

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-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.tw , ca@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)	https://evssldemo.twca.com.tw/index.html
CRL URL	http://RootCA.twca.com.tw/TWCARCA/revoke_2048.crl http://sslserver.twca.com.tw/sslserver/EVSSL_Revoke_2011.crl CPS section 5.4.9: CRL issuance frequency shall be 24 hours.

OCSP URL	http://evssl_ocsp.twca.com.tw/ From TWCA: OCSP use the CRL as the certificate status information source, so the update service frequency is same as CRL update frequency. (24 hours)
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

CA Hierarchy	<p>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:</p> <ol style="list-style-type: none"> 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.

Verification Policies and Practices

Policy Documentation	<p>Repository (English): http://www.twca.com.tw/Portal/english/coporate_profile/Repository.html On this page there are links to: CPS, CP, EV CPS, and sub-CA CPS. Corporate Profile: http://www.twca.com.tw/Portal/english/coporate_profile/mission.html Repository (Chinese): http://www.twca.com.tw/Portal/save/save.html</p>
Audits	<p>Audit Type: WebTrust CA and EV Auditor: SunRise CPAs' Firm, a member firm of DFK, http://www.dfk.com/ WebTrust CA Audit Report: https://cert.webtrust.org/ViewSeal?id=1322 (2012.03.13) WebTrust EV Audit Report: https://cert.webtrust.org/ViewSeal?id=1323 (2012.03.13)</p>

Organization Verification Procedures	CPS section 2.2.1.1: Level of Assurance CPS section 4.1.8: Authentication of Organization Identity CPS section 4.1.9 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 and 5.1 of the CPS.
EV SSL Organization Verification	EV CPS Section 1.2: 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 CPS section 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 and 5.1 of the CPS.
Code Signing Subscriber Verification Procedures	Code signing certificate will only issue to organization, the authentication requirement is described in the CPS. CPS section 4.1.8, Authentication of Organization Identity CPS section 4.1.9, Authentication of Individual Identity
Multi-factor Authentication	All accounts of CA have to use smartcard to login to certificate management system. EV CPS section 6.2.3, Identification and Authentication for Each Role In using system resources, supervising personnel, administrators, operators, system maintenance personnel and system resource controllers shall be assigned with a unique role identification codes, an IC card and a PIN (or fingerprint recognition) in order to identify and verify the identity of system resource users. When operators run a function according to the business needs, every action shall be recorded in detail to ensure the accountability of system resource use and to control system security threats and risk assessments.
Network Security	EV CPS section 7.7.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_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 describes the CA may revoke the certificate are proven or alleged to be compromised.
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	Yes
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 - CPS section 4.2: The maximum validity of subscriber certificate ... is 3 years. - EV CPS section 6.3.2: key pairs of subscribers are valid for a maximum term of 27 months.
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
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 CDP Extension	No
Generic names for CAs	No
Lack of Communication With End Users	No