VISTA KENCANA

TIME STAMPING AUTHORITY POLICY & PRACTICE STATEMENT

Version 1.2

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	10/12/2023	NURUL NATASHA CHE SAID	Creation
1.1	14/05/2024	NURUL NATASHA CHE SAID	Revision
1.2	23/01/2025	NURUL NATASHA CHE SAID	**Section 1** Add new paragraph **Section 3.1** Add: Term and definition = Vista Kencana Sdn Bhd **Section 4** Remove Time Stamping Authority Policy and Practice Statement **Section 5.2** Add The object identifier of this policy 1.3.6.1.4.1.62612.3 **Section 6.1.2** Add Vista Kencana uses an independent external time source to provide time. The time source use **Section 6.4** Add new paragraph

Table of Contents

LIST OF TABLES

LIST OF FIGURES

No table of figures entries found.

1 Scope

This Time Stamping Authority Policy & Practice Statement (TSAPPS) is intended to specify policy and security requirements relating to the operation and management practices of Vista Kencana as a Time Stamp Authority (hereinafter, Vista Kencana TSA) for issuing recognised date time stamps.

Vista Kencana TSA issues Time-Stamping Tokens in accordance with the ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" standard.

This document also ensures Vista Kencana as the Time Stamping Authority ("TSA") is conforming to the guidelines and principles established by Malaysian Communications and Multimedia Commission ("MCMC") to enable trust and confidence towards the date-time stamping services based on the applicable requirements stated in the DSA (Part VI, Section 70) and DSR (Part IX, Regulation 58 – 70). This document is also based on the time-stamping protocol in RFC 5816 (update for RFC 3161)

2 References

a) Digital Signature Act 1997
b) Digital Signature Regulations 1998
c) Malaysian Communications and Multimedia Commission (MCMC) "Requirements for Certification Authority (CA) to be recognised as a Time Stamping Authority (TSA) 2018"
d) Malaysian Communications and Multimedia Commission (MCMC) "Recognition Framework for Time Stamping Authority (TSA) 2018'
e) Certification Practice Statement (CPS) of Vista Kencana
f) IETF RFC 3161 "Internet X.509 Public Key Infrastructure Time-stamp Protocol"
g) IETF RFC 5816 "ESSCertIDv2 Update for RFC 3161"
h) IETF RFC 3628 "Policy Requirements for Time-Stamping Authorities (TSAs)"
i) ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
j) ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Time Stamps".
k) ETSI EN 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities"
l) ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles"
m) WebTrust for CA 2.0: "Trust Service Principles and Criteria for Certification Authorities version 2.0"

3 Definition and Acronym

3.1 Definitions

Term	Definition
NTP	Network Time Protocol (NTP) is a networking protocol for clock synchronization of computer systems over network packet routing with variable latency. The standard for reference is the IETF RFC 1305 (Network Time Protocol (NTP v3)).
Relying party	A recipient of a time-stamp certificate who acts in reliance on that certificate and/or signature verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.
Service Availability	The amount of time expressed as a percentage during which the Service is available for the Customer over a defined period.
Subscriber	Organisation or a person who - • is the subject listed in a certificate. • accepts the certificate. • holds a private key which corresponds to a public key listed in that certificate.
Time-stamp	Data in electronic form which binds other electronic data to a time, providing evidence that these data existed at such time.
Time-Stamping Authority (TSA)	It is the TSP providing time-stamping services using one or more time-stamping units.
Time-stamp policy	A set of rules that indicate the applicability of a time-stamp to a community and/or class of application of the common security requirements. This is a specific type of trust service policy as defined in ETSI EN 319 421.
Time-stamping service	Time stamp service recognized by the Controller for issuing timestamps
Time-Stamping Unit (TSU)	The set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.
Trust Service Provider (TSP)	Entity which provides one or more trust services
TSA Disclosure statement	Set of statements about the policies and practices of a TSA which particularly require emphasis in the disclosure to subscribers and relying parties, for example to meet regulatory requirements.
TSA practice statement	Statement of the practices that a TSA employs in issuing timestamps.
TSA system	Set of IT products and components employed to provide support to the provision of time-stamping services.

Term	Definition
Vista Kencana Sdn Bhd (VK)	Vista Kencana Sdn Bhd and its affiliated and associated companies.

Table 1: Definition

3.2 Acronyms

Term	Definition
CA	Certification Authority
DSA	Digital Signature Act 1997
DSR	Digital Signature Regulations 1998
MCMC	Malaysian Communications and Multimedia Commission
MST	Malaysian Standard Time
TSAPPS	Time-Stamping Authority Policy and Practice Statement
TSA	Time Stamping Authority
TSP	Time Stamp Policy
TST	Time-Stamp Token
UTC	Coordinated Universal Time

Table 2: Acronyms

4 GENERAL CONCEPTS

Vista Kencana TSAPPS is a detailed description of the terms and conditions regarding the provision of the services, and managerial and operational practices that the Vista Kencana TSA follows in the provision of time-stamping services.

It also follows the requirements established in the CPS of Vista Kencana.

4.1 Time-Stamping Services

The certificate issued by the Vista Kencana will be used to sign and verify the stamp. Use beyond the limits and contexts specified in the TSAPPS and Vista Kencana's project / service contracts is strictly prohibited.

Vista Kencana TSA adheres to the standards and regulations established in Section 2 (References) of this document to keep trustworthiness of the time-stamping services for subscribers and relying parties.

4.2 Time-stamping Authority

TSA provides time-stamping services to the public. The TSA has the overall responsibility for the provision of the time-stamping services and the operation of one or more TSUs which creates and signs on behalf of the TSA.

Vista Kencana TSA hereby confirms that the TSA is audited at least every 12 months by a conformity assessment auditor. When the auditor requires the TSA to remedy any breach of the requirements, the TSA shall act accordingly and in due course. The control body shall be informed of any changes to the TSA provision.

Vista Kencana TSA may operate several identifiable time-stamping units.

4.3 Subscriber

Subscriber could be individuals or organisations who hold and/or rely on TST or certificates in electronic transactions. Subscribers are entities that hold a service contract with Vista Kencana and have agreed to the Vista Kencana TSA Subscriber Agreement.

If the Subscriber is an organisation, some of the TSA Subscriber Agreement obligations that apply to the organisation must apply as well to the end-users in the organisation. In any case, the organisation will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such organisation is expected to suitably inform its end users.

When the Subscriber is an end-user, the end-user will be held directly responsible if its TSA Subscriber Agreement obligations are not correctly fulfilled.

4.4 Time-Stamp Policy and TSA Practice Statement

4.4.1 Purpose

Vista Kencana TSP and Vista Kencana Time-Stamp Practice Statement have been merged into one document, the Vista Kencana TSA Policy and TSAPPS. TSAPPS specifies a time-stamp policy and practice statement to meet general requirements for trusted time-stamping services as defined by the standards in Section 2 (References).

5 TIME-STAMPING POLICIES

5.1 Overview

Vista Kencana TSP defines a set of processes for the trustworthy creation of time-stamp tokens in accordance with ETSI EN 319 421. The private keys and the TSU meet the technical specifications of ETSI EN 319 422 and RFC 3161.

Vista Kencana TSA signs time-stamps using private keys that are reserved specifically for that purpose. Each TST contains an identifier to the applicable policy, and TSTs are issued with time accurate to ±1 second of MST or better.

5.2 Identification

The object-identifier of Vista Kencana time-stamping is reference in every Vista Kencana issued time-stamp, and by including in the generated time-stamps. The object identifier of this policy is 1.3.6.1.4.1.62612.3

5.3 User Community and Applicability

Vista Kencana time-stamp is applicable to the Subscriber and their Relying Parties.

Vista Kencana provides public time-stamp services or time-stamping services that are used within a closed community. Vista Kencana time-stamp may be applied to any application which requiring proof that a datum existed before a particular time.

6 OBLIGATION AND LIABILITY

6.1 TSA OBLIGATIONS

6.1.1 General

Vista Kencana implements all requirements specified in its TSAPPS.

Vista Kencana ensures conformance with the procedures prescribed its TSAPPS.

All TSA functionality is undertaken by Vista Kencana.

Vista Kencana will adhere to any additional obligations indicated in time-stamps either directly or incorporated by reference.

6.1.2 TSA Obligations toward Subscribers

Vista Kencana provides permanent access to the time-stamping service except during maintenance intervals and except during periods where a reliable time source is not available or other events that do not lie in Vista Kencana's sphere of influence (force majeure, war strike, governmental restrictions, etc.). Vista Kencana Service Availability (per year) for its time-stamping service is 97%.

Planned maintenance windows may be contractually agreed upon with Subscribers; they may also be announced on Vista Kencana's website.

Vista Kencana implements and operates a reliable and trustworthy infrastructure for information exchange and communication. This is regularly verified by independent third-party audits. These external audits include audits pursuant to the standards and regulatory requirements mentioned in Section 2 (References).

All these audits require demonstration of a maximum level of security and conformity to documented policies and practices. The respective provisions supplement one another and serve to enhance the overall security controls, which are audited regularly by independent third parties.

Vista Kencana respects the role of trademarks and intellectual property.

Vista Kencana uses an independent external time source to provide time. The time source used by Vista Kencana is – Malaysian NTP source provided by SIRIM.

Vista Kencana provides subscribers and relying parties with the necessary information about the terms and conditions regarding the use of Vista Kencana time-stamping service as specified in Section 7: TSA Disclosure Statement.

Vista Kencana shall communicate any changes in relation to its time-stamping services via announcements in its online registration system and updates to its TSAPS document which shall be made available in Vista Kencana's website. Additionally, Vista Kencana will also inform, by appropriate means, to the subscribers and relying parties in the case of any time drift detected or in the event of any cryptographic algorithms and / or the key sizes used are no longer considered safe.

6.2 Subscriber Obligations

It is the responsibility of the Subscriber to ensure that it uses and configures the TSA services as instructed by Vista Kencana.

It is the responsibility of the Subscriber to ensure all the information that has been provided to Vista Kencana TSA for the purpose of obtaining a TSU certificate is accurate and kept up to date as soon as practicable.

Subscribers are to maintain the integrity of the private key of the corresponding public key pair that is kept in Vista Kencana's repository. Vista Kencana will not be held liable, be in breach of this TSAPPS, negligent, or be subject to any form of liability because of a breach in the integrity of the private key. Subscribers must inform Vista Kencana within 48 hours of a change to any information included in their certificate or certificate application request. Subscribers must also inform Vista Kencana within 8 hours of a suspected compromise of one/both of their private keys.

Subscribers are not to submit to Vista Kencana any material that is offensive, racially discriminative or prejudiced in any other manner, obscene, pornographic, illegal,

hateful within the context of Malaysian laws or the subscriber's local applicable law (where there is discrepancy between the laws, Malaysian law will take precedence), or stolen. The list provided is not meant to be exhaustive. In a more general term, the material submitted must not be of such a manner that it will:

a) violate any law whether Malaysian or otherwise; and/or
b) causes the Vista Kencana to be liable for breach of a law whether Malaysian or otherwise.

6.3 Relying Party Obligations

The relying parties are obliged to:

a) restrict reliance on the certificates issued by Vista Kencana to the appropriate usage for those certificates in accordance with Vista Kencana's CPS / this TSAPPS and with the certificate policy under which the certificate was issued.
b) verify certificates before verifying a digital signature, including the use of CRLs and in accordance with the certification path validation procedure specified in ITU-T Rec. X.509:19971 ISO/IEC 9594-8 (1997), considering any critical extensions; and
c) trust and make use of certificates only if a valid certificate chain is established between the relying party and the certificate owner.

6.4 Liability

Vista Kencana is only liable for damages to Subscribers or Relying Parties that result from Vista Kencana's failure to comply with the DSA and DSR. Vista Kencana TSA must supply evidence that they have adhered to applicable laws, rules, and regulations. Vista Kencana shall in no event be liable, for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law. The Vista Kencama TSA shall not be liable for any damages resulting from infringements by the Subscriber or the Relying Party on the applicable terms and conditions, including the exceeding of the transaction limit. Vista Kencana shall under no circumstances be liable for damages that result from force majeure events as detailed in Section 7.6 of this Vista Kencana TSAPS document and in Section 9.16.5 of Vista Kencana CP/CPS. Vista Kencana shall take commercially reasonable measures to mitigate the effects of force majeure in due time. Any damages resulting from any delay caused by force majeure will not be covered by the Vista Kencana TSA

7 TSA PRACTICES

7.1 Practice and Disclosure Statement

7.1.1 Entire Agreement

Vista Kencana's TSA Disclosure Statement (this section of this document) discloses to all subscribers and potential relying parties the terms and conditions regarding the use of Vista Kencana's time-stamping services. Vista Kencana TSA Disclosure Statement is specified in Annex C: TSA Disclosure Statement.

7.2 Tsu Key Management Life Cycle

This section sets forth practices related to the key life cycle management controls of the Timestamp TSA.

7.2.1 Tsu Key Generation

Vista Kencana generates the cryptographic keys used in its TSA services under the authorisation of at least two (2) Authorised Prseonnals at any time and in a secure physical environment. The personnel authorized to carry out this function shall be limited to those requiring doing so under Vista Kencana practices. Additional information is provided in section 6.1 (Key Generation and Installation) of Vista Kencana CPS.

The generation of the TSU's signing key(s) is carried out within a cryptographic module which is conformant to FIPS PUB 140-2 level 3.

The TSU uses an RSA key pair with a length of 2048-bit. This key pair is used only for signing TSTs.

7.2.2 TSU Private Key Protection

The practices of TSU key protection, storage, backup, and recovery, described in section 6.2 and 6.3 of Vista Kencana CPS.

The TSU's private key shall be backed up and stored safely for the unlikely event of key loss due to unexpected power interruption or hardware failure. The backup of the private key is kept in secret and its integrity and authenticity is preserved in a safe box. These include use of HSMs certified to FIPS 140-2 Level 3 or higher to hold and sign with the keys.

7.2.3 TSU Public Key Distribution

Vista Kencana TSU Public Keys are made available in a Digital Certificate. Additional information is provided in section 6.1 (Key Generation and Installation) of the Vista Kencana CPS.

7.2.4 Rekeying TSU's Key

TSU private signing keys are replaced before the end of their validity period, (i.e., when the algorithm or key size is determined to be vulnerable). Additional information is provided in section 4.6 (Certificate Renewal) and section 4.7 (Certificate Re-Key) of Vista Kencana CPS.

7.2.5 End of TSU Key life Cycle

TSU private signing keys are replaced upon their expiration. After expiration of the private keys, the private keys within the cryptographic module are securely destroyed in a way the private keys cannot be retrieved. The TSU rejects any attempt to issue time-stamps once a private key has expired.

7.2.6 Life Cycle Management of Cryptographic Module to Sign Time-Stamps

Vista Kencana has in place procedures to ensure that hardware security modules intended for non-repudiation services are not tampered with in shipment or storage. Acceptance testing is performed to verify that cryptographic hardware is performing correctly. Additional information is provided in section 6.6 (Life Cycle Technical Controls) of Vista Kencana CPS.

7.3 Time-Stamping

7.3.1 Time-Stamp Token Issuance

Vista Kencana offers time-stamping services using RFC 3161 "Time Stamp Protocol (TSP)".Each TST contains the Time-Stamping Policy identifier, a unique serial number and a certificate containing the identification information Vista Kencana TSA`s TSU.

The TSU, in the time-stamp requests, accepts SHA256 and above hash algorithms and uses the SHA-256 cryptographic hash function to sign TST.

The TSU keys are 2048-bit RSA keys. The key is used only for signing TSTs.

The TSU does not issue any TST when the end of the validity of the TSU private key has been reached.

7.3.2 Clock Synchronization with MST

Vista Kencana TSA provides time with ±1 second of UTC which is its clock is synchronized with UTC using the NTP protocol. TSU clocks are recalibrated at least twice daily against the reference UTC time source, primarily being the National Metrology Institute of Malaysia.

TSU clocks are also able to monitor time drift outside pre-set boundaries and request additional recalibrations as needed. If the re-calibration fails, Vista Kencana TSA will not issue timestamps until correct time is restored.

7.3.3 Time or frequency of publication

Every time issuance of certificate will publish to repository. For CRL, will publish once a day. Vista Kencana shall notify the subscribers in writing, in the event the recognised date/time stamp service is unable to comply with the time limit specified in Regulation 62 (1).

7.4 TSA MANAGEMENT AND OPERATIONS

7.4.1 Security Management

Vista Kencana TSA has implemented an information security management system to maintain the security of the service. Vista Kencana's organisational structure, policies, procedures, and controls are applicable to Vista Kencana TSA. Additional information is provided in section 5 (Facility, Management, and Operational Controls) and section 6 (Technical Security Controls) of Vista Kencana CPS.

7.4.2 Asset Classification and Management

Vista Kencana maintains a classification system for all IT systems and assets to ensure that the information and the assets itself receive appropriate security treatment. All media and data are handled securely. Data from disposed media is securely deleted, electronically or by destroying the disposed media. All software components of the PKI developed by Vista Kencana are developed in conditions and following a process that ensure their security. Vista Kencana ensures, during software updates, the origin and integrity of the software. Vista Kencana ensures that all software updates are done in a secure way. Updates are performed by personnel in a Trusted

Role. Vista Kencana separate the development and testing infrastructures from the production infrastructure of the PKI.

7.4.3 Personnel Security

The practices defined in section 5.2 and 5.3 of Vista Kencana CPS are applicable. Vista Kencana has understood that talented and motivated employees are a key factor for the success of the business. The hiring practices are a very important process in the organisation. Only well educated, with respect to their job role, and trustworthy personnel fulfil operations of the time-stamping service.

Vista Kencana verifies that the necessary knowledge is possessed, or it is transferred via training courses and that they have passed the necessary tests proving the acquisition of knowledge.

7.4.4 Physical and Environmental Security

Vista Kencana's office is located at Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia. Vista Kencana TSA ensure that time-stamping management facilities are operated in an environment that protects physically and logically the transaction services with controls of unauthorized access to systems or data.

Physical access to Vista Kencana is restricted to authorised personnel. Each entry in the physically secure area accompanied, registering the identity, entry and exit time. The TSA's physical and environmental security policy, for systems concerning with the time-stamping management, addresses the physical access control, natural disaster protection, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery. Vista Kencana deploys uninterruptible power source (UPS) system that shall ensure uninterrupted services for all CA systems and applications in case of power failures which all essential power is connected to standby generator system. Vista Kencana uses air-conditioning system and raised floor to ensure optimum ventilation and protection. For water exposures Vista Kencana installs the core CA systems at a reasonable height to protect them from flood damage. For fire safety factors, Vista Kencana installs fire detector, portable fire extinguisher, and automatic fire extinguishing facilities to prevent the core certification systems from fire damage.

Vista Kencana controls physical access to its major storage media that are stored in safes. Vista Kencana critical system data is incrementally backed-up daily. Full back-ups are performed on a weekly, monthly, and annual basis. Vista Kencana shreds and crushes documents, CD-ROMS, diskettes, and other items to prevent information from such materials from being leaked.

For off-site backup, Vista Kencana maintains offline backup storage of subscriber certificates, including CRL for ten (10) years after the corresponding digital certificates are issued.

7.4.5 Operations Management

Computer Security Controls

Specific Computer Security Technical Requirements

The CA workstation is physically secured as described in TSAPPS Part 7.4.4. All computers installed with the CA software are configured to perform CA operations only. All irrelevant services of the operating system are disabled. The operating system enforces identification and authentication of all users. The archive files are backed up as they are created. Originals are stored on-site and housed with the Vista Kencana CA system. Backup of the archive files is stored at a secure and separate geographic location. On monthly basis the archive tapes are retrieved by a PKI / System Engineer and verified to ensure that no damage or loss of data has occurred. If any loss has occurred, the backup archive is retrieved to become the new master archive and a new backup is produced.

7.4.6 Network Security

Vista Kencana performs all its TSA functions using secured networks in compliance with Webtrust for CA and ISMS ISO/IEC 27001 standards to prevent unauthorised access and malicious activity. Vista Kencana protects its communications of sensitive information using firewalls, intrusion detection encryption and digital signatures.

7.4.7 Incident Management

Incident and Compromise Handling Procedures

Vista Kencana will use its business continuity procedures that consist of process or steps to be taken in the event of disaster including corruption or loss of computing resources that can affect Vista Kencana business or services. The business continuity plan is included in the audit scope to validate the effectiveness restoration process and the recovery plan. CA personnel in trusted role should be trained accordingly to ensure they operate in accordance with the procedures defined in the recovery plan.

Computing Resources, Software, and / or Data Are Corrupted

Vista Kencana has established business continuity procedures that outline the action steps in the event of the corruption or loss of computing and networking resources, software and/or data.

7.4.8 Collection of Evidence

In the event of detecting a potential hacking attempt or other form of compromise, Vista Kencana TSA shall refer to its incident management procedure and disaster recovery plan, and eventually perform an investigation to determine the nature and the degree of damage:

TSU key management

a) Records concerning all events relating to the life cycle of TSU keys will be logged.
b) Records concerning all events relating to the life cycle of TSU certificates will be logged.

Clock Synchronization

a) Records concerning all events relating to synchronization of a TSU's clock to MST will be logged. This includes information concerning normal re-calibration or synchronization of clocks used in time-stamping.
b) Records concerning all events relating to detection of loss of synchronization will be logged.

The confidentiality and integrity of current and archived records concerning operation of services shall be maintained. They will be completely and confidentially archived in accordance with disclosed business practices. Those records will be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings. Those events will be securely saved in a way that they cannot be easily deleted or destroyed for a period of 10 years.

7.4.9 System Development and Maintenance

Applications are developed and implemented in line with Vista Kencana systems development and change management standards. Vista Kencana provides client software to its clients for the performance of the subscribed TSA functions and services. Such software is developed in accordance with Vista Kencana system development standards.

The hardware and software are dedicated to performing TSA activities. There are no other applications, hardware devices, network connections, or component software installed which are not parts of the TSA operation.

7.4.10 Business Continuity Management

In the event of TSU private key compromised or suspected to be compromised, Vista Kencana TSA shall inform Subscribers and Relying Parties to stop using the compromised key.

In the event of loss of clock synchronization, Vista Kencana TSA suspends its operation until further notice and to ensure the recovery procedure is operated accordingly. The Recovery Plan is activated to restore the synchronization and service.

The time-stamping service itself is in a physical secured environment that minimizes the risk of natural disasters for example fire. The private keys of the TSU are stored in a cryptographic security module. In case private keys become compromised, the archive of saved Vista Kencana helps differentiate between correct and false time-stamps in an audit trail.

Vista Kencana Data Centre is in Selangor, Malaysia and it is built with standard supporting infrastructure to ensure the continuity of Vista Kencana's daily operations. Meanwhile Vista Kencana's Disaster Recovery Centre is in Cyberjaya (about 30kms away from Selangor, Malaysia) whereby it is a facility that Vista Kencana uses to recover and restore its technology infrastructure and operations when its primary Data Centre becomes unavailable.

7.4.11 Operations Management

Vista Kencana maintains operation controls based on ETSI EN 319 421. Vista Kencana shall undergo internal and external audits to review the effectiveness of these controls. Additional information in relation to Operations Management is provided in TSAPPS Part 7.4.4.

7.4.12 System Access Management

Vista Kencana shall maintain an appropriate physical and logical access controls on the affected facilities, equipment, system and information as stipulated in TSAPPS Part 7.4.4 The systems access management controls of Vista Kencana TSA are incorporate with Vista Kencana PKI system access management controls.

7.4.13 Trustworthy System Development and Maintenance

Vista Kencana TSA's systems deployment and maintenance controls are incorporated with overall Vista Kencana systems deployment and maintenance controls. Additional information is provided in section 6 (Technical Security Controls) of the Vista Kencana CPS.

7.4.14 Compromise and Disaster Recovery of TSA Services

If TSA services are compromised or suspected to be compromised, Vista Kencana shall perform the following procedures:

a) inform regulator / the controller i.e.: MCMC.
b) inform subscribers, cross-certifying TSAs and relying parties.
c) terminate the certificates and CRLs distribution service for certificates/CRLs issued using the compromised private key.
d) request the revocation of the TSA's certificate.

7.4.15 TSA Termination

If Vista Kencana ceases operation, the Controller shall appoint another licensed certification authority to take over the time-stamping certificates by certification authority whose license has been revoked or surrendered or has expired and such certificates shall, to the extent that they comply with the requirements of the appointed licensed certification authority, be deemed to have been issued by that licensed certification authority. Vista Kencana has a termination plan in place to minimise disruption to Customers, Subscribers, and Relying Parties. The plan meets the following requirements:

a) ensure that any disruption caused by the termination of an issuing TSA is minimised as much as possible;
b) ensure that archived records of the TSA are retained;
c) ensure that prompt notification of termination is provide to Subscribers, Authorised Relying Parties, Application Software Providers, and other relevant stakeholders;
d) ensure certificate status information services are provided and maintained or the applicable period after termination.

7.4.16 Compliance with Legal Requirement

In compliance with the Malaysia's Digital Signature Act 1997 and the Digital Signature Regulations 1998 and any other instruments issued under the Digital Signature Act 1997 and the Digital Signature Regulations 1998, this TSAPPS intends to prescribe

all matters concerning Vista Kencana as TSA and the certification services including certificate issuance and management, operation of certification systems, and responsibilities and liabilities of the related parties such as Vista Kencana TSA, and its Subscribers.

7.4.17 Recording of Information Concerning Operation of Time-Stamping Services

Vista Kencana shall maintain and archive with all relevant information concerning the operation of Vista Kencana TSA for a retention period of 10 years. All the records shall be time-stamped to maintain and protect the data integrity. The records in custody are treated as confidential in accordance with VISTA KENCANA CPS. Records concerning the operation of time-stamping services are available at the request of Subscribers or if required by court order or another legal requirement.

7.4.18 Notification of Incidences

Vista Kencana shall notify the subscribers in the event the recognised date/time stamp service is unable to comply with the time limit specified in Regulation 62 (1).

7.5 Organisational

Vista Kencana's organisational structure, policies, procedures, and controls are applicable to Vista Kencana TSA. The organisational procedures comply with the rules and regulations defined in Section 2 (References) of this document.

Additional References:

Annex A : Time stamping protocol and profile

Vista Kencana Time Stamping Root CA (Root CA Certificate)

Certificate Field	Critical Extension	Content
Issuer		Must match subject
Subject		Must contain countryName, organisationName, and commonName
Extension: basicConstraints	Critical	Critical cA is TRUE; pathLenConstraint is not present
Extension: keyUsage	Critical	keyCertsign and cRLSign bits are set

Vista Kencana TSA (Sub CA Certificate)

Certificate Field	Critical Extension	Content
Validity: notAfter		Not later than the notAfter of the signing certificate
Subject		Must contain countryName, organisationName, and commonName
Extension: certificatePolicies	Not Critical	Must contain at least one et of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Critical	Critical cA is TRUE
Extension: keyUsage	Critical	keyCertsign and cRLSign bits are set

End-entity Certificate

Certificate Field	Critical Extension	Content
Validity: notAfter		Not more than 24 months after the validity:notBefore or the date the Certificate was issued

Subject		Must contain countryName, organisationName, and commonName
Extension: authorityKeyIdentifier	Not critical	Matches subjectKeyIdentifier of signing certificate
Extension: certificatePolicies	Not Critical	Must contain at least one set of policyInformation containing at least a policyIdentifier
Extension: basicConstraints	Not Critical	Empty or not present
Extension: keyUsage	Critical	digitalSignature bits must be set
Extension: extKeyUsage	Critical	Must include timeStamping
Extension: cRLDistributionPoints	Not critical	Must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

Annex B : Malaysian Standard Time

On August 5, 1992, the Malaysian Cabinet appointed the National Metrology Institute of Malaysia to be the national timekeeper, and to assume a variety of responsibilities, including the:

- maintenance of time interval standards;
- establishment of the national atomic time scale; and
- establishment and maintenance of the local Universal Coordinated Time (UTC), which is designated as UTC (NMLS) by the International Bureau of Weights and Measures.

The national atomic time scale is established and maintained using five Caesium atomic clocks, two of which are high performance and three of which are standard performance. These five atomic clocks are compared to one another to detect any abnormality or instability. One of the clocks is designated as the reference clock. By virtue of its participation in the International Bureau of Weights and Measures GPS common view time transfer, the Malaysian atomic timescale is traceable to the International Atomic Timescale.

Annex C: TSA Disclosure Statement

TSA contact info	VISTA KENCANA TSA is responsible for the development, implementation, and publishing of the VISTA KENCANA TSA Policy and Practice Statement, and all relevant documents pertaining to time-stamping services provided by VISTA KENCANA. VISTA KENCANA TSA is operated at **Vista Kencana Sdn Bhd (457608-K)** **Suite 1-2, Level 1, Wisma UOA Damansara 2, No 6 Changkat Semantan, Bukit Damansara, 50490 Kuala Lumpur.** **Tel: +603 2773 4182 Fax: +603 2773 4183** For any business inquiries, certification services, PKI and technical inquiries pleaseemail to **customercare@vistakencana.com.my**.
Electronic time-stamp types and usage	VISTA KENCANA offers time-stamping services based on RFC 3161 standard. VISTA KENCANA accept the time-stamp request hashed SHA-1, SHA-256 and SHA-512. VISTA KENCANA digital signature on the TST has a validity period of between 1 to 2 years depending on the requirement. Use of VISTA KENCANA TSA may be limited to Certificate Holders of a valid VISTA KENCANA digital certificate. Service fee is chargeable for any TST and services issued by VISTA KENCANA TSA.
Reliance limits	The level of accuracy of time that is provided by VISTA KENCANA TSA in a TST is +/- one (1) second with respect to MST. If a trusted MST time source cannot be acquired the time stamp will not be issued. Please refer to **Section 6.4 Liability** of TSAPPS.
Obligations of Subscribers	Please refer to **Section 6.2 Subscriber Obligations** of TSAPPS.
TSU public key certificate status checking obligations of relying parties	Please refer to **Section 6.3 Relying Parties Obligations** of TSAPPS.

Limited warranty and disclaimer/Limitation of liability	Please refer to **Section 6.4 Liability** of TSAPPS.
Applicable agreements and practice statement	Applicable agreements include Obligations of Subscribers and Obligations of Relying Parties described in our TSAPPS. Applicable agreements also included in VISTA KENCANA CPS.
Privacy policy	VISTA KENCANA shall post its privacy policy on its website. VISTA KENCANA shall follow its privacy policy to handle the personal information of the subscriber or the CA itself.
Refund policy	Application fee is non-refundable.
Applicable law, complaints, and dispute resolution	VISTA KENCANA TSA delivers time-stamping services used in support of qualified electronic signatures such as ETSI Standards, as well as Digital Signature Act 1997, Digital Signature Regulations 1998, MCMC "Requirements for Certification Authority (CA) to be recognized as a Time Stamping Authority (TSA) 2018" and MCMC "Recognition Framework for Time Stamping Authority (TSA) 2018 applicable law and regulation. Within the VISTA KENCANA domain, disputes between subscribers, one of which acts in the role of a subscriber and the other which acts in the role of a relying party, or between subscribers and VISTA KENCANA, will initially be reported to VISTA KENCANA for dispute resolution.
TSA and repository licenses, trust marks, and audit	VISTA KENCANA TSA has been certified for conformance to: a) ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Time Stamps", b) ETSI EN 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities" c) ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

	In addition, VISTA KENCANA maintains the following certifications of its PKI: a) Digital Signature Act 1997 b) Digital Signature Regulations 1998 c) WebTrust for CA 2.0: "Trust Service Principles and Criteria for Certification Authorities version 2.0". Annual performance audit will be performed by qualified auditors registered with the Office of the Controller. Please refer to www.skmm.gov.my for further details.

(**end of document**)