MSC TRUSTGATE.COM SDN BHD

DATE TIME STAMPING SERVICE AUDIT FOR THE YEAR ENDED 31 DEC 2022

Baker Tilly MH Consulting Sdn Bhd
(1068792-P)
Sunway Nexis, C-10-07 & D-13A-06
No 1 Jalan PJU5/1, Kota Damansara
47810 Petaling Jaya, Selangor,
Malaysia

T 603 6145 0889 (General)
M 6012 620 9868
F 603 6158 9923

02 March 2023

The Board of Directors
MSC Trustgate.com Sdn Bhd
Suite 2-9, Level 2, Block 4801
CBD Perdana, Jalan Perdana
63000 Cyberjaya, Selangor, Malaysia

Dear Sirs,

DATE TIME STAMPING AUDIT FOR YEAR ENDED 31 DECEMBER 2022

We have reviewed the description of controls relating to the Date Time Stamping (DTS) service of MSC Trustgate.com Sdn Bhd (MSCTG) throughout the year ended 31 December 2022, to obtain reasonable assurance that:

- The description of controls presents fairly, in all material respects, the aspects of MSCTG's controls over DTS service in accordance with the Requirements for Certification Authority (CA) to be recognised as a Time Stamping Authority (TSA) issued by Malaysian Communications and Multimedia Commission (MCMC) effective during the audit.
- The controls included in the description were suitably designed to achieve the level of compliance specified in the description and whether those controls were complied with satisfactorily.
- Such controls had been placed in operation during the year of audit.

MSCTG's management has specified the control objectives and is responsible for the description of these controls. The management of MSCTG is also responsible for maintaining an effective internal control structure, including control systems and procedures in relation to the DTS service.

Our responsibility is to express an opinion on management's description of the controls. Our audit was performed in accordance with generally accepted practices for Certification Authorities and Malaysian regulatory requirements which include procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, for the 12 months period ended 31 December 2022, the DTS service in all material respects of MSCTG's controls that had been placed in operation during the period of review is rated as "*SUBSTANTIAL COMPLIANCE*".

This report is intended solely for use by the Board of Directors of MSCTG and MCMC which regulates MSCTG. This report is not intended for and should not be used by anyone other than the parties specified.

Yours Faithfully,

SECTION I: CONTROL OBJECTIVES AND DESCRIPTION OF CONTROLS

MSCTG is licensed by the Malaysia Communications and Multimedia Commission ("MCMC") for the following areas:

- Licensed Certification Authority (License No: LPBP-2/2020 (4), Issuing Date: 25 July 2020, Expiry Date: 24 July 2025): https://www.mcmc.gov.my/en/sectors/digital-signature/list-of-licensees (Accessed 3 February 2023)
- Recognised Repository (License No: PPR-2/2020(4), Issuing Date: 25 July 2020, Expiry Date: 24July 2025): https://www.mcmc.gov.my/en/sectors/digital-signature/list-of-licensees (Accessed 3 February 2023)
- Recognised Date/Time Stamp Services (License No: PPTM-2/2021 (1), Issuing Date: 25 July 2021, Expiry Date: 24 July 2024): https://www.mcmc.gov.my/en/sectors/digital-signature/list-of-licensees (Accessed 3 February 2023)

Additionally, our references for this review included:

- Malaysia Digital Signature Act 1997
- Malaysia Digital Signature Regulations 1998
- WebTrust for Certification Authorities
- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification and Practices Framework
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)
- RFC 5816: ESSCertIDV2 update to RFC 3161
- 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 Certificates

MSCTG provides Public Key Infrastructure ("PKI") services to businesses and government, incorporating digital certificates, digital signatures, and encryption. Certification services are organised by class, assurance level and usage. It is also a recognised Date/Time Stamp Service provider providing a digital date/time stamp as cryptographically digital declaration that can be used as evidence of the date/time a record was created and can be attached to a digital signature, message, or other documents.

1.1 Reference To Regulatory Guidelines

Our review has been conducted under the Malaysian Communications and Multimedia Commission (MCMC) Recognition Framework for Time Stamping Authority (TSA) effective 1 February 2018, the WebTrust Principles and Criteria along with industry practice. This control framework provides the basis for the systems, policies and procedures, specifically in the following areas:

- TSA Practice Statement
- TSA Disclosure Statement
- TSA Obligations
- TSA Obligations towards Subscribers
- Subscriber Obligations
- Relying Party Obligations
- TSA Management and Operation
- TSA Key Management Life Cycle
- Time-stamp Issuance
- Clock Synchronisation
- TSA Termination and Termination Plans

- General Security and Controls
- Security Management
- Asset Classification and Management
- Human Resource Security
- Physical and Environmental Security
- Operation Security
- Incident Management
- Access Control
- System Development and Maintenance
- Business Continuity Management
- Compliance
- Collection of Evidence
- Time-stamping protocol and time-stamp token profiles

1.2 Overview of MSC Trustgate Date Time Stamping Service

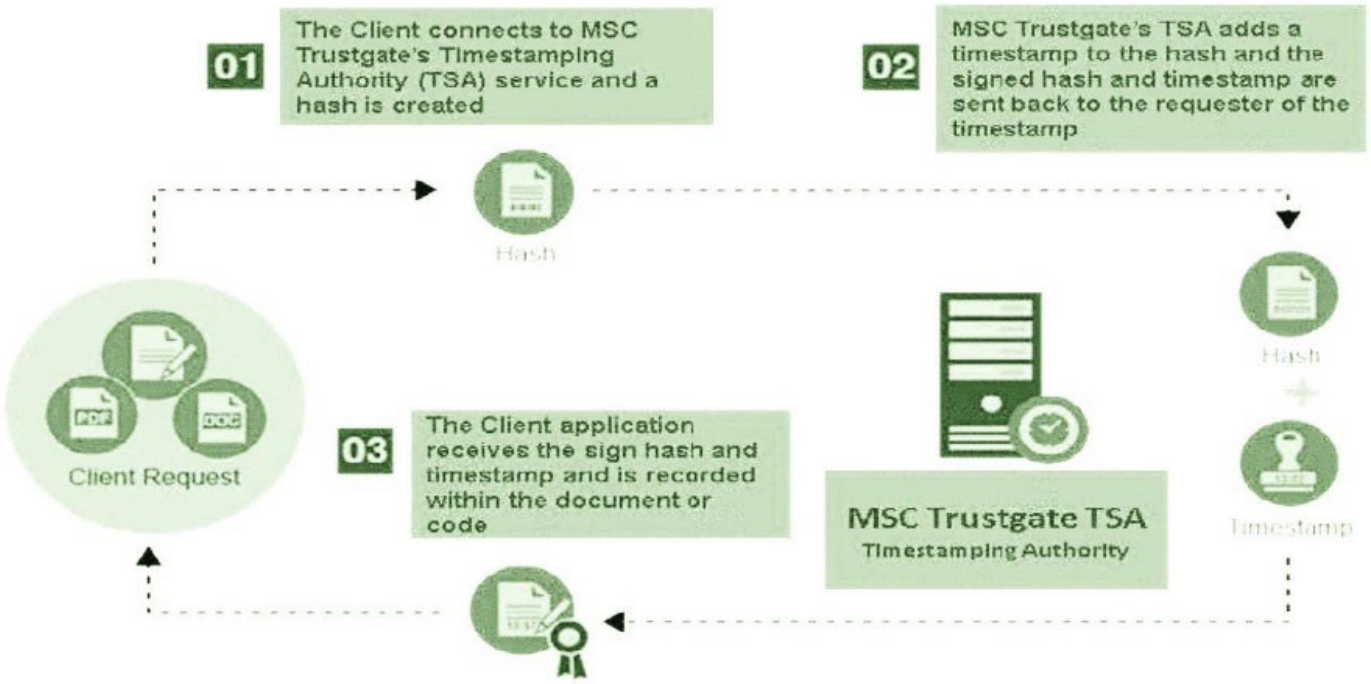
MSCTG's trusted date time stamping Software-as-a-Service (SaaS) provides a low cost and easy method to apply RFC 3161 trusted timestamps to time-sensitive transactions through Malaysia Standard Time (MST) and Coordinated Universal Time (UTC) sources. MSCTG's service helps organisations reduce potential liability associated with time-sensitive transactions by providing long-term validation and non-repudiation of the time and date the transaction took place using a standards-based implementation that is easily recognisable and compatible.

Adding a trusted timestamp to code or an electronic signature provides a digital seal of data integrity and a trusted date and time of when the transaction took place. Recipients of documents and code with a trusted timestamp can verify when the document or code was digitally or electronically signed, as well as verify that the document or code was not altered after the date the timestamp is applied.

Features and Benefits:

- Quick and easy to set up with no technical expertise required
- Recognised and compatible with most systems and applications, including Google, Microsoft and Adobe
- RFC 3161 is compliant with a strong 256-bit hash algorithm
- Verifies when the document/data was signed and that it has not been altered
- Produces legally admissible and secure non-repudiation signatures
- The SaaS-based model means MSCTG manages all maintenance, security and audits

1.3 MSCTG Process Flow



2 Time-Stamping Policies

MSCTG defined its time-stamp policies.

Control Objectives	Control Description	Reference
One time-stamp policy for TSA issuing time-stamps, supported by public key certificates, with an accuracy of 1 second or better.	Time-stamp tokens of MSCTG are issued with an accuracy of 1 second or better. MSCTG further provided assurance that the profiles of public key certificates used by its TSA comply with RFC 3161.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

3 TSA Practice Statement

MSCTG undertook that the following controls and disclosures for TSA Practice Statement are in place.

Control Objectives	Control Description	Reference
The TSA shall have a risk assessment carried out to evaluate business assets and threats to those assets to determine the necessary security controls and operational procedures.	MSCTG TSA conducts risk assessments to evaluate threats and to determine the necessary security controls and operational procedures.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The TSA shall have a statement of the practices and procedures used to address all the requirements identified in this time-stamp policy.	MSCTG TP/TPS and additional internal documents define how MSCTG TSA meets the technical, organisational, and procedural requirements identified in TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

Control Objectives	Control Description	Reference
The TSA's Practice statement shall identify the obligations of all external organisations supporting the TSA services including the applicable policies and practices.	MSCTG TP/TPS and additional internal documents define how MSCTG TSA meets the technical, organisational, and procedural requirements identified in TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The TSA shall make available to subscribers and relying parties its Practice statement, and other relevant documentation, as necessary to assess conformance to the time-stamp policy.	MSCTG TP/TPS and additional internal documents define how MSCTG TSA meets the technical, organisational, and procedural requirements identified in TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding the use of its time-stamping services as specified in clause 5.3. of the requirements.	MSCTG TP/TPS and additional internal documents define how MSCTG TSA meets the technical, organisational, and procedural requirements identified in TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The TSA shall have a high-level management body with final authority for approving the TSA Practice statement.	MSCTG TP/TPS and additional internal documents define how MSCTG TSA meets the technical, organisational,and procedural requirements identified in TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The senior management of the TSA shall ensure that the practices are properly implemented.	MSCTG TP/TPS and additional internal documents define how MSCTG TSA meets the technical, organisational, and procedural requirements identified in TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The TSA shall give due notice of changes it intends to make in its practice statement and shall, following approval as in (f) above, make the revised TSA Practice statement immediately available as required under (d) above.	MSCTG TP/TPS and additional internal documents define how MSCTG TSA meets the technical, organisational, and procedural requirements identified in TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

4 TSA Disclosure Statement

MSCTG disclosed to all subscribers and potential relying parties the terms and conditions regarding the use of time-stamping services. This statement specifies for each time-stamp policy supported by the TSA.

Control Objectives	Control Description	Reference
The TSA contact information.	MSCTG has disclosed its contact information and can be found on their website as well as its TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

Control Objectives	Control Description	Reference
The time-stamp policy is being applied.	Each time-stamp token issued by the MSCTG contains the policy object-identifier. By including this object identifier in a timestamp, MSCTG claims conformance to the identified TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
At least one hashing algorithm which may be used to represent the datum being time-stamped.	The cryptographic algorithms and key lengths used by MSCTG comply with ETSI TS 101.861 as follows: • Hash: SHA2 • Signature: SHA2WithRSAEncryption, 2048 bit key SHA2WithECDSAEncryption , 256 bit key	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The expected lifetime of the signature used to sign the time-stamp token (depends on the hashing algorithm being used, the signature algorithm being used and the private key length).	MSCTG does not set reliance limits for time-stamp services beyondthose outlined in Section 5.4.4 Relying Party Obligations of the TP/TPS. MSCTG will post a public notice on its website if the cryptographic algorithms and key lengths have been changed.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The accuracy of the time in the time-stamp tokens with respect to MST.	The MSCTG TSA assures time with ±1 second of a trusted UTC time source and will not issue timestamps outside this declared accuracy.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
Any limitations on the use of the time-stamping service.	MSCTG does not set reliance limits for time-stamp services beyondthose outlined in Section 5.4.4 Relying Party Obligations of the TP/TPS. MSCTG will post a public notice on its website if the cryptographic algorithms and key lengths have been changed.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The subscriber's obligations as defined in clause 5.4.2, if any.	Subscriber obligations are described in section 5.4.3 Subscriber Obligations of its TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The relying party's obligations as defined in clause 5.4.4.	Relying Party obligations are described in section 5.4.4 Relying Party Obligations of its TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

Control Objectives	Control Description	Reference
Information on how to verify the time-stamp token such that the relying party is considered to "reasonably rely" on the time-stamp token (see clause 5.4.4) and any possible limitations on the validity period.	MSCTG TP/TPS and additional internal documents define how MSCTG meets the technical, organisational, and procedural requirements identified in TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The time during which TSA event logs (see clause 5.6.10) are retained.	MSCTG TP/TPS and additional internal documents define how MSCTG meets the technical, organisational, and procedural requirements identified in TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The applicable legal system, including any claim to meet the requirements on time-stamping services under national law.	The applicable legal system and dispute resolution procedures relating to MSCTG are within the underlying Subscriber agreement.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
Limitations of liability.	MSCTG bears specific liability for damage to Subscribers and Relying Parties in relation to valid qualified digital certificates relied upon in accordance with specific laws and regulations of Malaysia. These liabilities are described in section 5.4.4 Limitation of Liability of the MSCTG CPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
Procedures for complaints and dispute settlement.	The applicable legal system and dispute resolution procedures relating to the MSCTG are dealt with within the underlying Subscriber agreement.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
If the TSA has been assessed to be conformant with the identified time-stamp policy, and if so by which independent body.	MSCTG conformance with the applicable TP/TPS is confirmed by an independent certification body.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

5 TSA Obligations

MSCTG undertakes that the following controls relating to TSA obligations are in place.

5.1 General

Control Objectives	Control Description	Reference
The TSA shall ensure that all requirements on TSA, as detailed in clause 5.2, are implemented as applicable to the selected trusted time-stamp policy.	MSCTG has disclosed all requirements in its TP/TPS section 5.4.1 Obligations.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The TSA shall ensure conformance with the procedures prescribed in this policy, even when the TSA functionality is undertaken by sub-contractors.	MSCTG performs internal and external audits to assure compliance with the TP/TPS and other related policies and procedures.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The TSA shall also ensure adherence to any additional obligations indicated in the time-stamp either directly or incorporated byreference. The TSA shall provide all its time-stamping services consistentwith its Practice statement and disclosure statement.	MSCTG ensures that all requirements and procedures detailed in the TP/TPS are implemented and authenticate requests for time countermarks using digital certificates.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

5.2 TSA Obligations towards Subscribers

Control Objectives	Control Description	Reference
The present document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the TSA's terms and conditions.	When the subscriber is an organisation, some of the obligations that apply to that organisation will have to apply to the end-users. In any case, the organisation will be held responsible if the obligations from its end-users are not correctly fulfilled and therefore the 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 obligations are not correctly fulfilled.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

5.3 Relying Party Obligations

Control Objectives	Control Description	Reference
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.	MSCTG has disclosed in its TP/TPS in section 5.4.4 Relying Party Obligations.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

5.4 Liability

Control Objectives	Control Description	Reference
The present document does not specify any requirement on liability. In particular, it should be noticed that a TSA may disclaim or limit any liability unless otherwise stipulated by the applicable law.	MSCTG has disclosed in its TP/TPS in section 5.4.4 Relying Party Obligations that MSCTG undertakes to operate in accordance with the TP/TPS and the terms of service level agreements with the Subscriber. MSCTG makes no express or implied representations or warranties relating to the availability or accuracy of the time-stamping service. MSCTG bears specific liability for damage to Subscribers and Relying Parties in relation 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 MSCTG TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

6 TSA Management and Operation

MSCTG undertakes that the following controls for TSA management and operations are in place.

6.1 Key Management Life Cycle

Control Objectives	Control Description	Reference
Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle	MSCTG generates the cryptographic keys used in its TSA services under the control of authorised personnel in a secure physical environment	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The requirements identified in WebTrust for CA Principle and Criteria clause 4 shall apply.	MSCTG has disclosed the requirements identified in clause 4.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

6.2 Time-stamp Issuance

Control Objectives	Control Description	Reference
The time-stamp token shall include an identifier for the time-stamp policy.	MSCTG has technical prescriptions in place to ensure that TSTs are issued securely and include the correct time. In line with the protocols referenced in Section 4 of MSC MSCTG TP/TPS	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
Each time-stamp token shall have a unique identifier.	MSCTG has disclosed this in its TSA TPS section 5.5.2 time-stamp issuance	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The time values the TSU uses in the time-stamp shall be traceable to at least one of the real-time values distributed by an NMIM laboratory.	The time-calibrated to within 1 second of UTC, traceable to a UTC(k) source	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The time included in the time-stamp shall be synchronised with MST within the accuracy defined in the policy and, if present, withinthe accuracy defined in the time-stamp itself.	MSCTG has disclosed this in its TSA TPS section 5.5.2 time-stamp issuance	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
If the timestamp provider's clock is detected (see clause 5.5.3) as being out of the stated accuracy (see clause 5.3) then time-stamps shall not be issued.	MSCTG has disclosed this in its TSA TPS section 5.5.2 time-stamp issuance	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The time-stamp token shall include a representation (e.g. hash value) of the datum being time-stamped as provided by the requestor. The time-stamp shall be signed using a key generated exclusively for this purpose.	MSCTG has disclosed this in its TSA TPS section 5.5.2 time-stamp issuance	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

6.3 Clock Synchronisation with MST

Control Objectives	Control Description	Reference
The calibration of the TSU clocks shall be maintained such that the clocks do not drift outside the declared accuracy.	The TSUs have technical measures in place to ensure that the clocks do not drift outside the declared accuracy	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The declared accuracy shall be of 1 second or better.	MSCTG TSA provides time with ±1 second of a trusted UTC time source.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

Control Objectives	Control Description	Reference
The TSU clocks shall be protected against threats that could result in an undetected change to the clock that takes it outside its calibration.	TSU clocks are protected within the HSMs and are periodically recalibrated against the NMIM time source.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The TSA shall detect if the time that would be indicated in a time-stamp drifts or jumps out of synchronisation with MST.	TSU clocks are also able to detect time-stamp drifts outside pre-set boundaries and request additional recalibrations as needed.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
If it is detected that the time indicated in a time-stamp drift or jumps out of synchronisation with MST, the TSU shall stop time-stamp issuance.	If the TSU clock drifts or jumps out of synchronisation with MST, and recalibration fails, the TSA will not issue time-stamps until the correct time is restored. Manual administration of the TSU clock requires authorised personnel.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The clock synchronisation shall be maintained when a leap second occurs as notified by the appropriate body. The change to take account of the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record shall be maintained of the exact time (within the declared accuracy) when this change occurred.	MSCTG shall obtain written confirmation on annual basis from NMIM to verify that the TSU clocks are synced with MST within the declared accuracy	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
The TSA shall obtain written confirmation on annual basis from NMIM to verify that the TSU clocks are in sync with MST within the declared accuracy	MSCTG shall obtain written confirmation on annual basis from NMIM to verify that the TSU clocks are in synced with MST within the declared accuracy.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

6.4 TSA Termination and Termination Plans

Control Objectives	Control Description	Reference
The TSA shall ensure that potential disruptions to subscribers and relying parties are minimised as a result of the cessation of the TSA's time-stamping services, and in particular ensure continued maintenance of information required to verify the correctness of time-stamp tokens.	MSCTG has disclosed this in the TP/TPS in section 5.5.4 Termination and Termination Plans	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7 General Security and Controls

MSCTG informed that the following security controls are in place.

7.1 Security Management

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.1 shall apply.	The configuration of the MSCTG system, as well as any modifications and upgrades, are documented and controlled by MSCTG management.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7.2 Asset Classification and Management

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.2 shall apply.	MSCTG has ensured an appropriate level of protection of its assets including information assets. All information assets have been assigned a classification consistent with the risk assessment.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7.3 Human Resource Security

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.3 shall apply.	MSCTG has disclosed compliance in the MSCTG TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7.4 Physical and Environmental Security

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.4 shall apply.	MSCTG 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.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7.5 Operation Security

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.5 shall apply.	MSCTG has disclosed the identified Principle and Criteria in the TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7.6 Incident Management

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.5 shall apply.	MSCTG handles incident and compromise according to the incident and compromises handling procedures in order to minimise the impact of such events.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7.7 Access Control

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.6 shall apply.	MSCTG has disclosed the identified Principle and Criteria in the TP/TPS particularly in Section 5.6.7.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7.8 System Development and Maintenance

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.7 shall apply.	MSCTG has disclosed the identified Principle and Criteria in the TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7.9 Business Continuity Management

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.8 shall apply.	MSCTG has disclosed the identified Principle and Criteria in the TP/TPS, particularly Section 5.6.9.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7.10 Compliance

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.9 shall apply.	MSCTG 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.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

7.11 Collection of Evidence

Control Objectives	Control Description	Reference
The requirements identified in WebTrust for CA Principles and Criteria clause 3.10 shall apply.	The archive collection system complies with the security requirements described in MSCTG CPS Section 5.4 Audit Logging Procedure and 5.5 Records Archival.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022 read together with the MSCTG CP and CPS

8 TSU key management

Control Objectives	Control Description	Reference
Records concerning all events relating to the life-cycle of TSU keys shall be logged.	MSCTG has disclosed its key management life cycle in the TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022
Records concerning all events relating to the life-cycle of TSU certificates (if appropriate) shall be logged.	MSCTG has disclosed its key management life cycle in the TP/TPS.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

8.1 Clock Synchronisation

Control Objectives	Control Description	Reference
Records concerning all events relating to synchronisation of a TSU's clock to MST shall be logged. This shall include information concerning normalre-calibration or synchronisation of clocks used in time-stamping.	MSCTG TSA provides time with ±1 second of a trusted UTC time source. The TSUs have technical measures in place to ensure that the clocks do not drift outside the declared accuracy. The TSUs use DS/NTP, a mutually authenticated extension of the Network Time Protocol (NTP), to secure synchronisations with NMIM time sources and to provide audit records that the time in a given TST is accurate.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

Control Objectives	Control Description	Reference
Records concerning all events relating to the detection of loss of synchronisation shall be logged.	TSU clocks are protected within the HSMs and are periodically recalibrated against the NMIM time source. TSU clocks are also able to detect time-stamp drifts outside pre-set boundaries and request additional recalibrations as needed. If the TSU clock drifts or jumps out of synchronisation with MST, and recalibration fails, the TSA will not issue time-stamps until the correct time is restored. Manual administration of the TSU clock requires authorised personnel.	MSC Trustgate Time Stamp Policy and Time Stamp Practice Statement Version 1.2, 27 October 2022

SECTION II: FINDINGS AND RECOMMENDATIONS

Requirements	Findings and Recommendations	Reference	Management Response
Part VI: Recognition of Date/Time Stamp Services - Section 20 of the DSA 1997 **Part IX: Date/Time Stamp Services, DSR1998**	**1. Data not backed-up regularly** There is a high risk of data loss as there areno data replication from Data Centre to theBackup Centre in case of disaster. TSA data are stored in the Data Centre andit doesn't have backup data via replication with the latest data in Alternate Site. We recommend that MSCTG TSA team tostart replication for TSA with the latest backup to ensure data consistency.	**MCMC requirement 5.6.9 Business Continuity Management** The requirements identified in WebTrust for CA Principle and Criteria clause 3.8, shall apply	Action Plan: TSA Data replication to DR will be made. Timeline: Q2, 2023 Responsibility: Infra Team Status: **In progress (50%) - The data already replicated in DC**
Part VI: Recognition of Date/Time Stamp Services - Section 20 of the DSA 1997 **Part IX: Date/Time Stamp Services, DSR1998**	**2. Service agreement not updated** We noted that the support and maintenance service agreement between MSC Trustgate and the TSA system vendor,Ascertia is for 12 months effective 1 March2018. ADSS TSA system is in high risk of system failure as there are no vendor support andmaintenance service. We understand that this Agreement is auto-renewal. It is important to periodically review on the anniversary of renewal.	**MCMC requirement 5.6.8 System Development and Maintenance** The requirements identified in WebTrust for CA Principle and Criteria clause 3.7, shall apply	Action Plan: The service agreementis still in force during the audit period. Timeline: N/A Responsibility: N/A Status: **Completed**
Part VI: Recognition of Date/Time Stamp Services - Section 20 of the DSA 1997 **Part IX: Date/Time Stamp Services, DSR1998**	**3. Enhance authentication with SIRIM'sNTP Server** There is a risk of man-in-the-middle attackusing SIRIM NTP Services via IP protocol. If one can manipulate the NTP server on a target, you could then pass the max-age setby HSTS (HTTP Strict Transport Security), thereby making the client connect without SSL again before HSTS sets a new one.	**MCMC requirement 5.6.5 Operation Security** The requirements identified in WebTrust for CA Principle and Criteria clause 3.5 shall apply.	Action Plan: IP whitelisting has been put in place to prevent cyber-attack. We believe the current Practice is sufficient. To enhance the authentication mechanism, this need to be done by SIRIM. Timeline:

Requirements	Findings and Recommendations	Reference	Management Response
	Consequently, NTP is vulnerableto attacks, ranging from time shifting that stealthily shift clocks on victim clients to denial-of-service attacks. In particular, man-in-the-middle attackers, capable of intercepting traffic between a client and server, can wreak havoc on time synchronisation. We recommend the additional securitymeasures and or authentication to be considered to reduce the risk of man in the middle attack		N/A Responsibility: NMIM SIRIM Status: **Completed**
Part VI: Recognition of Date/Time Stamp Services - Section 20 of the DSA 1997 **Part IX: Date/Time Stamp Services, DSR1998**	**4. Assessment of the outsourced TSA timeauthority for NTP** We were informed that MSCTG TSA relies on SIRIM for the provision of accurate timefor the time-stamping services of TrustgateTSA. We note that in section 5.5.3 of the MSC Trustgate.com Time-Stamp Policy and Practice Statement Version 1.2 states "Trustgate shall obtain written confirmation on annual basis from NMIM to verify that the TSU clocks are in [sync] with MST within the declared accuracy" noevidence of such written confirmation was received for the period under audit. We recommend that MSCTG TA receive written confirmation from SIRIM, on the declared basis within the TP/TPS. In addition, we recommend that MSCTG TSA conduct an independent confirmation that is satisfactory to MSCTG TSA regardingthe accuracy of the TSU clocks.	**MCMC requirement 5.6.5 Operation Security** MSC Trustgate.com Time-Stamp Policy and Practice Statement Version 1.2 section 5.4.2 on NTP providers and section 5.5.3 regarding clock synchronisation with NMIM.	Action Plan: SIRIM has provided the annual written report for the auditperiod that confirmed MSC Trustgate NTP server sync with MST within the declared accuracy. Timeline: N/A Responsibility: N/A Status: **Completed**