TRUSTGATE
SECURE TRANSACTON . TRUSTED BUSINESS

MSC Trustgate Time-Stamp Policy and Practice Statement

Version 1.4

20 January 2026

MSC Trustgate.com Sdn. Bhd. (199901003331)
Suite 2-9, Level 2, Block 4801 CBD Perdana
Jalan Perdana, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
Tel: +603 8318 1800
www.msctrustgate.com

MSC Trustgate Time-Stamp Policy and Practice Statement

Trademark Notices

MSC Trustgate.com Sdn. Bhd.
Suite 2-9, Level 2, CBD Perdana
Jalan Perdana, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
Attn : Digital Trust & Governance Manager
Email : digital-trust@msctrustgate.com
Tel : +603 8318 1800 Fax : +603 8319 1800

Revision History

No.	Date	Changes	Version	Approved by
1	1 December 2018	First Release	1.0	PMA
2	11 January 2019	Annual Review	1.1	PMA
3	27 October 2022	This version: • Changed the document format to be standardized with MSC Trustgate.com document format. • Added Revision History section. • Revised the existing Time-Stamp Policy and Practice Statement structure to meet the MCMC requirements for certification Authority (CA) to be recognized as a Time Stamping Authority (TSA) structure. • Amended Section 5.3: TSA Disclosure Statement. • Added Section 5.4.1: General Obligations • Amended Section 5.4.2: TSA obligations towards subscribers • Amended Section 5.4.3: Subscriber Obligations. • Added Section 5.5.1.6: Life Cycle Management of The Cryptographic Module Used to Sign Time-Stamps. • Amended Section 5.6.7: Access Control • Amended Section 5.6.9: Business Continuity Management • Amended Section 5.6.11: Collection of Evidence • Added Annex B: TSA Disclosure Statement • Amended TSA Disclosure	1.2	PMA
4	2 October 2023	Annual Review	1.2	PMA
5	20 June 2024	This version: • Added the Expected life-time of the signature used to sign the time-stamp token in the Disclosure Statement.	1.3	PMA
6	19 June 2025	• Annual Review	1.3	PMA
7	16 January 2026	This version: • Document Contact Information: Updated the email address from compliance@msctrustgate.com to digital-trust@msctrustgate.com and revised the attention line to Digital Trust & Governance Manager. • Page (ii) – Document Year: Updated the year from 2025 to 2026. • Section 3.1 – Definitions: Revised to improve accuracy and consistency of terminology. • Section 3.2 – Abbreviations: Updated to reflect current and applicable abbreviations. • Document Reference: Updated references from MSC Trustgate.com CPS to MSC Trustgate CP/CPS. • Section 4.4 – Subscribers: Revised to enhance clarity and strengthen the description of subscriber roles and responsibilities. • Section 5.1.1 – Overview: Updated to provide a clearer and more comprehensive overview of the Time-Stamping Policies.	1.4	DTC

		• Section 5.4.3 – Subscriber Obligations: Refined to improve clarity and better define subscriber obligations. • Section 5.5.3 – Clock Synchronization with MST: Updated to enhance the description of TSU clock integrity and validity controls. • Section 5.5.4 – TSA Termination and Termination Plan: Updated to include procedures for the destruction of TSU private keys upon TSA termination, in accordance with MCMC guidelines. • Section 5.6.6 – Incident Management: Enhanced to explicitly address incidents related to time-stamping services. • Section 5.6.9 – Business Continuity Management: Revised to improve clarity of business continuity measures specific to the time-stamping service. • Annex B – TSA Disclosure Statement: Updated to include applicable law, complaints handling, and dispute resolution provisions in line with MCMC guidelines.		

Contents

1. INTRODUCTION

This Time-Stamp Policy and Time-Stamp Practice Statement (TSPPS) document is the principal policy governing MSC Trustgate Time-Stamping Authority ("Trustgate TSA"). It addresses areas of policy, practices, procedures and technical used for the provision of qualified electronic time stamps. The time stamps can be used in support of digital signatures or for any application requiring proving that a datum existed before a particular time.

This TSPPS describes the obligations that the Trustgate TSA should respect while generating, handling, or delivering time-stamps. It is also intended to inform subscribers and relying parties about their obligations towards the time-stamps usage.

The structure and contents of this TSPPS are laid out in accordance with ETSI EN 319 421"Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps". In addition, it aims to meet the international community's general requirements to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014.

This TSPPS can be found on the MSC Trustgate's repository at https://www.msctrustgate.com/repository. It may be updated from time to time.

2. SCOPE

This TSPPS defines the policies and practices used for the operation and management of the Time-Stamping Services ("TSS") of Trustgate TSA so that subscribers and relying parties can assess the confidence level of the operation of this service. Trustgate TSA uses public key cryptography, public key certificates, and reliable time sources to provide reliable standard based time-stamps and in accordance with patterns globally accepted.

The Trustgate TSA aims to provide time-stamping services used in support of qualified electronic signatures, as well as under applicable Malaysian laws and regulations. In addition, the time-stamps can also be used for any other purpose that requires proof that certain data existed at a specific time.

Subscribers and relying parties should consult Trustgate's TSPPS to obtain further details of precisely how this time-stamp policy is implemented (e.g., protocols used in providing this service)

2.1 References

This TSPPS derives from the Internet Engineering Task Force (IETF) RFC 3628: Policy Requirements for Time-Stamping Authorities. It conforms to current versions of the requirements of the following schemes:

- Regulation:
    - Malaysia Digital Signature Act 1997
    - Malaysia Digital Signature Regulations 1998
- Protocol:
    - RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)
    - RFC 5816: ESSCertIDV2 update to RFC 3161
- Audit Criteria:
    - WebTrust Principles and Criteria for Certification Authorities – Latest version
- Internation Standard:
    - ETSI TS 102 023: Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities
    - CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

3. TERMS AND DEFINITIONS

3.1 Definitions

"Certification Authority (CA)" means an entity who issues certificate.

"Coordinated Universal Time (UTC)" means time scale based on the second as defined in recommendation ITU-RTF.460-6.

"ETSI EN 319 421" is Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

"ETSI EN 319 422" is Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

"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" is a recipient of a time-stamp who relies on that time-stamp.

"Subscriber" is a legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.

"Time-Stamp" is data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

"Time-Stamp Policy (TP)" is a named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements.

"Time-Stamp Authority (TSA)" is an entity that issues time-stamps using one or more time-stamping units.

"Time-Stamping Unit (TSU)" is a 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" is an electronic service that enhances trust and confidence in electronic transactions.

"TSA Disclosure statement" means a set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements.

"TSA Practice Statement (TPS)" means a statement of the practices that a TSA employs in issuing time-stamp TSA system: composition of IT products and components organized to support the provision of time-stamping services.

"TSA System" means set of IT products and components employed to provide support to the provision of time-stamping services.

3.2 Abbreviations

CA	Certification Authority
GMT	Greenwich Mean Time
MCMC	Malaysian Communications and Multimedia Commission
MST	Malaysia Standard Time
NMIM	National Metrology Institute of Malaysia
TSA	Time-Stamping Authority
TSPPS	Time-Stamping Policy and Practice Statement
TSS	Time Stamp Services
TSU	Time-Stamping Unit Trustgate
UTC	Universal Time Coordinated

3.3 Modal Verbs Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT","RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described below.

- MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT This phrase, or "SHALL NOT", means that the definition is an absolute prohibitionof the specification.
- SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional.

4. GENERAL CONCEPTS

4.1 General Policy Requirements Concepts

MSC Trustgate TSPPS is a detailed description of the terms and conditions regarding the provision of the services, and managerial and operational practices that the MSC Trustgate Time Stamping Authority follows in the provision of time-stamping services.

It also follows the requirements established in the MSC Trustgate's CP/CPS which follows Trust Service Principles and Criteria for Certification Authorities latest version (Web Trust for CA) for generic policy requirements common to all Certification Authorities.

4.2 Time-Stamping Services

The provision of time-stamping services can be broken down into the following components:

- **Time-stamping provision**: technical components that issue timestamps;
- **Time-stamping management**: management, control and monitoring components of time-stamping services, including synchronization with reliable UTC time sources, to ensure that the services provided are as specified by the TSA.

4.3 Time-Stamp Authority

The main task of Trustgate TSA is to provision time-stamping services identified in clause 4.1. Trustgate TSA can operate one or more TSU's which creates and signs on behalf of Trustgate TSA. Trustgate TSA is to be trusted by subscribers and relying parties for the issuance of time-stamp tokens.

Trustgate TSA may use other parties to provide parts of the TSS. However, it always maintains overall responsibility and ensures that the policy requirements identified in the present document are met.

4.4 Subscribers

A Subscriber is a natural person, legal entity, or a system acting on their behalf, that has entered into a contractual agreement with MSC Trustgate for the provision of time-stamping services. The Subscriber is responsible for the actions of its authorized end-users and must ensure they are informed of their obligations under this TSPPS.

4.5 Time-Stamp Policy and TSA Practice Statement

This document specifies the Time-Stamp Policy and the corresponding TSA Practice Statement. The Time-Stamp Policy defines the requirements governing the provision and use of the Time Stamping Service, while the TSA Practice Statement describes how those requirements are implemented in practice. No restriction is placed on the form or structure of either specification.

4.5.1 Purpose

In general, the MSC Trustgate Time-Stamp Policy (TP), which defines what shall be adhered to, and the Time-Stamp Practice Statement (TPS), which defines how it shall be adhered to, have been combined into a single document, the MSC Trustgate Time-Stamp Policy and Practice Statement (TSPPS). The relationship between TP and TPS is analogous to other business policy frameworks in which high-level requirements are established by policy, while operational units define and implement the corresponding practices and procedures to ensure compliance with those requirements.

4.5.2 Level of Specificity

MSC Trustgate TSPPS extends the CP/CPS which regulates the operation of Trustgate CA and associated non-repudiation services. This TSPPS provides a detailed description of the terms and conditions and business and operational practices of Trustgate TSA in issuing and otherwise managing time-stamping services. In addition, it enforces the rules established by Trustgate TSA. The rules cover the technical, organizational and procedural requirements.

4.5.3 Approach

The MSC Trustgate TSPPS establishes the general rules concerning the operation of Trustgate TSA. Additionalinternal documents define how Trustgate meets the technical, organizational, and procedural requirements identified in the Trustgate TSPPS. These documents may be provided only under strictly controlled conditions.

5. REQUIREMENTS

5.1 Time-stamp Policies

5.1.1 Overview

Trustgate TSP defines a comprehensive set of rules governing the applicability of a Time-Stamp Token (TST) to specific communities or application classes with shared security requirements. These policies ensure that:

- **Standards Compliance**: The TSU, including private keys management and public key certificates profiles, strictly adheres to the technical specifications of the RFC 3161 and RFC 3628.
- **Key Management**: Trustgate TSA maintains exclusive control and secure custody of the private keys utilized for digital signing time-stamps.
- **Temporal Accuracy**: TSTs are issued with a synchronized clock accuracy of ± 1 second, relative to UTC, as further detailed in Section 6.1 (TimestampAuthority Obligations).
- **Transport Protocol**: Time-stamp requests shall be submitted via the Hypertext Transfer Protocol Secure (HTTPS) to ensure the integrity and confidentiality of the communication channel between the Subscriber and the TSA.

5.1.2 Identification

The object identifier (OID) for the Trustgate TSPPS is:

1.3.6.1.4.1.49530.1.3.1

By including this object identifier in a time-stamp, Trustgate TSA claims conformance to the identified TP and also the ETSI time-stamping identifier is being supported.

5.1.3 User Community and Applicability

Trustgate TSA's User Community is composed of subscribers and relying parties. Accordingly, subscribers are also regarded as relying parties.

MSC Trustgate TSPPS is aimed at meeting the requirements of time-stamping qualified digital signatures for long-term validity but is generally applicable to any requirement for an equivalent quality.

This policy does not define restrictions on the applicability of the time-stamps issued.

5.1.4 Conformance

To show conformance with this document, the Trustgate TSA uses the identifier for the time-stamp policy established in Section 5.1.2 of this document in its issued TSTs.

Trustgate TSA is subject to periodic independent internal and external audits. Trustgate TSA guarantees conformance to its implemented controls and ensures that it meets its obligations specified in Section 5.4 (Time-Stamp Authority Obligations) of this document.

5.2 TSA Practice Statement

This TSPPS establishes the general rules concerning the operation of the Trustgate TSA. The MSC Trustgate CP/CPS and additional internal documents define how Trustgate TSA meets the technical, organizational, and procedural requirements identified in TSPPS.

This TSPPS and other public documents may be found at http://www.msctrustgate.com/repository. Internal documents may be provided only under strictly controlled conditions.

Trustgate TSA conducts risk assessments to evaluate threats and to determine the necessary security controls and operational procedures.

5.3 TSA Disclosure Statement

MSC Trustgate Time-Stamping Authority Disclosure Statement (this section of this document) discloses to all subscribers and potential relying parties the terms and conditions regarding the use of Trustgate TSA. Trustgate TSA Disclosure Statement is specified in Annex B (TSA Disclosure Statement).

5.4 TSA Obligations

5.4.1 General Obligations

Trustgate TSA implements all requirements specified in its TSPPS.

Trustgate TSA ensures conformance with the procedures prescribed by its TSPPS.

All TSA functionality is undertaken by Trustgate TSA.

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

5.4.2 TSA Obligations towards Subscribers

Trustgate TSA 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 Trustgate TSA sphere of influence (force majeure, war, strike, governmental restrictions, etc.). Trustgate TSA Service Availability (per year) for its time-stamping service is 97.5%.

Planned maintenance windows may be contractually agreed upon with Subscribers; they may also be informed via email.

Trustgate TSA 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 of these audits require demonstration of a maximum level of security and conformity to documented policies and practices.

Trustgate TSA use the following independent external time sources which are permanently compared to guarantee a deviation from UTC of less than one second.

- NTP service provided by NMIM:
  i. 202.185.190.216 (ntp1.sirim.my)
  ii. 202.185.190.217 (ntp2.sirim.my)
  iii. 175.136.234.45
  iv. 175.136.234.46

Trustgate TSA provides subscribers and relying parties with the necessary information about the terms and conditions regarding the use of Trustgate TSA time-stamping service as specified in Section 5.3 (TSA Disclosure Statement).

5.4.3 Subscriber Obligations

Subscribers of the Trustgate Time-Stamping Service shall comply with the following obligations:

- **Accountability for Usage**: Where the Subscriber is an organization, it is responsible for ensuring that all end-users comply with the obligations set forth in this TSPPS. The organization shall remain primary and legally accountable for the actions of its end-users. Individual Subscribers (Natural Persons) shall be held directly responsible for their use of the service.
- **Technical Compliance**: The Subscriber shall ensure that Time-Stamp Requests (`TimeStampReq`) are generated and submitted in strict accordance with RFC 3161, RFC 5816, and the technical integration guidelines provided by Trustgate TSA.
- **Data Integrity**: The Subscriber is solely responsible for ensuring that the data or hash values submitted for time-stamping accurately represent the original electronic record. Trustgate TSA is not responsible for verifying the content or accuracy of the data submitted.

- **Lawful Use**: The Subscriber shall not submit data or hash values that are unlawful, offensive, obscene, discriminatory, or otherwise prohibited under applicable Malaysian law.
- **Incident Reporting**: The Subscriber shall promptly notify Trustgate TSA of any actual or suspected misuse , security compromise, or unauthorized access to the Time Stamping Service.
- **Verification Prior to Reliance**: Before relying on Time Stamp Tokens (TST), the Subscriber shall:
    - Verify that the TST was correctly generated and digitally signed by Trustgate TSA.
    - Validate the TST using the current and valid Trustgate TSA public key.
    - Confirm that the TST has not been tampered with and is being used within the limitations defined in this TSPPS.

5.4.4 Relying Party Obligations

The terms and conditions made available to relying parties shall include an obligation on the relying party that, when relying on a time-stamp token, the relying party shall:

- Verify that the time-stamp token has been correctly signed and that the private key used to sign the timestamp has not been compromised until the time of the verification;
- Take into account any limitations on the usage of the time-stamp indicated by the timestamp policy;
- Take into account any other precautions prescribed in agreements or elsewhere. After expiry of the time-stamp certificate, the relying party should:
    i. verify that the TSU private key is not revoked, and
    ii. verify that the cryptographic hash function and the signing algorithm used in the timestamp token are still considered secure.

5.4.5 Liability

Trustgate undertakes to operate Trustgate TSA in accordance with this TSPPS, MSC Trustgate CP/CPS, and the terms of service level agreements with the Subscriber. Trustgate makes no express or implied representations or warranties relating to the availability or accuracy of the time-stamping service.

Trustgate bears specific liability for damage to Subscribers and Relying Parties in relationship to valid qualified digital certificates relied upon in accordance with specific national laws and regulations. These liabilities are described in section 9.8 Limitation of Liabilities of the MSC Trustgate CP/CPS.

5.5 TSA Management and Operation

5.5.1 TSU Key Management Life Cycle

5.5.1.1 TSU Key Generation

Trustgate generates the cryptographic keys used in its TSA services under the control of authorised personnel in a secure physical environment. Additional information is provided in Section 6.1 Key Generation and Installation of the MSC Trustgate CP/CPS. The keys are generated within TSU hardware security modules that are certified to FIPS 140-2 Level 3. Algorithms and key size are described in section 5.3 Disclosure Statement of this document.

5.5.1.2 TSU Private Key Protection

Trustgate takes specific steps to ensure that TSU private keys remain confidential and maintain their integrity. These include use of HSMs certified to FIPS 140-2 Level 3 to hold and sign with the keys.

5.5.1.3 TSU Public Key Distribution

Digital certificates used in the Trustgate TSA are issued by Trustgate CA according to certificate policies which provide a level of security equivalent to this time-stamping policy. These include use of HSMs certified to FIPS 140-2 Level 3 to hold and sign with the keys. Additional information is provided in section 6.1 Key Generation and Installation of the Trustgate CP/CPS.

5.1.1.4 Rekeying TSU's Key

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

5.5.1.5 End of TSU Key Life Cycle

TSU private signing keys are replaced upon their expiration. The TSU rejects any attempt to issue time- stamps once a private key has expired. After expiry, private keys are destroyed.

5.5.1.6 Life Cycle Management of the Cryptographic Module used to Sign Time-Stamps

Trustgate TSA has in place procedures and controls in accordance with the MSC Trustgate CP/CPS, to ensure that TST signing cryptographic hardware (HSM) is not tampered with during shipment, while it is stored, that installation, activation, and duplication of TSU's signing keys in HSM's shall be done only by personnel in trusted roles, and in a physically secure environment. Additional information is provided in section 6.6 (Life Cycle Technical Controls) of MSC Trustgate CP/CPS.

5.5.2 Time-Stamp Issuance

Trustgate has technical prescriptions in place to ensure that TSTs are issued securely and include the correct time. Each TST includes:

- a representation (e.g., hash value) of the datum being time-stamped as provided by the requestor
- a unique serial number that can be used to both order TSTs and to identify specific TSTs
- an identifier for the time stamp policy
- the time calibrated to within 1 second of UTC, traceable to a UTC(k) source
- an electronic signature generated using a key used exclusively for time-stamping
- an identifier for the TSA and the TSU

Trustgate maintains audit logs for all calibrations against the UTC(k) references, and will not issue TSTs when the time is out of the stated accuracy.

5.5.3 Clock Synchronization with MST

Trustgate TSA ensures that TSU clocks are synchronized with Malaysian Standard Time (MST) to maintain the integrity and legislative validity of issued Time-Stamp Tokens.

- **Declared Accuracy**: Trustgate TSA provides time with an accuracy of **±1 second** or better relative to UTC. The TSUs implement technical controls to ensure internal clocks do not drift beyond this declared accuracy.
- **Synchronization Source**: TSU clocks are synchronized with the **National Metrology Institute of Malaysia (NMIM)** time source via the Network Time Protocol (NTP). To protect against unauthorized access and time manipulation, synchronization is restricted to **authorized IP addresses whitelisted by NMIM**.
- **Clock Protection**: TSUs are housed in a secure environment protected against physical and electronic threats—including tampering, radio interference, or electrical shocks—that could cause undetected changes to the clock calibration.
- **Drift Detection and Service Continuity**: The TSA continuously monitors for clock drift or "time jumps." If the system detects that the TSU clock has drifted or jumped out of synchronization with MST beyond the permitted 1-second threshold:
    - The TSU shall immediately cease the issuance of Time-Stamp Tokens.
    - Notification shall be managed in accordance with the procedures defined in Section 5.6.6 (Incident Management).
    - Issuance will only resume once the clock is successfully recalibrated and synchronized.
- **Leap Second Management**: Clock synchronization accounts for leap seconds as notified by the appropriate international bodies. Leap second adjustments occur during the final minute of the scheduled day. A record is maintained of the exact time such changes occur, accurate within the declared threshold.
- **Annual Verification**: Trustgate SHALL obtain written confirmation from NMIM on an annual basis to verify that the TSU clocks remain synchronized with MST within the declared accuracy.

5.5.4 TSA Termination and Terminations Plans

Trustgate TSA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of its time-stamping services, and in particular ensure continued maintenance of information required to verify the correctness of time-stamp tokens.

Trustgate TSA shall:

- make available to all subscribers and relying parties information concerning its termination;
- terminate authorization of all subcontractors to act on behalf of Trustgate TSA in carrying out any functions relating to the process of issuing time-stamp tokens;
- transfer obligations to another licensed certification authority appointed by the MCMC for maintaining event log, audit archives and to demonstrate the correct operation of the TSA for a reasonable period;
- maintain or transfer to another licensed certification authority appointed by the MCMC its obligations to make available its public key or its certificates to relying parties for a reasonable period;
- take appropriate steps to ensure that all TSU private keys, including backup copies, are securely destroyed in a manner that prevents their retrieval.
- arrange to cover the costs to fulfil these minimum requirements in case Trustgate becomes bankrupt or for other reasons is unable to cover the costs by itself

5.6 General Security and Controls

5.6.1 Security Management

Trustgate TSA ensures that administrative and management procedures are applied, which are adequate and parallel with the best practices recognized. All requirements and subjects related to security management are implemented as described in section 6 (Technical Security Controls) of MSC Trustgate CP/CPS.

5.6.2 Asset Classification and Management

Trustgate TSA has ensured an appropriate level of protection of its assets including information assets. All information assets and has assigned a classification consistent with the risk assessment. All media are handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data is securely disposed of when no longer required.

5.6.3 Human Resource Security

The practices of the personnel security rules as well as the trusted roles used in TSA services environment is provided in the MSC Trustgate CP/CPS.

5.6.4 Physical and Environmental Security

Trustgate TSA maintains physical and environmental security policies for systems used for time-stamps issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering and disaster recovery. Controls should be implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities. The implementation of physical environmental security is provided in accordance with the rules described in MSC Trustgate CP/CPS.

5.6.5 Operation Security

Trustgate TSA possesses the procedures, processes and infrastructure provided in the MSC Trustgate CP/CPS section 5 (Facility, Management, And Operational Controls).

5.6.6 Incident Management

Trustgate TSA shall manage security incidents and compromise events in accordance with documented incidents and compromise handling procedures in order to minimize the impact of such events on the Time Stamping Service.

In the event that equipment is damaged or rendered inoperative and the TSU private keys remain uncompromised, Trustgate TSA shall re-establish operations as quickly as practicable, giving priority to the secure generation of Time Stamp Tokens and the preservation of information necessary to verify previously issued time-stamp tokens, in accordance with the MSC Trustgate Disaster Recovery Plan. In the event of a TSU clock synchronization failure or "time jump" exceeding the declared accuracy (as specified in Section 5.5.3), Trustgate TSA shall treat the event as a security incident. In addition to ceasing TST issuance, Trustgate shall notify affected Subscribers and Relying Parties via the Trustgate website or other official communication channels, detailing the period of the synchronization failure and the remedial actions taken.

5.6.7 Access Control

In line with MSC Trustgate Information Security Policy, TSA profiles and access rights are granted through a controlled process involving formal access requests and approval by the relevant managers before assignment by system administrators.

The principles of least privilege, need to know and the segregation of duties principle are respected. Access rights of users involved in TSA operations are promptly modified in case of change of roles or revoked in case the users leave the organization.

Periodic review of user access is conducted to validate the continuing appropriateness of user access rights and confirm the revocation of rights that are no longer required.

Trustgate TSA shall maintain appropriate physical and logical access controls on the affected facilities, equipment, system and information as stipulated in the MSC Trustgate CP/CPS section 5 (Facility, Management, and Operational Controls).

5.6.8 System Development and Maintenance

The system development controls for Trustgate TSA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;
- All hardware will be inspected during commissioning process to ensure conformity to supply and no evidence of tampering found;
- Hardware and software are developed in a controlled environment, and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- 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 part of the TSA operation;
- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the TSA operations are installed on the equipment and are obtained from sources authorised by local policy. Trustgate TSA hardware and software are scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates are purchased or developed in the same manner as original equipment and are installed by trusted and approved personnel in a defined manner.

5.6.9 Business Continuity Management

Trustgate TSA maintains a comprehensive Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to ensure the availability and integrity of the Time-Stamping Service. These plans are aligned with the requirements described in MSC Trustgate CP/CPS Section 5.7.

- **Disaster Recovery**: In the event of a natural or other type of disaster including hardware failure, corruption or loss of computing resources that can affect Trustgate TSA business or services, the operation of Trustgate TSA will be re-established at disaster recovery site.

- **Key Compromise**: If a TSU private key is compromised or suspected of compromise, Trustgate TSA shall immediately:
    - Cease the issuance of TSTs using the affected key.
    - Revoke the TSU certificate.
    - Inform Subscribers and Relying Parties via the Trustgate repository and official channels to stop using and relying on the compromised key.

- **Loss of Clock Synchronization**: In the event of a synchronization failure exceeding the declared accuracy (as defined in Section 5.5.3), Trustgate TSA shall suspend operations immediately. The Recovery Plan will be activated to restore synchronization with MST. Service shall remain suspended until synchronization is verified and a formal restoration notice is issued.

5.6.10 Compliance

Trustgate TSA offers its services in strict compliance with Digital Signature Act 1997 and Digital Signature Regulations 1998. Verification is performed through internal and external audits.

5.6.11 Collection of Evidence

The archive collection system complies with the security requirements described in MSC Trustgate CP/CPS Section 5.4 Audit Logging Procedure and 5.5 Records Archival.

Records include:

- Events relating to the life-cycle of TSU keys and Certificates; and
- Events related to clock re-calibration and synchronisation.

(this space is intentionally left blank)

Annex A (Normative) – Time-stamping protocol and time-stamp token profiles

A.1 Requirements for a time-stamping client

A.1.1 Profile for the format of the request

A.1.1.1 Core requirement

A time-stamping client shall support the time-stamping request as defined in IETF RFC 3161,clause 2.4.1 with the amendments defined in the following clauses.

A.1.1.2 Fields to be supported

The use of the following fields in the time-stamping request should be supported:

- the reqPolicy;
- the nonce; and
- the certReq.

A.1.1.3 Hash algorithms to be used

Hash algorithms used to hash the information to be time-stamped should be as specified inAnnex A.4

A.1.2 Profile for the format of the response

A.1.2.1 Core requirement

A time-stamping client shall support the time-stamping response as defined in IETF RFC3161, clause 2.4.2 with the amendments defined in the following clauses.

A.1.2.2 Fields to be supported

The following requirements apply:

- the accuracy field shall be supported; and
- the nonce field should be supported.

A TSU needs not support ordering hence clients should not depend on the ordering of time-stamps. If the nonce field is present in the request, the nonce field shall be present in the response with the same value.

A.1.2.3 Algorithms to be supported

Time-stamp token signature algorithms to be supported should be as specified in Annex A.4

A.1.2.4 Key lengths to be supported

Signature algorithm key lengths for the selected signature algorithm should be supported asrecommended in Annex A.4

A.2 Requirements for a time-stamping server

A.2.1 Profile for the format of the request

A.2.1.1 Core requirement

A time-stamping server shall support the time-stamping request as defined in IETF RFC 3161,clause 2.4.1 with the amendments defined in the following clauses.

A2.1.2 Fields to be supported

The following requirements apply:

- reqPolicy field shall be supported;
- the nonce field shall be supported; and
- certReq field shall be supported.

A.2.1.3 Algorithms to be supported

Hash algorithms for the time-stamp data to be supported should be as specified in AnnexA.4

A.2.2 Profile for the format of the response

A.2.2.1 Core requirement

A time-stamping server shall support the time-stamping response as defined in IETF RFC3161, clause 2.4.2 with the amendments defined in the following clauses.

A.2.2.2 Fields to be supported

The requirements from IETF RFC 3161, clause 2.4.2 shall apply and the followingrequirements apply:

- the policy field shall be present as an identifier for the time-stamp policy and shall conform to annex A;
- a genTime field shall have a value representing time with a precision necessary to supportthe declared accuracy shall be supported;
- the accuracy field shall be present and a minimum accuracy of one second shall besupported;
- the ordering field shall not be present or shall be set to false; and
- no extension shall be marked as critical.

The following requirement applies to the content of the SignedData structure in which theTSTInfo structure is encapsulated:

- the certificate identifier of the TSU certificate (ESSCertID as in IETF RFC 3161 or ESSCertIDv2 as in IETF RFC 5816) shall be included as a signerInfo attribute inside a SigningCertificate or a SigningCertificateV2 attribute as specified in IETF RFC 5816, clause2.2.1.

A.2.2.3 Algorithms to be used

Hash algorithms used to hash the information to be time-stamped and time-stamp tokensignature algorithms should be as specified in Annex A.4.

A.3 TSU certificate profile

The TSU certificate shall meet the following requirements

A.3.1 Subject name requirements

The countryName attribute shall specify the country in which the TSA is established (which is notnecessarily the name of the country where the TSU is located).

For a TSA being a legal person or a natural person associated with a legal person the organizationName shall contain the full registered name of the TSA responsible for managing theTSU. That name should be an officially registered name of the TSA.

The commonName specifies an identifier for the TSU. Within the TSA, the attribute commonNameuniquely identifies the TSU used.

For a TSA being a natural person, one instance of the attribute serialNumber should be included inthe subject field.

A.3.2 Key lengths requirements

The key length for the selected signature algorithm of the TSU certificate should be as recommended in Annex A.4

A.3.3 Key usage requirements

The TSU certificate extended key usage setting shall be as defined in IETF RFC 3161, clause 2.3

The TSU certificate private key usage period extension should be used in order to limit the validity ofthe TSU's signing key.

A.3.4 Algorithm requirements

The TSU public key and the TSU certificate signature should use the algorithms as specified in AnnexA.4

(this space is intentionally left blank)

A.4 Algorithms for Time Stamping

A.4.1 Time Stamping Token (TST)

The following requirements apply to hash functions and TST signature algorithms.

Time Stamping Token	TST Requesters	TST Issuers	TST Verifiers
Hash Function	support minimum SHA-256	support minimum SHA-256	support minimum SHA-256
TST Signature Algorithms	support minimum RSA with SHA-256	support minimum RSA with SHA-256 or EC-DSA with SHA-256	support minimum RSA with SHA-256 or EC-DSA with SHA-256

A.4.2 TSU Certificate

TSU Certificates	Issuers of TSU Certificates	Users of TSU Certificates
TSU Public Key	support minimum RSA with SHA-256 or EC-DSA with SHA-256	support minimum RSA with SHA-256 or EC-DSA with SHA-256
Issuer CA Public Key	support minimum RSA with SHA-256 or EC-DSA with SHA-256	support minimum RSA with SHA-256 or EC-DSA with SHA-256

(this space is intentionally left blank)

Annex B (Informative) – TSA Disclosure Statement

Trustgate TSA Contact Information	Trustgate TSA operates at: MSC TRUSTGATE.COM Sdn Bhd (199901003331) Suite 2.9, Level 2, Block 4801, CBD Perdana, Jalan Perdana, 63000 Cyberjaya, Selangor Darul Ehsan, Malaysia Tel: +603 8318 1800 Fax: +603-831 1800 For any business inquiries, certification services, PKI and technical inquiries please email to digital-trust@msctrustgate.com.
Electronic Timestamp types and usage	Trustgate TSA aims to deliver time-stamping services in accordance with the DSA 1997 and DSR 1998 However, Trustgate TSA time-stamps may be equally applied to any application requiring proof that a datum existed at a particular time, including digital signature and code signing. Trustgate TSA is in compliance with RFC3161. The time-stamp policy is as per section 5.1.2. Supported signing algorithms are sha256WithECDSAEncryption. Acceptable Time Stamp Request Hashes include SHA-256, SHA-384 and SHA-512. The validity of the digital signature on the timestamping token depends on the hashing algorithm, the signature algorithm being used, and the private key length of TSU. The accuracy of the time in the time-stamp tokens is as per section 5.5.3. Trustgate TSA may charge fees for the services provided. The Trustgate TSA service is available 24x7.
Expected life-time of the signature used to sign the time-stamp token	5 years
Reliance limits	Trustgate TSA does not set reliance limits for time-stamp services beyond those outlined in section 5.4.5 Relying Party Obligations of this document. Trustgate TSA will post public notice on its website if the cryptographic algorithms and key lengths have been changed. Trustgate TSA ensures that the time accuracy in a TST is within +/- one (1) second of MST. If a reliable MST time source cannot be obtained, the timestamp will not be issued.
Obligations of Subscribers	Please refer to Section 5.4.3 Subscriber Obligations of Trustgate TSPPS.
TSU public key certificate status checking obligations of relying parties	Please refer to Section 5.4.4 Relying Parties Obligations of Trustgate TSPPS.
Verify the time-stamp token	Relying parties may verify a Time Stamp Token by validating the TSA digital signature using the TSA public key certificate, confirming the integrity of the time-stamped hash value, and ensuring that the certificate was valid at the time of issuance. Reliance on a Time Stamp Token is subject to the limitations defined in this document and the Trustgate TSPPS, including any constraints on cryptographic algorithms and key validity periods.
Retention of Event Logs	TSA event logs are retained according to section 5.4.3 (Retention period for audit log) of the MSC Trustgate CP/CPS.

Limited warranty and disclaimer/Limitation of liability	Please refer to Section 5.4.5 Liability of Trustgate TSPPS.
Applicable agreements and practice statement	The applicable documents are published at https://www.msctrustgate.com/repository.
Privacy policy	The applicable documents are published at https://www.msctrustgate.com/repository.
Refund policy	Trustgate TSA does not refund fees for time-stamping services.
Applicable law, complaints and dispute resolution	Any controversy or claim relating to the Trustgate TSA shall be addressed according to Section 9.13 (Dispute Resolution Procedures) and Section 9.14 (Governing Law) of the MSC Trustgate CP/CPS.
TSA and repository licenses, trust marks, and audit	Trustgate TSA is subject to periodic internal audit and external audit. The external audit is performed annually by a qualified auditor as provided by MCMC (https://www.mcmc.gov.my/en/sectors/digital-signature/list-of-qualified-auditors).

(end of document)