Bugzilla ID:
Bugzilla Summary:

General information about the CA's associated organization

CA Company Name	Telekom Applied Business Sdn Bhd (TAB)
Website URL	https://www.tmca.com.my
Organizational type	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.
Primary Market / Customer Base	TAB is mandated to serve the government and the public as part of the license issued by the regulatory body. Please refer to ATTACHMENT 1. TAB client based 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.
Impact to Mozilla Users	As a leading broadband and internet service provider (ISP) in Malaysia, TM has grown to become a respected service provider/partner to the Malaysian Government, SME, Enterprise and Consumers. The CA authentication services ensure TM products and services are secured and trusted at all times. The greatest challenge for TAB as a public CA provider is to answer customer complaints on the security alert message of "Not a trusted CA" and manual installation/registration of TAB CA Root Certificate at servers and customer client devices. The manual works is to avoid problems when installing/using TAB CA certs. This additional step is counterproductive, unnecessary and costly. Therefore, if TAB CA Root Cert is registered with Mozilla root store, TAB can avoid the additional steps required and greatly improve TMCA 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, 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.
Inclusion in other major browsers	Yes. Microsoft CA Program since November 2012.
CA Primary Point of Contact (POC)	a. Thaib Mustafa (Head, TMCA eSecurity Business) thaibmus@tm.com.my +6013 3402827 +603 79810239 b. Noorul Halimin Mansol (Manager, TMCA Business Assurance)

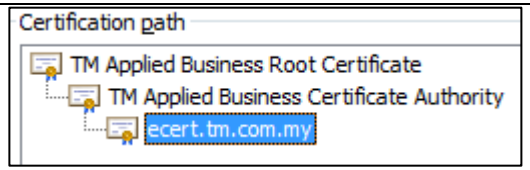
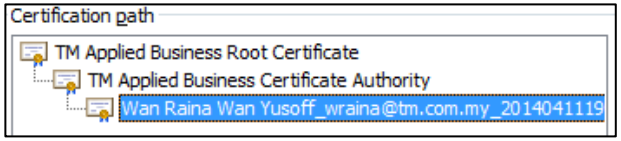
	noorulhalimin.mansol@tab.com.my +6013 3974644 +603 79844989

Technical information about each root certificate

Certificate Name	TAB is submitting only one root certificate authority which is named as TM Applied Business Root Certificate.
Certificate Issuer Field	CN = TM Applied Business Root Certificate OU = TM Applied Business Certification Authority O = TM C = my
Certificate Summary	Type of certificates issued under this root certificate: - SSL - SAN - Wildcard - Individual Certificate (Personal)
Mozilla Applied Constraints	Not Applicable
Root Cert URL	TAB Root CA is available at https://www.tmca.com.my/portal/info/repositoryPage.html
SHA1 Fingerprint	99 57 c5 3f c5 9f b8 e7 39 f7 a4 b7 a7 0e 9b 8e 65 9f 20 8c
Valid From	10/10/2011
Valid To	10/10/2031
Certificate Version	V3
Certificate Signature Algorithm	sha256RSA
Signing key parameters	RSA 4096 bits
Test Website URL (SSL) Example Certificate (non-SSL)	https://www.tmca.com.my
CRL URL	URL=ldap://ldap.tmca.com.my:389/cn=arl1dp1,ou=ARL,ou=TM Applied Business Certification Authority,o=TM,c=my
OCSP URL NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS.	http://ocsp.tmca.com.my:20001
Requested Trust Bits	TAB root CA required the following Extended Key Usage to be granted in Mozilla's CA Program: i. SSL Server Authentication

	ii. Client Authentication iii. Secure E-mail iv. Time Stamping v. Code Signing vi. OCSP
SSL Validation Type	DV and OV
EV Policy OID(s)	Not Applicable
Non-sequential serial numbers and entropy in cert	Current version of certificates use sequential serial number with the subject key identifier is 20 bits hash value of public key which is unpredictable random value.
Response to Recent CA Communication(s)	As stated in Mozilla CA Communication forum committee, TMCA shall use this communication channel for any updates on TMCA certificates for Mozilla Root CA Program.

CA Hierarchy information for each root certificate

CA Hierarchy	 
Externally Operated SubCAs	Not Applicable
Cross-Signing	Not Applicable
Technical Constraints on Third-party Issuers	Not Applicable

Verification Policies and Practices

Policy Documentation	Language used is in English. https://www.tmca.com.my/portal/info/repositoryPage.html
Audits	Audit Type: WebTrust for CA Trust Service Principles and Criteria for Certification Authorities Version 2.0

	Auditor: PricewaterhouseCoopers (PwC), Malaysia Auditor website: http://www.pwc.com/my URL to Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1670
Baseline Requirements (SSL)	TMCA is complied with WebTrust Audit for CA version 2.0 requirements. Please refer this URL for Audit Report or statement & Management Assertions. https://cert.webtrust.org/ViewSeal?id=1670
SSL Verification Procedures	ATTACHMENT 2 – IDENTITY VALIDATION PROCEDURE
Organization Verification Procedures	ATTACHMENT 2 – IDENTITY VALIDATION PROCEDURE
Email Address Verification Procedures	ATTACHMENT 2 – IDENTITY VALIDATION PROCEDURE
Code Signing Subscriber Verification Procedures	ATTACHMENT 2 – IDENTITY VALIDATION PROCEDURE
Multi-factor Authentication	TMCA confirmed use hardware tokens, secure thumb drive to do multi-factor authentication.
Network Security	TMCA is complied with WebTrust Audit for CA version 2.0 network security requirements. Please refer this URL for Audit Report or statement & Management Assertions. https://cert.webtrust.org/ViewSeal?id=1670