CA Owner Name:
MSC Trustgate

-- General information about CA's associated organization --

CA Email Alias 1:
msctg-root@msctrustgate.com

Company Website:
https://www.msctrustgate.com/

Organizational Type :
Private Corporation

Geographic Focus:
Malaysia.

Primary Market / Customer Base:
- Public, Commercial and Government
- Malaysia

Recognized CAA Domains:
msctrustgate.com

Problem Reporting Mechanism:
support@msctrustgate.com
helpdesk@msctrustgate.com

-- CP/CPS and Audit Statements --

Policy Documentation:
Information about the CA's relevant documentation, such as the primary language the documents are provided in and which languages the documents are translated into.
According to Mozilla's Root Store Policy, the CP/CPS documents must be publicly disclosed, available on the CA's official website, reviewed and updated at least once every year, and translated into English.

CA Document Repository:
https://www.msctrustgate.com/repository.php

Certificate Policy (Link): https://www.msctrustgate.com/tgcp

Certification Practice Statement (Link): https://www.msctrustgate.com/tgcps

Other Relevant Documents:

Auditor: Baker Tilly Consulting Sdn Bhd

Auditor Location: Kuala Lumpur, Malaysia

Standard Audit Statement (Link): https://www.cpacanada.ca/webtrustseal?sealid=10085
Standard Audit Type: http://www.webtrust.org/principles-and-criteria/item83172.aspx
Standard Audit Statement Date: 29th October 2018
Standard Audit Period Start Date: 1st September 2017
Standard Audit Period End Date: 31st August 2018

BR Audit Statement (Link):
BR Audit Type:
BR Audit Statement Date:
BR Audit Period Start Date:
BR Audit Period End Date:

EV SSL Audit Statement (Link):
EV SSL Audit Type:
EV SSL Audit Statement Date:
EV SSL Audit Period Start Date:
EV SSL Audit Period End Date:

Audit statements must be publicly accessible, not confidential, and translated into English. Audit statements will be rejected if they do not list the Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope, and if they do not meet all of the requirements listed in Mozilla's Root Store Policy.

-- Required and Recommended Practices --

BR Self Assessment:

URL to the CA's latest BR Self Assessment per https://wiki.mozilla.org/CA/BR_Self-Assessment

CA's Response to Required Practices:

CP/CPS section numbers addressing each of the items listed in https://wiki.mozilla.org/CA/Required_or_Recommended_Practices

1. Publicly Available CP and CPS:
1.1 Revision Table, updated annually:
1.2 CAA Domains listed in CP/CPS:
1.3 BR Commitment to Comply statement in CP/CPS:
1.4 CP/CPS Structured According to RFC 3647, appropriate use of 'No Stipulation':
2. Audit Criteria:
2.1 Complete Audit History:
3. Revocation of Compromised Certificates:
4. Verifying Domain Name Ownership:
4.1 Baseline Requirements:
4.2 WHOIS:
4.3 Email Challenge-Response:
5. Verifying Email Address Control:
6. DNS names go in SAN:
7. OCSP:
- OCSP SHALL NOT respond "Good" for unissued certs:
8. Network Security Controls:

-- Forbidden and Potentially Problematic Practices --

CA's Response to Forbidden Practices:

CP/CPS section numbers addressing each of the items listed in https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices

1. Long-lived Certificates:
2. Non-Standard Email Address Prefixes for Domain Ownership Validation:
3. Issuing End Entity Certificates Directly From Roots:
4. Distributing Generated Private Keys in PKCS#12 Files:
5. Certificates Referencing Local Names or Private IP Addresses:
6. Issuing SSL Certificates for .int Domains:
7. OCSP Responses Signed by a Certificate Under a Different Root:
8. Issuance of SHA-1 Certificates:
9. Delegation of Domain / Email Validation to Third Parties:

-- Root Certificate # 1 --

Certificate Data Extracted from PEM:

The CCADB will automatically extract the following information from the PEM of the root certificate.

Subject
Issuer
Valid From
Valid To
Certificate Serial Number
SHA-1 Fingerprint
SHA-256 Fingerprint
Signature Hash Algorithm
Public Key Algorithm
SPKI SHA256
Subject + SPKI SHA256

-- Audits that apply to this Root Certificate --

Indicate/Check which of the provided audit statements apply to this root certificate. As per Mozilla's Root Store Policy, each audit statement must clearly provide the distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope.

Standard Audit:
BR Audit:
EV SSL Audit:

-- Application Information --

Explanation:

Explain why this root cert needs to be included in the root store, rather than being signed by another CA's root certificate that is already included.

Role:

Explain the unique function of this root, especially if requesting inclusion of multiple roots.

Root Certificate Download URL:

Public URL through which the CA certificate can be directly downloaded.

-- Mozilla Fields --

Mozilla Trust Bits:

One or both of Email (S/MIME) or Websites (TLS/SSL)

SSL Validation Type:

Indicate all that apply of domain-validated only (DV), domain and organization validated (OV), and enhanced validation (EV).
DV -- The ownership of the domain name is verified, but the identity/organization of the subscriber is not verified.
OV -- In addition to verifying the domain ownership, you also validate the organization to be listed in the O field - making sure public record and government resources can verify the address, existence, and good legal standing of the organization itself. Verifying that the whois listed address matches the verified address, and any other additional checks that a given CA lists in its CPS.
EV - Verification meets the requirements of the CA/Browser Forum CA/Browser Forum's EV Guidelines

Mozilla EV Policy OID(s):

2.23.140.1.1
Before requesting EV treatment, CAs should understand how Firefox processes EV certificates and determine if they should use the standard CA/Browser Forum EV OID (2.23.140.1.1) or a CA-specific OID. Unless the CA already has a CA-specific OID enabled in Firefox, Mozilla strongly recommends that CAs use the standard CA/Browser Forum EV OID.

Mozilla Applied Constraints:

*Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs.*

-- CA Hierarchy Information --

Indicate/Check all of the following that apply:
Cross-Signed by another Root Cert:
Has Externally Operated SubCAs:
CP/CPS allows Externally Operated SubCAs:
Has External Registration Authorities:
CP/CPS allows External RAs:

Description of PKI Hierarchy:

- *URL and/or Description of this PKI Hierarchy.*
- *Provide details related to any of the check-boxes above that are selected.*
- *Add records for the existing intermediate certs to the CCADB as described here:*
  - *https://ccadb.org/cas/intermediates#adding-intermediate-certificate-data*
- *If Mozilla accepts and includes your root certificate, then we have to assume that we also accept any of your future sub-CAs and their sub-CAs. Therefore, the selection criteria for your sub-CAs and their sub-CAs will be a critical decision factor. As well as the documentation and auditing of operations requirements that you place on your sub-CAs and their sub-CAs.*
- *If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist in a separate document.*

Constraints on External SubCAs & RAs:

- *Describe constraints on external subordinate CAs and RAs.*

- *As per section 5.3 of Mozilla's Root Store Policy, provide the required data for all of your non-technically-constrained subordinate CA certificates that chain up to this root certificate.*
    - *This data may be provided as follows:*
        - *If your CA has access to the CCADB, then you may provide this information directly in the CCADB.*
        - *Otherwise, provide this information in your Bugzilla Bug.*

-- Test Websites or Example Cert --
If requesting Websites trust bit provide 3 URLs to 3 test websites (valid, expired, revoked) whose TLS/SSL cert chains up to this root.

Test Website - Valid:

Test Website - Expired:

Test Website - Revoked:

Test Notes:
If not requesting the Websites trust bit, then provide an example cert that chains up to this root.

Make sure you test your three 'Test Websites' in Firefox as follows:
1. *Create a new Firefox Profile for testing, as described in Mozilla's knowledge base articles: Profile Manager and Creating a new Firefox Profile.*
2. *Import the root certificate as described here.*
3. *Set OCSP hard fail as described here.*
4. *Clear browser history*
5. *Browse to the test websites.*
6. *Open the Web Console to check for any warnings (e.g. SHA-1, etc.) that should be addressed.*

- *Intermediate CA certificates are expected to be distributed to the certificate subjects (the holders of the private keys) together with the subjects' own certificates. Those subject parties (e.g. SSL servers) are then expected to send out the intermediate CA certificates together with their own certificates whenever they are asked to send out their certificates. That is required by SSL/TLS.*
- *Certificate authorities MUST advise their subscribers that all intermediate certificates should be installed in the servers containing the dependent subscriber certificates.*

-- Test Results (When Requesting the SSL/TLS Trust Bit) --

Revocation Tested:
Test with http://certificate.revocationcheck.com/ and make sure there aren't any errors.

CA/Browser Forum Lint Test:
Provide evidence that you have tested and verified that no certificates issued in this CA hierarchy violate any of the CA/Browser Forum Baseline Requirements (BRs).
BR Lint Test: https://github.com/awslabs/certlint

***Mozilla will check that the CA is not issuing certificates that violate any of the BRs** by using crt.sh on the root and subordinate CAs via:*
https://crt.sh/?caid=<CA ID>&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01
and/or

The Lint tests in https://crt.sh/?a=1

Test Website Lint Test:

Provide evidence that you have tested and verified that no certificates issued in this CA hierarchy violate the X.509 rules.
X.509 Lint Test: https://github.com/kroeckx/x509lint

https://wiki.mozilla.org/CA:TestErrors -- Meaning and recommended solutions to errors that CAs have run into while doing the tests listed above.

EV Tested:

If EV treatment is being requested, then provide successful output from EV Testing as described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version

-- End Root Certificate #1 --

If you are requesting inclusion for multiple root certificates that are covered in the same audit statements, then repeat the information in the "Root Certificate # 1" section for each additional root.