Print this page

Mozilla - CA Program

Case Information

Case Number	00000218	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Pos Digicert Sdn. Bhd (Malaysia)	**Request Status**	Need Information from CA

Additional Case Information

Subject	Include PosDigicert Class 2 Root CA G2	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1396760

General information about CA's associated organization

CA Email Alias 1	customercare@digicert.com.my		
CA Email Alias 2			
Company Website	https://www.posdigicert.com.my	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Malaysia	**Verified?**	Verified
Primary Market / Customer Base	Pos Digicert serves Malaysia with a potential growth in the ASEAN region. Pos Digicert client based includes Enterprise, Government, Small Medium Enterprise (SME) and Consumer.	**Verified?**	Verified
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. In Malaysia, CA is a licensed services, governed and regulated by	**Verified?**	Verified

Malaysian Communication and Multimedia Commission (MCMC) under Digital Signature Act 1997 and Digital Signature Regulation 1998.

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	CA reviewed, reported no problems.	**Verified?**	Verified

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's lists of Forbidden and Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	CA reviewed, reported no problems. NEED: CA reported that SSL certs are valid up to 3 years, but the rule changes to 825 days on March 1. See sections 4.2.1 and 6.3.2 of https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.6.pdf	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	PosDigicert Class 2 Root CA G2	**Root Case No**	R00000399
Request Status	Need Information from CA	**Case Number**	00000218

Certificate Data

Certificate Issuer Common Name	PosDigicert Class 2 Root CA G2

O From Issuer Field	Digicert Sdn. Bhd.
OU From Issuer Field	
Valid From	2016 Oct 17
Valid To	2036 Oct 17
Certificate Serial Number	0098205c
Subject	CN=PosDigicert Class 2 Root CA G2, OU=null, O=Digicert Sdn. Bhd., C=MY
Signature Hash Algorithm	sha512WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	31:3B:8D:0E:7E:2E:4D:20:AE:86:68:FF:E5:9D:B5:19:3C:BF:7A:32
SHA-256 Fingerprint	19:AB:CD:FF:3A:74:40:2F:A8:F0:CA:20:6B:F7:FA:B0:DF:FF:F3:AE:2B:BD:71:95:84:D2:10:90:A4:35:32:07
Certificate Fingerprint	DC:70:9B:05:8B:4B:E4:CE:0F:8B:28:0F:A5:13:77:20:20:2D:6E:99:5E:E7:57:11:04:95:36:ED:A6:77:9B:F8
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This request is to include the 'PosDigicert Class 2 Root CA G2' root certificate and enable the Websites trust bit. This root certificate has internally-operated intermediate certificates.	**Verified?**	Verified
Root Certificate Download URL	https://www.posdigicert.com.my/public/uploads/certificate/PosDigicert_Class_2_RootCA_G2.cer	**Verified?**	Verified
CRL URL(s)	http://crl.digicert.com.my/PosDigicertSID.crl NEED: CRLs that conform to the CA/Browser Forum's Baseline Requirements (BRs). See BRs section. 4.9.7.	**Verified?**	Need Response From CA
OCSP URL(s)	NEED: OCSP and authorityInformationAccess (AIA) that conform to the BRs. See BRs sections 4.9.9, 4.9.10, 7.1.2.2, 7.1.2.3,	**Verified?**	Need Response From CA
Mozilla Trust Bits	Websites	**Verified?**	Verified

SSL Validation Type	DV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: 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. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid	https://testvalid.posdigicert.com.my/	**Verified?**	Need Response From CA
Test Website - Expired	https://testexpired.posdigicert.com.my/		
Test Website - Revoked	https://testrevoke.posdigicert.com.my/		
Example Cert			
Test Notes	NEED: Cert for Revoked test website cannot be expired.		

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

Revocation Tested	NEED: Resolve errors: https://certificate.revocationcheck.com/testvalid.posdigicert.com.my	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: Explain/Resolve errors listed here: https://crt.sh/?caid=51025&opt=cablint,zlint,x509lint&minNotBefore=2000-01-01	**Verified?**	Need Response From CA
Test Website Lint Test		**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	This root certificate has internally operated subordinate certificates.	**Verified?**	Verified
Externally Operated SubCAs	None	**Verified?**	Verified

Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Not Applicable	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English	**Verified?**	Verified
CA Document Repository	https://www.posdigicert.com.my/repository/cps	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.posdigicert.com.my/public/uploads/files/CPS-Rev-60.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.posdigicert.com.my/public/uploads/files/CPS-Rev-60.pdf	**Verified?**	Verified
Other Relevant Documents	https://www.posdigicert.com.my/downloadpage/root-certificate	**Verified?**	Verified
Auditor Name		**Verified?**	Not Applicable
Auditor Website		**Verified?**	Not Applicable
Auditor Qualifications		**Verified?**	Not Applicable
Standard Audit	NEED: Current Audit statements meeting the requirements of Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: Current BR audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV SSL Audit	Not requesting EV treatment	**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 8.4	**Verified?**	Verified

BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8911654	**Verified?**	Verified
SSL Verification Procedures	NEED: CPS must have clear description of how the CA verifies that the domain names to be included in the SSL certificate are owned/controlled by the certificate subscriber. There is currently not sufficient description of the domain validation procedures in the CPS. Also, it must be clear which subsections of BR section 3.2.2.4 the CA uses. See https://wiki.mozilla.org/CA/Communications#January_2018_CA_Communication	**Verified?**	Need Response From CA
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	CPS section 3.2.2	**Verified?**	Verified
Email Address Verification Procedures	Not requesting Email trust bit.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS section 6.4.2	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified