CLASSIFICATION : PUBLIC

LANKASIGN CERTIFICATION PRACTICE STATEMENT (CPS)

IN COMPLIANCE WITH NATIONAL CERTIFICATION AUTHORITY (NCA) OF SRI LANKA

Version	**: 1.1**
Issue Date	**: 04th January 2024**
Issued By	**: LankaPay (Private) Limited**

Your Trusted
Payment Network

Document Control

No	Type of Information	Document Data
1	Document Title	LankaSign Certification Practice Statement (CPS)
2	Date of Release	04th January 2024
3	Version No.	V1.1
4	Document Superseded	V1.0
5	Document Owner	Policy Authority
6	Document Author	Manager IT

Approval from Policy Authority (PA) members:

No.	Approver	Designation	Signature
1	Channa de Silva	Chief Executive Officer (CEO)	Digitally signed by Channa de Silva Date: 2024.01.05 15:53:39 +05'30'
2	Dinuka Perera	Deputy Chief Executive Officer (DCEO)	Digitally signed by Dinuka Perera Date: 2024.01.05 12:12:48 +05'30'
3	Dilantha Samarasinghe	Chief Information Officer (CIO)	Digitally signed by D_Samarasinghe Date: 2024.01.05 11:46:03 +05'30'
4	Chamath Algawatte	Chief Information Security Officer (CISO)	Digitally signed by Chamath Algawatta Date: 2024.01.05 11:07:08 +05'30'
5	Prabhash Wisidagama	Asst. Manager – Risk and Compliance	Prabhash Wisidagama Digitally signed by Prabhash Wisidagama Date: 2024.01.05 10:23:22 +05'30'

Document Revision History

Version No	Date Applicable	Author / Owner	Notes (If any)
0.1	13th February 2023	Dinuka Perera, Chief Operating Officer (COO)	Yet to be reviewed by Policy Authority
1.0	17th July 2023	Thusha Mukunthan (Chief Delivery Officer) & Lakshanth Jayasekera (Manager-IT)	Incorporated changes proposed by the web trust auditor
1.1	04th January 2024	Lakshanth Jayasekera (Manager-IT) Malan Mendis (Project Manager)	Incorporated changes after the key ceremony

Trademark Notices

The LankaSign logo and service trademarks are the properties of LankaPay (Pvt.) Ltd. 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.

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. Helpdesk. Tel: +9411 2356900 Fax: +94 11 2544346 E-mail: helpdesk@lankapay.net

Table of Contents

1. Definitions

The following definitions are to be used while reading this CPS. Unless otherwise specified, the words “LankaSign CA” or “LankaSign CSP” or “CA” used throughout this document refers to LankaSign Sub CA, likewise CPS means CPS of LankaSign CA. Words and expressions used herein and not defined but defined in Electronic Transactions Act, No. 19 of 2006 and subsequent amendments, hereafter referred to as the ACT shall have the meaning respectively assigned to them in the Act.

The following terms bear the meanings assigned to them hereunder and such definitions are applicable to both the singular and plural forms of such terms:

a) CA - Certification Authority is an entity appointed by the National Certification Authority (NCA)

b) ETA - Electronic Transaction Act, No. 19 of 2006

c) DPA – Data Protection Act 09 of 2022

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

e) OCSP - Online Certificate Status Protocol

f) 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)

g) 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.

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

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

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

k) Subscriber - Once a digital certificate is issued, the legal entity is referred to as the subscriber. A natural person or a legal entity to whom a digital certificate is issued and who is legally bound by a subscriber agreement or terms of use is referred as a subscriber.

l) 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.

m) Applicant - The natural person or legal entity that applies for (or seeks renewal of) a certificate.

n) Signature verifier - An entity or person that validates a certificate.

o) 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.

p) Registration Authority (RA) - An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (ie a registration authority is delegated certain tasks on behalf of an authorized CA).

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

r) Object identifiers - Identifies the purpose to which the certificate is used. Email signing, client authentication etc.

2 Introduction

LankaSign Certification Practice Statement (CPS) states the practices that LankaSign Certification Service Provider (CSP) provides that include, but not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the LankaSign CSP. LankaSign CSP is a provider of trusted infrastructure services to websites, enterprises, electronic commerce service providers, and individuals. The entity'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 and providing associated trust services. This applies to all stakeholders of LankaSign and thereby provides assurances of uniform trust throughout LankaSign trusted network.

The term "LankaSign CA", "LankaSign CSP", "LankaSign", "Certification Authority" or CA as used in this CPS, refers to LankaSign subCA as the entity that holds the CA license from the National Certification Authority (NCA) of Sri Lanka. NCA PKI is a hierarchical PKI with the trust chain starting from the Root Certifying Authority of NCA. NCA is operated by Sri Lanka CERT (SLCERT) of Government of Sri Lanka. Under the NCA, there are Certification Authorities (CAs) licensed by NCA to issue Digital Signature Certificates (DSCs) under the provisions of Electronic Transactions Act. LankaSign CA is a licensed CA under NCA.

2.1 Overview

NCA defines certificate policies to facilitate interoperability among subscribers and relying parties for e-commerce and e-governance in Sri Lanka. The CP and Certification Authorities (CAs) are governed by the NCA. The Certification Practice Statement (CPS) of LankaSign CA details the practices and operational procedures implemented to meet the assurance requirements in compliance with the CP of NCA. This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement framework. NCA issues license to operate as Certification Authority subject to successful compliance audit of CA of NCA and as per the CPS of LankaSign. The CPS is also

i. intended to be applicable to and is a legally binding document between the CA, the subscribers, the applicants, the relying parties, employees and contractors; and
ii. intended to serve as notice to all parties within the context of the CA CPS

CPS refers to the various requirements specified under the following guidelines issued by NCA.

i. The identity verification guidelines: For the identity verification for different types of certificates like personal, organizational person, SSL, encryption, code signing, system certificate etc.
ii. Interoperability guidelines for certificate profile including content and format of the certificates, key usage, extended key usage etc.
iii. Adherence to assurance class, certificate policy ID, validity of certificates, key size, algorithm, storage requirements, audit parameters etc.
iv. Guidelines for Issuance of SSL Certificates: Additional requirements for the issuance of SSL certificates.
v. Authentication guidelines: The security procedures for key generation, key protection and audit logs, signature format, identity verification requirements etc.
vi. Security Requirements for Crypto Devices: The crypto device (secure token) management and security requirements for holding subscribers' private key.
vii. CA site specification: Physical security requirements of the CA site.

2.2 Identification

The contact details are mentioned in section 2.5.2 of this CPS. The following are the levels of assurance defined in the Certificate Policy. Each level of assurance has an OID that can be asserted in certificates issued by CA if the certificate issuance meets the requirements for that assurance level. The OIDs which are registered for Class 3 certificates is 2.16.144.1.1.1.5. The LankaSign CA will only offer Class 3 certificates.

The OIDs allocated to CA and CPS are as given below:

Serial No.	Product	OID
1	LankaSign Certification Authority	2.16.144.1.1.1
2	LankaSign CA CPS	2.16.144.1.1.1.2

2.3 PKI Participants

2.3.1 PKI Authorities

2.3.1.1 National Certification Authority (NCA)

In the context of the CPS, the NCA is responsible for:

1. Developing and administering national certification policy (CP).
2. Compliance analysis and approval of the licensed CAs CPS.
3. Laying down guidelines for identity verification, interoperability of digital signature certificates and private key storage.
4. Ensuring continued conformance of licensed CAs with the NCA CP and their own CPS by examining compliance audit results.

2.3.1.2 Certification Authority (CA)

The LankaSign CA is licensed by NCA as per Electronic Transaction Act. The primary function of CA is to issue end entity certificates. LankaSign CA certificates are certified by NCA. In the PKI hierarchy, root certificate is the trust anchor for CA certificates. The following are the CA certificates issued to CA.

SI Number	CA Name	Certified By
1	LankaSign Certification Authority	NCA

LankaSign CA issues digital signature certificates to end entities directly. CA also suspends or revokes the digital signature certificates. The CA maintains the Certificate Revocation List (CRL) for the revoked and suspended digital signature certificates in its repository. CRL is signed by issuing CA.

2.3.2 PKI services

1. Certificate Services: CA issues class 3 documents singing certificates. The category of certificates includes individual and organisational personnel. The certificates are issued subjected to the verification requirements specified under NCA.

2. CRL Services: Certificate Authority makes available CRL on the http://rsa-cdp.lankasign.net:8092/cdp/LankaSign%20RSA%20Certification%20Authority.crl which can be crosschecked by subscribers and relying parties when checking for the validity of digital signatures.

3. OCSP (Online Certificate Status Protocol) Validation Services: CA provides OCSP validation services to relying parties for certificate status verification in real time. The OCSP service of the CA is operated as per NCA guidelines.

4. Online digital signature services: CA offers online digital signature service via third party application service providers (ASPs) for subscribers to use LankaSign digital signatures for via Android and iOS powered devices. The users of Application Service Provider (ASP) interface with the Sub CA for obtaining digital signatures. ASPs are certified by LankaSign CA after a verification process. CA verifies the source of request and authenticates users for each certificate request received from ASP before issuing a certificate. Certificates are electronically verified to ensure that all the fields and extensions are properly populated.

5. Document signing certificates (DSCs): LankaSign CA is also provides document signing signatures or DSCs. The DSCs are issued to applicants for the purpose of document signing and provided via physical secure tokens. Identity of the applicants are verified through a 'know-your-customer' (KYC) process.

2.3.3 Registration Authority (RA)

RA is an entity engaged by CA to collect DSC application forms (along with supporting documents) and to facilitate verification of subscriber credentials. RA interacts with the CA and submits the applicant's request for certificate issuance to CA.

2.3.4. Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate.

2.3.5. Relying parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed document, message, or to identify the creator of a message. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

2.3.6. Applicability

LankaSign issues class 3 digital signature certificates (DSCs) which are the most secure and safest form of a certificate. Its applications are derived where security and safety of the data are the most essential factors. DSCs are issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for document signing and digital transactions, they are issued to individuals after a rigorous verification process.

2.4 Certificate Usage

2.4.1 Appropriate certificate uses

Certificate usage is governed by the Electronic Transaction Act (ETA) and interoperability guidelines published by NCA.

2.4.2 Prohibited certificate uses

Certificate usage is governed by the Electronic Transaction Act (ETA) and interoperability guidelines published by NCA.

2.5 Policy Administration

2.5.1 Organisation administering the document

This CPS is administered by LankaSign CA and is revised with the approval of NCA.

2.5.2 Contact person

Questions/Queries regarding this CPS may be directed to the CA at helpdest@lankapay.net
LankaSign CA can be contacted at the following address:

Manager – IT
LankaPay Private Limited
Level 18, Bank of Ceylon Head Office
"BOC Square"
No. 01, Bank of Ceylon Mawatha
Colombo 00100
Sri Lanka
Contact No : (94) 11 2356900

2.5.3 Person determining certification practice statement suitability for the policy

The entity 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.

The determination of suitability of the CPS will be based on LankaSign's Policy Authority. LankaSign Policy Authority will review the CPS annually for suitability as well as whenever the changes are made to the CPS.

Composition of the Policy Authority would be as follows:

1. CEO of LankaPay
2. Deputy Chief Executive Officer (DCEO)of LankaPay
3. Chief Information Security Officer of LankaPay
4. Chief Information Officer (CIO) of LankaPay
5. Compliance Officer of LankaPay

2.5.4 CPS approval process

LankaSign Policy Authority will first review and approve the CPS to ensure that the CPS is compliant and consistent with the Certificate Policy of the NCA.

2.5.5 Waivers

There will not be any waivers to this CPS.

3. Publication and PKI repository responsibilities

3.1 PKI repositories

CA maintains Hypertext Transfer Protocol (HTTP) based repositories that contain the following information:

1. NCA Certificates
   a) Issued to their Sub CAs
2. Certificate Revocation List (CRL)
   b) Issued by the CA
3. Digital Signature Certificates (DSCs) issued by CA

LankaSign publishes details of its own certificate as well as all other operational related information on its website. The location for the information is listed in the table below:

Information	Location
Certificate Practice Statement	https://www.lankapay.net/knowledge-center/lankasign/
LankaSign certificate	https://www.lankapay.net/knowledge-center/lankasign/
CRL	CDP http://rsa-cdp.lankasign.net:8092/cdp/LankaSign %20RSA%20Certification%20Authority.crl AIA http://rsa-aia.lankasign.net:8091/aia/RSA-SUBCA.lankasign.net_LankaSign%20RSA%20Certification%20Authority.crt
OCSP responder location	http://rsa-ocsp.lankasign.net:8093/ocsp

3.1.1 Repository obligations

LankaSign CA maintains a repository and is available at https://www.lankapay.net/knowledge-center/lankasign/

3.2 Publication of repository information

3.2.1 Publication of CA information

LankaSign CA related information including certification revocation lists (CRLs) are available in a publicly accessible repository. LankaSign CA publishes its CPS, Subscriber Agreements, and Relying Party agreements at https://www.lankapay.net/knowledge-center/lankasign The CPS include all the material required by RFC 3647, and are structured in accordance with RFC 3647. LankaSign CA shall ensure its commitment to the latest baseline requirements. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

4. Identification and authentication

The requirements for identification and authentication are specified under Electronic Transaction Act, rules and guidelines issued there under. Before issuing a certificate, the LankaSign CA ensures that all subject information in the certificate conforms to the requirements that has been verified in accordance with the procedures prescribed in this CPS.

4.1 Naming

4.1.1 Types of names

LankaSign CA issues certificates containing an X.500 Distinguished Name (DN) in the Issuer and Subject fields. The subject name appearing on the X.509 certificate is the name of the LankaSign CSP in the form of an X.500 distinguished name. The structure of the distinguished name is shown in the table below:

Attribute Names	Values (NCA)	Values (CSP)
Country (C)	LK	LK
Organisation (O)	Sri Lanka CERT	LankaPay (Private) Limited
Common Name (CN)	National Certification Authority of Sri Lanka	LankaSign Certification Authority

Subscriber certificate names:

Attribute Names	Values (CSP)
Common Name (CN)	Subscriber’s name
Organisational Unit (OU)	Subscriber’s designation
Organisation (O)	Subscriber’s organisation name
Country (C)	Subscriber’s residence/business country

4.1.2 Need for names to be meaningful

The subject name will be in English and will have a reasonable association with the authenticated information of the CSP.

The certificates issued pursuant to this CPS will take care of the following:

i. Names used in the certificates identify the person or object to which they assigned in a meaningful way.
ii. The DNs and associated directory information tree reflect organizational structures.
iii. The common name represents the subscriber in a way that is easily understandable by humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process.

4.1.3 Anonymity of subscribers

LankaSign CA does not issue subscriber certificates for anonymous or pseudonymous identities.

4.1.4 Rules for interpreting various name forms

Distinguished names in certificates are interpreted using X.500 standards and ASN.1 syntax. Refer to RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

4.1.5 Uniqueness of names

The subject name or a combination of the subject name and other data fields listed in a certificate would be unambiguous and unique for all certificates issued by the LankaSign CA. If necessary, additional characters may be appended to the authenticated common name to ensure the name’s uniqueness within the domain name of certificates issued by the LankaSign CA.

Name uniqueness for interoperability or trustworthiness is enforced in association with serial number or unique identifier.

4.1.6 Recognition, authentication and role of trademarks

LankaSign would not provide certificates to subscribers with content that infringes on the intellectual property rights of another entity.

4.1.7 Name claim dispute resolution procedure

LankaSign CA will resolve any name conflicts (in association with serial number or unique identifier) brought to its attention that may affect interoperability or trustworthiness.

4.2 Initial identity validation

4.2.1 Method to prove possession of private key

In all cases where the DSC subscriber named in a certificate generates his or her own key, the subscriber is required to prove possession of the private key, which corresponds to the public key in the certificate request. This is performed by the DSC subscriber using its private key to sign a value and providing that value to the issuing CA. The CA then validates the signature using the DSC subscriber’s public key.

4.2.2 Authentication of organization user identity

Requests for certificates in the name of an organizational user are mandated to include the username, organization name and address, and documentation providing the existence of the organization. Subscribers should follow the instructions given in https://www.lankapay.net/knowledge-center/lankasign/ under ‘Instructions for filling forms’ when submitting applications.

LankaSign Registration Authority (RA) verifies the authenticity of the information given by the subscribers through a rigorous process. The below table explains how the Individual applications are processed in that regard.

Table – Verification process

Sub fields in the Subject field of the Certificate	Actual Name	Existing verification process	Proposed verification process
OU	User Designation	User designation is verified by the application form	The verification process confirms the user's designation by means of an application form, wherein an authorized approving officer of the entity has endorsed the information provided
CN	User Name	The Username is verified by NIC & Application Form	The Username is verified by the National Identity Card/Passport/Driving License issued by the relevant government agency. In addition, photograph of the user will be taken during the video conference with the user and LankaPay agent.
O	Company Name	The name of the company is Verified by the Certificate of Incorporation	The name of the company is confirmed by the certificate of incorporation issued by the department of the registrar of companies. Company registration can also be verified through eROC online system.
C	Country	Country is verified by NIC/Passport	Country is verified by National Identity Card/Passport/ Driving License.

If a company is requesting digital signatures, company should submit the company registration issued by the Registrar of Companies of Sri Lanka in addition to the information required for the individuals as in above table. Further, the individual requesting the certificates on behalf of the company should have the delegated authority to request such certificates. Delegation of authority should be proven via a Board resolution. If a government entity is requesting digital signatures, the head of the government entity should sign the requests and the establishment of the government entity should be proven via acts or relevant regulations, where applicable.

4.2.3 Authentication of individual identity

LankaSign CA follows a comprehensive process for verifying an applicant's identity. The process documentation and authentication requirements include the following:

i. The applicant should submit a duly completed application (consisting of the fields required as per the Table -Verification process in section 4.2.2) which should be signed by the applicant using a handwritten signature or equivalent as acceptable under the Sri Lankan law.

ii. The applicant should submit the National Identity Card (NIC). This NIC will be verified against the Department of Persons Registrations portal for additional authenticity.

4.2.3.1 Authentication of component identities

LankaSign CA does not issue certificates for requests made by human sponsors for computing and communications components (routers, firewalls, servers etc.), which are named as the certificate subject.

4.2.4 Non-verified subscriber information

LankaSign CA does not include non-verified information provided by applicants in certificates.

4.2.5 Validation of authority

Certificates that contain explicit or implicit organizational affiliation are issued only after ascertaining the applicant has the authorization to act on behalf of the organization in the asserted capacity.

4.2.6 Criteria for interoperability

Certificates are issued as per the guidelines given by the National Certification Authority (NCA) of Sri Lanka in order to ensure interoperability.

4.3 Identification and authentication of re-key requests

4.3.1 Identification and authentication for routine re-key

The subscribers do not have to undergo fresh identity-proofing process for the period for which the certificate has been issued. The maximum time for which initial identity-proofing can be relied upon for issuance of fresh certificate is as per the table below:

Assurance level	Initial identity proofing
Class 3	Five years

4.3.2 Identification and authentication for re-key after revocation

If a certificate has been revoked, LankaSign CA issues a fresh certificate to the applicant only after the following the registration process described in section '4.2.3 Authentication of identity' to issue a new certificate. With the revocation of the certificate Lankasign team inform the subscriber confirming the revocation of the certificate.

4.4 Identification and authentication for revocation

Revocation requests are authenticated in the following manner.

1. Electronic requests to revoke a certificate authenticated using that certificate's associated public key, regardless of whether or not the private key has been compromised.

2. In case the possession of the key is not with the subscriber, suspend/revoke the certificate after verifying the subscriber's identity.

3. In the case where the subscriber is not in a position to communicate (death, unconscious state, mental disorder), revoke the certificate after verification.

4. In the case of a court order or a request made by a law enforcement authority.

5. Certificate life-cycle operational requirements

Communication among the LankaSign CA, RA, and subscriber are implemented with requisite security services (ie source authentication, integrity, non-repudiation, and confidentiality). Such security services applied to them commensurate with the assurance level of the certificate being managed. Confidentiality of the documents submitted by the applicants, whether as physical documents or scanned images of the documents securely stored to meet integrity and confidentiality requirements.

5.1 Certificate requests

All applicants must complete the application process, which include:

a) Completion of the LankaSign digital certificate subscriber agreement. This is a service agreement that is signed between an individual or an organisation and LankaSign CSP.

b) Completion of the relevant application form based on the digital certificate that is required by the applicant. Provision of proof of identity and other authenticated/official documentation as requested by LankaSign CSP during the certificate issuance process.

The applicant intending to obtain the digital signature from LankaSign CA need to submit the subscriber agreement, duly completed relevant application form with duly attested supporting documents to LankaSign CA. On receipt of the request and information in the prescribed format, LankaSign CA carries out the verification of documents and video and mobile number verification if applicable.

A signed declaration by the person performing the identity verification is recorded on the application form or in the system to record that he or she verified the identity of the applicant. Upon the approval of the application request, a digital signature is issued to the applicant.

5.1.1 Submission of certificate application

The applicant is required to submit the duly filled application form along with the supporting documents to registration authority (RA). The application forms for various types of certificates are available to be downloaded from the LankaPay website at https://www.lankapay.net/knowledge-center/lankasign/

5.1.2 Enrolment process and responsibilities

For certificates, all end-user applicants undergo an enrolment process consisting of:

1. Completing and submitting a certificate application form and providing the required information,
2. Generating a key pair.
3. Delivering his/ her, or its public key to CA
4. Demonstrating to CA that the certificate applicant has possession of the private key corresponding to the public key delivered to CA.
5. Manifesting assent to the relevant subscriber agreement.

5.2 Certificate application processing

LankaSign CA verifies the information in certificate applications for their accuracy based on the attested supporting documents, telephonic interaction, video verification if necessary and other procedures.

5.2.1. Performing identification and authentication functions

See Section 4.2 and subsections thereof.

5.2.2. Approval or rejection of certificate applications

Certificate applications submitted to the LankaSign CA for processing could result in either approval or denial.

5.2.3. Time to process applications for digital certificates

If the required information is stated in the certificate applications submitted to the LankaSign CA for processing and is duly signed where there are no discrepancies, a certificate would be issued within three (03) working days. However, if an application is incomplete, the potential subscriber needs to resubmit the application.

5.3 Certificate issuance

After a certificate applicant submits a certificate application, LankaSign CA confirms or refutes the information in the certificate application. Upon successful confirmation based on all required authentication procedures for various classes of certificates, forwards the certificate application for approval. The applicant's request for certificate issuance is reviewed by a trusted person which may result in approval or denial of certificate.

5.3.1 CA actions during certificate issuance

LankaSign CA verifies the source of a certificate request before issuance. If crypto medium is opted for the key generation and storage, the details such as make, model, serial no etc are also recorded. Certificates are checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, LankaSign CA publishes the certificate in the repository.

5.3.2 Notice to subscriber of certificate issuance

LankaSign CA will notify the subscriber of certificate issuance through email/SMS and internet link.

5.4 Certificate acceptance

5.4.1 Conduct constituting certificate acceptance

The applicant must confirm acceptance of the certificate upon notification of issuance by the LankaSign CA. Notification and link are sent to subscriber for downloading the certificate or it would be issued in a security token. Downloading the certificate or taking custody of the security token constitutes the subscriber's acceptance of the certificate.

5.4.2 Publication of the certificate by the CA

See Section 3 and sub sections thereof.

5.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

5.5 Key pair and certificate usage

5.5.1 Subscriber private key and certificate usage

Subscribers are liable to protect their private keys from access by any other party. For individual signature certificates, subscribers are required to generate key pair in FIPS 140-2 level 2 crypto devices.

Subscribers are also required to use their private keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies etc.) in the certificates issued to them.

5.5.2 Relying party public key and certificate usage

Relying parties are required to use public key certificates and associated public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies etc.) in the certificates.

5.6 Certificate renewal

Renewing a certificate means creating a new certificate with the same name and other information as the old one, but a new, extended validity period and a new serial number. Certificates are renewed by LankaSign CA only if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the subscriber name and attributes are unchanged.

5.6.1 Circumstances for certificate renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the subscriber's name and other attributes are unchanged.

5.6.2 Who may request renewal

In the normal scenario, a subscriber may request the renewal of his/her certificate. An organization who has obtained certificates for its staff or customers may also request renewal of certificates.

5.6.3 Processing certificate renewal requests

In the normal scenario, a certificate renewal will be using one of the following processes:

1. Initial registration process as described in Section '4.2.3 Authentication of identity'; or
2. Identification and Authentication for Re-key as described in Section 4.3, except the old key can also be used as the new key.

5.6.4 Notification of new certificate issuance to subscriber

See section 5.3.2.

5.6.5 Conduct constituting acceptance of a renewal certificate

See section 5.4.1.

5.6.6 Publication of the renewal certificate by the CA

See Section 3 and sub sections thereof.

5.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

5.7 Certificate re-key

Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

5.7.1 Circumstance for certificate re-key

LankaSign CA issues a new certificate to the subscriber when the subscriber has generated a new key pair and is entitled for a certificate subjected to the requirements set forth by NCA.

5.7.2 Who may request certification of a new public key

A subscriber may request the re-key of its certificate. A PKI Sponsor may request re-key of component certificate.

5.7.3 Processing certificate re-keying requests

A certificate re-key shall be achieved using one of the following processes:

1. Initial registration process as described in Section 5.1; or
2. Identification and authentication for re-key as described in Section 4.3.

5.7.4 Notification of new certificate issuance to subscriber

See Section 4.3

5.7.5 Conduct constituting acceptance of a re-keyed certificate

See Section 5.4.1

5.7.6 Publication of the re-keyed certificate by the CA

See Section 3.2

5.7.7 Notification of certificate issuance by the CA to other entities

No stipulation

5.8 Certificate modification

Modifying a certificate means creating a new certificate for the same subject with authenticated information that differs slightly from the old certificate (ie changes to email address or nonessential parts of names or attributes) provided that the modification otherwise complies with this CPS. The new certificate may have the same or a different subject public key.

5.8.1 Circumstance for certificate modification

Subscribers can request for modifications in certificates if the details of his or her certificate has changed such as the email address and/or the organization person works for.

5.8.2 Who may request certificate modification

Individual subscriber, or the company or the government organization with the approval of the duly authorized person to request such modifications can request for modifications in certificates.

5.8.3 Processing modification requests

LankaSign RA will process the modification requests. If the required information is in order, a modification request would be completed within three (03) working days.

5.8.4 Notification of new certificate issuance to subscriber

LankaSign RA will inform the subscribers of the new certificate issuance once the modification to a certificate is completed via an email or by phone.

5.8.5 Conduct constituting acceptance of modified certificate

LankaSign CA will incorporate the modified information to the digital certificate.

5.8.6 Publication of modified certificate by the CA

LankaSign CA will publicize the modified certificate.

5.8.7 Notification of certificate issuance by the CA to other entities

LankaSign CA will notify the other entities of the certificate issuance once the modifications are done to a certificate.

5.9 Certificate revocation and suspension

LankaSign CA authenticates the request for revocation prior to revocation. Subscribers are required to submit revocation requests as specified in the guidelines. Electronic requests to revoke a certificate have to be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised. Requests for suspension of certificates are not practiced.

5.9.1 Circumstance for revocation of a certificate

A certificate is revoked when the binding between the subscriber and the subscriber’s public key defined within a certificate is no longer considered valid. Some of the circumstances that invalidate the binding are:

- Identifying information or affiliation components of any name(s) in the certificate become invalid;
- The subscriber can be shown to have violated the stipulations of its agreement with CA;
- The private key is suspected of compromise; or
- The subscriber or other authorized party (CPS) asks for the subscriber’s certificate to be revoked.
- Private key is lost
- Subscriber is not in a position to use certificate (Death – copy of Death certificate made available to CA)
- As per a court order or an order made by a law enforcement authority
- If a mistake has been made by the CA when creating the certificate

Whenever any of the above circumstances occur, LankaSign CA revokes the certificate and places it on the CRL. Revoked certificates are included on all new publications of the certificate status information until the certificates expire. LankaSign CA ensures that the revoked certificate will appear on at least one CRL.

5.9.2 Who can request revocation of a certificate

A subscriber, a supervisor of a subscriber (for organizational user), human resources (HR) person for the subscriber (for organizational user), PKI Sponsor for component, or CA, may request revocation of a certificate.

5.9.3 Procedure for revocation request

A revocation should be submitted by filling the 'LankaSign digital certificate renew/revocation' form which is available in https://www.lankapay.net/knowledge-center/lankasign/. The duly completed form with the authorized signature can be submitted to LankaSign CA via email, in person or through courier service.

LankaSign CA identifies the certificate to be revoked as mentioned in the request for revocation, the reason for revocation, and verifies the authentication requirements (ie digitally or manually signed by the subject). LankaSign CA may perform telephonic verification and video verification to ensure the identity of the requester. Upon receipt of a revocation request, LankaSign CA authenticates the request and then revokes the certificate.

5.9.4 Revocation request grace period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

5.9.5 Time within which CA must process the revocation request

LankaSign CA make best efforts to process revocation request so that it is posted in the next CRL unless a revocation request is received and approved within two hours of next CRL generation.

5.9.6 Revocation checking requirements for relying parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the relying party. If it is temporarily infeasible to obtain revocation information, then the relying party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

5.9.7 CRL issuance frequency

LankaSign CA issues CRLs periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. LankaSign CA ensures that superseded certificate status information is removed from the PKI Repository upon posting of the latest certificate status information. CA publishes CRLs not later than the next scheduled update.
LankaSign CA issue CRLs at least once every 9 hours with minimum validity of 7 days. In addition, LankaSign CA issues CRLs and posts the CRL immediately if a certificate is revoked for the reason of LankaSign CA key compromise.

5.9.8 Maximum latency for CRLs

LankaSign CA publishes CRLs immediately after generation. Furthermore, each CRL will be published no later than the time specified in the 'nextUpdate' field of the previously issued CRL. CAs issue CRLs at least once every 9 hours, and the 'nextUpdate' time in the CRL may be no later than 7 days after issuance time (ie the 'thisUpdate' time).

5.9.9 Online revocation checking availability

LankaSign CA supports on-line certificate status checking. Client software using on-line certificate status checking need not obtain or process CRLs.

5.9.10 Online revocation checking requirements

No stipulation.

5.9.11 Other forms of revocation advertisements available

Other than implementation of CRLs and on-line revocation status, no other forms of on-line revocation status will be provided by LankaSign CA.

5.9.11.1 Checking requirements for other forms of revocation advertisements

Not applicable.

5.9.11.2 Special requirements related to key compromise

None beyond those stipulated in Section 5.9

5.9.12 Circumstance for suspension

Suspension of certificates are not practiced.

5.9.13 Who can request suspension

LankaSign CA does not allow suspension requests at the moment.

5.9.14 Procedure for suspension request

LankaSign CA does not allow suspension requests at the moment.

5.9.15 Limits on suspension period

LankaSign CA does not allow suspension requests at the moment.

5.10 Certificate status services

5.10.1 Operational characteristics

LankaSign CA provides both CRL and OCSP to obtain status of digital certificates.

5.10.2 Service availability

CRL and OCSP will be available 24x7x365 to obtain status of digital certificates except for the downtimes which will be announced in advance for scheduled maintenance activities.

5.10.3 Optional features

No stipulation.

5.11 End of subscription

A digital certificate issued by the LankaSign CA will reach the end of its subscription when the certificate reaches the end of its validity period or is revoked.

5.12 Key Escrow and recovery

5.12.1 Key Escrow and recovery policy and practices

Under no circumstances end entity signature key will be escrowed by a third-party.

5.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

6. Facility management and operational controls

Access to the LankaSign CA operations center operated and managed by LankaPay 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 CA operations center is only allowed for authorized personnel selected and verified through a documented process. All access to the secure sections of the LankaSign CA operations center are controlled with two-factor authentication using biometrics and all activities are monitored and logged. LankaSign CA 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:

a) Fire and smoke damage
b) Flood and water damage
c) Malicious physical damage by intruders

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

6.1 Physical controls

LankaSign CA operation premises are actively monitored with redundant power and notification methods. Sensitive areas within the facility, such as power and network connection are also controlled within the protected facility. The operation site has multiple tiers of security enforced through Photo ID badges, proximity cards and biometric access devices. All visitors are escorted by trusted persons and every visitor signs the visitor’s log. The facility is continually staffed (24x7), either by trusted persons or by an on-site maintenance service personnel during non-business hours.

6.1.1 Site location and construction

The system components and operation of LankaSign CA are contained within a physically protected environment to deter, detect and prevent unauthorized use of, access to, or disclosure of sensitive information. The physical security standards are modelled as per the physical and operational security guidelines stipulated by NCA. LankaSign CA's primary site consists of five physical security tiers comprising of:

- Tier 1: The common area in the vicinity of the CA operations set-up where in physical access check is performed. This is the area where common facilities are incorporated. The receiving and dispatch are carried out in this area. This area enforces physical proximity access control restricting entries only to authorized personnel. Any non-pre-authorized personnel is always escorted beyond this tier.

- Tier 2: This is the first level where CA operations commence. Enables two factor authentications (biometrics and physical proximity).

- Tier 3+ (onwards):

    - Enables two factor authentications (biometrics and physical proximity). The receiving and dispatch are carried out in this area.

    - Trusted personnel perform continuous monitoring, maintenance or support to CA facility and to the software/hardware running in it. This is where Certificate issuance and revocation is done.

    - Subsequent tiers are where the core CA operations are housed. Servers are installed in this area.

    - The internal tier is the place which houses the certificate manager server. The key ceremony is also done here. The HSM module is housed in this area. This is secured with multi-person access control.

6.1.2 Physical access

6.1.2.1 LankaSign CA physical access

LankaSign CA has implemented mechanism to protect equipment from unauthorized access. The physical security requirements laid down for the LankaSign CA equipment are:

a. No unauthorized access to the hardware is permitted.
b. All removable media and paper containing sensitive plain-text information is stored in secure containers.
c. All entry/exits are monitored either manually or electronically.
d. Access logs are maintained and inspected periodically.
e. Multiple layers of increasing security are provided in areas such as perimeter, building, and CA room.
f. Two-person physical access controls are required to both the cryptographic module and computer system for CAs issuing Class 3 certificates.

6.1.3 Power and air conditioning

LankaSign CA’s secure facilities are equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power and also these secure facilities are equipped with air conditioning systems to control temperature and relative humidity.

PKI repositories are provided with uninterrupted power sufficient for a minimum of 24 hours operation in the absence of commercial power, to support continuity of operations.

6.1.4 Water exposures

LankaSign CA locations are reasonably protected against floods and other damaging exposure to water.

6.1.5 Fire Prevention and protection

LankaSign CA facility is equipped to prevent and extinguish fires. Appropriate procedures have also been implemented to minimize the damage due to smoke and fire exposure. These measures also meet all applicable fire safety regulations.

6.1.6 Media storage

All media containing production software and data, audit, archive, or backup information are stored within CA facilities and also in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access only authorized personnel and protect such media from accidental damage (ie water, fire, and electromagnetic exposure).

6.1.7 Waste disposal

Sensitive documents and material are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroed in accordance with the manufacturer's guidance prior to disposal. Other waste is disposed of in accordance with the LankaSign CA's normal waste disposal requirements.

6.1.8 Off-site backup

Real time replication is performed for LankaSign CA servers where data is replicated between Primary and Disaster Recovery (DR) sites. In addition, back-up of the Primary virtual servers and DR virtual servers are taken once a day and stored in a separate storage. The data is properly secured based on the classification of data, which is defined by the Certifying Authority in the security policy.

6.2 Procedural controls

6.2.1 Trusted roles

LankaSign CA ensures that:

a) The person filling the role is trustworthy and properly trained.

b) The functions are distributed among more than one person, so that any malicious activity would require collusion.

CA operations are carried out by four roles which are listed below:

a) CA administrator – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate keys runnel for section system communication.

b) CA officer – authorized to verify and approve certificates or certificate revocations.

c) Audit administrator – authorized to view and maintain audit logs.

d) System administrator – authorized to perform system backup and recovery.

The following sections define these and other trusted roles.

6.2.1.1 CA Administrator

The administrator is responsible for:

a) Installation, configuration, and maintenance of the CA;
b) Establishing and maintaining CA system accounts;
c) Configuring certificate profiles or templates and audit parameters, and;
d) Generating and backing up CA keys.
e) Administrators shall not issue certificates to subscribers.

6.2.1.2 CA Officer

The CA officer is responsible for issuing certificates, that is:

a) Registering new subscribers and requesting the issuance of certificates;
b) Verifying the identity of subscribers and accuracy of information included in certificates;
c) Approving and executing the issuance of certificates, and;
d) Requesting, approving and executing the revocation of certificates.

6.2.1.3 Audit Administrator

The Audit Administrator is responsible for:

a) Reviewing, maintaining, and archiving audit logs;
b) Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS;

6.2.1.4 System Administrator

The System Administrator is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

6.2.1.5 Organizational registration authority

For organizational RA, the responsibilities are:

a) Verifying organizational identity of the applicant.
b) Entering applicant's information, and verifying correctness;
c) Securely communicating requests and responses from/to the CA;

The roles of RAs engaged by CAs are limited only to the collection of DSC application form and supporting documents and facilitation of issuance of DSC to applicants.

6.2.1.6 PKI Sponsor

A PKI sponsor fills the role of a subscriber for non-human system components (routers, servers, firewalls etc.) that are named as public key certificate subjects. However, LankaSign CA does not issue certificates for non-human components.

6.2.2 Number of persons required per task

Separate individuals are identified for each trusted role to ensure the integrity of the CA operations. Two or more persons are required to perform the following tasks for CAs that issue Class 3 certificates:

I. CA key generation;
II. CA signing key activation; and
III. CA private key backup.

In addition, sensitive CA operations like operations of the cryptographic units and certificate manager requires the m-out-of-n control to handle the operations of these sensitive functions. Also, split control is implemented to ensure segregations between physical and logical access to systems. Personnel having secret shares do not have physical access and vice-versa. All roles are assigned to multiple persons in order to support continuity of operations.

6.2.3 Identification and authentication for each role

All personnel seeking to become trusted persons are required to be in the payroll of CA. Thorough background checks are carried out prior to engaging such personnel for CA operations. The Certifying Authority follow the procedures approved by management for the background check and there are documented for audit purpose. CA ensures that personnel have achieved trusted status and approval has been given before such personnel are:

- Issued access devices and granted access to the required facilities
- Issued electronic credentials to access and perform specific functions on LankaSign CA's IT systems.

6.2.4 Roles Requiring Separation of Duties

6.2.4.1 Class 1, Class 2 and Class 3

Role separation is enforced either by the CA equipment, or procedurally, or by both means. Individuals may assume more than one role, except:

1. Individuals who assume an Officer role will not assume CA Administrator or Audit Administrator role;
2. Individuals who assume an Audit Administrator role will not assume any other role on the CA; and
3. Under no circumstances any of the four roles will perform its own compliance audit function.

No individual will be assigned more than one identity.

6.3 Personnel controls

6.3.1 Qualifications, experience, and clearance requirements

All personnel filling trusted roles shall be selected on the basis of trustworthiness, and integrity, and shall be subject to background investigation. Personnel will be appointed to trusted roles (CA trusted roles) on the basis of:

1. Having successfully completed an appropriate training program;
2. Having demonstrated the ability to perform their duties;
3. Being trustworthy;
4. Having no other duties that would interfere or conflict with their duties for the trusted role;
5. Having not been previously relieved of duties for reasons of negligence or non-performance of duties;
6. Having not been denied a security clearance, or had a security clearance revoked for cause;
7. Having not been convicted of an offense; and
8. Being appointed in writing by an appointing authority.

6.3.2 Background check procedures

All persons filling trusted roles (including LankaSign CA trusted roles trusted roles) shall have completed a favorable background investigation. The scope of the background check shall include the following areas covering the past five years:

1. Employment;
2. Education (regardless of the date of award, the highest educational degree shall be verified);
3. Place of residence (3 years);
4. Law Enforcement; and
5. References

The background will be verified once a year.

6.3.3 Training requirements

LankaSign CA ensures that all personnel performing duties with respect to the operation of a CA receive comprehensive training. Training will be conducted in the following areas:

1. CA security principles and mechanisms
2. All PKI software versions in use on the CA system
3. All PKI duties they are expected to perform
4. Disaster recovery and business continuity procedures.
5. Subscriber verification requirements

6.3.4 Retraining frequency and requirements

Training (awareness) is conducted to make the trusted personnel aware of any significant change to the operations, and the executions of such plan are documented. Such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment. Periodic security awareness and any new technology changes training is provided on an ongoing basis, based on the newer versions or releases of the products.

6.3.5 Job rotation frequency and sequence

No stipulation.

6.3.6 Sanctions for unauthorized actions

LankaSign CA will take appropriate administrative and disciplinary actions against personnel who violate this policy. Action taken will be documented.

6.3.7 Independent contractor requirements

All contractors who require access to the LankaSign CA secure facilities, must be always escorted and supervised by at least one personnel from the LankaSign CA trusted role. For system maintenance purposes, the contractor must present their employees identification card and their national identification card to personnel from the LankaSign CA trusted role.

6.3.8 Documentation supplied to personnel

All the relevant documents relating to CA operation required for trusted personnel to perform their duties such as Certificate Policy, the applicable CPS, verification guidelines, user manuals, administrator manual, policies or contracts etc are made available to LankaSign CA personnel. LankaSign CA maintains the documents identifying all personnel who received training and the level of training completed.

6.4 Audit logging procedures

Audit log files are generated for all events relating to the security of the LankaSign CA. The security audit logs are either automatically collected or if not possible, a logbook, paper form, or other physical mechanisms are used. All security audits logs, both electronic and non-electronic, are retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained.

6.4.1 Types of events recorded

All security auditing capabilities of the LankaSign CA operating system and the CA applications required by this CPS are enabled. Each audit record shall include the following (either recorded automatically or manually for each auditable event):

1. The type of event,
2. The date and time the event occurred,
3. Success or failure where appropriate, and
4. The identity of the entity and/or operator that caused the event.

The following events will be audited:

1. Security audit
2. Identity proofing
3. Local data entry
4. Remote data entry
5. Data export and output
6. Key generation
7. Private key load and storage
8. Trusted public key entry, deletion and storage
9. Private and secret key export

10. Certificate registration
11. Certificate revocation
12. Certificate status change approval
13. Configuration
14. Account administration
15. Certificate profile management
16. Certificate status provider management
17. Revocation profile management
18. Certificate revocation list profile management
19. Configuration changes
20. Physical access / site security
21. Anomalies

6.4.2 Frequency of processing audit logs

Audit logs are examined for key security and operational events at least on a weekly basis. In addition, LankaSign CA reviews its audit logs as required in the event of any suspicious or unusual activity based on irregularities and incidents within CA systems. The processing of audit logs includes a review of the audit logs and recording of significant events in an audit log summary. It includes a verification that the log has not been tampered with, a brief inspection of all log entries, and a detailed investigation of any irregularities in the logs. Actions taken based on audit log reviews are recorded.

6.4.3 Retention period for audit logs

Audit logs will be retained for a period of two years.

6.4.4 Protection of audit logs

System configuration and procedures are implemented together to ensure that:

1. Only authorized people have read access to the logs;
2. Only authorized people may archive audit logs; and,
3. Audit logs are not modified.

After back-up and archived, the audit logs are allowed by the system to be over-written.

6.4.5 Audit log backup procedures

Audit logs and audit summaries shall be archived as per Section 6.4.3.

6.4.6 Audit collection system (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by CA personnel. Audit processes are invoked at system start-up, and cease only at system shutdown. In the case of failure of audit collection system, CA operations are suspended until the problem is remedied.

6.4.7 Notification to event-causing subject

This CPS imposes no requirement to provide notice (that an event was audited) to the individual, organization, device, or application that caused the event.

6.4.8 Vulnerability assessments

Events in the audit log are recorded, in part, to monitor system vulnerabilities. A vulnerability assessment is performed, reviewed, and revised following an examination of these monitored events. Vulnerability assessments are conducted quarterly.

6.5 Records archival

6.5.1 Types of records archived

LankaSign CA retains an archive of information and actions that are material to each certificate application and to the creation, issuance, revocation, expiration, and renewal of each certificate issued by the LankaSign CA. These records include all relevant evidence regarding:

Data to be archived
Certification Practice Statement
Contractual obligations
System and equipment configuration
Modifications and updates to system or configuration
Certificate requests
Revocation requests
Subscriber identity authentication data as per Section
Documentation of receipt and acceptance of certificates
Documentation of receipt of Tokens
All certificates issued or published
Record of Component CA Re-key
All CRLs and CRLs issued and/or published
All Audit Logs
All Audit Log Summaries
Other data or applications to verify archive contents
Compliance audit reports

6.5.2 Retention period for archive

Records associated with certificates are archived for a period of 6 years from the date of expiry of the certificate.

6.5.3 Protection of archive

LankaSign CA protects its archived records so that only authorized persons can access the archived data. LankaSign CA protects the archive against unauthorized viewing, modification, deletion, or other tampering, by storage within a trustworthy system. The media holding the archive data and the systems required to process the archive data are maintained to ensure that the archive data can be accessed for the time period.

6.5.4 Archive backup procedures

LankaSign CA creates back-up copies of archives compiled as and when the archives are created. Backup copies of the archive and copies of paper-based records are maintained in an off-site disaster recovery/ warehouse facility. LankaSign CA has implemented a process to scan and digitize the physical documents to ensure tracking and easy retrieval.

6.5.5 Requirements for time-stamping of records

Archived records are time stamped such that order of events can be determined. Certificates, CRLs, other revocation databases and usage entries contain time and date information provided by system time, which is synchronized with standard Sri Lanka time (GMT+5:30).

6.5.6 Archive collection system (internal or external)

The archive collection system is internal to the LankaSign CA.

6.5.7 Procedures to obtain and verify archive information

Only LankaSign CA's trusted personnel are permitted to access the archived data. Additionally, the archive information may be made available to the NCA upon request.

6.6 Key changeover

LankaSign CA keys are changed periodically as stipulated by the NCA and the key changes are processed as per key generation specified in this CPS. If LankaSign CA private key is used to sign CRLs, then the key shall be retained and protected. LankaSign CA provides reasonable notice to the subscribers' relying parties of any change to a new key pair used by CA to sign digital certificates under its trust hierarchy. The subscribers are issued digital certificates for a specified period of time. The subscribers generate a new private-public key pair and submit the public key along with the new application to the CA for generating a new certificate, preferably before the existing certificate expires. The following table provides the lifetimes for certificates and associated private keys.

Key	4096 Bit Keys	
	Private Key	Certificate
Sub-CA	8 years	8 years
OCSP Responder	3 years	3 years
Key	2048 Bit Keys	
Subscriber Certificate (LPPL Document Signing)	5 years	5 years

6.7 Compromise and disaster recovery

6.7.1 Incident and compromise handling procedures

If LankaSign CA detects a potential hacking attempt or other form of compromise, it will perform an investigation in order to determine the nature and the degree of damage. If the LankaSign CA key is suspected of compromise, the procedures outlined shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the LankaSign CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised. LankaSign CA will inform NCA if any of the following cases occur:

1. Suspected or detected compromise of the LankaSign CA system;
2. Physical or electronic attempts to penetrate the LankaSign CA system;
3. Denial of service attacks on the LankaSign CA system; or
4. Any incident preventing LankaSign CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL. LankaSign CA will make all efforts to restore capability to issue CRL as quickly as possible.

6.7.2 Computing resources, software, and/or data are corrupted

LankaSign CA has a disaster recovery center. The disaster recovery site will be made operational using the real time replicated data.

If LankaSign CA equipment is damaged or rendered inoperative, but the signature keys are not destroyed, LankaSign CA will make all efforts to establish the operation as quickly as possible, giving priority to the ability to generate CRL or make use of disaster recovery facility for CRL generation. If both primary and disaster recovery sites cannot be used to establish revocation capability in a reasonable time-frame, LankaSign CA may request for revocation of its certificate(s) to NCA.

6.7.3 Private key compromise procedures

If LankaSign CA signature keys are compromised, lost, or suspected to be compromised: NCA shall be notified at the earliest possible time so that NCA can revoke the LankaSign CA certificate.

6.7.4 Business continuity capabilities after a disaster

In the case of a disaster whereby LankaSign CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, LankaSign CA shall request that its certificates be revoked. The CA shall follow steps 1 through 4 given below:

i. CA key pair shall be generated by LankaSign CA in accordance with procedures set forth in this applicable CPS;
ii. New CA certificates shall be requested in accordance with the initial registration process set elsewhere in this CPS;
iii. If the LankaSign CA can obtain accurate information on the certificates it has issued and that are still valid (ie not expired or revoked), LankaSign CA may re-issue (ie renew) those certificates until the expiry date of the original certificates; and
iv. The LankaSign CA shall also investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

6.8 CA termination

In the event of termination of LankaSign CA, LankaSign CA will revoke all certificates issued. LankaSign CA will archive all audit logs and other records prior to termination. LankaSign CA will destroy all its private keys upon termination.

7. Technical security controls

7.1 Key pair generation and installation

7.1.1 Key pair generation

The following table provides the requirements for key pair generation for the various entities.

Entity	FIPS 140-2 Level	Hardware or Software	Generated in Entity Module
CA	3	Hardware	Yes
Time Stamp Authority	3	Hardware	Yes
OCSP Responder	3	Hardware	Yes
RA	2	Hardware	Yes
Subscriber Signature	2 for Class 3	Hardware for Class 3	Yes

Multiparty controls are used by LankaSign CA for key pair generation. LankaSign CA creates a verifiable audit trail for CA key pair generation as well as the subscriber key that LankaSign generates on behalf of the subscriber as per the security requirement procedures which are followed and the same will be documented. The process is validated by an auditor.

7.1.2 Private key delivery to subscriber

Subscriber private key is generated by the LankaSign CA into the hardware based secure token (ie HSM module of the secure token) prior to delivery of the secure token to the subscriber. These pre-formatted hardware based secure tokens are sent to the subscribers and the associated PIN (ie password) is sent by an out-of-band process. Subscriber is advised to change the default PIN prior to using the document signing certificates.

7.1.3 Public key delivery to certificate issuer

End user subscribers generate a PKCS#10 request containing their public key and send it to the LankaSign CA. This is accomplished using the client software which initiates an online session with the CA server and deliver the signed certificates to the subscriber. The online session is secured by SSL.

7.1.4 CA public key delivery to relying parties

LankaSign CA makes its public keys available to relying parties in repository available at https://www.lankapay.net/knowledge-center/lankasign

7.1.5 Key sizes

The key length and hash algorithms used by LankaSign CA and subscriber certificates are given below:

Certificate template	Cryptographic function	Cryptographic algorithm
Lankasign CA	Signature	4096-bit RSA
	Hashing	SHA-512
Subscriber Certificate	Signature	2048-bit RSA
	Hashing	SHA-512

7.1.6 Public key parameters generation and quality checking

LankaSign CA shall generate key pairs in accordance with FIPS 140-2 and shall use reasonable techniques to validate the suitability of public keys presented by subscribers. LankaSign CA's public key is generated using the FIPS 140-2 level 3 cryptographic module. The cryptographic module automatically sets the public key generation parameters.

7.1.7 Key usage purposes (as per X.509 v3 key usage field)

Key usages are covered in certificate profiles defined by LankaSign CA.

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates include critical key usage extension.

7.2 Private key protection and cryptographic module engineering controls

7.2.1 Cryptographic module standards and controls

The relevant standard for cryptographic modules is FIPS PUB 140-2, Security Requirements for Cryptographic Modules. The table in Section 7.1.5 summarizes the minimum requirements for cryptographic modules; higher levels may be used.

7.2.2 Private key multi-person control

Use of a LankaSign CA private signing key requires action by at least two persons.

7.2.3 Private key escrow

LankaSign CA does not escrow the private keys.

7.2.4 Private key backup

7.2.4.1 Backup of LankaSign CA private signature key

LankaSign CA private signature keys are backed up under the same multi-person control as the original signature key. Numbers of backup copies are limited to five and securely stored under the same multi-person control as the operational key.

7.2.4.2 Backup of subscriber private signature key

Where LankaSign CA generates key pair on behalf of the subscriber, LankaSign CA does not keep copies of such key pairs.

7.2.5 Private key archival

At the end of the validity period, LankaSign CA private key will be destroyed and will not be archived.

7.2.6 Private key transfer into or from a cryptographic module

LankaSign CA key pairs are generated and secured by hardware cryptographic modules (ie HSMs). LankaSign CA ensures that the LankaSign CA private keys are backed up in secure manner and transferred in an encrypted form.

7.2.7 Private key storage on cryptographic module

LankaSign CA stores private keys in hardware cryptographic module and keys are not accessible without authentication mechanism that is in compliance with FIPS 140-2 rating of the cryptographic module.

7.2.8 Method of activating private key

The user must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, Personal Identification Numbers (PINs) or biometrics. Entry of activation data is protected from disclosure (ie the data should not be displayed while it is entered).

7.2.9 Methods of deactivating private key

Cryptographic module that has been activated is never left unattended or otherwise available to unauthorized access. After use, cryptographic modules are deactivated. After deactivation, the use of the cryptographic modules-based CA key pair requires the presence of the trusted roles with the activation data in order to reactivate the said LankaSign CA key pair.

7.2.10 Method of destroying private key

Private signature keys will be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. Destroying private key inside cryptographic modules requires destroying the key(s) inside the HSM using the 'zeroization' function of the cryptographic modules in a manner that any information cannot be used to recover any part of the private key. All the private key back-ups are destroyed in a manner that any information cannot be used to recover any part of the private key. If the functions of cryptographic modules are not accessible in order to destroy the key contained inside, then the cryptographic modules will be physically destroyed. The destruction operation is realized in a physically secure environment.

7.2.11 Cryptographic module rating

See Section 7.2.7.

7.3 Other aspects of key management

7.3.1 Public key archival

The public key is archived as part of the certificate archival.

7.3.2 Certificate operational periods/key usage periods

Default operational periods/key usage periods are defined in Section 6.6. However, LankaSign CA may change the operational periods/key usage periods based on subscriber requirements.

7.4 Activation data

7.4.1 Activation data generation and installation

The activation data used to unlock private keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection. When they are not used, activation data are always stored in a safe for which access is controlled by holders in limited roles.

7.4.2 Activation data protection

The activation data used to unlock private keys is protected from disclosure. After a predetermined number of failed login attempts, a facility to lock the account temporarily has been provided. The activation data written on paper is stored securely in a safe.

7.4.3 Other aspects of activation data

LankaSign CA changes the activation data whenever the HSM is re-keyed or returned from maintenance. Before sending a cryptographic module for maintenance, all sensitive information contained in the cryptographic module is destroyed. Subscribers are responsible to ensure the protection of their activation data.

7.5 Computer security controls

7.5.1 Specific computer security technical requirements

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards.

1. Require authenticated logins for trusted roles.
2. Provide discretionary access control.
3. Provide a security audit capability.
4. Require a trusted path for identification and authentication.
5. Provide domain isolation for process.
6. Provide self-protection for the operating system.

LankaSign CA computer systems are configured with minimum required accounts and network services. LankaSign CA has implemented a combination of physical and logical security controls to ensure that LankaSign CA administration is not carried out with less than two-person control.

7.5.2 Computer security rating

No Stipulation.

7.6 Life-cycle technical controls

7.6.1 System development controls

The system development controls for the CA are as follows:

i. Hardware and software are purchased in such a way so as to reduce the likelihood that any particular component was tampered with.
ii. All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
iii. The hardware and software are dedicated to performing the PKI activities. There are no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation.

iv. Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required performing the PKI operations is obtained from sources authorized by local policy.

v. LankaSign CA hardware and software are scanned for malicious code on first use and periodically thereafter.

7.6.2 Security management controls

The configuration of the LankaSign CA system as well as any modification and upgrade are documented and controlled. There is a mechanism for detecting unauthorized modification to the LankaSign CA software or configuration. A formal configuration management methodology is used for installation and ongoing maintenance of the LankaSign CA system. LankaSign CA software, when first loaded, is verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

7.6.3 Life cycle security controls

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

7.7 Network security controls

LankaSign CA employs appropriate security measures to ensure that they are guarded against denial of service and intrusion attacks. Such measures include the use of hardware firewalls, hardware filtering routers, and intrusion detection systems. Unused network ports and services are turned off. Protocols that provide network security attack vector(s) is not permitted through the boundary control devices. Any boundary control devices used to protect the network on which PKI equipment is hosted will deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

7.8 Time stamping

All LankaSign CA components are regularly synchronized with a time service provided via a time server (ie a locally setup NTP time server). Time derived from the time service is used for establishing the time of:

1. Initial validity time of a subscriber's certificate
2. Revocation of a subscriber's certificate
3. Posting of CRL updates
4. OCSP

Asserted times are accurate to within three minutes. Electronic or manual procedures are used to maintain system time. Clock adjustments are auditable events as listed in Section 6.4.1.

8. Certificate, CRL and OCSP Profiles

8.1 Certificate profile

Certificate profiles are listed by NCA. The CA certificates issued under this CPS conform to X-509 Version 3 digital Certificate. The end user certificate profile (issued for personal use) and CA certificate profiles are listed below:

1. CA Certificate Profile

CA certificate – basic fields	
Version	Version 3
Serial number	Positive number of maximum Length 20 bytes and unique to each certificate issued by issuer CA
Signature Algorithm	SHA512 with RSA Encryption (null parameters)
Issuer DN	Subject DN of the issuing CA
Validity	Validity expressed in UTC Time for certificates valid through 2030
Subject DN	The X.500 distinguished name of the entity associated with the public key certified in the subject public key field of the certificate (Common Name (CN), Organisation (O),Country (C))
Subject Public Key	rsaEncryption {1 2 840 113549 1 1 1}, 4096 RSA Key, public exponent
Signature	Issuer CA's signature
EXTENSIONS	
authorityKeyIdentifier	Identifies the CA certificate that must be used to verify the CA certificate. It contains subjectKeyIdentifier of the issuing CA certificate
subjectKeyIdentifier	unique value associated with the Public key
basicConstraints	Subject Type=CA, pathLengthConstraint=None
keyUsage	CertificateSigning , cRLSign, Off-line CRL Signing
certificatePolicies	The value must contain the OID representing PKI certificate policy the certificate is valid for.
CRLDistributionPoints	Location of CRL information - http://www.nca.gov.lk/resources/cdp.crl

2. LPPL User certificate profile (personal)

End entity certificate – basic fields	
Version	Version 3
Serial number	Positive number of maximum Length 20 bytes and unique to each certificate issued by a issuer CA
Signature Algorithm	SHA512 with RSA Encryption (null parameters) or ECDSA with SHA512 {1 2 840 10045 4 3 2}
Issuer DN	Subject DN of the issuing CA
Validity	Validity expressed in UTC Time for certificates valid through 2028
Subject DN	The X.500 distinguished name of the entity associated with the public key certified in the subject public key field of the certificate (Common Name, Organization Unit, r, Organisation, Country)
Subject Public Key	rsaEncryption {1 2 840 113549 1 1 1}, 2048 RSA Key modulus, public exponent OR ecPublicKey {1.2.840.10045.2.1}, namedCurve, {1.2.840.10045.3.1.7} (NIST curve P-256)
Signature Hash Algorithm	Issuer CA's signature
EXTENSIONS	
authorityKeyIdentifier	Identifies the CA certificate that must be used to verify the subscriber's certificate. Issuing CA SubjectkeyIndetifier
subjectKeyIdentifier	Octet String of unique value associated with the Public key
Authority information access	Location of AIA http://rsa-aia.lankasign.net:8091/aia/RSA-SUBCA.lankasign.net_LankaSign%20RSA%20Certification%20Authority.crt Location of OCSP Responder http://rsa-ocsp.lankasign.net:8093/ocsp
Extended Key Usage	Document Signing: {1.3.6.1.4.1.311.10.3.12} Document Encryption (1.3.6.1.4.1.311.80.1)
keyUsage	DigitalSignature, Key Encipherment
certificatePolicies	The value must contain the OID representing PKI certificate policy the certificate is valid for.
cRLDistributionPoints	Location of CRL information - http://rsa-cdp.lankasign.net:8092/cdp/LankaSign%20RSA%20Certification%20Authority.crl

8.1.1 Version number(s)

Certificate issued by LankaSign CA is in accordance with ITU-T Recommendation X.509 standard ISO / IEC 9594-8:2008 and designated to be version 3.

8.1.2 Certificate extensions

LankaSign CA shall issue certificates in compliance with RFC 5280. Criticality shall follow best practices and where possible prevent unnecessary risks to Relying Parties when applied to name constraints.

8.1.3 Algorithm object identifiers

The OIDs of digital signature and encryption of certificate is shown below.

Algorithm	Object Identifier
RSA encryption	1.2.840.113549.1.1.1
SHA512 with RSA encryption	1.2.840.113549.1.1.13
SHA512	1.2.840.113549.1.1.13

8.1.4 Name forms

The subject field in certificates shall be populated with an X.500 Distinguished Name with the values described in Section 4.1.1.

8.1.5 Name constraints

LankaSign CA asserts name constraints as specified in the 'General instructions on LankaSign Document Submission' available in https://www.lankapay.net/knowledge-center/lankasign/

8.1.6 Certificate policy object identifier

Refer the tables given under Section 8.1.

8.1.7 Usage of policy constraints extension

Refer the tables given under Section 8.1.

8.1.8 Policy qualifiers and syntax and semantics

Refer the tables given under Section 8.1.

8.1.9 Processing semantics for critical certificate policies extension

Refer the tables given under Section 8.1.

8.2 CRL profile

8.2.1 Version number(s)

LankaSign CA shall issue version 2 CRLs that conform to RFC 5280.

8.2.2 CRL and CRL entry extensions

CRLs have the following extensions: CRL Number and Authority Key Identifier.

8.2.3 Full and complete CRL

LankaSign CA makes a full and complete CRL available to the OCSP responders as specified below. This CRL is provided to the relying parties and published on the repository.

Field	Value
Version	V2 (1)
Issuer Signature Algorithm	Sha512WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Per the requirements in NCA
nextUpdate	expressed in UTC Time (>= thisUpdate + CRL issuance frequency)
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in Generalized Time)
CRL Number (Critical)	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier (Critical)	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)
CRL Entry Extension	**Value**
Reason Code	c=no; optional

8.2.4 Distribution point based partitioned CRL

LankaSign CA issues only full and complete CRL signed by LankaSign CA.

8.3 OCSP profile

OCSP requests and responses are in accordance with RFC 2560 as listed below.

8.3.1 Version number(s)

LankaSign CA shall issue version 2 OCSPs that conform to RFC 2560.

8.3.2 OCSP extensions

Not applicable.

8.3.3 OCSP request format

Requests sent to Issuer CA OCSP responders are not required to be signed. The following table lists the fields that are expected by the OCSP responder.

Field	Value
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	List of certificates as specified in RFC 2560
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

8.3.4 OCSP response format

See RFC2560 for detailed syntax. The following table lists which fields are populated by the OCSP responder.

Field	Value
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Octet String (same as subject key identifier in Responder certificate)
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status1, thisUpdate, nextUpdate2,
Responder Signature	sha512 WithRSAEncryption {1 2 840 113549 1 1 11}
Certificates	Applicable certificates issued to the OCSP Responder
Response Extension	Value
Nonce	c=no; Value in the nonce field of request (required, if present in request)
Response Entry Extension	Value
None	None

9. Compliance Audit and Other Assessments

9.1 Frequency or circumstances of assessments

Annual compliance audit by NCA empaneled auditor is carried out on LankaSign CA's infrastructure apart from half yearly internal audits.

9.2. Identity and qualifications of assessor

NCA empaneled auditors based on the competence in the field of compliance audits, qualifications and thorough familiarity with requirements of the ETA, NCA CP and CPS perform such compliance audits as per the terms of empanelment and also under the guidance of NCA.

9.3 Assessor's relationship to assessed entity

The auditor is independent from the entity being audited. The office of NCA determines whether an auditor meets this requirement.

9.4 Topics covered by assessment

LankaSign CA has a compliance audit mechanism in place to ensure that the requirements of this CPS are enforced as follows:
WebTrust for CA v2.2.2 or later

9.5 Actions taken as a result of deficiency

Office of NCA may determine that LankaSign CA is not complying with its obligations set forth in this CPS or the applicable CP of NCA. When such a determination is made, the office of NCA may suspend operation of LankaSign CA, or may revoke the LankaSign CA certificate, or may direct that other corrective actions be taken which allow operation to continue. When the auditor finds a discrepancy between how the LankaSign CA is designed or is being operated or maintained, and the requirements of this CPS, or the applicable CP of NCA, the auditor take the following actions:

1. The auditor notes the discrepancy;
2. The auditor notifies the audited CA; and
3. LankaSign CA notifies the office of NCA.

4. CA responsible for correcting the discrepancy will propose a remedy, including expected time for completion.
5. The plan will be submitted to auditors to ensure that sufficient security of the system is still in place.

9.6 Communication of results

The WebTrust Assurance report will be a report that is available to the public.

On completion of an audit by an internal or external auditor, auditor submits an audit report, including identification of corrective measures taken or being taken by CA, to the LankaSign CA. This is a report which has restricted circulation and LankaSign CA would decide with whom to share it.

10. Other Business and Legal Matters

10.1 Fees

10.1.1 Certificate issuance and renewal fees

The fees for various types of certificates are made available on LankaSign CA website https://www.lankapay.net/knowledge-center/lankasign and will be updated from time to time.

10.1.2 Certificate access fees

CA is not charging any fees to relying parties or other public for accessing the certificate information from the repository.

10.1.3 Revocation status information access fees

LankaSign CA does not charge a fee for access to any revocation status information through CRL.

10.1.4 Fees for other services

No stipulation

10.1.5 Refund policy

The refund policy and other payments terms are governed as per the terms in the subscriber agreement. A subscriber pays the applicable fees only after an application is approved and therefore if an application is rejected, the subscriber does not have to pay any fees.

10.2 Financial responsibility

10.2.1 Insurance coverage

LankaSign CA maintains reasonable levels of insurance coverage to address all foreseeable liability obligations to PKI participants described in Section 2.3 of this CPS.

10.2.2 Other assets

LankaSign CA also maintains reasonable and sufficient financial resources to maintain operations, fulfil duties, and address commercially reasonable liability obligations to PKI participants described in Section 2.3 of this CPS.

10.2.3 Insurance or warranty coverage for end entities

LankaSign CA offers no protection to end entities that extends beyond the protections provided in this CPS.

10.3 Confidentiality of business information

LankaSign CA maintains the confidentiality of business information that is clearly marked or labelled as confidential, or by its nature reasonably is understood to be confidential and treat such information with the same degree of care and security as the LankaSign CA treats its own confidential information.

10.3.1 Scope of confidential information

LankaSign CA keeps following information under the scope of confidential information:

- Private key of LankaSign CA and required information to access private key including credentials to access LankaSign CA's hardware and software
- Registration application of subscribers for both approved and rejected applications
- Audit trail records
- Contingency plan or Disaster Recovery Plan
- Security controls of LankaSign CA's hardware and software
- Sensitive information with potential to have impact on security and reliability of LankaSign CA's system

10.3.2 Information not within the scope of confidential information

Following information is not within the scope of confidential information:

- Certificate Practice Statement of certification authority
- Certificate policy

- Information inside certificate
- Certificate revocation
- Information without impact on security and reliability of LankaSign CA's system such as articles and news

10.3.3 Responsibility to protect confidential information

LankaSign CA has security measures in place to protect confidential information. LankaSign CA's employees, agents and contractors are held responsible for protecting confidential information and are contractually obliged to do so. Employees shall receive training on handling confidential information.

10.4 Privacy of personal information

LankaSign CA stores, processes, and discloses personally identifiable information in accordance with the provisions of data protection act (DPA) rules made thereunder.

10.4.1. Privacy Plan

LankaSign CA develop, implement and maintain a privacy policy and procedures documenting what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed.

10.4.2. Information treated as private

LankaSign CA shall treat all information received from subscribers that will not ordinarily be placed into a certificate as private. This applies both to those subscribers who are successful in being issued a certificate and those who are unsuccessful and rejected. LankaSign CA periodically train all LankaSign staff as well as anyone who has access to the information about due care and attention that must be applied.

10.4.3. Information not deemed private

Certificate status information and any Certificate content is deemed not private.

10.4.4. Responsibility to protect private information

LankaSign CA is responsible for securely storing private information and may store information received in either paper or digital form. Any backup of private information must be encrypted when transferred to suitable backup media.

10.4.5. Notice and consent to use private information

Personal information obtained from subscribers during the application and enrolment process is deemed private and permission is required from the subscriber to allow the use of such information.

10.4.6. Disclosure pursuant to judicial or administrative process

In the event of court order or administrative order, LankaSign CA is entitled to disclose personal information required by law or officers under the law.

10.4.7. Other information disclosure circumstances

No stipulation.

10.5 Intellectual property rights

LankaSign owns all intellectual property rights associated with its databases, websites, and digital certificates and related documents. LankaSign CA will not knowingly violate any intellectual property rights held by others.

10.5.1 Intellectual Property rights in certificates and revocation information

LankaSign CA claims all Intellectual Property Rights in and to the certificates and revocation information that the LankaSign CA issues.

10.5.2 Intellectual Property rights in the CPS

This CPS is based on the proforma CPS published by Office of NCA for licensed CAs and as amended from time-to-time. All Intellectual Property Rights in this CPS pertaining to CA are owned by the LankaSign CA.

10.5.3 Intellectual Property rights in names

LankaSign CA may claim all rights, if any, in any trademark, service mark, or trade name of its services under the law for the time being in force.

10.5.4 Intellectual Property rights in keys

LankaSign CA may claim property rights to the keys used (ie CA key pair, OCSP responder key pair, time stamp authority key pair etc.) under the law for the time being in force. Subject to any agreements between LankaSign CA and its customers, ownership of and property rights in key pairs corresponding to certificates of subscribers is specified in this CPS.

10.6 Representations and warranties

10.6.1 CA representations and warranties

10.6.1.1 Certification Authority (CA)

LankaSign CA represents and warrants in accordance with provisions of ETA that;

1. signing private key is protected and that no unauthorized person shall ever has access to that private key;
2. Each subscriber has been required to represent and warrant that all information supplied by the subscriber in connection with, and/or contained in the certificate is true.
3. Only verified information appears in the certificate.

10.6.1.2 Subscriber

A subscriber is required to sign a document (ie a subscriber agreement) containing the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. In signing the document described above, each subscriber should agree to the following:

i. Subscriber shall accurately represent itself in all communications with the LankaSign CA.

ii. The data contained in any certificates about subscriber is accurate.
iii. Subscriber shall protect its private key at all times, in accordance with this policy, as stipulated in the certificate acceptance agreements, and local procedures .
iv. Subscriber lawfully holds the private key corresponding to public key identified in the subscriber's certificate.
v. Subscriber will abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.
vi. Subscriber shall promptly notify LankaSign CA upon suspicion of loss or compromise of his/her private keys. Such notification shall be made directly or indirectly through mechanisms consistent with this CPS.
vii. Subscriber shall follow the ETA.

10.6.2 Relying party

Parties who rely upon the certificates issued under a policy defined in this document shall:

i. Use the certificate for the purpose for which it was issued, as indicated in the certificate information (ie the key usage extension);
ii. Check each certificate for validity, using procedures described in RFC 5280, prior to reliance;
iii. Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades will often invalidate digital signatures and should be avoided.

10.6.3 Representations and warranties of other participants

No stipulation.

10.7 Disclaimers of warranties

To the extent permitted by applicable law and any other related agreements, LankaSign CA disclaims all warranties other than any express warranties contained in such agreements or set forth in this CPS.

10.8 Limitations of liabilities

LankaSign CA limits liabilities as long as the LankaSign CA meets the liability requirements stated in ETA. LankaSign CA is responsible for verification of any subscriber to whom it has issued a certificate and to all relying parties who reasonably rely on such certificate in accordance with this CPS, for damages suffered by such persons that are caused by the failure of the LankaSign CA to comply with the terms of its CPS or its subscriber agreement, and sustained by such persons as a result of the use of or reliance on the certificate. The verification requirements for certificate issuance by LankaSign CA are as specified by NCA and rules made thereunder and reasonable efforts taken by the LankaSign CA. LankaSign CA cannot guarantee the activities or conduct of the subscribers. LankaSign CA shall not be liable for any indirect, exemplary, special, punitive, incidental, and consequential losses, damages, claims, liabilities, charges, costs, expenses or injuries (including without limitation to loss of use, data, revenue, profits, business and for any claims of subscribers or users or other third parties including relying parties). LankaSign CA shall not be liable for any delay, default, failure, breach of its obligations under the subscriber's agreement and relying party terms and conditions.

All liability is limited to actual and legally provable damages. LankaSign CA's liability is as per the ETA and other governing Sri Lankan laws and agreement. If the liability is not dealt under the provisions of ETA, the following caps limit LankaSign CA's damages concerning specific certificates.

Class	Liability Caps/per Certificate
Class 3	LKR Ten thousand

10.9 Indemnities

10.9.1 Indemnification by subscribers

The subscriber/certificate owner/user agrees to indemnify and hold LankaSign CA 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 CA, and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from:

1) False and misrepresentation of fact by the subscriber on the subscriber's certificate application.
2) Any failure of the certificate subscriber/owner/user to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the LankaSign CA, or any person receiving or relying on the certificate.
3) Failure to protect the certificate subscriber's/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 subscriber's/owner's/user's confidential data.
4) The subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.
5) Breach of any laws applicable in Sri Lanka and in the country or territory in which activities related to the use of LankaSign CA issued digital certificates are being used including those related to intellectual property protection, viruses, accessing computer systems etc.

10.9.2 Indemnification by relying parties

To the extent permitted by applicable law, relying party agreement requires, relying parties to indemnify LankaSign CA for:

1) The relying party's failure to perform the representations and warranties as outlined in the section 10.6.2 of this CPS.
2) The relying party's reliance on a certificate that is not reasonable under the circumstances, or
3) The relying party's failure to check the status of such certificate to determine if the certificate is expired or revoked.

10.10 Term and termination

10.10.1 Term

The CPS becomes effective upon approval by the Office of NCA. Amendments to this CPS become effective upon ratification by approval by NCA and publication by LankaSign CA at URL https://www.lankapay.net/knowledge-center/lankasign. There is no specified term for this CPS.

10.10.2 Termination

While this CPS may be amended from time to time, it shall remain in force until replaced by a newer version or explicitly terminated by NCA.

10.10.3 Effect of termination and survival

Upon termination of this CPS, LankaSign CA is nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates. The sections 6.5 and 10 of this CPS shall survive the termination or expiration of this CPS.

10.10.4 Individual notices and communications with participants

Unless otherwise specified by agreement between the parties, LankaSign CA uses commercially reasonable methods to communicate, taking into account the criticality and subject matter of the communication.

10.11 Amendments

10.11.1 Procedure for amendment

LankaSign CA will review this CPS at least once every year. Additional reviews may be enacted at any time at the discretion of the NCA. If the Office of NCA wishes to recommend amendments or corrections to this CPS, such modifications will be submitted to NCA for approval.

LankaSign CA will use reasonable efforts to notify subscribers and relying parties of changes.

10.11.2 Notification mechanism and period

Errors and anticipated changes to this CPS resulting from reviews are published online at URL https://www.lankapay.net/knowledge-center/lankasign.
This CPS and any subsequent changes are made publicly available within seven days of approval.

10.11.3 Circumstances under which OID must be changed

NCA determines the requirement for changing the certificate policy OIDs.

10.12 Dispute resolution provisions

10.12.1 Disputes among licensed CAs and customers

Any dispute based on the contents of this CPS, between LankaSign CA and one of its subscribers who has availed specific services will be resolved according to provisions in the applicable agreement between the parties. Any dispute based on the contents of this CPS, between/among CAs shall be resolved by NCA.

10.12.2 Alternate dispute resolution provisions

No stipulations.

10.13 Governing law

The laws of Sri Lanka and more particularly the ETA, DPA, and the guidelines issued and clarifications made from time to time by the NCA shall govern the construction, validity, enforceability and performance of actions per this CPS.

10.14 Compliance with applicable law

This CPS is subject to applicable national rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

10.15 Miscellaneous provisions

10.15.1 Entire agreement

No stipulation.

10.15.2 Assignment

Except where specified by other contracts, no party may assign or delegate this CPS or any of its rights or duties under this CPS, without the prior written consent of NCA. Further, the Office of NCA in its discretion may assign and delegate this CPS to any party of its choice.

10.15.3 Severability

If any provision of this CPS is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

10.15.4 Waiver of rights

No waiver of any breach or default or any failure to exercise any right hereunder is construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CPS are for convenience only and cannot be used in interpreting this CPS.

10.15.5 Force Majeure

LankaSign CA is not liable for any failure or delay in its performance under this CPS due to causes that are beyond their reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, and failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action.

10.16 Other provisions

No stipulation.

11. Bibliography

The following documents were used in part to develop this CPS:

FIPS 140-2	Security Requirements for Cryptographic Modules, 1994-01 http://csrc.nist.gov/cryptval/
FIPS 186-2	Digital Signature Standard, 2000-01-27 http://csrs.nist.gov/fips/fips186.pdf
ETA	Electronic Transactions Act No. 19 of 2006, Government of Sri Lanka
RFC 3647	Certificate Policy and Certificate Practices Framework, Chokhani, Ford, Sabett, Merrill, and Wu. November 2003.
NCA-CP	National Certification Authority (NCA) certification policy (CP) https://nca.gov.lk/index.php/Main/cp
NCA-CPS	NCA certification practice statement (CPS) https://nca.gov.lk/index.php/Main/cps
NCA-CRL	NCA certificate revocation list https://nca.gov.lk/index.php/Main/crl
NCA-OCSP	NCA OCSP guidelines for CAs https://nca.gov.lk/index.php/Main/ocsp
NCA-Gazzette	NCA gazette designating SLCERT as NCA https://nca.gov.lk/index.php/Main/gazette
NCA-Circulars	NCA issued circulars https://nca.gov.lk/index.php/Main/circulars
NCA-Guidelines	NCA issued guidelines https://nca.gov.lk/index.php/Main/guidelines

12. Acronyms and abbreviations

AES	Advanced Encryption Standard
CA	Certifying Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Status Provider
DN	Distinguished Name
DNS	Domain Name Service
DPA	Data Protection Act
ETA	Electronic Transactions Act No. 19 of 2006
FIPS	(US) Federal Information Processing Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
HR	Human Resources
HTTP	Hypertext Transfer Protocol
IAO	Information Assurance Officer
ID	Identifier
IETF	Internet Engineering Task Force
IT	Information Technology
NCA	National Certification Authority
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-2	Secure Hash Algorithm, Version 1
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply