**Bugzilla ID:** 745671 **Bugzilla Summary:** Enable EV and Turn on Code Signing trust bit for TWCA Root certificate

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  | ~~Taiwan Certification Authority~~ TAIWAN-CA Inc. (TWCA)  |
| Website URL  | http://www.twca.com.tw/  |
| Organizational type  | Commercial CA  |
| Primark 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: rootca@twca.com.twca@twca.com.tw CA Phone Number: 886-2-23708886 Title / Department: Policy Management Authority (PMA)  |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name  | TWCA Root Certification Authority  |
| Certificate Issuer Field  | CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW  |
| Certificate Summary  | This request is to turn on the Code Signing trust bit and enable EV for the “TWCA Root Certification Authority” root certificate that was included in NSS per bug #518503.  |
| Root Cert URL  | https://bugzilla.mozilla.org/attachment.cgi?id=402647  |
| SHA1 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  |
| Certificate Version  | 3  |
| Certificate Signature Algorithm  | PKCS #1 SHA-1 With RSA Encryption  |
| Signing key parameters  | 2048  |
| Test Website URL (SSL) Example Certificate (non-SSL)  | The TWCA EVSSL test web site is: https://evssldemo.twca.com.tw/index.html (normal) https://evssldemo1.twca.com.tw/index.html (revoked) https://evssldemo2.twca.com.tw/index.html (expired)  |
| CRL URL  | <http://RootCA.twca.com.tw/TWCARCA/revoke_2048.crl> <http://sslserver.twca.com.tw/sslserver/EVSSL_Revoke_2011.crl> The application cannot import the Certificate Revocation List (CRL). Error Importing CRL to local Database. Error Code:ffffe095 Please ask your system administrator for assistance. Please see [https://wiki.mozilla.org/CA:Problematic\_Practices#CRL\_with\_critical\_CIDP\_Extension](https://wiki.mozilla.org/CA%3AProblematic_Practices#CRL_with_critical_CIDP_Extension) TWCA will modify the system to remove the IDP extension in CRL.CP section 4.9.7: CAs shall generate a CRL once every 24 hours  |
| OCSP URL  | <http://evssl_ocsp.twca.com.tw/> Perform EV Testing: [https://wiki.mozilla.org/PSM:EV\_Testing\_Easy\_Version](https://wiki.mozilla.org/PSM%3AEV_Testing_Easy_Version)As per section #14 of https://wiki.mozilla.org/CA:Information\_checklist#Technical\_information\_about\_each\_root\_certificate Maximum expiration time of OCSP responses Please provide the sections of your CP/CPS specifying availability and update requirements for the OCSP service. --CA/Browser Forum's EV Guidelines Section 26(b): “If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.” OCSP use the CRL as the certificate status information source, so the update service frequency is same as CRL update frequency.**4.9.7 CRL Issuance Frequency** This CA updates and issues the CRL once a day. |
| Requested Trust Bits  | Websites (SSL/TLS) Email (S/MIME) Code Signing  |
| SSL Validation Type  | OV and EV  |
| EV Policy OID(s)  | 2.16.886.3.1.6.5  |

**CA Hierarchy information for each root certificate Verification Policies and Practices**

|  |  |
| --- | --- |
| CA Hierarchy  | This root has internally-operated subordinate CAs. The root does not sign end-entity certificates directly. All of these must follow TWCA UCA CPS to conduct their operations. 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. 5. CN = TWCA EVSSL Certification Authority, OU = EVSSL Sub-CA, O = TAIWAN-CA, C = TW Issues EV SSL certs.  |
| Externally Operated SubCAs  | 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.  |
| Technical Constraints on Third-party Issuers  | Not applicable.  |

**Verification Policies and Practices**

|  |  |
| --- | --- |
| Policy Documentation  | Corporate Profile: http://www.twca.com.tw/Portal/english/coporate\_profile/mission.html Repository (Chinese): <http://www.twca.com.tw/Portal/save/save.html> Repository (English): <http://www.twca.com.tw/Portal/english/coporate_profile/Repository.html> TWCA UCA CPS English: http://www.twca.com.tw/picture/file/20110523-180517756.pdfChinese: http://www.twca.com.tw/picture/file/20110714-1339027.pdfThe 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/20100114-180619944.pdf Chinese: http://www.twca.com.tw/picture/file/20090806-171745500.pdf All sub-CAs shall comply with the rules in the TWCA PKI CP to define their own CPS and follow the rules in their own CPS for operations. TWCA Root CA CPS English: Please provide URL to current document. Chinese: Please provide URL to current document. This document establishes the policies for applying, verifying, issuing, and maintaining subordinate CAs. EV CA CPS (English): <http://www.twca.com.tw/picture/file/20120102-152000370.pdf> EV CA CPS (Chinese): Please provide URL Issuing CA CPS for S/MIME and Object Signing certs (English): <http://www.twca.com.tw/picture/file/20110523-180517756.pdf> Please also provide URL for the Chinese version.  |
| Audits  | Auditor: SunRise CPAs’ Firm, a member firm of DFK Auditor Website: http://www.dfk.com/  |
|  | Audit of TWCA Root CA services in Taipei, Taiwan. WebTrust for CA Audit Report: https://cert.webtrust.org/ViewSeal?id=900 (2011.03.13) Audits of TWCA EV SSL CA services in Taipei, Taiwan. WebTrust for CA Audit Report: https://cert.webtrust.org/ViewSeal?id=1248 (2012.01.04) WebTrust for EV Audit Report: https://cert.webtrust.org/ViewSeal?id=1249 (2012.01.04)  |
| Organization Verification Procedures  | TWCA UCA CPS section 2.2.1.1: Level of Assurance CP section 3.2.2 Authentication of Organization Identity CP section 3.2.3 Authentication of Individual Identity  |
| SSL Verification Procedures  | SSL certificates are issued under assurance level class 2 or 3. TWCA verifies the legal existence of the organization requesting the certificate, the identity and authorization of the certificate subscriber, and that the certificate subscriber has the exclusive right to use the domain name(s) to be listed in the certificate. This is documented in sections 2.2.1.1, 3.2.2, and 5.1 of the TWCA UCA CPS.  |
| EV SSL Organization Verification  | EV CA CPS: http://www.twca.com.tw/picture/file/20120102-152000370.pdf Section 2: This CA operates according to Assurance Level 4 specified in the TWCA PKI CP and issues Class 3 certificates specified in the CP to EV SSL certificate subscribers Section 3.2.2.1: When authenticating the identity of an organization, documents issued by the competent authorities or other documents proven the existence of such organization shall be verified. Also, the identity of its statutory representative shall be authenticated. Application documents and identity documents can be delivered either over the counter or by mail. In addition to verifying the documents submitted by subscribers, information shall be verified according to the identity identification and authentication requirements specified in the EV SSL Guidelines. At least the following actions shall be taken to verify the identity of an organization: …  |
| EV SSL Domain Verification  | EV CA CPS: http://www.twca.com.tw/picture/file/20120102-152000370.pdf 3.2.2.2 Internet Host Authentication Procedure (1) Private organizations: To validate in the database of the administration unit of public Internet domain name that the domain name used by the Internet host name provided by a private organization in the initial registration is managed and used by that private organization. (2) Public organizations: To validate the domain name of public organizations at the government’s public directory service and verify that the domain name used by the Internet host name provided in the initial registration exists, and the name of the user unit is identical to the public organization validated in 3.2.2.1.  |
| Email Address Verification Procedures  | S/MIME certificates are issued under assurance level class 1, 2, or 3. TWCA verifies the identity and PIN of the subscriber, verifies the domain name ownership of the email address to be listed in the certificate, and exchanges email with the subscriber to confirm the application request. This is documented in sections 2.2.1.1, 3.2, and 5.1 of the TWCA UCA CPS.  |
| Code Signing Subscriber Verification Procedures  | Please provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that provide information about Code Signing certificates (e.g. the required authentication levels), and the information listed here: [https://wiki.mozilla.org/CA:Recommended\_Practices#Verifying\_Identity\_of\_Code\_Signing\_Certificate\_Subscriber](https://wiki.mozilla.org/CA%3ARecommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber)TWCA code signing certificate will only issue to organization, the authentication requirement is described in TWCA UCA CPS.**4.1.8 Authentication of Organization Identity**If a company registers its level of assurance to Class 3, when TWCA and the RA verify its registration status and DN, this company shall provide the relevant supporting documents (the company stamp and signature of the statutory representative shall appear in each photocopy) issued by the competent authorities or legally authorized units or the relevant legal documents if it is an overseas company. If the registration is made by an agent, the agent shall apply for the registration in person. Also, the identity documents of this agent shall be verified. The level of assurance for registration is specified in “Level of Assurance, Clause 2.2.1.1.”**4.1.9 Authentication of Individual Identity**If individual registers his/her level of assurance to Class 3, this individual shall apply for registration in person and submit the relevant identity documents (an ID or passport with his/her photo) for the RA to verify. No application shall be made by an agent. When the applicant is an alien, the verification shall be conducted according to the relevant business regulations (e.g. verification of passport with photo). The level of assurance for registration is specified in “Level of Assurance, Clause 2.2.1.1.” |
| Multi-factor Authentication  | Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices Is the multi-factor authentication requirement stated in any of the CP/CPS documents? All accounts of CA have to use smartcard to login to certificate management system.EVCPS also described: **5.2.3 Identification and Authentication for Each Role** System resources are assigned to administrators, officers, auditors and operators according to their scope of business. The unique ID, smartcard, and relevant PIN are applied for identifying and authenticating the trusted roles. |
| Network Security  | Confirm that you have performed the actions listed in #7 of [https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices](https://wiki.mozilla.org/CA%3AInformation_checklist#Verification_Policies_and_Practices) Section 6.7 of EV CA CPS.  |

**Response to Mozilla's CA Recommended Practices** ([https://wiki.mozilla.org/CA:Recommended\_Practices](https://wiki.mozilla.org/CA%3ARecommended_Practices))

|  |  |
| --- | --- |
| Publicly Available CP and CPS  | Yes  |
| CA Hierarchy  | Yes  |
| Audit Criteria  | Yes  |
| Document Handling of IDNs in CP/CPS  | No. All IDNs certificate will be revoked before 2012/9/30. |
| Revocation of Compromised Certificates  | Yes. CPS 4.9.1 described the CA may revoke the certificate are proven or alleged to be compromised.  |
| Verifying Domain Name Ownership  | Yes |
| Verifying Email Address Control  | Yes |
| Verifying Identity of Code Signing Certificate Subscriber  | Yes |
| DNS names go in SAN  | TWCA is modifying the CA system to comply with CAB Forum Baseline Requirements. It will be done before 2012/9/30. |
| Domain owned by a Natural Person  | No. |
| OCSP  | Yes.  |

**Response to Mozilla's list of Potentially Problematic Practices** (https://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. --Please see the CAB Forum Baseline Requirements regarding re-validating the information in the certificates at a more frequent time period than 4 years.  |
| Wildcard DV SSL certificates  | No. TWCA issue wildcard SSL certificate to organization only. |
| Email Address Prefixes for DV Certs  | Not applicable.  |
| Delegation of Domain / Email validation to third parties | No. The Domain / Email validation is verified by TWCA. There is no external 3rd party RA. |
| Issuing end entity certificates directly from roots  | Not applicable.  |
| Allowing external entities to operate subordinate CAs  | No |
| Distributing generated private keys in PKCS#12 files  | No.**6.1.2 Private Key Delivery to Subscriber** Private keys are generated by subscribers and thus need no delivery. |
| Certificates referencing hostnames or private IP addresses  | No. |
| Issuing SSL Certificates for Internal Domains  | No. |
| OCSP Responses signed by a certificate under a different root  | No.  |
| CRL with critical CIDP Extension  | Yes, see above.  |
| Generic names for CAs  | No  |
| Lack of Communication With End Users  | No  |