Print this page

Mozilla - CA Program

Case Information

Case Number	00000046	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	Telekom Applied Business Malaysia (TMCA)	**Request Status**	Need Information from CA

Additional Case Information

Subject	New Owner/Root inclusion requested	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1090014

General information about CA's associated organization

Company Website	https://www.tmca.com.my	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)	Telekom Applied Business (TAB) is a licensed public CA service provider. TAB is a private organization registered in Malaysia and a wholly owned subsidiary of Telekom Malaysia Berhad (TM), a Government Link Company or GLC.	**Verified?**	Verified
Geographic Focus	Malaysia	**Verified?**	Verified
Primary Market / Customer Base	TAB client base includes Enterprise, Government, Small Medium Enterprise (SME) and Consumer with potential market size of 20 million users in Malaysia by 2020. The focus market is Malaysia with a potential growth in the ASEAN region.	**Verified?**	Verified
Impact to Mozilla Users	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, TMCA'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.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of 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	* Document Handling of IDNs in CP/CPS: TMCA does not allow the use of IDNs in certificates. * Revocation of Compromised Certificates: TMCA shall revokes the certificates if one of the reasons occur as stated in CPS section 4.4. TMCA will follow the baseline requirements which not allow the CA to do certificate suspension. * DNS names go in SAN: TMCA is subjected to BR#9.2.1 and BR#9.2.2.	Verified?	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	Problematic Practices Statement	I have reviewed Mozilla's list of 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	* TMCA does not issues wildcard DV SSL certificates. * Distributing generated private keys in PKCS#12 files : TMCA distributed generated PKCS#12 files using encrypted email and secure token (e.g secure thumbdrive. * TMCA does not issue SSL with a hostname which not resolvable through public DNS or private IP address. * SHA--1 Certificates: TMCA issues SHA256RSA certificates * TMCA should be contactable via e-mail as stated in the above and helpdesk@tab.com.my * TMCA does not practice notBefore date. TMCA issues certificate using time set by the CA which synchronized with GMT time zone.	Verified?	Verified

Root Case Record # 1

Root Case Information

Root Case No	R00000061	Case Number	00000046
Request Status	Need Information from CA	Root Certificate Name	TM Applied Business Root Certificate

Additional Root Case Information

Subject	Include TM Applied Business Root Certificate

Technical Information about Root Certificate

O From Issuer Field	TM	Verified?	Verified
OU From Issuer Field	TM Applied Business Certification Authority	Verified?	Verified
Certificate Summary	This root currently has one internally-operated subordinate CA.	Verified?	Verified
Root Certificate Download URL	https://www.tmca.com.my/portal/info/repositoryPage.html	Verified?	Verified
Valid From	2011 Oct 10	Verified?	Verified
Valid To	2031 Oct 10	Verified?	Verified
Certificate Version	3	Verified?	Verified

Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://www.tmca.com.my	**Verified?**	Verified
CRL URL(s)	ldap://ldap.tmca.com.my:389 /cn=arl1dp1,ou=ARL,ou=TM Applied Business Certification Authority,o=TM,c=my ldap://ldap.tmca.com.my:389 /cn=crl1dp85,ou=CRL,ou=TMCA,o=TM,c=my Note to CA: This might be considered problematic that the CRL URL is LDAP and not HTTP.	**Verified?**	Verified
OCSP URL(s)	NEED OCSP URI in the AIA of the end-entity and intermediate certificates. Mozilla requires end-entity certs to have OCSP URI in the AIA. See Appendix B of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	99:57:C5:3F:C5:9F:B8:E7:39:F7:A4:B7:A7:0E:9B:8E:65:9F:20:8C	**Verified?**	Verified
SHA-256 Fingerprint	A9:C7:7A:F1:BC:DF:AA:37:39:44:2B:0B:27:34:C6:8E:AF:2E:98:33:F0:D7:66:FB:CA:A6:F2:AE:B4:2D:EC:02	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root certificate currently has one internally-operated subordinate CA certificate, “TM Applied Business Certificate Authority”, which issues certificates for TLS, S/MIME, and code signing.	**Verified?**	Verified
Externally Operated SubCAs	Currently, TMCA has no externally-operated subCAs. CPS section 1.2.3, Sub Certificate Authority (Sub CA): In a distributed trust model, organizations may wish to become the issuer of Subscriber"s certificates. A Sub CA shall be the party who accepts applications, verifies, issues and revokes Subscriber certificates, subject to the agreement between TMCA and the party being the Sub CA. Sub CA has the authority to act as its own RA as depicted in Figure 1 above.	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified

Technical Constraint on 3rd party Issuer	CPS section 1.2.4 Registration Authorities (RAs) RAs are trusted entities appointed by TMCA to assist Subscribers in applying for certificates, to approve certificate requests and/or to help TMCA in revoking certificates. For RA, TMCA sends approval notification before end-user cert is activated (CPS section 4.1.2). TMCA shall do the process as stated in CPS section 4.2 before sending approval	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English	**Verified?**	Verified
CA Document Repository	https://www.tmca.com.my/portal/info/legalRepository.html	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.tmca.com.my/portal/documents/repositories/TMCA%20CP%20version%201.0.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.tmca.com.my/portal/documents/repositories/TMCA%20CPS%20version%201.13.pdf	**Verified?**	Verified
Other Relevant Documents	https://www.tmca.com.my/portal/documents/repositories/Generate%20CSR%20&%20SSL%20Certificate%20Installation%20User%20Guide%20v1.1.pdf	**Verified?**	Verified
Auditor Name	PricewaterhouseCoopers	**Verified?**	Verified
Auditor Website	http://www.pwc.com/my	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1670&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	4/30/2014	**Verified?**	Verified
BR Audit	NEED URL to BR audit statement: Need an audit statement specific to the Baseline Requirements. Please carefully review: https://wiki.mozilla.org/CA:BaselineRequirements (also have your auditor carefully review this wiki page)	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.	**Verified?**	Need Response From CA

SSL Verification Procedures	NEED See https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. If you are requesting to enable the Websites Trust Bit, then provide all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
EV SSL Verification Procedures	Not requesting EV treatment.	**Verified?**	Not Applicable
Organization Verification Procedures	CPS section 1.3 and 3.1.5: * Class 1: email authentication only * Class 2: verification of user is mandatory. This class of digital certificate is applicable for individual user certificate and server certificate. * Class 3: This class of digital certificate is used for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority (CA) or Authorized RA. CPS section 3.3: Authentication of Individual Identity CPS section 4.1.3: Class 3 authentication of organization, and authority of person to act on behalf of organization.	**Verified?**	Verified
Email Address Verification Procedures	CPS secton 4.1.1: This is an online registration process for Class 1 digital certificate application, in which the applicant can apply for the digital certificate at TMCA portal at his convenience. The email verification will be incorporated as part of the registration process, therefore, the email address of the applicant must be valid before TMCA is able to acknowledge the application and then send a notification email for him to activate the certificate.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	NEED What class of certificates are Code Signing certs? Where in the CP/CPS is this documented? If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Multi-Factor Authentication	TMCA confirmed use hardware tokens, secure thumb drive to do multi-factor authentication.	**Verified?**	Verified
Network Security	TMCA is complied with WebTrust Audit for CA version 2.0 network security requirements.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.tmca.com.my/portal/info/repositoryPage.html	**Verified?**	Verified