Mozilla Root CA Program

General information about the CA’s

Name	Pos Digicert (Full name Pos Digicert Sdn. Bhd.)
Website URL	https://www.posdigicert.com.my
Organizational type	Pos Digicert is operated by a private corporation. Pos Digicert is a licensed public Certification Authority (CA) provider in Malaysia with a registered address in Malaysia and also a wholly owned subsidiary of POS Malaysia Berhad (POS), a Government Link Company or GLC.
Primary Market / Customer Base	Pos Digicert is mandated to serve the public and goverment sector as part of the license issued by the regulatory body. Pos Digicert client based includes Enterprise, Government, Small Medium Enterprise (SME) and Consumer with potential market size of more than 15 million users in Malaysia by 2020. Pos Digicert main focus is serve Malaysian with a potential growth in the ASEAN region.
Impact to Mozilla Users	As a leading CA in Malaysia, Pos Digicert has grown to become a respected service provider/partner to the Malaysian Government, SME, Enterprise and Consumers. The CA authentication services ensure Pos Digicert products and services are secured and trusted at all times. The greatest challenge for Pos Digicert as a public and leading CA provider is to answer customer complaints on the security alert message of “Not a trusted CA” and manual installation/registration of Pos Digicert CA Root Certificate at servers and customer client devices. The manual works is to avoid problems when installing/using Pos Digicert CA certs. This additional step is counterproductive, unnecessary and costly. Therefore, if Pos Digicert CA root certificate is registered with Mozilla root store, Pos Digicert can avoid the additional steps required and greatly improve Pos Digicert customer experience. In Malaysia, CA is a licensed services, governed and regulated by Malaysian Communication and Multimedia Commission (MCMC) under Digital Signature Act 1997 and Digital Signature Regulation 1998. Therefore, Pos Digicert's root certificate for all major browsers especially Mozilla users in the government, public and private sectors is required for providing PKI services such as secure authentication, encryption/decryption, digital signing/time stamping, secure messaging and email, etc. Pos Digicert have been accepted & included in Microsoft Trusted Root CA Store.

CA Primary Point of Contact (POC)	a. Musliza Mohd Mustafa (Senior Manager, Strategic Initiative) musliza@digicert.com.my +6012-3869963 +603-88006006 b. Noorul Halimin Mansol (Manager, Strategic Initiative) noorul.mansol@digicert.com.my +6013-3974644 +603-88006019 c. Mohamad Zaharem Muslan (Manager, PKI Services) zaharem@digicert.com.my +6019-3644341

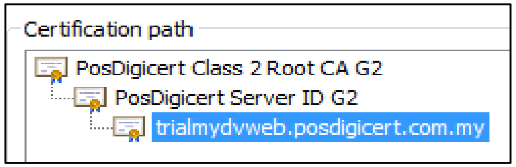
Technical information about each root certificate

Certificate Name	Pos Digicert is submitting only one root certificate authority which is named as PosDigicert Class 2 Root CA G2

Certificate Issuer Field	CN = PosDigicert Class 2 Root CA G2
	O = Digicert Sdn. Bhd.
	C = my

Certificate Summary	Type of certificates issued under this root certificate: - SSL - SAN - Wildcard
Root Certificate URL	Pos Digicert root certificate is available at https://www.posdigicert.com.my/downloadpage/root-certificate
SHA1 Fingerprint	31 3b 8d 0e 7e 2e 4d 20 ae 86 68 ff e5 9d b5 19 3c bf 7a 32
Valid From	Monday, 17 October, 2016
Valid To	Friday, 17 October, 2036
Certificate Version	V3
Certificate Signature Algorithm	sha512RSA
Signing key parameters	RSA 4096 bits
Test Website URL (SSL)	https://trialmydvweb.posdigicert.com.my
Certificate Revocation Lists (CRLs)	URL=http://crl.digicert.com.my/PosDigicertSID.crl
OCSP URL (OCSP is required for the SSL trust bit to be enabled)	
Requested Trust Bits	Pos Digicert root CA required the following Trust Bits for inclusion of Root certificate Mozilla's CA Program: 1. Websites (SSL/TLS)
SSL Validation Type	DV
EV Policy OID(s)	Not Applicable
Mozilla Applied Constraints	Name constraint is not applied to Pos Digicert root certificate.

CA Hierarchy information for each root certificate

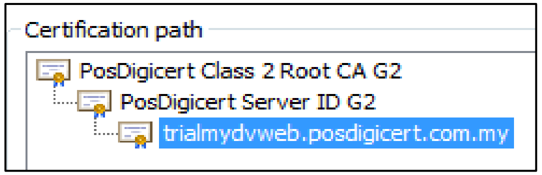
CA Hierarchy	PosDigicert Class 2 Root CA G2 owned & operated by Pos Digicert. Pos Digicert's Subordinate CA that is signed by this root is PosDigicert Server ID G2. PosDigicert Server ID G2 is created to issue Class 2 SSL certificates, for example as illustrated as below:  Certification path PosDigicert Class 2 Root CA G2 PosDigicert Server ID G2 trialmydvweb.posdigicert.com.my
Externally Operated SubCAs (Sub CAs Operated by 3rd Parties)	Currently, Pos Digicert has no externally operated subCAs.
Cross-Signing	Not applicable.
Technical Constraints on Third-party Issuers	Noted. Shall file the bug to provide this information to Bugzilla system.

Verification Policies and Practices

Documentation: CP, CPS & Relying Party Agreements	Pos Digicert's CPS is in English language. CPS can be retrieved from https://www.posdigicert.com.my/repository/cps CPS includes statements of commitment to CAB Forum BR in Section 8.4 Topic covered by Assessment.
Audits	Audit Type: WebTrust for CA version 2.0 Auditor: PricewaterhouseCoopers, Malaysia Auditor Website: http://www.pwc.com/my URL to Audit Report & Management's Assertions: https://cert.webtrust.org/SealFile?seal=2177&file=pdf
Baseline Requirements (SSL)	Pos Digicert shall undergo CAB Forum BR Audit in October 2017. Pos Digicert's CPS has stated in their CPS for the need of "Commitment to Comply" statement in section 8.4: Topics covered by Assessment.
SSL Verification Procedures	Section 3.2.2 Authentication of Organization Identity for Class 2 verification. Pos Digicert does not issue EV certificates. Therefore, Pos Digicert does not performed EV SSL Verification Procedures.
Email Address Verification Procedures	Not Applicable.
Code Signing Subscriber Verification Procedures	Not Applicable.
Multi-factor Authentication	CPS Section 6.4.1: Activation Data Generation and Installation & 6.4.2: Activation Data Protection. Pos Digicert enforces a combination of cryptographic and physical access control mechanisms for certificate issuance system. Pos Digicert confirmed use hardware tokens, secure thumb drive to do multi-factor authentication.
Network Security	Pos Digicert is complied with WebTrust Audit for CA version 2.0 network security requirements.

Response to Mozilla's CA Recommended Practices

Review Mozilla's CA Recommended Practices. If your practices differ from any of these recommended practices, then describe those differences and explain how the concern(s) are addressed.

Publicly Available CP and CPS	CPS is publicly available at https://www.posdigicert.com.my/repository/cps Pos Digicert's CPS is in English version & pdf format.
CP/CPS Documents will be Reviewed!	Noted.
CA Hierarchy	This root certificate currently has one internally-operated subordinate CA certificate, “PosDigicert Server ID G2” which issues certificates for TLS & S/MIME.  Certification path PosDigicert Class 2 Root CA G2 PosDigicert Server ID G2 trialmydvweb.posdigicert.com.my
Audit Criteria	Audit Type: WebTrust for CA version 2.0 Auditor: PricewaterhouseCoopers, Malaysia Auditor Website: http://www.pwc.com/my URL to Audit Report & Management's Assertions: https://cert.webtrust.org/SealFile?seal=2177&file=pdf
Document Handling of IDNs in CP/CPS	Pos Digicert does not allow the use of IDNs in certificates.
Revocation of Compromised Certificates	Pos Digicert shall revokes the certificates if one of the reasons occur as stated in CPS section 4.9.3: Procedure for revocation request. Pos Digicert follows the baseline requirements which not allow the CA to do certificate suspension.
Verifying Domain Name Ownership	Pos Digicert take the reasonable measures to verify the entity submitting the CSR has registered the domain as stipulated in CPS section 3.2.2 & 3.2.6.
Baseline Requirements:	Pos Digicert take the reasonable measures to validate the identity for domain submitted by the organization as stipulated in CPS section 3.2.2 & 3.2.6.
WHOIS:	Pos Digicert is enforced WHOIS check method.
Email Challenge-Response:	Pos Digicert is not using E-mail Challenge-Response as the mechanism for verification.

Domain owned by a Natural Person	Noted. Currently POS Digicert does not issue or performed application by domain name that is owned by a natural person. Pos Digicert certificate can be bought only by organisation.
OCSP	Currently, POS Digicert Root certificate set up OCSP responders to listen on standard port.
Network Security Controls	Yes. POS Digicert is complied with WebTrust Audit for CA version 2.0 network security requirements & Network abd Certificate System Security Requirements (https://www.cabforum.org/documents.html)

Response to Mozilla's list of Potentially Problematic Practices

	YES/NA	URLS/SECTION/PAGE NO.
Long-lived DV certificates	NA	Pos Digicert does not issues Long-lived DV certificates. Certificates are valid for up to 3 years.
Wildcard DV SSL certificates	NA	Pos Digicert does not issues wildcard DV SSL certificates.
Email Address Prefixes for DV Certs		
Delegation of Domain / Email validation to third parties	NA	Pos Digicert does not performed delegation of Domain / Email validation to third parties.
Issuing end entity certificates directly from roots	NA	
Allowing external entities to operate subordinate CAs	NA	Pos Digicert has no externally operated subCAs.
Distributing generated private keys in PKCS#12 files	YES	Pos Digicert distributed generated PKCS#12 files using encrypted email and secure token (e.g secure thumbdrive). The password is not transferred together with the token.
Certificates referencing hostnames or private IP addresses	NA	Pos Digicert does not issue SSL with a hostname which not resolvable through public DNS or private IP address.
Issuing SSL Certificates for Internal Domains	NA	
OCSP Responses signed by a certificate under a different root	NA	
SHA-1 Certificates	NA	Pos Digicert issues certificates with SHA256RSA and above.
Generic names for CAs	NA	Pos Digicert is not owned generic names Cas.
Lack of Communication With End Users	YES	Pos Digicert is contactable via e-mail as stated in the above and customercare@digicert.com.my
Backdating the notBefore date	NA	Pos Digicert does not practice notBefore date. Pos Digicert issues certificate using time set by the CA which synchronized with GMT time zone.