Bugzilla ID: 518503
Bugzilla Summary: Add TWCA Root Certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	Taiwan Certification Authority (TWCA)
Website URL (English version)	http://www.twca.com.tw/Portal/english/coporate_profile/mission.html
Organizational type	Commercial
Primary market / customer base	Taiwan CA. Inc. (TWCA) provides a consolidated on-line financial security certificate service and a sound financial security environment, to ensure the security of on-line finance and electronic commercial trade in Taiwan.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	TWCA Root Certification Authority
Cert summary / comments	
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=402647
SHA-1 fingerprint.	cf:9e:87:6d:d3:eb:fc:42:26:97:a3:b5:a3:7a:a0:76:a9:06:23:48
Valid from	2008-08-28
Valid to	2030-12-31
Cert Version	3
Modulus length / key length	2048
Test Website	For testing purposes, please provide a URL to a website whose SSL cert chains up to this root.
CRL URL	http://RootCA.twca.com.tw/TWCARCA/revoke_2048.crl (Need CRL nextUpdate for end-entity certs)
OCSP Responder URL	none
Subordinate CAs operated by the CA organization	4 subordinate CAs Please provide further information about the hierarchy. A diagram would also be useful. What are the names of the 4 sub-CAs? Are all of the subordinate CAs operated internally by TWCA? Does the root issue any end-entity certificates directly? What is the difference between each of the subordinate CAs? Eg are they based on organization, or level of verification, or certificate type?

SubCAs operated by 3rd parties	Does (or will) this root have any subordinate CAs that are operated by external third parties? For the subordinate CAs that are operated by third parties, please provide a general description and explain how the CP/CPS and audits ensure the third parties are in compliance. Also, see https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	Please list any other root CAs that have issued cross-signing certificates for this root CA
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type DV, OV, and/or EV	DV, OV Do you perform identity/organization verification for all SSL certificates? Is it ever the case for SSL certs that the ownership of the domain name is verified, but the identity/organization of the subscriber is not verified?
EV policy OID(s)	Not EV
CP/CPS	Certificate Policy URL: http://www.twca.com.tw/picture/file/20090403-113227911.pdf (Traditional Chinese) CPS URL: http://www.twca.com.tw/picture/file/20090114-11212952.pdf (Traditional Chinese)
AUDIT	Audit Type: WebTrust CA Auditor: SunRise CPAs' Firm, a member firm of DFK international. Auditor Website: http://www.dfk.com/ Audit: https://cert.webtrust.org/ViewSeal?id=900 (2009.03.13)
Organization Identity Verification	Please provide translations into English of the sections of the CP/CPS documents pertaining to Verification of Identity and Organization. Please also list the documents and section or page numbers where the original text can be found.
Domain Name Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text. All documents supplied as evidence should be publicly available and must be addressed in any audit. Any substantial omissions submitted afterwards may need to be confirmed by auditor, at Mozilla's discretion.
Email Address Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to

	act on the account holder's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section/page numbers containing the original text. All documents supplied as evidence should be publicly available and must be addressed in any audit. Any substantial omissions submitted afterwards may need to be confirmed by auditor, at Mozilla's discretion.
Identity of Code Signing Subscriber	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the identity verification procedures for code signing certs. Please also list the corresponding document(s) and section or page numbers containing the original text.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information and translations into English of the CP/CPS where relevant. • Long-lived DV certificates o • Wildcard DV SSL certificates o • Delegation of Domain / Email validation to third parties o • Issuing end entity certificates directly from roots o • Allowing external entities to operate unconstrained subordinate CAs o • Distributing generated private keys in PKCS#12 files o • Certificates referencing hostnames or private IP addresses o • OCSP Responses signed by a certificate under a different root o • CRL with critical CIDP Extension o • Generic names for CAs