

**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](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](https://wiki.mozilla.org/CA:Recommended_Practices).

General Information	Data
CA Name	Taiwan Certification Authority (TWCA)
Website URL (English version)	<a href="http://www.twca.com.tw/Portal/english/coporate_profile/mission.html">http://www.twca.com.tw/Portal/english/coporate_profile/mission.html</a>
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 (2048-bit root)
Certificate Name	TWCA Root Certification Authority
Root Cert URL	<a href="https://bugzilla.mozilla.org/attachment.cgi?id=402647">https://bugzilla.mozilla.org/attachment.cgi?id=402647</a>
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	<a href="https://ssldemo.twca.com.tw/index.html">https://ssldemo.twca.com.tw/index.html</a>
CRL URL	<a href="http://RootCA.twca.com.tw/TWCARCA/revoke_2048.crl">http://RootCA.twca.com.tw/TWCARCA/revoke_2048.crl</a> <a href="http://sslserver.twca.com.tw/sslserver-test/revoke10_test.crl">http://sslserver.twca.com.tw/sslserver-test/revoke10_test.crl</a> (NextUpdate: 24 hours)

CRL Issuing Frequency	CPS Section 2.3: The CRL shall be published at least once every 24 hours.
OCSP Responder URL	None
CA Hierarchy	<p>CA Hierarchy Diagram: <a href="https://bugzilla.mozilla.org/attachment.cgi?id=426285">https://bugzilla.mozilla.org/attachment.cgi?id=426285</a></p> <p>This root has 4 internally-operated subordinate CAs. The root does not sign end-entity certificates directly. Only level 1 or level 2 sub-CAs may sign end-entity certificates.</p> <p>The difference is the sub-CA is base on their certificate application and usage scope.</p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> <li>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.</li> </ol>
	<p>CPS section 2:</p> <p>The RCA of the TWCA issues certificates to subordinate certification authorities (Sub-CA) for verifying their identity. The RCA operates according to the Class 4 assurance level specified in its certificate policy (CP) and issues to the Sub-CAs certificates of the following 5 assurance level as defined in the CP:</p> <p>Assurance Level:</p> <p>Testing Class: Guarantee for the certificate testing of subscribers or relying parties, and usage other than certificate testing is prohibited.</p> <p>Class 1: Basic guarantee for identifying data integrity in network environments of very low threat of malicious interpolation.</p> <p>Class 2: Preliminary guarantee for basic identity authentication suitable for use in network environments of lower risk of malicious interpolation but still with the potential threat of information interpolation.</p> <p>Class 3: Intermediate guarantee suitable for use in network environments of higher risk of malicious information interception or interpolation.</p> <p>Class 4: High guarantee suitable for use in network environments of high risk of malicious information interpolation requiring a high recovery cost.</p>
Externally Operated sub-CAs	TWCA has not accepted any 3 <sup>rd</sup> party as a sub-CA and has no plan to do this type of business now.

Cross-Signing	<p>None.</p> <p>Parts of TWCA UCA CPS: <a href="https://bugzilla.mozilla.org/attachment.cgi?id=437191">https://bugzilla.mozilla.org/attachment.cgi?id=437191</a></p> <p>Comment #36: About the diagram, it means “TaiCA Secure CA” will be separate to 2 sub-CAs, one is for S/MIME and another is for SSL, because of the CRL download performance issue. The 2 sub-CAs were certified by “TWCA Root Certification Authority”, not cross-signed by other UCA. The arrow symbol in the diagram means that we will change the CA hierarchy, not the cross-signed activity.</p>
Requested Trust Bits	<p>Websites (SSL/TLS)</p> <p>Email (S/MIME)</p>
SSL Validation Type	<p>OV</p> <p>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.</p>
EV policy OID(s)	Not EV
CP/CPS	<p>Document Repository: <a href="http://www.twca.com.tw/Portal/save/save.html">http://www.twca.com.tw/Portal/save/save.html</a></p> <p>TWCA PKI CP (English): <a href="http://www.twca.com.tw/picture/file/20100114-180619944.pdf">http://www.twca.com.tw/picture/file/20100114-180619944.pdf</a></p> <p>TWCA PKI CP (Traditional Chinese): <a href="http://www.twca.com.tw/picture/file/20090806-171745500.pdf">http://www.twca.com.tw/picture/file/20090806-171745500.pdf</a></p> <p>Comment #16: 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. So all sub-CAs operations shall not have conflicts with the rules in the CP. The CP defines policies and procedures for applying, verifying, issuing, and maintaining end-entity certificates in the section "4. Certificate Life-Cycle Operational Requirement"</p> <p>TWCA Root CA CPS (English) <a href="http://www.twca.com.tw/picture/file/20100114-180956726.pdf">http://www.twca.com.tw/picture/file/20100114-180956726.pdf</a></p> <p>TWCA Root CA CPS (Traditional Chinese): <a href="http://www.twca.com.tw/picture/file/20090114-11212952.pdf">http://www.twca.com.tw/picture/file/20090114-11212952.pdf</a></p> <p>The purpose of the TWCA Root CA CPS document is to establish the policies for applying, verifying, issuing, and maintaining subordinate CAs.</p> <p>TWCA UCS CPS (Traditional Chinese): <a href="http://www.twca.com.tw/picture/file/20090724-110350827.pdf">http://www.twca.com.tw/picture/file/20090724-110350827.pdf</a></p> <p>Parts of TWCA UCS CPS (English): <a href="https://bugzilla.mozilla.org/attachment.cgi?id=437191">https://bugzilla.mozilla.org/attachment.cgi?id=437191</a></p> <p>Comment #25: TWCA UCA CPS must follow the policy specified in TWCA PKI CP. The reference is the CP OID. When issue the certificate, Sub-CAs described in TWCA UCA CPS must include the CP OID specified in TWCA PKI CP in the certificate. For example, the Sub-CA will issue the test class of certificate whose CP OID will include the CP OID described in TWCA PKI CP page 11 to 12.</p>
AUDIT	<p>Audit Type: WebTrust CA</p> <p>Auditor: SunRise CPAs' Firm, a member firm of DFK international.</p> <p>Auditor Website: <a href="http://www.dfk.com/">http://www.dfk.com/</a></p>

	<p>Audit: <a href="https://cert.webtrust.org/ViewSeal?id=900">https://cert.webtrust.org/ViewSeal?id=900</a> (2009.03.13)</p> <p>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.</p>
<p>Organization Identity Verification</p>	<p>CP section 3.2.2 Authentication of Organization Identity</p> <p>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:</p> <p>Testing Class: To be specified by CAs in their CPS.</p> <p>Class 1: Limited verification of the subscriber name and email information with simple procedures by email.</p> <p>Class 2: In addition to organization name clearance, subscribers shall submit legal and correct certifications, without completing the procedures over the counter.</p> <p>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.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>· equipment identification (e.g. serial number) or service name (e.g. domain name);</li> <li>· equipment public key;</li> <li>· 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);</li> <li>· the contact information of administrators for contacts made by the RA or CA;</li> <li>· 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).</li> </ul> <p>CP section 3.2.3 Authentication of Individual Identity</p>

	<p>The following show the requirements for the identity authentication of individual subscribers under various assurance level:</p> <p>Testing Class: To be specified by CAs in their CPS.</p> <p>Class 1: Limited verification of the subscriber name and email information with simple procedures by email.</p> <p>Class 2: In addition to individual name clearance, subscribers shall submit legal and correct certifications, without completing the procedures over the counter.</p> <p>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</p> <p>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.</p> <p>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.</p>
<p>Domain Name Ownership / Control</p>	<p>TWCA UCS CPS (Traditional Chinese): <a href="http://www.twca.com.tw/picture/file/20090724-110350827.pdf">http://www.twca.com.tw/picture/file/20090724-110350827.pdf</a>  Parts of TWCA UCS CPS (English): <a href="https://bugzilla.mozilla.org/attachment.cgi?id=437191">https://bugzilla.mozilla.org/attachment.cgi?id=437191</a></p> <p>Section 2.2.1.1: TWCA SSL certificate is issued under assurance level/class 2. TWCA will check with domain name management org such as TWNIC or similar foreign agency for confirmation.</p> <p>Further details are provided in their internal SOP documents:  For Domain name control:  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 registration 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.  Some organizations will claim they are under authorized to use the domain name by the owner. The organization will must provide the authorization letter of owner's official register stamp to RA for verification.</p>
<p>Email Address Ownership / Control</p>	<p>TWCA UCS CPS (Traditional Chinese): <a href="http://www.twca.com.tw/picture/file/20090724-110350827.pdf">http://www.twca.com.tw/picture/file/20090724-110350827.pdf</a>  Parts of TWCA UCS CPS (English): <a href="https://bugzilla.mozilla.org/attachment.cgi?id=437191">https://bugzilla.mozilla.org/attachment.cgi?id=437191</a></p> <p>Section 2.2.1.1: TWCA S/MIME certificate is issued under assurance level/class 2. TWCA will send a notification to the subscriber via the email address provided by the subscriber for registration and the certificate will only be issued after TWCA gets an acknowledgement from the subscriber via the same email address.</p> <p>Further details in their internal SOP documents:  When verify the email address of S/MIME certificate, RA must check the mail address domain name filled in registration form is owned by the organization. After check the ownership of domain name, RA will manually send email to notify the subscriber 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 subscriber replies and confirms the application, the verification</p>

	<p>will be success, otherwise it will be fail.</p> <p>***Note: TWCA only issue S/MIME certificate to organization subscriber, so extra verification of domain name ownership is required.</p>
Identity of Code Signing Subscriber	Not applicable – Not requesting Code Signing trust bit at this time.
Potentially Problematic Practices	<p><a href="http://wiki.mozilla.org/CA:Problematic_Practices">http://wiki.mozilla.org/CA:Problematic_Practices</a></p> <ul style="list-style-type: none"> <li>• <a href="#">Long-lived DV certificates</a> <ul style="list-style-type: none"> <li>○ SSL certs are OV</li> <li>○ SSL certificate valid period issued by TWCA will no longer than 3 years.</li> </ul> </li> <li>• <a href="#">Wildcard DV SSL certificates</a> <ul style="list-style-type: none"> <li>○ SSL certs are OV</li> <li>○ 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.</li> </ul> </li> <li>• <a href="#">Delegation of Domain / Email validation to third parties</a> <ul style="list-style-type: none"> <li>○ Not applicable.</li> </ul> </li> <li>• <a href="#">Issuing end entity certificates directly from roots</a> <ul style="list-style-type: none"> <li>○ Not applicable.</li> </ul> </li> <li>• <a href="#">Allowing external entities to operate unconstrained subordinate CAs</a> <ul style="list-style-type: none"> <li>○ Not applicable.</li> </ul> </li> <li>• <a href="#">Distributing generated private keys in PKCS#12 files</a> <ul style="list-style-type: none"> <li>○ Not applicable.</li> </ul> </li> <li>• <a href="#">Certificates referencing hostnames or private IP addresses</a> <ul style="list-style-type: none"> <li>○ 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.</li> </ul> </li> <li>• <a href="#">OCSP Responses signed by a certificate under a different root</a> <ul style="list-style-type: none"> <li>○ Not applicable.</li> </ul> </li> <li>• <a href="#">CRL with critical CIDP Extension</a> <ul style="list-style-type: none"> <li>○ CRLs imported into Firefox without error.</li> </ul> </li> <li>• <a href="#">Generic names for CAs</a> <ul style="list-style-type: none"> <li>○ The CN for the CA includes TWCA</li> </ul> </li> </ul>