary using secure encryption methodologies.
vii. 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. viii. Subscribers' personal/business information should not be sold or otherwise distributed to any third party.
ix. 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

i. All the critical systems of the LANKASIGN-CSP should be kept inside the CSP server room with dual layer access control system.
ii. All the staff should use their biometric authentication to enter in to the LANKASIGN-CSP server room.
iii. No outside personnel will be allowed to enter in to the LANKASIGN-CSP server room without being accompanied by an authorized person from LCPL.
Authorization will be done by GM/CEO or DGM – IT & Ops.

iv. All the access to the LANKASIGN-CSP server room should be logged.

v. 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

i. The root certificate key of the CSP should be used only for the signing of intermediate CSP certificates.

ii. It should be performed under the supervision of AGM and DGM – Operations or GM/CEO.

iii. The intermediate CA certificate should be used to sign subscriber certificates or revocation lists.

iv. No removable media or devices should exist on the operating online systems.

v. Removals of any device from the LANKASIGN-CSP systems are strictly prohibited and must be authorized by the LCPL CEO.

vi. All the systems should be monitored regularly for intrusion and compromise of the system.