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) is a commercial CA that 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. Taiwan-CA INC. (TWCA) is a joint-venture company formed by Taiwan Stock Exchange Corporation (TWSE), Taiwan Depository and Clearing Corporation (TDCC) Financial Information Service Corporation (FISC), and HiTrust Inc (HiTrust).
CA Contact Information	CA Email Alias: ca@twca.com.tw CA Phone Number: 886-2-23708886 Title / Department: Policy Management Authority (PMA)

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
Root Cert 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	https://ssldemo.twca.com.tw/index.html
CRL URL	http://RootCA.twca.com.tw/TWCARCA/revoke_2048.crl http://sslserver.twca.com.tw/sslserver-test/revoke10_test.crl (NextUpdate: 24 hours)
CRL Issuing Frequency	CP section 4.9.7: CAs shall generate a CRL once every 24 hours
OCSP Responder URL	None

CA Hierarchy	CA Hierarchy Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=426285 This root has 4 internally-operated subordinate CAs. The root does not sign end-entity certificates directly. The sub-CAs are: 1. CN=TaiCA Secure CA, OU=SSL Certification Service Provider, O=TAIWAN-CA.COM Inc., C=TW The certificate issued by this sub-CA is used to be the identity of Web or Application Server. (SSL certificate) The liability and applicable limitation depends on the assurance level. 2. CN=TaiCA Secure CA, OU=Certification Service Provider, O=TAIWAN-CA.COM Inc., C=TW The certificate issued by this sub-CA is used to be the identity for on-line commerce transactions, such as the stock trading, or email security, depends on the assurance level. The liability and applicable limitation also depends on the assurance level. 3. CN=TaiCA Information Policy CA, OU = Policy CA, O = TaiCA, C =TW ; CN=TaiCA Information User CA, OU = User CA, O = TaiCA, C = TW The certificate issued by this sub-CA is used to be the identity for on-line taxation, e-Government or e-Commerce transactions. The liability and applicable limitation depends on the assurance level. 4. CN=TaiCA Finance CA, OU = Policy CA, O = TaiCA, C =TW ; CN=TaiCA Finance User CA, OU = User CA, O = TWCA, C = TW The certificate issued by this sub-CA is used to be the identity for on-line fund transfer, e-Finance or e-Banking transactions. The liability and applicable limitation depends on the assurance level. Comment #44: By now, TWCA root has signed only one sub-CA of the four you mentioned. Only the second sub-CA(the EC+) on your list has got signed last year. The others are supposed to be signed in the future. Comment #45: However, the four CAs on your list must follow TWCA UCA CPS mentioned above to conduct their operations, and these four CAs accept independent 3rd-party audit against the TWCA UCA CPS annually.
Externally Operated sub-CAs	TWCA has not accepted any 3rd party as a sub-CA and has no plan to do this type of business now.
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type	OV From TWCA: Currently, TWCA do RA function itself while issue SSL certificate. All personnel identity and organization must be verified before SSL certificate issue. Then authentication requirement is described in section 3.2.2 and 3.2.3. TWCA did not issue SSL certificate without authentication of identity and organization. The ownership of domain name must be verified when authenticate an organization.
EV policy OID(s)	Not EV
CP/CPS	Document Repository: http://www.twca.com.tw/Portal/english/coporate_profile/Repository.html TWCA UCA CPS (Traditional Chinese): http://www.twca.com.tw/picture/file/20090724-110350827.pdf

	TWCA UCA CPS (English): http://www.twca.com.tw/picture/file/20110315-113121435.pdf The User Certification Authority (UCA) issues, manages and delivers the RA and subscriber certificates according to the TWCA UCA CPS. TWCA PKI CP (English): http://www.twca.com.tw/picture/file/20100910-115805367.pdf TWCA PKI CP (Traditional Chinese): http://www.twca.com.tw/picture/file/20090806-171745500.pdf All sub-CAs shall comply with the rules in the CP to define their own CPS and follow the rules in their own CPS for operations. The CP defines policies and procedures for applying, verifying, issuing, and maintaining end-entity certificates in the section 4, “Certificate Life-Cycle Operational Requirement" TWCA Root CA CPS (English) http://www.twca.com.tw/picture/file/20100114-180956726.pdf TWCA Root CA CPS (Traditional Chinese): http://www.twca.com.tw/picture/file/20090114-11212952.pdf The purpose of the TWCA Root CA CPS document is to establish the policies for applying, verifying, issuing, and maintaining subordinate CAs.
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 (2010.03.13) Comment #18: TWCA conduct internal audits regularly following its management system rule(at least annually) to make sure all sub-CAs operated by TWCA comply with the CP and their CPS. Besides, all sub-CAs(whether operated by TWCA or not) of TWCA root shall have third-party audits and send reports to TWCA for examination. TWCA has not signed any sub-CA yet.
Organization Identity Verification	TWCA UCA CPS section 2.2.1.1: Level of Assurance Class 1 Identity authentication: The user certification authority (UCA) or RA only conducts limited verification of the user account (ID, such as personal name, registered company name or universal resource location (URL)) and e-mail account through simple procedures. Level of assurance: The UCA and RA only assure the uniqueness of the user account and e-mail account in the database, and all other information related to the user is considered as unverified. Applicability: Allows subscribers to send electronic documents by e-mail or protect their own electronic documents; except for business transactions required identity verification. Class 2 Identity authentication: Apart from checking the personal name, registered company name or URL, and the general relevant information, subscribers shall provide legal and correct identity documents (e.g. the photocopy of the citizen identity card or the profit business registration of company) during the registration which can be applied for by an agent. The UCA or RA

	will verify the identity of the applicant either by phone or through other means (e.g. a third-party database). Level of assurance: The UCA and RA only assure the uniqueness of the user account and e-mail account in the database, as well as general verification of the relevant subscriber information instead of assurance for absolutely correct subscriber information. Applicability: It is recommended to use in enterprise intranets, non-financial or non-securities small amount e-commerce transactions or encryption for data transmission. Class 3 Identity authentication: Apart from checking the information specified in Class 2, the subscriber shall personally apply for the registration. A legal person or corporate subscriber shall apply for registration through an agent holding valid authorization documents and documents that can identify his/her identity (e.g. citizen identity card or passport with a photo of the agent). Level of assurance: Identity verification higher than the Class 2 certificate is provided through various strict operating procedures to greatly enhance the certificate reliability of subscribers and trustees. Applicability: It is recommended to use in financial or securities transactions. Testing Certificates Identity authentication: Testing certificates are intended for testing purpose and neither the UCA nor the RA will run any identity authentication. Therefore, they cannot be used in any applications or businesses. Level of assurance: No assurance will be made by the UCA or RA. Applicability: Used by UCA-authorized subscribers for testing only. No use in any applications or businesses other than testing is allowed. Comment #47: TWCA UCA do not issue class level 4 assurance level EE certificate. CP section 3.2.2 Authentication of Organization Identity When authenticating the status of organizations, the organization shall submit documents issued by the competent authorities or other certifications proving its existence. The identity and authorization of its statutory representative shall be verified. If the application is made by the authorized agent of an organization, this agent shall also submit his/her identify certifications. All documents and/or certifications shall be submitted in writing or carried to the count by the agent in person. The following shows the requirements for the identity authentication of organization under various assurance level: Testing Class: To be specified by CAs in their CPS. Class 1: Limited verification of the subscriber name and email information with simple procedures by email. Class 2: In addition to organization name clearance, subscribers shall submit legal and correct certifications, without completing the procedures over the counter. Class 3: In addition to the information clearance specified in Class 2, an authorized agent carrying a valid letter of assignment shall make the application over the counter, and the agent shall submit his/her own certifications of identity or any procedures valid for authenticating the true identity of subscribers. Class 4: In addition to the information clearance specified in Class 3, the application shall be made by the statutory

	representative in person over the counter, and the statutory representative shall submit certifications valid for identifying his/her identity. When performing the initial verification of the information or communication hardware and software equipment of an organization (e.g. routers, firewalls, and servers), the equipment administrator shall submit the following registration information: · equipment identification (e.g. serial number) or service name (e.g. domain name); · equipment public key; · the licensing usage and attributes of equipment (e.g. the licensing usage or attributes shall be only be specified when it is included in the certificate); · the contact information of administrators for contacts made by the RA or CA; · CAs shall verify registration data with methods corresponding to the assurance level of certificates being applied for. The verification methods shall include, but not limited to, the methods specified in this part for authenticating the identity or the digital signature of subscribers (signature certificates shall be issued according to this CP). CP section 3.2.3 Authentication of Individual Identity The following show the requirements for the identity authentication of individual subscribers under various assurance level: Testing Class: To be specified by CAs in their CPS. Class 1: Limited verification of the subscriber name and email information with simple procedures by email. Class 2: In addition to individual name clearance, subscribers shall submit legal and correct certifications, without completing the procedures over the counter. Class 3: In addition to the information clearance specified in Class 2, the individual subscriber or his/her agent carrying a valid letter of assignment shall make in person the application over the counter Class 4: In addition to the information clearance specified in Class 3, the application shall be made by the individual subscriber in person over the counter. For the information or communication hardware and software equipment held by individual subscribers, the individual subscribers shall be deemed as the administrator of such equipment and shall complete the verification according to section 3.2.2.
Domain Name Ownership / Control	TWCA UCA CPS Sections 1.2 and 2.2.1.1: SSL server certificates are of assurance level 2 or 3. (EC+ Certificate type) TWCA UCA CPS section 5.1.B.2: SSL server certificates 1. Subscribers shall prepare the “photocopy of the profit business registration”; “domain name authorization”; “ SSL Server Digital Certificate Application Form”; and the check or draft of the service fees; and send them to the RA to apply for the SSL server certificate. 2. After entering the SSL server certificate application website via the Internet, subscribers shall generate the subscriber certificate application file according to the regulations for SSL server certificate application and registration. Then,

	subscribers shall complete the information of the technical contact person, business contact person and accounting contact person based on the information completed in the "SSL Server Digital Certificate Application Form" and the password to complete the certificate application. 3. If the domain name is registered in Taiwan (*.com.tw), RA must query the TWNIC WHOIS database to verify the ownership of domain name which filled in the certificate application form. If the domain name is not registered in Taiwan, RA must use the global WHOIS service (Network Solutions or others) to verify the ownership of the domain name. 4. After checking the subscriber's application documents and certificate application message, operators shall issue the subscriber certificate if there is no error and deliver a notice to the subscriber to download the certificate from the TWCA website by e-mail.
Email Address Ownership / Control	TWCA UCA CPS section 5.1.C: Application for CXML certificates 1. After completing at least the identity verification and PIN verification procedures, subscribers may register to the RA and sign the certificate application message generated with their private key before delivering the message to the RA. 2. After verifying the subscriber identity identification code and PIN and the integrity of subscriber certificate application message, the RA shall sign the subscriber certificate application message with the RA private key if there is no error. After encrypting the message with the server, the RA shall deliver the subscriber certificate application message to the UCA. 3. If certificate applicant applies the S/MIME certificate, RA must verify the applicant's email address. When verify the email address of S/MIME certificate, RA must verify the domain name ownership of mail address which is filled in certificate application form. After verify the ownership of domain name, RA operator will manually send email to applicant's mailbox to notify the certificate applying procedure is under process, and ask subscriber to reply to verify that the email address is correct and subscriber did do the certificate application. If certificate applicant replies using the same mail address and confirms the certificate application request, the verification of email address will be success, otherwise it will be fail. 4. After checking the subscriber certificate application message delivered from the RA, the legitimacy of the RA and subscriber identity, and the integrity of message, the UCA shall issue the certificate and deliver it to the RA if there is no error. 5. After checking the legitimacy and integrity of the subscriber certificate reply message from the UCA, the RA shall deliver the certificate to the applicant if there is no error.
Identity of Code Signing Subscriber	Not applicable – Not requesting Code Signing trust bit at this time.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ SSL certs are OV
	  ○ TWCA UCA CPS section 4.2: The maximum validity of the SSL server certificate is 4 years and is subject to extension with the approval of PMA when there is a special need.
	• Wildcard DV SSL certificates
	  ○ SSL certs are OV
	  ○ From TWCA: TWCA issued some wildcard SSL certificates. Before TWCA issue wildcard

	certificate, it must be verified the ownership of the domain. The issuance of wildcard SSL certificate without organization verification is not allowed.
	• Delegation of Domain / Email validation to third parties
	  ○ Not applicable.
	  ○ Comment #47: for SSL and SMIME certificate, TWCA's employee is responsible for subscriber information verification.
	• Issuing end entity certificates directly from roots
	  ○ Not applicable.
	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ The TWCA UCA CPS includes provisions for externally operated sub-CAs if needed in the future.
	  ○ Comment #47: Currently, TWCA do not issue sub-CA certificate to 3rd party because of no business value and the risk must be under control. If we have to issue sub-CA certificate to other 3rd party, we will follow TWCA Root CA CPS to do the following control:
	  ▪ 3rd party information verification including organization and representative person information.
	  ▪ Certificate life cycle management.
	  ▪ Sub-CA must follow TWCA PKI CP to do the CA practice audit including the CP, sub-CA CPS and sub-CA compliance with CP.
	• Distributing generated private keys in PKCS#12 files
	  ○ Not applicable.
	• Certificates referencing hostnames or private IP addresses
	  ○ From TWCA: The SSL certificate issued by TWCA must use DNS name as the CN part of subjectDN, the IP address is not allowed. In some application servers, they use subjectAlterName to identify themselves, such as Microsoft Exchange Server 2007. TWCA will issue the SSL certificate with subjectAlterName contains the NETBIOS hostname or IP address for such applications.
	• OCSP Responses signed by a certificate under a different root
	  ○ Not applicable.
	• CRL with critical CIDP Extension
	  ○ CRLs imported into Firefox without error.
	• Generic names for CAs
	  ○ The CN for the CA includes TWCA