Bugzilla ID: 1090014
Bugzilla Summary: Add TM Applied Business Root CA Certificate to Trusted Root Store

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Telekom Applied Business Malaysia (TMCA)
Website URL	https://www.tmca.com.my
Organizational type	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.
Primark Market / Customer Base	TAB is mandated to serve the government and the public as part of the license issued by the regulatory body. 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.
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. 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)	Thaib Mustafa (Head, TMCA eSecurity Business) thaibmus@tm.com.my +6013 3402827, +603 79810239 Noorul Halimin Mansol (Manager, TMCA Business Assurance) noorulhalimin.mansol@tab.com.my +6013 3974644, +603 79844989 Mohamad Hafiz Bin Ismail hafiz.ismail@tm.com.my

Technical information about each root certificate

Certificate Name	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	None
Root Cert URL	https://bugzilla.mozilla.org/show_bug.cgi?id=1090014 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	2011-10-10
Valid To	2031-10-10
Certificate Version	3
Cert Signature Algorithm	SHA-256
Signing key parameters	2048
Test Website URL	https://www.tmca.com.my
CRL URL	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 CA/Browser Forum Baseline Requirements Appendix B: If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service. See Section 13.2.1 for details.
OCSP URL (Required now for end-entity certs)	OCSP URI in the AIA of end-entity certs – None – the SSL cert in the test website did not have an AIA with the OCSP URI, as required by Appendix B of the CA/Browser Forum's Baseline Requirements.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV and OV
EV Policy OID(s)	Not Applicable. Not requesting EV treatment.
Non-sequential serial numbers and entropy	**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)	Please provide TMCA's answers to the action items (as applicable) in these CA Communications: https://wiki.mozilla.org/CA:Communications#May_13.2C_2014 https://wiki.mozilla.org/CA:Communications#July_30.2C_2013 https://wiki.mozilla.org/CA:Communications#January_10.2C_2013

CA Hierarchy information for each root certificate

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.
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. So, externally-operated subCAs are allowed by the CPS. Are there currently any?
Externally Operated RAs	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. CPS section 2.2: To perform identity verification services, TMCA may outsource the functions to several Registration Authorities (RAs). RAs are reputable organizations that are capable to carry out the functions without compromising to the security procedures adopted by TMCA. Before RAs are appointed, the RAs need to sign up contract with TMCA and acceptance test will be carried out to ensure they are in compliance to the procedures. CPS section 4.1.2: This is a Class 2 digital certificate application process flow, in which the applicant will obtain the application form from TMCA website/Authorized Registration Authority (RA), fill in the form with required details and supporting documents and submit it personally to the Authorized RA for processing. Subscriber must first verify and confirm the application information captured by Authorized RA into system is correct before the key pair generation process. TMCA will acknowledge receipt of the Certificate Signing Request (CSR) from Authorized RA after the registration has been successfully completed at the Authorized RA‟s side. TMCA will, in turn, send out the notification email to the Subscriber to activate the certificate. In the case of digital certificate has been successfully issued by Authorized RA, TMCA will send the approval notification to the Authorized RA.
Cross-Signing	None
Technical Constraints on Third-party Issuers	According to the CPS, there may be external subordinate CAs and external Registration Authorities (RAs). Both are considered third-party issuers For RA, TMCA sends approval notification before end-user cert is activated (CPS section 4.1.2) – What checks does TMCA do before sending approval? How are the externally-operated subCAs constrained and how do they meet the CA/Browser Forum Baseline Requirements? See Baseline Requirements sections 9.7 and 17.

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: English Document Repository: https://www.tmca.com.my/portal/info/legalRepository.html CP: https://www.tmca.com.my/portal/documents/repositories/TMCA%20CPS%20version%201.13.pdf CPS: https://www.tmca.com.my/portal/documents/repositories/TMCA%20CP%20version%201.0.pdf
Audits	Audit Type: WebTrust for CA version 2.0 Auditor: PricewaterhouseCoopers, Malaysia Audit Report: https://cert.webtrust.org/SealFile?seal=1670&file=pdf (2014.04.30)
Baseline Requirements (SSL)	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) Also 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.
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.
SSL Verification Procedures	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 (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
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.

Code Signing Subscriber Verification Procedures	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
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.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	See above.
CA Hierarchy	See above
Audit Criteria	See above.
Document Handling of IDNs in CP/CPS	???
Revocation of Compromised Certificates	See Baseline Requirements section 13.1.5. CPS section 4.5 – Suspension of certificates – The Baseline requirements do not allow for Suspension of certificates. See BR section 13.2.7.
Verifying Domain Name Ownership	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	???
Domain owned by a Natural Person	See above
OCSP	See above

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	Certs are valid for up to 3 years.
Wildcard DV SSL certificates	???
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification.
Delegation of Domain / Email validation to third parties	See above
Issuing end entity certificates directly from roots	See above
Allowing external entities to operate subordinate CAs	See above
Distributing generated private keys in PKCS#12 files	???
Certificates referencing hostnames or private IP addresses	???

Issuing SSL Certificates for Internal Domains	???
OCSP Responses signed by a certificate under a different root	See above
SHA-1 Certificates	???
Generic names for CAs	See above
Lack of Communication With End Users	???
Backdating the notBefore date	???