Vista Kencana

Certificate Policy

Version 1.3

15th May 2025

Vista Kencana Sdn. Bhd. (201201027076)
Suite 1-2, Level 1, Wisma UOA Damansara 2
No 6 Changkat Semantan, Bukit Damansara
50490 Kuala Lumpur, Malaysia
Tel: +60 3 2773 4182
www.vistakencana.com.my

Version History

Ver. No.	Date	Author	Description
1.0	10/09/2024	NURUL NATASHA CHE SAID	Creation
1.1	4/5/2025	NURUL NATASHA CHE SAID	This version updates a) **5.5.7** Procedure to Obtain and verify archive information b) **6.2.10** Method of destroying private key c) **4.6.1** Circumstances for certificate renewal
1.2	13/5/2025	NURUL NATASHA CHE SAID	This version updates: a) **9.6.3** Subscriber representations and warranties b) **4.7.3** Processing certificate re-keying request
1.3	15/5/2025	NURUL NATASHA CHE SAID	This version updates: a) **9.6.3** Subscriber representations and warranties

Table of Contents

LIST OF TABLE

LIST OF FIGURES

1 INTRODUCTION

1.1 Overview

This documentation is Certification Policy (CP) was prepared by our teams to provides information about the policies, practices, and procedures to perform Certificate Authority services. This document follows the formal requirements of Internet Engineering Task Force (IETF) RFC 3647 for the content, layout, and format. This document outlines the standard procedures of issuing, managing, suspending, revoking, and renewing digital certificates by Vista Kencana.

This documentation contains 9 Section which is,

Section 1 Introduction of Vista Kencana and information about infrastructure.

Section 2 Explains about publication and repository responsibilities.

Section 3 Explain the procedures and operational requirements for the identification and authentication during initial registration.

Section 4 Explain the procedures and operational requirements for the application, acceptance, issuance, revocation, suspension, renewal, re key and modification.

Section 5 Describe non-technical security control which is physical, procedural, and personnel control used by the Vista Kencana.

Chapter 6 Describe technical security control, site location and construction, physical access, power and air conditioning, water exposures, and other.

Chapter 7 Explain the certificate, CRL and OCSP.

Chapter 8 Define the audit requirements by qualified auditors.

Chapter 9 Explain the general business and legal matters.

Any section headings that do not apply have the statement ‘No stipulation’.

1.2 Document Name and Identification

This CP document describe and explain all matter Vista Kencana as CA and the certification services such as issuance and management, operation certification system and responsibilities and liabilities of the related parties such as Vista Kencana, RA and subscriber.

1.3 PKI Participants

Based on figure below, overview of Vista Kencana PKI model:

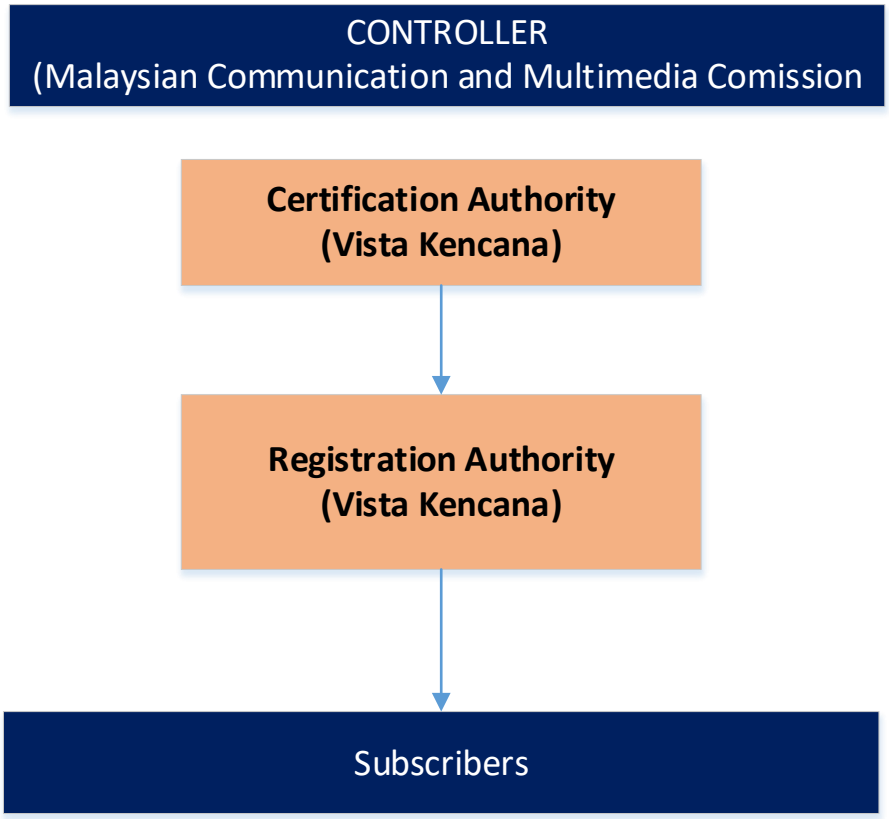

Figure 1 : Vista Kencana PKI TRUST MODEL

The controller is designed by Minister to monitor, regulate and ensure the legitimacy of CA operations in Malaysia.

This subcomponent describes the identity or type of entities that fill the roles of participants within a PKI.

Certification Authorities (Issuing CA)

Vista Kencana is a Certification Authorities (CA) that issue digital certificates using its own PKI. It is trusted entity responsible for issuing digital certificates that verify the ownership of public keys. The operation involved in Vista Kencana, receiving certificate requests, issuing, revoking, and renewing digital certificate and maintaining, issuing and publishing CRL and OCSP responses.

Registration Authorities

Registration Authorities is the entities that establish enrolment procedures for subscriber certificate applicants, perform identification and authentication of certificate applicants, initiate, or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of Vista Kencana. Subscriber can be individual, organization or infrastructure component such as firewalls, routers, trusted servers, or other devices for security purposes.

Subscribers

A subscriber refers to an entity or individual that requests and receives a digital certificate from the Vista Kencana. The subscriber is typically the party that needs to prove it identity or ownership of a public key.

Relying Parties

Relying parties are entities that rely in a certificate or digital signature issued by the Vista Kencana. Relying parties must verify the validity of the digital certificate by checking the appropriate Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) prior to relying on information featured in a certificate.

Other Participants

No stipulation.

1.4 Certificate Usage

Appropriate Certificate Uses

a) **SSL/TLS Certificate**: Used to secure website connections, encrypting data transmitted between a user's browser and a web server. They ensure that data remains private and secure during online transactions, login sessions, and browsing.

b) **Code Signing Certificates**: Developers use these certificates to sign software and applications, ensuring their authenticity and integrity. It assures users that the software they are downloading hasn’t been tampered with and is from a trusted source.

c) **Email Certificates (S/MIME**): Employed to sign and encrypt emails, enhancing email security. They verify the sender's identity and protect the confidentiality of the email content.
d) **Client Authentication Certificates**: Used in mutual SSL/TLS authentication scenarios where both the server and the client (such as devices, applications, or users) need to verify each other's identity before establishing a secure connection.
e) **Document Signing Certificates**: Used to digitally sign documents, ensuring their authenticity and integrity. They validate the identity of the signer and provide a level of assurance regarding the document's origin and content. It can be use by individual and organization to digitally sign documents such as Adobe. This certificate will use service of Adobe Approved Trust List (AATL).
f) **Identity Certificates**: Utilized in various authentication processes, like logging into systems, accessing secure networks, or proving identity in online transactions.
g) **IoT Device Certificates**: Employed to authenticate and secure communication between Internet of Things (IoT) devices and servers, ensuring the integrity and confidentiality of data transmitted in IoT ecosystems.
h) **Time Stamping Certificates**: Time Stamp Authority Certificates are used to identify the existence of data at that point in time.

All certificate type, except for timestamping and code signing certificates can be used to ensure confidentiality of communication effected.

Prohibited Certificate Uses

a) **Forgery or Fraudulent Activities**: Using certificates to falsify identities, forge digital signatures, or misrepresent oneself in online transactions is strictly prohibited.
b) **Malware Distribution**: Using certificates to sign malware or malicious software, thereby attempting to deceive users or security systems into thinking the software is legitimate or safe.
c) **Unauthorized Access**: Employing certificates to gain unauthorized access to systems, networks, or data that the user is not permitted to access.
d) **Impersonation or Spoofing**: Misusing certificates to impersonate legitimate entities or websites, leading users to believe they are interacting with a trusted source when they are not.
e) **Certificate Manipulation**: Tampering with or altering certificates to bypass security measures, deceive verification processes, or compromise the integrity of digital communications.

f) **Illegal Activities**: Using certificates to facilitate illegal activities, such as money laundering, trafficking, or any other unlawful actions.

g) **Violating Privacy Rights**: Employing certificates to compromise individuals' privacy by intercepting or decrypting their confidential communications without proper authorization or legal justification.

1.5 Policy Administration

Organization Administering the Document

Company	Vista Kencana Sdn Bhd
Address	Wisma UOA Damansara, No 6 Changkat Semantan, Bukit Damansara 50490 Kuala Lumpur, Malaysia
Telephone	+603 2773 4182
Fax	+603 2773 4183
E-mail	admin@vistakencana.com.my
Website	https://www.vistakencana.com.my/vksb/public/

Table 1: Organization Administering the Document

Contact Person

PIC	Vista Kencana Manager
Company	Vista Kencana Sdn Bhd
Address	Wisma UOA Damansara, No 6 Changkat Semantan, Bukit Damansara 50490 Kuala Lumpur, Malaysia
Telephone	+603 2773 4182
Fax	+603 2773 4183
E-mail	admin@vistakencana.com.my
Website	https://www.vistakencana.com.my

Table 2: Contact Person

Person Determining CP Suitability for the Policy

Vista Kencana provider determines CP suitability for the policy based on the recommendations received from the accessor.

CP Approval Procedures

This CP are reviewed and approved by the management of Vista Kencana.

1.6 Definition and Acronym

Definitions

Term	Definition
AATL	Adobe Approved Trust List
AP	Authorised Personnel
Asymmetric cryptosystem	An algorithm or series of algorithms that provide a secure key pair.
Authentication	A process used to confirm the identity of a person or to prove the integrity of specific information.
Certificate	A computer-based record which – • identifies the certification authority issuing it. • names or identifies its subscriber. • contains the subscriber's public key; and • is digitally signed by the certification authority issuing it
Certification Authority (CA)	An authority who issues a certificate.
Certification Authority Disclosure Record	An on-line and publicly accessible record which concerns a licensed certification authority which is kept by the Controller.
Certification Path	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
Certification Practice Statement	A declaration of the practices which a certification authority employs in issuing certificates generally, or employed in issuing a particular certificate.
Certification Revocation List (CRL)	A list of revoked certificates.
Controller	The Controller of Certification Authorities appointed under Section 3

Term	Definition
	of the DSA.
Digital Signature	A transformation of a message using an asymmetric cryptosystem so that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key; and whether the message has been altered since the transformation was made.
DSA 97	Malaysian Digital Signature Act 1997
DSR 98	Malaysian Digital Signature Regulations 1998
HSM	HSM is an acronym for Hardware Security Module. It is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing.
Issue a Certificate	The act of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate.
Object Identifier (OID)	A value comprised of a sequence of integer components, which can be assigned to a registered object, and which has the property of being unique among all object identifiers
Private key	The key of a key pair used to create a digital signature
Publish	To record or file in a repository.
Recognised Repository	A repository recognised by the Controller under Section 68 of the DSA.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (e.g., a RA is delegated certain tasks on behalf of a CA).
Repository	A system for storing and retrieving certificates and other information relevant to digital signatures.
Revoke Certificate	To make a certificate ineffective permanently from a specified time forward.
RSA	The first significant asymmetric cryptographic algorithm; the initials stand for Rivest, Shamir and Adleman, its inventors. Note that RSA can also refer to a particular commercial entity; see RSA DSI. RSA is protected by US patents held by RSA DSI. It is not protected outside the US.
Sub-CA	Sub-CAs are allowed to be created for different organizations and

Term	Definition
	agencies, for ease of operations and management.
Trustworthy System	Computer hardware and software which- • are reasonably secure from intrusion and misuse. • provide a reasonable level of availability, reliability and correct operation; and • are reasonably suited to performing their intended functions.
X.509	A digital certificate based on widely accepted International Telecommunications Union ('ITU') X.509 standard, which defines the format of Public Key Infrastructure (PKI) certificates. They are used to manage identity and security in internet communications and computer networking.

Table 3: Definition

Acronyms

Term	Definition
AATL	Adobe Approve Trusted List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
HSM	Hardware Security Module
ITU	International Telecommunication Union
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number (e.g., a secret access code)
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments (at IETF.org)
RPS	Registration Practice Statement
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SHA	Secure Hashing Algorithm
SSL	Secure Socket Layer

Term	Definition
TSA	Time Stamping Authority
TST	Time-Stamp Token
UTC	Coordinated Universal Time
AATL	Adobe Approve Trusted List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request

Table 4: Acronyms

References

a) RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
b) WebTrust Principle and Criteria for Certification Authorities, Principles and Criteria for Certification Authorities -Version 2.2.1.
c) Adobe Approved Trust List V.2.0

Conventions

No stipulation.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Vista Kencana will operate the Repository and publish all CA certificates, revocation, CP and CPS in repositories. Vista Kencana complies with the requirements of the DSA 97 and DSR 98. It available 24 hours a day,7 days a week through online resources with a minimum downtime.

2.2 Publication of certification information

Vista Kencana repository will publicly accessible except for the institutional procedures and confidential commercial information.

2.3 Time or frequency of publication

Every time issuance of certificate will publish to repository. For CRL, will publish once a day.

2.4 Access Controls on Repositories

Vista Kencana repository will not restrict public accessible to view Certificate Policy, Certificate Practice Statement, and others document. It can be read only.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Type of Names

All certificate issued with non-null subject Distinguished Name (DN) which is complies with ITU-T X.500 standard. Information contained in individual certificates are real name as in MyKad, Passport No, or email address. For corporate certificates should contained real name as in company registration, SSM no and email address. Lastly for server certificates need to contain real name as in company registration and internet domain name.

Need for Names to be Meaningful

Vista Kencana uses distinguished name to identify the identity. The name of individual or organization uses as subject for certificate.

Anonymity or pseudonymity of subscribers

Vista Kencana will not accept the entity anonymous or pseudonymous certificates.

Rules for Interpreting Various name Forms

No stipulation.

Uniqueness of Names

Vista Kencana will check and verify the uniqueness of identification subscriber in subject Distinguished Names.

Recognition, Authentication, and Role of Trademarks

Vista Kencana does not allow subscriber using intellectual property right of others. However, Vista Kencana does not verify whether the subscribers have the intellectual property rights in the name display in a certificate application.

3.2 Initial Identity Validation

Method to Prove Possession of Private Key

The possession of the private key Subscriber shall be proven by performing signature verification like digital signed. Vista Kencana verify whether the Public Key matches the private key based on application.

Authentication of Organization Identity

As stipulated in 3.2.3.

Authentication of Individual Identity

Class	Subscribers	Identification
Class 1	Individual	Applicants need to demonstrate control of their email address to which the certificate relates. Vista Kencana does not verify additional information/attributes provided applicant. For confirmation identity can be based on identification document MyKad or Passport.
Class 2	Individual & organization	Applicants need to demonstrate control of certain identity attributed include in the request such as his/her email address. Vista Kencana will verify by 2 type method which is. 1) In – person a) uses biometric verification. b) If cannot be verified using biometric, applicant required to provide identification document, license, EPF statement, bank statement, utilities, bill telecommunication bill. Supporting document 2) Online application

Class	Subscribers	Identification
		a) e-KYC Verification: Using unique biological traits like fingerprints, facial recognition, iris scans, or voice recognition for identity verification. e-KYC provide a high level of assurance due to their uniqueness. b) Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA): Requiring users to provide two or more forms of verification, such as a password combined with a code sent to a registered phone number or email address, Token-Based Authentication. c) One-Time Passwords (OTP): Generated for a single use during authentication. They are usually time-based or event-based codes delivered through SMS, email,
Class 3	Individual & organization	Class 3 certificate means a certificate that provides the higher level of confirmation and higher level of assurance as to the subscriber's identity then Class 1 and Class 2 certificate, which includes in-person and supervised remote proofing. The application for the Class 3 certificate must be certified by a notary public duly

Class	Subscribers	Identification
		appointed under the Notaries Public Act 1959. Applicants need to demonstrate control of certain identity attributed include in the request such as his/her email address. For Class 3, Vista Kencana will verify In – person only, which is applicant need to visit counter for proceed the application, there are 2 type verification will do in counter which is a) uses biometric verification such as finger print. b) If cannot be verified using biometric, applicant required to provide identification document, license, EPF statement, bank statement, utilities, bill telecommunication bill. Supporting document

Table 5: Authentication of Individual Identity

Non -Verified Subscriber Information

Vista Kencana does not require to verify Class 1 in 3.2.3. Any other information designated as non- verified in the certificate.

Validation of Authority

Certificate	Subscribers	Validation
Class 1	Individual	Vista Kencana or RA will do checking with and individual or organization which controls over the email address listed in

Certificate	Subscribers	Validation
		the certificate or possesses technical or administrative control over the domain the email address to be listed in the certificate.
Class 2	Individual & organization	Individuals & organization affiliated with the organization who confirm the applicant's authority to obtain a certificate indicating the affiliation and who agree to request revocation of the certificate when that affiliation ends.
Class 3	Individual & organization	Individuals & organization affiliated with the organization who confirm the applicant's authority to obtain a certificate certified by a notary public duly appointed under the Notaries Public Act 1959 indicating the affiliation and who agree to request revocation of the certificate when that affiliation ends.
SSL Certificate and Device Certificate		An authorized contact listed with the Domain Name Registrar, a person with control over the domain name, or through communication with the Applicant using a reliable method of communication, as defined in the baseline requirements.

Table 6: Validation of Authority

Criteria for Interoperation

No Stipulation.

3.3 Identification and Authentication for Re-Key Requests

Identification and Authentication for Routine Re-Key

Subscribers allow request re-key of certificate prior to a certificate expiration. After receiving request for re-key, Vista Kencana creates a new certificate with the same certificate contents but new Public Key.

Identification and Authentication for Re-Key After Revocation

If certificate was revoked, subscriber need to apply for new certificates and replace the certificate that has been revoked.

3.4 Identification and Authentication for revocation Request

Vista Kencana will verify revocation request by subscriber before proceeding to do revocation process. There are 3 procedures to verification the revocation request:

a) Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof) and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record. (Note that this option may not be available to all customers.)
b) Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
c) Communication with the Subscriber providing reasonable assurances considering the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

Vista Kencana administrator is allowed to request the revocation of subscriber certificates and authenticate the identity of administrator via access control using SSL and client authentication before permitting them to perform revocation functions.

4 CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1 Certificate Application

Who can Submit a Certificate Application

Anyone can submit application of certificate if they are not listed in government denied list, list of prohibited persons or other list that prohibits doing business with such organization or person under the Malaysia Law.

Enrolment Process and Responsibilities

All end-user Certificate Subscribers need to fulfil any condition for application which is,

a) Completing a Certificate Application and providing true and correct information.
b) Generating or arranging to have generated, a key pair.
c) Generating a Certificate Signing Request (CSR) using an appropriately secure tool.
d) Delivering their public key directly or through an RA to Vista Kencana.
e) Demonstrating possession or exclusive control of the private key corresponding to the public key delivered to Vista Kencana.
f) Agreeing to the applicable Subscriber Agreement or Term of Access
g) Paying any applicable fees

4.2 Certificate Application Processing

Performing identification and authentication function

Vista Kencana will maintain systems and processes to authenticate the Applicants identity in compliance with this CP, Vista Kencana will assign RA to do validation and ensure all communication and information regarding any process in CP.

Approval or rejection of certificate applications

There are several conditions need to meet for approval the application by Vista Kencana or RA which is,

a) Successfully completed the identification and authentication of all required Subscriber information.
b) Payment fees received.

Also, application will reject by Vista Kencana or RA if,

a) Identification and authentication of all required Subscriber information as set forth in Section 3.2 cannot be completed.
b) The Subscriber fails to furnish supporting documentation upon request.

c) The application has previously been rejected or violation of subscriber agreement.
d) Payment has not been received.
e) The RA believes that issuing a certificate to the Subscriber could damage or diminish Vista Kencana reputation or business.

Time to process certificate applications

Normally, Vista Kencana verifies an applicant information and issue a digital certificate within a reasonable time frame. Issuance time frames depends on when applicant provides the details and documentation necessary to complete validation. Vista Kencana will complete the process of application within 3 days working.

4.3 Certificate issuance

CA actions during certificate issuance

Before issuance, Vista Kencana need to confirm the source of certificate request before issuance. RA will perform validation to ensure the information is verified in secure manner. Then, when process issuance is completed, the certificate will be sent to the Subscriber.

Notification to subscriber by the CA issuance of certificate

Once certificate successfully issued, Subscriber will notify by Vista Kencana or RA. Then, Subscribers allow to download certificates from a website or email was sent to the Subscriber.

4.4 Certificate acceptance

Conduct constituting certificate acceptance

Subscribers are solely responsible for installing the issued certificate on the Subscribers computer or hardware security module (HSM). Certificates are considered accepted thirty (30) days after the issuance the certificate or earlier upon use of the Certificate when evidence exists that the Subscriber used the certificate. Failure of the Subscriber to object to the to the certificate or its content constituted certificates.

Publication of the certificate by the CA

Vista Kencana publishes all CA certificates and the certificates in its publicly accessible repository.

Notification of certificate issuance by the CA to other entities

RAs may receive notification of a Certificate's issuance if the RA was involved in the issuance process.

4.5 Key pair and certificate usage

Subscriber private key and certificate usage

Subscribers are allowed to use Private Key corresponding to the public key in the certificate once agrees to the Subscriber Agreement and accept the certificate. The certificate shall be used lawfully in accordance with Vista Kencana Subscriber Agreement, the terms of this CP and CPS document.

Subscribers need to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated certificate and use certificate in accordance with their intended purpose.

Relying party public key and certificate usage

Relying parties allowed to check the validity and revocation status of the certificate by using authorize mechanism for appropriate applications as state in this CP. Authorize relying parties need to use a trustworthy system under defined under the legislation and standard during operations.

Vista Kencana will not responsible if relying parties not fulfilling the conditions stated in this CP before relying on the certificates.

4.6 Certificate renewal

Circumstance for certificate renewal

Vista Kencana will renew a certificate if:

1. The associated Public Key has not reached the end of its validity period.
2. The subscriber and attribute are consistent.
3. The associated Private Key remains uncompromised.
4. Re-verification of subscriber identity is not required by Section 3.3.1.
5. CA certificate is re-keyed.

Vista Kencana will notify subscriber prior to their certificate expiration date. For renewal also, Vista Kencana requires payment of additional fee. Vista Kencana can renew the certificate to maintain continuity of certificate usage. Vista Kencana does not renew certificates that have been revoked, expired or suspended

Who may request renewal

Authenticated Subscriber only can request renewal.

Processing certificate renewal request

Vista Kencana shall require reconfirmation or verification of the information in a certificate prior to certificate issuance. During walk-in renewal request, officer will do checking the subscriber's Distinguished name and the serial number of the certificate for confirmation before proceed the request.

Notification of new certificate issuance to subscriber

As stipulated in 4.3.2.

Conduct constituting acceptance of a renewal certificate

As stipulated in 4.4.1.

Publication of the renewal certificate by the CA

As stipulated in 2.2.

Notification of certificate issuance by the CA to other entities

As stipulated in 4.4.3.

4.7 Certificate re-key

Circumstance for certificate re-key

Subscriber requesting re-key should identify and authenticate themselves. A certificate may also can be re-keyed after expiration.

Who may request certification of a new public key

Authenticated Subscriber only can request re-key.

Processing certificate re-keying request

Vista Kencana will only accept re-key requests from the authenticated subscriber. If Private Key and any identity certificates does not change, then Vista Kencana can issue a replacement certificate using previous certificates. Vista Kencana will reuse existing verification information unless re-verification and authentication is required if any information inaccurate. During walk-in rekey request, officer will do checking the subscriber's Distinguished name and the serial number of the certificate for confirmation before proceed the request.

Notification of new certificate issuance to subscriber

As stipulated in 4.3.2

Conduct constituting acceptance of a re-keyed certificate

As stipulated in 4.4.1.

Publication of the re-keyed certificate by the CA

As stipulated in 2.2.

Notification of certificate issuance by the CA to other entities

As stipulated in 4.6.7

4.8 Certification modification

Circumstance for certificate modification

Creation of new certificate for the same subject authenticated information but slightly different from older certificate, because there is some information have changed such as like a email address, name or others. Because of that, new certificate may have the same or different subject Public Key.

Who may request certificate modification

Authenticated Subscriber only can request modification.

Processing certificate modification request

Once receiving request for modification, Vista Kencana will verify any information that will change in the current certificate. Vista Kencana will only issue the process after completing the verification process and will not issue if validity period exceeds the applicable time limits.

Notification of new certificate issuance to subscriber

As stipulated in 4.3.2

Conduct constituting acceptance of modified certificate.

As stipulated in 4.4.1.

Publication of the modified certificate by the CA

As stipulated in 2.2.

Notification of certificate issuance by the CA to other entities

As stipulated in 4.6.7

4.9 Certificate revocation

Circumstances for revocation

There are several circumstances Vista Kencana will do revoke a certificate which is,

a) Request from subscriber.
b) Vista Kencana will notify by subscriber which is the original certificate was not authorized and does not retroactively grant authorization.
c) The subscriber's Private Key corresponding to the Public Key in the certificate suffered a Key Compromise.
d) The validation of domain authorization or control for any IP address in the certificate should not be relied upon.
e) Misused certificate.
f) Violation material obligation under the CP or any relevant agreement.
g) There are changes or inaccurate information in certificate.
h) Vista Kencana received legal instructions from government or others to revoke the certificates.

Who can request revocation

Revocation can be requested by controller, Vista Kencana and subscriber.

Procedure for revocation request

Subscribers or RA needs to request revocation by application to Vista Kencana. They need to verify their identity and show the reason why they want to do revocation process for requested certificates. Revocation request grace period.

Time within which CA must process the revocation request

After the identity of subscriber and reason for revocation is validated and accepted, Vista Kencana will proceed to do revocation within reasonable time.

Revocation checking requirement for relying parties

Relying parties need verify the relevant certificate and ensure the certificate is valid. To verify certificates status, revocation status, policy and other.

CRL issuance frequency

For subscriber are issued at least once per day. For CA, at least every 6 months.

Maximum latency for CRL

CRL for certificate issues to subscriber are posted automatically to the online repository within reasonable time after generation.

On-line revocation/status checking availability

Status of revocation is publicly accessible in website and Vista Kencana provide online certificate status checking service through OCSP protocol, it provides a real time certificate status inquiry.

On-line revocation checking requirements

Relying partis must confirm the validity and latest certificate information via OCSP.

Other forms or revocation advertisements available

No stipulation.

Special requirements re key compromise

Vista Kencana or RA will use commercially reasonable effort to notify the Relying Parties to Subscriber that their private key has been compromised. If this issue happens, Vista Kencana will generate a new signing key pair and corresponding Root Certificate and revoked the compromise certificate and publish a revised CRL within reasonable time.

Circumstances for suspension

No stipulation.

Who can request suspension

No stipulation.

Procedure for suspension request

No stipulation.

Limits on suspension period

No stipulation.

4.10 Certificate Status Services

Operational Characteristics

Certificate status information available via CRL and OCSP responder. For list revoked certificates on the appropriate CRL where they remain until one additional CRL is published after the end of the certificate's validity period.

Service Availability

Services available 24x7.

Optional Features

No stipulation.

4.11 End of Subscription

A subscriber subscription service ends if its certificate expired or revoked.

4.12 Key Escrow and Recovery

Key Escrow and Recovery Policy and Practices

No stipulation.

Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

Site Location and Construction

Vista Kencana CA and RA operations are conducted within a physically protected environment that prevents and detects unauthorized use of access to or disclosure of sensitive information and system whether covert or overt. Vista Kencana also maintains disaster recovery facilities for its CA operation, its protected by multiple tiers of physical security.

Physical Access

Physical access to the Vista Kencana is restricted to authorised personnel. Vista Kencana will provide high security zone such as location CA operations, RA operations, Database and others in a secure computer room monitored by person in charge, surveillance system or security alarms and every movement from zone to zone must accomplished using a token, biometric and access control list.

Power and Air Conditioning

Vista Kencana secure facilities are equipped with primary and backup:

a) Power system to ensure continuous.
b) Heating, ventilation, air conditioning to control temperature and humidity.

Water Exposures

CA system and data centres area equipped with raised flooring and with monitoring system to detect any water exposures.

Fire Prevention and Protection

Vista Kencana facilities area equipped with fire suppression mechanism.

Media Storage

Vista Kencana will backup files are created on daily basis.

Waste Disposal

Before disposal, all unnecessary copies of printed contain privacy will be shredded. Media which transmit privacy information are rendered unreadable. For cryptographic devices are physically destroyed or reformat as manufactured guidance.

Off-Site Backup

Vista Kencana will keep the backup storage of subscriber certificates, including CRL.

5.2 Procedural Controls

Trusted Roles

Trusted Persons include all employees, contractors and consultants that have access to or control authentication or cryptographic operations. All operative area segregated based on CA function. Then system administrators and PKI engineers have access to the computer that hosts Vista Kencana CA software to do the maintenance.

Number of Persons Required per Task

Vista Kencana has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks in CP.

Identification and Authentication for Each Role

All person in charge involved need to be authenticated and authorized with security system.

Roles Requiring Separation of Duties

As stipulated in 5.2.1 and 5.2.2.

5.3 Personnel Controls

Qualifications, Experience, and Clearance Requirements

All Vista Kencana operative personnel area competent in their performance and have appropriate educational levels with proper security clearance and training to perform its CA operation in reliable manner.

Background Check Procedures

Background checks procedure required:

a) Verification of the individual identity
b) Previous employment
c) Professional reference
d) Highest level education
e) Criminal record
f) Credit/financial record
g) Driving record – driver licenses
h) Employees Provident Fund (EPF)

Training Requirements

Vista Kencana makes available training for their personnel to carry out CA or RA functions. Training will include CP requirements, operations of the CA software and hardware, operational and security procedures, disaster recovery and business continuity management.

Retraining Frequency and Requirements

Refresh training is conducted as and when required.

Job Rotation Frequency and Sequence

No stipulation.

Sanctions for Unauthorized Actions

Appropriate disciplinary area taken for unauthorized action or other violation policies and procedures. If a person is trusted person do something unauthorized action, the person will immediately remove from the trusted role depends on decision management.

Independent Contractor Requirements

Independent Contractor Personnel will sign agreements as part of their initial contractor employment.

Documentation Supplied to Personnel

Vista Kencana will supply and share the available documentation including CP and CPS, security policy, system environmental documents to personnel, during training or employment.

5.4 Audit Logging Procedures

Types of Events Recorded

Vista Kencana require identification and authentication at system logon with a unique username and password. Vista Kencana enables all essential event auditing capabilities of its CA applications to record related to the key generating system, certificate generating system, management system, directory system, and time-stamping system in log files and manage accordingly.

Frequency of Processing Log

Audit Log should be reviewed periodically for any process that have critical activities.

Retention Period for Audit log

The yearly backup of the audit trails file is retained for 10 years under normal operations.

Protection of Audit Log

Audit logs are secure by physical and electronic security measures and be accessible by authorize personnel by configure and establish operational procedure. The record of any activities happening will protect from alterations and data tempering.

Audit log Backup Procedures

Vista Kencana makes regular backup copies of audit logs and audit log summaries and saves a copy of the audit log to a secure, off-site location on at least a monthly basis.

Where required, Vista Kencana creates incremental backups of audit logs daily and full backups weekly.

Audit Collection System (Internal vs. External)

Audit processes must be initiated at system start up and finish only at system shut down. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, Vista Kencana Administrators and the PMA shall be notified, and the PMA will consider suspending the CA's or RA's operations until the problem is remedied.

Notification to Event- Causing Subject

No stipulations.

Vulnerability Assessments

Audit logs are reported in the system will be analyzed and security gaps in the system including fault points in certification processes shall be identified and measure shall be taken.

5.5 Records Archival

Types of Records Archived

All process or event related in this CP such as certificate revocation, security policy modification and validation, Vista Kencana software maintenance restart and stop, database backup, cross-certification, attribute certificate management, DN change, certificate life- cycle management and audit trail and other miscellaneous events are recorded and archived.

Retention Period for Archive

Vista Kencana and the RA retains archived data associated Certificates for at least ten (10) years.

Protection of Archive

Archives records shall be protected by physical and electronic measures and can be accessed by Vista Kencana authorized personnel only. Copies of paper-based records shall be maintained in an off-site secure facility.

Archive Backup Procedures

The archive files are backed up as they are created. Originals are stored on-site and housed with the Vista Kencana CA system.

Requirements for timestamping of records

All electronic archives shall be recorded with system time as they are created. Manual archives have a manually entered date and time. Vista Kencana sync its system time at least every eight hours using a real time value.

Archive Collection System (Internal or External)

The Archive collection system complies with the security requirements in Section 5.

Procedures to Obtain and Verify Archive Information

To obtain and verify archive information for Vista Kencana, only trusted role can retrieve the information from archival. Archived records are stored monthly onto secure archive disks. A designated PKI Engineer shall verify, within the first week of the subsequent month, that no data loss, damage, or unauthorized modification has occurred by performing completeness checking against the archival audit log. Verification activities and results shall be documented in an Archive Verification Log and retained for audit purposes. Any discrepancies found shall be escalated and handled according to the organization's Incident Management Policy.

5.6 Key Changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of a CA Private Key's lifetime, Vista Kencana ceases using the expiring CA Private Key to sign Certificates and that uses the old Private Key only to sign CRLs and OCSP responder Certificates. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps to minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key Certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

5.7 Compromise and Disaster Recovery

Incident and Compromise Handling Procedures

If incident or system compromise occurs that would prevent CA operations, Vista Kencana shall carry out a risk assessment to evaluate the business risk and impact before determining the necessary security requirement and the operation procedures to be taken as consequence of its disaster recovery procedures and business continuity plans such as Disaster Recovery Plan. Vista Kencana still provide continuity business plans to subscriber, relying parties or application software suppliers.

Computing Resources, Software, and/or Data Are Corrupted

If any damage happens on computing resources, software and operational data that gives negative risk to CA, Vista Kencana will ensure the integrity of its CA system and reinitiate its operations by replacement hardware, using backup copies of its software, data and key material at the issuing VA secure facility.

Entity private key compromise procedures

If private key compromise or suspected, Vista Kencana will perform the following procedure:

a. The Certificate's revoked status is communicated to Relying Parties through the Vista Kencana Repository in accordance with Section 4.9.7
b. Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected Vista Kencana PKI Participants.
c. The CA will generate a new key pair in accordance with Section 5.6, except where the CA is being terminated in accordance with Section 5.8.

Business continuity capabilities after a disaster

Vista Kencana implement data backup and recovery procedures. Because of that Vista Kencana has the capability to recover and restore for essential operations.

5.8 CA or RA termination

If it is necessary for an Vista Kencana CA to cease operation, Vista Kencana makes a commercially reasonable effort to notify it Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, Vista Kencana will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

a. Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA.
b. Handling the cost of such notice.
c. Transfer all responsibilities to a qualified successor entity.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair generation and installation

Key pair generation

Vista Kencana CA key pair generation is performed by trusted individuals using Trustworthy System and process that provide for the security and required cryptographic strength for the generated keys. The cryptographic modules used for key generation using requirement of FIPS140-2 Level 3. Activation of hardware need to use two-factor authentication token.

Vista Kencana CA creates auditable evidence during the key generation process to prove that the CP was followed. The activities performed are recorded, dated and signed by all individuals involved. For generation of RA key pairs is generally performed by the RA using a minimum of FIPS 140-2 Level 2 certified cryptographic module.

Private key delivery to subscriber

For delivering the Private Key securely to the subscriber, Vista Kencana will deliver via electronic communication like email if required to do so as when necessary.

Public key delivery to certificate issuer

The CA Certificate containing the public key corresponding to the CA's signing key is delivered to each subscriber via email.

CA public key delivery to relying parties

Vista Kencana will provide the full certificate chain to the subscriber upon certificate issuance. Public keys are published at Vista Kencana website. Vista Kencana will distribute Public Key that are part of an update signature Key Pair as a self-signed certificate.

Key sizes

There are following key sizes for self-signed Root CA, Subordinate CA certificates, Subscriber's certificate as well as CRL/OCSP certificate status responder:

a) RSA: > 2048 bit
b) ECDSA: 256 bit
c) ECDSA: 384

Public key parameters generation and quality checking

Vista Kencana utilizes a cryptographic module that conforms to FIPS 186-4 standards for Digital Signature Algorithms. The module provides secure random number generation and on-board generation of public and private RSA key pairs. It supports a wide range of RSA key sizes, meeting current industry best practices for public key infrastructure (PKI) operations. All random number generation and key generation operations are performed within the FIPS-validated boundary of the module to ensure cryptographic strength and compliance with applicable standards.

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

The use of a specific key is determined by the key usage extension in the X.509 certificate Vista Kencana Certificates includes key usage extension fields that specify the intended use of the certificate and technically limit the certificate's functionality in X.509v3-compliant software. The signing key pair is used to provide authentication, integrity, and support for non-repudiation services.

The Private Keys associated with Root CA Certificates shall only be used for the following purposes:

1. Signing self-signed Certificates to represent the Root CA itself;
2. Signing Certificates for Subordinate Certification Authorities (Sub CAs)
3. Signing Certificates issued for infrastructure purposes, such as administrative role certificates.

4. Signing Certificates for Online Certificate Status Protocol (OCSP) Response verification.
5. Signing Certificates Revocations Lists (CRLs) issued by the Root CA.

The use of Root CA Private Keys for any other purpose is strictly prohibited.

The following is permitted Key Usage for CA certificate;

Entity	Permitted Key Usage
CA Certificate	keyCertSign, cRLSign

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Cryptographic module standards and controls

Assurance Level	Subscribers	Registration Authorities
Class 1	N/A	FIPS 140-2 Level 2 (Hardware)
Class 2	FIPS 140-2 Level 1 (Software or Hardware)	FIPS 140-2 Level 2 (Hardware)
Class 3	FIPS 140-2 Level 1 (Software) FIPS 140- 2 Level 2 (Hardware)	FIPS 140-2 Level 2 (Hardware)

Table 7: Cryptographic module standards and controls

Private key (n out of m) multi-person control

The storage of the private key of Vista Kencana requires multiple controls by appropriately authorised trust personnel.

Private key escrow

Vista Kencana does not escrow its Private Keys.

Private key backup

Vista Kencana Private Keys are generated and operated inside Vista Kencana cryptographic module, which has been evaluated to at least FIPS 140-2 Level 3. When keys are transferred

to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. Vista Kencana CA Key Pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted and video-recorded key backup process.

Vista Kencana may provide backup services for Private Keys that are not required to be kept on a hardware device. Access to back up Certificates is protected in a manner that only the Subscriber can control the Private Key. Backed up keys are never stored in a plain text form outside of the cryptographic module.

Private key archival

The CA signing key pair and the corresponding verification public key certificates are securely backed up in the Vista Kencana CA database. The archiving process for the Vista Kencana database adheres to the procedures specified in CPS Part 5.4.6, ensuring the implementation of adequate security measures for both backup and retrieval.

Private key transfer into or from a cryptographic module

All Private Keys exported from cryptographic module must be encrypted and never exist in plain text format.

Private key storage on cryptographic module

Vista Kencana shall store its Root CA and Subordinate CA on cryptographic hardware module which conforms to at least FIPS 140 Level 3.

Method of activating private key

Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the Certificate type. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. Subscribers should also take commercially reasonable measures for the physical protection of their workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

Method of deactivating private key

Vista Kencana Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. Vista Kencana prevent unauthorized access to any activated cryptographic modules. Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

Method of destroying private key

When Private Root Key are damage or leaked or compromised, Vista Kencana may destroy a Private Key by deleting it from all known storage partitions Vista Kencana also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, Vista Kencana destroy CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key.

Cryptographic Module Rating

As stipulated in 6.2.1.

6.3 Other aspect of key pair management

Public key archival

Vista Kencana archives copies of Public Keys in accordance with Section 5.5

Certificate operational periods and key pair usage periods

Maximum validity period:

Type	Private Key Use	Certificate term
Publicly Trusted Root CAs	No stipulation	25 years
Publicly Trusted Sub CAs / Issuer CAs	No stipulation	15 years
Domain Validation SSL/TLS Certificates	No Stipulation	395 days*
Organization Validation SSL/TLS Certificates	No Stipulation	395 days*
Extended validation SSL/TLS Certificates	No Stipulation	395 days*
AATL Certificate	No Stipulation	825 days
CRL and OCSP responder signing	3 years	31 days
Time Stamping Authority	15 months	135 months
All Subscriber Certificates	36 months	36 months
Publicly Trusted Root CAs	No stipulation	25 years

Table 8: Certificate operational periods and key pair usage periods

6.4 Activation data

Activation data generation and installation

All password is unique and unpredictable and offers a security level appropriate to that of the protected Key Pair. Vista Kencana activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. Vista Kencana will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

Activation data protection

Password used for Key Pair activation must be protected from unauthorised use by a combination of cryptographic and physical access control mechanisms.

Other aspects of activation data

No stipulation.

6.5 Computer security controls

Specific computer security technical requirements

a) Access control to Vista Kencana services and Trusted Roles
b) Enforced separation of duties for Trusted Roles identification and authentication of
c) Trusted Roles and associated identities
d) Use of cryptography for session communication and database security
e) Archival of Vista Kencana and Subscriber history and audit data
f) Audit of security-related events
g) Self-test of security-related CA services
h) Trusted path for identification of Trusted Roles and associated identities, and
i) Recovery mechanisms for keys and the Vista Kencana System.

Computer security rating

No stipulation.

6.6 Life cycle technical controls

System development controls

a) CA systems software that is provided by Vista Kencana. Vista Kencana shall have its own mechanisms in place to control and monitor the acquisition and development of the CA systems and shall be complied with the CP and CPS.

b) All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

c) Hardware and software that is dedicated only to performing the CA functions for CA operation purposes.

d) Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel.

e) All hardware and software essential to Vista Kencana operations are scanned for malicious code on first use and periodically thereafter.

f) Vista Kencana does not install software that are not part of the CA's operation.

Security management controls

Vista Kencana has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. Vista Kencana creates a hash of all software packages and Vista Kencana software updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, Vista Kencana validates the integrity of its CA systems.

Life cycle security controls

No stipulation

6.7 Network security controls

Vista Kencana implemented appropriate security measures to ensure they are guarded against denial of service and intrusion attacks which include security guards, firewall and filtering routers. Unused network ports and services are turn off. Any boundary control devices used to protect the network on which PKI equipment are hosted deny all but necessary services to the Vista Kencana CA equipment.

6.8 Time Stamping

Vista Kencana CA components are regularly synchronized with a time service such as an atomic clock or Network Time Protocol (NTP) service. A dedicated authority such as Time Stamping Authority, may be used to provide this trusted time.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate profile

Version number(s)

Vista Kencana issues X.509 version 3 standards to construct the certificate.

Certificate extension

Vista Kencana populates certificate extensions in accordance with the applicable industry standard. Vista Kencana follow best practice and where possible prevent unnecessary risk to the relying partis when applied to name constraints.

Algorithm object identifier

Vista Kencana signs certificate will be using one of the following algorithms and OIDs.

a) SHA256WithRSAEncryption: 1.2.840.113549.1.1.11
b) SHA384WithRSAEncryption: 1.2.840.113549.1.1.12
c) SHA512WithRSAEncryption: 1.2.840.113549.1.1.13
d) ECDSA-With-SHA1: 1.2.840.10045.4.1
e) ECDSA-With-SHA256: 1.2.840.10045.4.3.3
f) ECDSA-With-SHA384: 1.2.840.10045.4.3.4

Name forms

The Distinguished Name (‘DN’) and subject DN fields contain the full X.500 DN of the certificate issuer or certificate subject. Each Certificate includes a unique serial number.

Name constraints

Vista Kencana may include name constraints in the name Constraints field when appropriate.

Certificate policy object identifier

No stipulation.

Usage of Policy Constraints

No stipulation.

Policy qualifiers syntax and semantics

Vista Kencana generally populates X.509 Version 3 Vista Kencana PKI Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CP and CPS pointer qualifier that points to the applicable Relying Party Agreement or the Vista

Kencana CP. In addition, some Certificates contain a User Notice Qualifier which points to the applicable Relying Party Agreement.

Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

Version number(s)

Vista Kencana issues x.509 version 2 standard to construct the CRL.

CRL and CRL entry extensions

Vista Kencana uses extension according to RFC 5280.

7.3 OCSP profile

Version number(s)

Vista Kencana operates an OCSP in accordance with RFC 6960.

OCSP extensions

The OCSP Responder certificate shall comply with RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile).

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency of circumstances of assessment

A comprehensive compliance audit on Vista Kencana CA operations is performed annually as required by Section 20 of the DSA and the WebTrust for CA guidelines.

8.2 Identity/qualification of assessor

The auditors must be accredited as qualified auditor by the Malaysian Communications & Multimedia Commission (MCMC). The list of qualified auditors can be found here: https://www.mcmc.gov.my/en/sectors/digital-signature/list-of-qualified-auditors.

8.3 Assessor's relationship to assessed entity

The auditor shall be completely independent from Vista Kencana and the RA.

8.4 Topics covered by assessment

The audit covers Vista Kencana business practices disclosure, the integrity of Vista Kencana PKI operations, and Vista Kencana compliance with this CP and referenced requirements. The audit verifies that Vista Kencana is compliant with the CP.

8.5 Actions taken as a result of deficiency

If an audit reports noncompliance with the applicable law, this CP and corresponding CPS, or any contractual obligations related to the Vista Kencana certificate services and CA operation, then:

a) The auditor shall document the discrepancy.
b) The auditor shall promptly notify the issuing CA's management and the local CA regulation body.
c) The issuing CA shall submit the plan of action to the local CA regulation body on how to rectify the non-compliance issues.

The local CA regulation body may require additional action if necessary to rectify any significant issues created by noncompliance, including requiring suspension of certificate issuance to the Subscriber.

8.6 Communication of results

The results of each audit shall be reported to the local CA regulation body for review and resolution of any deficiency through subsequent corrective action plan. The results shall also be communicated to any third-party entities entitled by law, regulation, or agreement to receive a copy of the audit results.

8.7 Self-Audits

During the period in which the CA issues Certificates, the Vista Kencana monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Certificate issuance or renewal fees

For issuance or renewal certificates, Vista Kencana will require payment of fee. Condition and agreement will be made clear to the applicants.

Certificate	Fee per certificate (RM)
Class 1	RM 50.00

Certificate	Fee per certificate (RM)
Class 2	RM150.00
Class 3	RM 300.00

Certificate access fees

Vista Kencana does not charge any fee for accessing certificates through Vista Kencana website.

Revocation or status information access fees

Vista Kencana does not charge any fee for accessing the revocation list of certificates. However, Vista Kencana charge a fee providing customized CRL, OCSP services or other value-added revocation and status information services.

Fees for other services

Vista Kencana does not charge any fee for accessing this CP through Vista Kencana website.

Refund policy

Vista Kencana does not provide refund service for applications fee.

9.2 Financial Responsibility

Insurance coverage

No stipulation.

Other Assets

No stipulation.

Insurance or Warranty Coverage for end-entities

No stipulation.

9.3 Confidentiality of Business Information

Scope of confidential information

Based on applicable law in Malaysia, all confidential information and documents relating to the Vista Kencana certification services, transactional records, audit trail and report, disaster recovery plain and security measures controlling the operation hardware and software and enrolment services need be kept confidential

Information not within the scope of confidential information

Information certificate, certificate revocation, certificate practice and policy statement, are not confidential. It can view publicly.

Responsibility to protect confidential information

Trust personnel of Vista Kencana and contractor shall be responsible to protect confidential information.

9.4 Privacy of Personal information

Privacy plan

Vista Kencana has implemented privacy plans. It can be found in Vista Kencana website.

Information treated as private

Authenticated subsidizer information is treated as private.

Information not deemed private

As stipulated in 9.3.2.

Responsibility to protect private information

All confidential information in Vista Kencana should securely store and protected against accidental disclosure by trust person and contractor.

Notice and consent to use private information

Any private information submitted by subscriber or publication have its or their consent.

Disclosure pursuant to judicial or administrative process

Vista Kencana shall be entitled to disclose Confidential/ Private Information notice regarding to law enforcement compliance Act 562 DIGITAL SIGNATURE ACT 1997,

9.5 Intellectual Property Rights

Vista Kencana holds the intellectual property rights on the certificate issued, CRLs, customers guideline relating to the certificate services, CP and CPS documents, all internal and external documents related to certificate services, operation data, databases, and websites.

9.6 Representations and Warranties

CA representations and warranties

CA warrant that:

a. Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created.
b. Their private key is protected, and that no unauthorized person has ever had access to the Subscriber's private key.
c. All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true.
d. All information supplied by the Subscriber and contained in the Certificate is true.
e. The Certificate is being used exclusively for authorized and legal purposes, consistent with this CP; and
f. The Subscriber is an end-user Subscriber and not a CA and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

RA Representations and Warranties

RA warrant that:

a. There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate.
b. There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application because of a failure to exercise reasonable care in managing the Certificate Application.
c. Their Certificates meet all material requirements of this CP; and
d. Revocation services (when applicable) and use of a repository conform to the applicable CP in all material aspects.
e.

Subscriber Agreements may include additional representations and warranties.

Subscriber representations and warranties

Subscribers warrant that:

a. Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has

been accepted and is operational (not expired or revoked) at the time the digital signature is created.

b. Their private key is protected, and that no unauthorized person has ever had access to the Subscriber's private key.
c. All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true.
d. All information supplied by the Subscriber and contained in the Certificate is true,
e. The Certificate is being used exclusively for authorized and legal purposes, consistent with this CP; and
f. The Subscriber is an end-user Subscriber and not a CA and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.
g. The Subscriber shall immediately notify VK of the compromise of their private key in the event that it is observed.
h. The subscriber data with digital signatures may need to be re-signed before the security value of an available digital signature decreases with time.
i. The subscriber in respect of the generation of key pairs and the need to keep the private key secure from compromise and in a trustworthy manner and that software and hardware used shall satisfy the technical components prescribed under the Digital Signature Act 1997
j. If the subscriber is the recipient of a digital signature or certificate, the subscriber, as recipient, is responsible for deciding whether to rely on it, and that before making that determination, the subscriber should check the repository of the licensed certification authority issuing the certificate or certifying the public key listed in the certificate to confirm that the certificate is valid and not revoked or suspended. Then the subscriber should use the certificate the subscriber received to verify that the digital signature received was created during the operational period of the certificate by the private key corresponding to the public key listed in the certificate, and that the message associated with the digital signature received has not been altered.
k. If a time-stamp is required under any written law or if a particular time may be significant with regard to the use of digitally signed data, a time-stamp by a recognized data/time stamp service should be appended or attached to the message or digital signature or other document.

Subscriber Agreements may include additional representations and warranties.

Relying party representations and warranties

Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP. Relying Party Agreements may include additional representations and warranties.

Representations and warranties of other participants

No stipulations.

9.7 Disclaimer of warranties

Vista Kencana disclaims all warranties and obligations based on applicable law, Subscriber Agreement and Relying Party Agreement.

Vista Kencana CA' s liability

Vista Kencana shall not be held liable for losses due to false or forged signatures if they have complied with the Act, or for punitive or exemplary damages.

Registration Authorities' Liabilities

a) In case RA cause Subscribers and users to suffer damages by violating provisions in this CP, RA's will be subject to the same liabilities as applicable to Vista Kencana CA.
b) As a security for such Liability for Damages, Registration Authorities may subscribe to public liability insurance.

Subscriber's liability

In case, Subscribers have caused Vista Kencana CA to suffer losses due to violation of Subscriber's responsibilities in CP, Vista Kencana CA shall have the rights to claim the losses from the subscribers.

Claim by Subscriber

In case subscriber want to do claim, Vista Kencana will provide the procedure to subscriber on how subscriber do their claim as figure below;

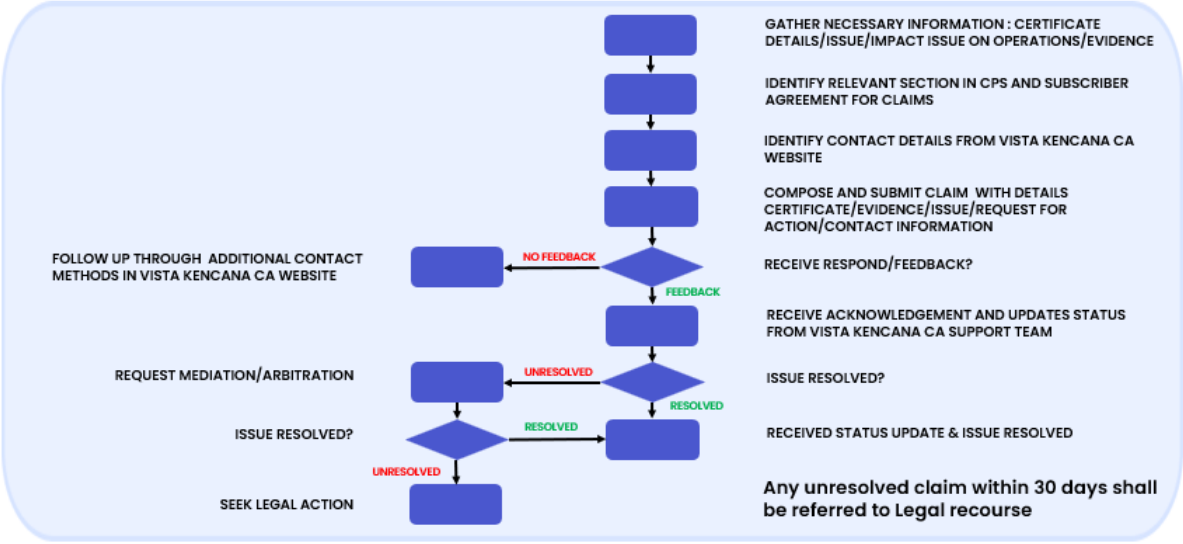

Figure 2 : Claim by subscriber operation procedure

9.8 Limitations of Liability

Vista Kencana may limit its liability to any extent not otherwise prohibited by this CP. In addition to Applicable Laws, Subscriber Agreement and Relying Parties Agreement, Vista Kencana shall limit Vista Kencana's liability not exceeding the reliance limit below:

Certificate	Reliance Limit
Class 1	RM500.00
Class 2	RM25,000.00
Class 3	RM400,000.00

9.9 Indemnities

Vista Kencana assumes no financial responsibility for improperly used certificates, CRLs, etc.

9.10 Term and Termination

Term

This version of CP is effective upon publication until new version is available.

Termination

This CP document will be amended from time to time until replaced by a latest version.

Effect of termination and survival

Vista Kencana communicates the validity of present CP version termination via the Vista Kencana Repository.

9.11 Individual Notices and Communications with Participants

Vista Kencana will use subscriber contact information to send individual notices. For relying parties, Vista Kencana will publish over the website.

9.12 Amendments

Procedure for amendment

Any amendment in this document will create new version of CP and publish in Vista Kencana website.

Notification mechanism and period

Vista Kencana post appropriate notice on the websites under the repository section.

Circumstances under which OID must be changed

No stipulation.

9.13 Dispute Resolution Provision

For Subscriber Agreements shall contain a dispute resolution clause. As state in Subscriber Agreement, any unresolved dispute within thirty (30) days shall be referred to legal action.

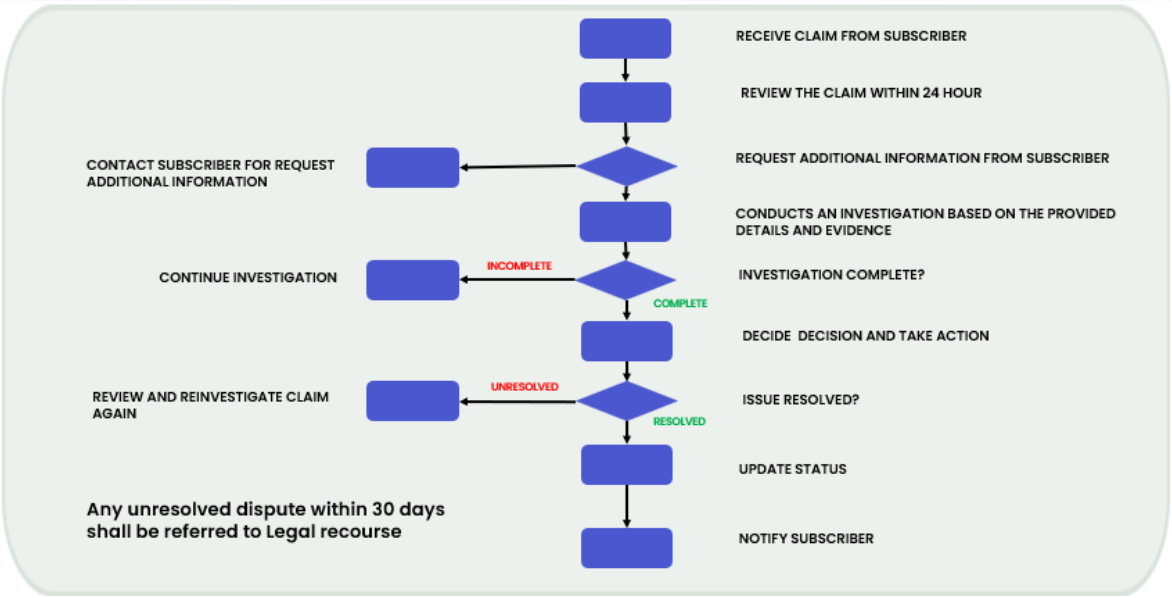

Figure 3 : Dispute Resolution operation procedure

9.14 Governing Law

This CP complies with the Malaysian Law, Digital Signature Act 1997 (Act 562) and the Digital Regulations 1998. Compliance with applicable law

9.15 Compliance with Applicable Law

Vista Kencana obliged to adhere with the applicable legislation as stated under 9.14.

9.16 Miscellaneous Provisions

Entire agreement

No stipulation.

Assignment

No stipulation.

Severability

If a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.

Enforcement (attorneys' fees and waiver of rights)

No stipulation.

Force Majeure

Vista Kencana shall not be liable for any losses, costs, expenses, liabilities, damages, or claims arising out of or related to delays in performance or from failure to perform its obligations if such failure or delay is due to circumstances beyond Vista Kencana reasonable control, including without limitation, acts of any governmental body, war, insurrection, sabotage, embargo, fire, flood, strike or other, interruption of or delay in transportation, unavailability of interruption or delay in telecommunications or third party services.

9.17 Other Provisions

No stipulation.