MOORE STEPHENS

TRUSTGATE
SECURE TRANSACTION. TRUSTED BUSINESS

WEBTRUST FOR CERTIFICATION AUTHORITIES PERFORMANCE AND COMPLIANCE AUDIT

REPORT

FOR

MSC TRUSTGATE.COM SDN BHD

29 SEPTEMBER 2017

TABLE OF CONTENTS

1. AUDITOR'S OPINION

To the Management of MSC Trustgate.com Sdn. Bhd.

We have examined the assertion by the management of MSC Trustgate.com Sdn. Bhd. ("MSCTG") that in providing its Certification Authority ("CA") services known as Trustgate CA, has:

- Disclosed its key and certification life cycle management business and information privacy practices in its Certification Practice Statement and provided such services in accordance with its disclosed practices, and
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated (for the registration activities performed by Trustgate CA);
  - Integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - Subscriber and relying party information was restricted to authorised individuals and protected from users not specified in the CA's business practices disclosure;
  - Continuity of key and certificate life cycle management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorised and performed to maintain the CA systems integrity based on the CPA Canada WebTrust for Certification Authorities Criteria.

MSCTG's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by Chartered Professional Accountants Canada ("CPA Canada"), and accordingly, included:

(1) obtaining an understanding of MSCTG CA's key and certification life cycle management business and information privacy practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance and operation of systems integrity;

(2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy practices;

(3) testing and evaluating the operating effectiveness on the controls; and

(4) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion even though inherent limitations in controls, errors or fraud may occur but undetected. Furthermore, the projection of any conclusion, based on our findings, to future periods is subject to the risk that the validity of such conclusion may be altered because of changes made to the systems or controls, or deterioration in the degree of effectiveness of the controls.

In our opinion, for the period from 1 August 2016 through 30 August 2017, MSCTG CA's management assertion, as set forth in the first paragraph, is fairly

stated, in all material respects, in accordance to the CPA Canada WebTrust for Certification Authorities Criteria.

The WebTrust seal of assurance for the Certification on MSCTG's website constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

The relative effectiveness and significance of specific controls at MSCTG and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

This report does not include any representation as to the quality of MSCTG's CA services beyond those covered by the WebTrust for Certification Authorities Criteria, nor the suitability of any of MSCTG's services for any customer's intended purposes.

Moore Stephens Advisory Sdn Bhd
29 September 2017

2. CONTROL OBJECTIVES, DESCRIPTION OF CONTROLS AND FINDINGS

Our assessment has been conducted in accordance with the Trust Service Principles and Criteria for Certification Authorities (Version 2.0 Effective July 1, 2011) ("WebTrust") and WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.

The Trust Services Principles and Criteria for CAs can be used as a control framework to assess the adequacy of the CA systems, policies and procedures.

2.1. MSCTG BACKGROUND

MSCTG is licenced by the Malaysia Communications and Multimedia Commission for the following areas: [1]

- Licensed Certification Authority (License No: LPBP-2/2015[2], Issuing Date: 25 July 2015, Expiry Date: 24 July 2020)
- Recognised Repository (License No: PPR-2/2015[2], Issuing Date: 25 July 2015, Expiry Date: 24 July 2020)

MSCTG is selling Secure Socket Layer ("SSL") and 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:[2]

2.1.1. MSCTG ROOT KEY

There are three Root Keys owned by MSCTG as follows:

Type of Certificate	Description
Class 1 Certificates	Self-signed MSC Trustgate Root CA for Class 1*
Class 2 Certificates	Self-signed MSC Trustgate Root CA for Class 2*
Class 3 Certificates	Self-signed MSC Trustgate Internal Root CA for Class 3*

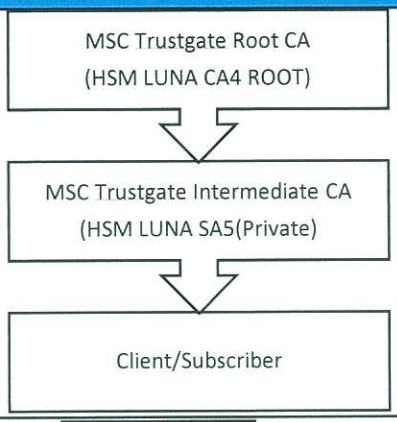
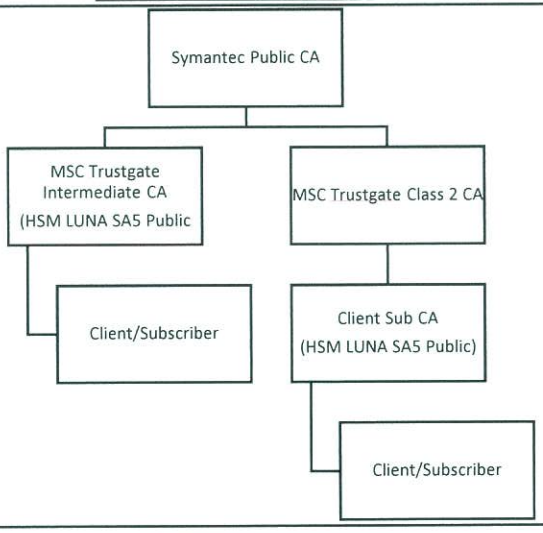
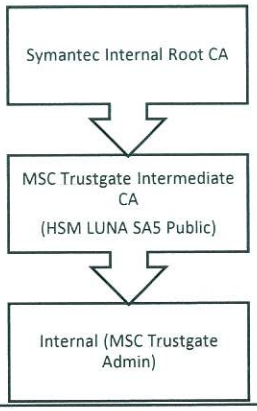
*Note that Root CAs are generated by an HSM.

Applicability of the WebTrust for CA's requirements:

CA Key Life Cycle Management Controls	Subscriber Key Life Cycle Management Controls	Certificate Life Cycle Management Controls	Subordinate CA Certificate Life Cycle Management Controls
✓			

[1] SKMM DSA Register: http://www.skmm.gov.my/Legal/Register/DSA-Registers.aspx (Accessed 7 September 2017)
[2] Symantec Trust Network (STN) Certificate Policy Version 2.8.13: https://www.msctrustgate.com/repository.htm (Accessed 7 September 2017)

There are three types of scenarios for the implementation of the CA/PKI services:

Types of Scenario	CA Hierarchy
CA Scenario 1: Private	
CA Scenario 2: Public	
CA Scenario 3: Internal	

2.1.2. CERTIFICATES ISSUED TO CLIENT/SUBSCRIBERS/ INDIVIDUALS

Certificate Class:	Low assurance level	Medium assurance level	High assurance level	Signing	Encryption	Client Authentication
Class 1 Certificates	✓			✓	✓	✓
Class 2 Certificates		✓		✓	✓	✓

Applicability of WebTrust for CA's requirements:

CA Key Life Cycle Management Controls	Subscriber Key Life Cycle Management Controls	Certificate Life Cycle Management Controls	Subordinate CA Certificate Life Cycle Management Controls
	✓	✓	✓

2.1.3. CERTIFICATES ISSUED TO MSCTG Admin

Certificate Class:	High assurance level	Code/Content Signing	Secure SSL/TLS-sessions	Authentication	Signing and Encryption
Class 3 Certificates	✓	✓	✓	✓	✓

Applicability of WebTrust for CA requirements:

CA Key Life Cycle Management Controls	Subscriber Key Life Cycle Management Controls	Certificate Life Cycle Management Controls	Subordinate CA Certificate Life Cycle Management Controls
	✓	✓	✓

2.1.4. OTHER SERVICES

In addition to providing services to subscribers, MSCTG offers managed PKI services to organisations to assist in the management of their certificates and directory services

Applicability of WebTrust for CA's requirements:

CA Key Life Cycle Management Controls	Subscriber Key Life Cycle Management Controls	Certificate Life Cycle Management Controls	Subordinate CA Certificate Life Cycle Management Controls
✓			

2.2. TRUST SERVICE PRINCIPLES AND CRITERIA FOR CA

The Trust Service Principles and Criteria for Certification Authorities are organised into the following areas:

- CA Business Practices Disclosure
- CA Business Practices Management
- CA Environmental Controls
- CA Key Life Cycle Management Controls
- Subscriber Key Life Cycle Management Controls
- Certificate Life Cycle Management Controls
- Subordinate CA Certificate Life Cycle Management Controls

2.3. SUMMARY OF FINDINGS

We set out below the overall findings for the control areas assessed followed by our detailed findings:

TRUST SERVICE PRINCIPLES AND CRITERIA	FINDINGS
CA BUSINESS PRACTICES DISCLOSURE	Update of CP & CPS to reflect requirements from SSL validation

TRUST SERVICE PRINCIPLES AND CRITERIA	FINDINGS
CA ENVIRONMENTAL CONTROLS	Action Required for CA Personnel Security Management
	Action Required for CA System Access Management
	Action Required Business Continuity Management
	Action Required for Audit Logging Management

3. CA BUSINESS PRACTICES DISCLOSURE

The Certification Authority:

- Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement
- Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control policies in its Certificate Policy (if applicable)
- Provides services in accordance with its disclosed practices

The following areas were examined during our assessment of CA business practices disclosure:

- Certificate Policy (CP)
- Certification Practice Statement (CPS)

3.1. CERTIFICATE POLICY

The CA discloses its business practices including but not limited to the topics listed in RFC 3647, RFC 2527, or WebTrust for Certification Authorities and The Certification Authority (CA) discloses its SSL Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Requirements.

3.1.1. ISSUES NOTED

3.1.1.1. Update of CP to meet SSL Validation Requirements

TRUST SERVICE PRINCIPLES AND CRITERIA AREA: CA BUSINESS PRACTICES DISCLOSURE		
OBSERVATION	**RECOMMENDATION**	**MANAGEMENT RESPONSE**
The disclosed CPS published on http://www.msctrustgate.com/repository.htm Effective as of 3 December 2016, the CA's CP/CPS are required to provide a link to a web page or an email address for contacting the person or persons responsible for operation of the CA	CP update to include web page or an email address for contacting the person or persons responsible for operation of the CA	**Action Plan**: To adopt auditor's recommendation **Timeline:** 31st October 2017 **Ownership:** Mohammed Salmi Ahmad Sabki

3.1.2. KEY PERSONNEL INTERVIEWED

Name	**Position**
Hazhar Bin Ismail	Head of Technology Division

Mohammed Salmi Ahmad Sabki	Security Manager

3.1.3. KEY DOCUMENTS REVIEWED

- Symantec Trust Network (STN) Certificate Policy version 2.8.13

3.2. CERTIFICATION PRACTICE STATEMENT (CPS)

The CA discloses its business practices including but not limited to the topics listed in RFC 3647, RFC 2527, or WebTrust for Certification Authorities v1 CA Business Practices Disclosure Criteria in its Certification Practice Statement.

The Certification Authority (CA) discloses its SSL Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Requirements

3.2.1. ISSUES NOTED

3.2.1.1. Update of CPS to meet SSL Validation Requirements

TRUST SERVICE PRINCIPLES AND CRITERIA AREA: CA BUSINESS PRACTICES DISCLOSURE		
OBSERVATION	**RECOMMENDATION**	**MANAGEMENT RESPONSE**
The disclosed CPS published on http://www.msctrustgate.com/repository.htm The CA discloses in the Certification Practice Statement (CPS) that it includes its limitations on liability, if the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement. Effective as of 3 December 2016, the CA's CP/CPS are required to provide a link to a web page or an email address for contacting the person or persons responsible for operation of the CA.	CPS update to include web page or an email address for contacting the person or persons responsible for operation of the CA	**Action Plan**: To adopt auditor's recommendation **Timeline:** 31st October 2017 **Ownership:** Mohammed Salmi Ahmad Sabki

3.2.2. KEY PERSONNEL INTERVIEWED

Name	Position
Hazhar Bin Ismail	Head of Technology Division
Mohammed Salmi Ahmad Sabki	Security Manager

3.2.3. KEY DOCUMENTS REVIEWED

- MSC Trustgate.com Certification Practice Statement (CPS) Version 3.8.8,

4. CA ENVIRONMENTAL CONTROLS

The Certification Authority maintains effective controls to provide reasonable assurance that:

- Logical and physical access to CA systems and data is restricted to authorised individuals;
- The continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance and operations are properly authorised and performed to maintain CA systems integrity.

The following areas were examined during our assessment of CA environmental controls:

- Security Management;
- Asset Classification and Management;
- Personnel Security;
- Physical and Environmental Security;
- Operations Management;
- System Access Management;
- Systems Development and Maintenance;
- Business Continuity Management;
- Monitoring and Compliance; and
- Audit Logging.

4.1. ISSUES NOTED

4.1.1. ACTION REQUIRED FOR PERSONNEL SECURITY MANAGEMENT

TRUST SERVICE PRINCIPLES AND CRITERIA AREA: WEBTRUST CA ENVIRONMENTAL CONTROLS		
OBSERVATION	**RECOMMENDATION**	**MANAGEMENT RESPONSE**
We noted that Operations and Systems Manual (OSM) V1.3 dated 4th September 2016 and User Procedures Manual (UPM) V1.2 Dated 4th September 2016 We also noted that staff are unware of the existence of the OSM and UPM. Lack of awareness of for CA Personnel. We also noted that ongoing trustworthiness assessment not conducted annually.	1. Ensure OSM and UPM are distributed and communicated to the appropriate staff 2. Ensure annual trustworthiness assessments are conducted	**Action Plan**: To adopt auditor's recommendation. **Timeline:** 31st December 2017 **Ownership:** Suzannah Abdul Syukur

4.1.2. KEY PERSONNEL INTERVIEWED

Name	Position
Suzannah Abdul Syukur	Admin & Human Resources Executive
Mohammed Salmi Ahmad Sabki	Security Manager

4.1.3. KEY DOCUMENTS REVIEWED

- Operations and Systems Manual (OSM) Version 1.3

4.1.4. ISSUES NOTED

4.1.4.1. Inadequate System Access Management

TRUST SERVICE PRINCIPLES AND CRITERIA AREA: WEBTRUST CA ENVIRONMENTAL CONTROLS		
OBSERVATION	**RECOMMENDATION**	**MANAGEMENT RESPONSE**
We note that Trusted Roles accounts using an username and password to authenticate into CA systems are configured with Password at least eight (8) characters, be changed at least every 90 days, use a combination of at least numeric and alphabetic characters, not be one of the user's previous four passwords; and implement account lockout for failed access attempts; Effective as of 3 December 2016, SSL Baseline requirements require at least twelve (12) characters be changed at least every 90 days, use a combination of at least numeric and alphabetic characters, not be one of the user's previous four passwords; and implement account lockout for failed access attempts	Passwords to authenticate into CA Systems are to be configured to: **1.** Twelve (12) characters be changed **2.** 90 Days expiry **3.** Combination of at least numeric and alphabetic characters, **4.** Not be one of the user's previous four passwords; **5.** Implement account lockout for failed access attempts	**Action Plan**: To adopt auditor's recommendation. **Timeline:** 31st October 2017 **Ownership:** Rusli Yasmin

4.1.1. KEY PERSONNEL INTERVIEWED

Name	Position
Rusli Yasmin	System Engineer, CA Operations and Support
Mohammed Salmi Ahmad Sabki	Security Manager

4.2. BUSINESS CONTINUITY MANAGEMENT

The CA maintains controls to provide reasonable assurance that CA system access is limited to authorised individuals. Such controls provide reasonable assurance that:

- operating system and database access is limited to authorised individuals with predetermined task privileges;
- access to network segments housing CA systems is limited to authorised individuals, applications and services; and
- CA application use is limited to authorised individuals.

4.2.1. ISSUES NOTED

4.2.1.1. Inadequate Business Continuity Management

TRUST SERVICE PRINCIPLES AND CRITERIA AREA: WEBTRUST CA ENVIRONMENTAL CONTROLS.		
OBSERVATION	**RECOMMENDATION**	**MANAGEMENT RESPONSE**
We reviewed the Disaster Recovery Plan Manual (DRPM) version 1.3 We noted the following: 1. Disaster Recovery Site not ready during Audit Period 2. Testing of Disaster Recovery being conducted for the Audit Period	Annual testing of Disaster Recovery should be conducted based on DRPM Section 2.7.7 Testing of Disaster Recovery Plan Policy.	**Action Plan:** Testing of Disaster Recovery shall be conducted. **Timeline:** 30th November 2017 **Ownership:** Hazhar Bin Ismail Rusli Yasmin

4.2.2. KEY PERSONNEL INTERVIEWED

Name	Position
Hazhar Bin Ismail	Head, Technology Department
Rusli Yasmin	System Engineer, CA Operations and Support
Mohammed Salmi Ahmad Sabki	Security Manager

4.2.3. KEY DOCUMENTS REVIEWED

- Disaster Recovery Plan Manual (DRPM) Version 1.3
- Operations and Systems Manual (OSM) Version 1.3

4.3. AUDIT LOGGING

The CA maintains controls to provide reasonable assurance that:

- significant CA environmental, key management, and certificate management events are accurately and appropriately logged;
- the confidentiality and integrity of current and archived audit logs are maintained;
- audit logs are completely and confidentially archived in accordance with disclosed business practices; and
- audit logs are reviewed periodically by authorised personnel.

4.3.1. ISSUES NOTED

4.3.1.1. Inadequate Audit Logging Management

TRUST SERVICE PRINCIPLES AND CRITERIA AREA: WEBTRUST CA ENVIRONMENTAL CONTROLS.		
OBSERVATION	**RECOMMENDATION**	**MANAGEMENT RESPONSE**
We noted the following: 1) Audit Logs are not reviewed periodically	MSCTG shall: 1) Review on audits logs should be done at least annually	**Action Plan:** To adopt auditor's recommendation. **Timeline:** 30th December 2017 **Ownership:** Hazhar Bin Ismail

4.3.2. KEY PERSONNEL INTERVIEWED

Name	Position
Hazhar Bin Ismail	Head, Technology Department
Rusli Yasmin	System Engineer, CA Operations and Support
Mohammed Salmi Ahmad Sabki	Security Manager

4.3.3. KEY DOCUMENTS REVIEWED

- MSC Trustgate Information Security Policies Manual (ISPM) Version 1.3
- Operations and Systems Manual (OSM) version 1.3
- Verisign Security and Audit Requirements

5. CA KEY LIFECYCLE MANAGEMENT CONTROLS

The Certification Authority maintains effective controls to provide reasonable assurance that the integrity of keys and certificates it manages is established and protected throughout their life cycles.

The following areas were examined during our assessment of CA key life cycle management controls:

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Cryptographic Hardware Life Cycle Management
- CA Key Compromise (if applicable)

5.1.1. NO ISSUES NOTED

5.1.2. KEY PERSONNEL INTERVIEWED

Name	Position
Hazhar Bin Ismail	Head, Technology Department
Mohammed Salmi Ahmad Sabki	Security Manager
Muhammad Syahhizal Abu Hashim	Key Manager

5.1.3. KEY DOCUMENTS REVIEWED

- MSC Trustgate.com Certification Practice Statement (CPS) Version 3.8.8
- Verisign Key Ceremony Reference Guide
- Cryptographic Key Management Procedures (CKMP) Version 1.3

6. SUBSCRIBER KEY LIFECYCLE MANAGEMENT CONTROLS

The Certification Authority maintains effective controls to provide reasonable assurance that the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles.

The following areas were examined during our assessment of CA subscriber key life cycle management controls:

- CA-Provided Subscriber Key Generation Services
- Requirements for Subscriber Key Management

6.1. NO ISSES NOTED

6.1.1. KEY PERSONNEL INTERVIEWED

Name	Position
Hazhar Bin Ismail	Head, Technology Department
Mohammed Salmi Ahmad Sabki	Security Manager
Muhammad Syahhizal Abu Hashim	Key Manager

6.1.2. KEY DOCUMENTS REVIEWED

- MSC Trustgate.com Certification Practice Statement (CPS) Version 3.8.8
- Symantec Trust Network (STN) Certificate Policy Version 2.8.13
- Key Ceremony Reference Guide

7. CERTIFICATE LIFECYCLE MANAGEMENT CONTROLS

The Certification Authority maintains effective controls to provide reasonable assurance that Subscriber information was properly authenticated

The following areas were examined during our assessment of the certificate life cycle management controls:

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

7.1. NO ISSUES NOTED

7.1.1. KEY PERSONNEL INTERVIEWED

Name	Position
Hazhar Bin Ismail	Head, Technology Department
Mohammed Salmi Ahmad Sabki	Security Manager
Noor Hazlah Md Drus	Lead Customer Services and Support Executive
Siti Sarah Bachok	Supervisor Product Executive

7.1.2. KEY DOCUMENTS REVIEWED

- MSC Trustgate.com Certification Practice Statement (CPS) Version 3.8.8, 1 July 2012
- Symantec Trust Network (STN) Certificate Policy Version 2.8.13 March 20, 2014
- User Procedures Manual Version 1.2, 4 September 2016

8. SUBORDINATE CA CERTIFICATE LIFECYCLE MANAGEMENT CONTROLS

The Certification Authority maintains effective controls to provide reasonable assurance that subordinate CA certificate requests are accurate, authenticated and approved.

8.1. SUBORDINATE CA CERTIFICATE LIFE CYCLE MANAGEMENT

The Parent CA maintains controls to provide reasonable assurance that:

- subordinate CA certificate requests are accurate, authenticated and approved;
- subordinate CA certificate replacement (renewal and rekey) requests are accurate, authorised, complete;
- new, renewed and rekeyed Subordinate CA certificates are generated and issued in accordance with the CA's disclosed business practices;
- upon issuance, complete and accurate Subordinate CA certificates are available to relevant entities (Subscribers and Relying Parties) in accordance with the CA's disclosed business practices;
- subordinate CA certificates are revoked based on authorised and validated certificate revocation requests; and
- timely, complete and accurate certificate status information (including CRLs and other certificate status mechanisms) is made available to any entity in accordance with the CA's disclosed business practices.

8.1.1. NO ISSUES NOTED

8.1.2. KEY PERSONNEL INTERVIEWED

Name	Position
Hazhar Bin Ismail	Head, Technology Department
Mohammed Salmi Ahmad Sabki	Security Manager
Noor Hazlah Md Drus	Lead Customer Services and Support Executive
Siti Sarah Bachok	Supervisor Product Executive

8.1.3. KEY DOCUMENTS REVIEWED

- MSC Trustgate.com Certification Practice Statement (CPS) Version 3.8.8
- Symantec Trust Network (STN) Certificate Policy Version 2.8.13