Bugzilla ID: 810133
Bugzilla Summary: Add one more Root Certificate of TWCA in Mozilla software

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 Global Root CA
Certificate Issuer Field	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW
Certificate Summary	This SHA-256 root will eventually replace the SHA-1 "TWCA Root Certification Authority" root certificate that was included in NSS per bug #518503.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=679898
SHA1 Fingerprint	9C:BB:48:53:F6:A4:F6:D3:52:A4:E8:32:52:55:60:13:F5:AD:AF:65
Valid From	2012-06-27
Valid To	2030-12-31
Certificate Version	3
Certificate Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	4096
Test Website URL (SSL)	https://evssldemo3.twca.com.tw/index.html Please perform the EV testing described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
CRL URL	http://RootCA.twca.com.tw/TWCARCA/global_revoke_4096.crl http://sslserver.twca.com.tw/sslserver/GlobalEVSSL_Revoke_2012.crl (nextUpdate: 24 hours)

	CPS section 5.4.9: CRL issuance frequency shall be 24 hours.
OCSP URL	http://RootOcsp.twca.com.tw/ http://evsslocsp.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)	1.3.6.1.4.1.40869.1.1.22.3

CA Hierarchy information for each root certificate

CA Hierarchy	This root has internally-operated subordinate CAs. The root does not sign end-entity certificates directly. All of these must follow TWCA CPS to conduct their operations. Eventually this SHA-256 root will have sub-CAs corresponding to the "TWCA Root Certification Authority" root certificate: 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	This new root is cross-signed with the SHA-1 "TWCA Root Certification Authority" root certificate due to need to chain to existing root in mobile devices.

Verification Policies and Practices

Policy Documentation	Document Repository (Chinese): http://www.twca.com.tw/Portal/save/save.html Repository (English): http://www.twca.com.tw/Portal/english/coporate_profile/Repository.html

	On this page there are links to: CPS, CP, Root CA CPS, EV SSL CPS, and Global CA CPS.
Audits	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)
Organization Verification Procedures	Global CA CPS Executive Summary: SSL Certificates are of Level of Assurance Class 3. Only InfoSec Certificates of Level of Assurance Class 3 can be used for code signing. Global CA CPS section 1.4.1: The assurance level of SSL certificate is Level 3. They are used for website authentication and information security control. Global CA CPS section 1.4.1: Organizational Authentication Procedure, Procedure for Identifying Server Hostname and IP Address Global CPS section 3.2.2: Authentication of Organization Identity Global CPS section 3.2.3: Authentication of Individual Identity In Section 1.4.1 of the Global CA CPS there is Testing Certificates. Can Testing Certificates be issued for SSL? For Code Signing? For S/MIME?
SSL Verification Procedures	Global CA CPS section 1.4.1: Procedure for Identifying Server Hostname and IP Address (A) Private organizations: This CA verifies if the Internet domain name or IP address initially registered for the sever hostname by private organizations is actually managed and used by respective private organizations in accordance with the database or documents of the management unit of Internet domain name or IP address. (B) Public organizations: This CA verifies if the Internet domain name or IP address that used by the initially registered server hostname exists, and if the name of user is the same as the signature of the above public organization after verification in accordance with the public directory service or the database or documents of the management unit of Internet domain name or IP address.
EV SSL Organization Verification	EV CPS section 1.1: The TWCA Extended Validation SSL Certification Authority Certification Practices Statement (this CPS) is established in accordance with the TWCA PKI Certification Policy (CP), the Guidelines for the Issuance and Management of Extended Validation Certificates (EV SSL Guidelines) formulated by CA/Browser Forum, and the Regulations on the Required Information for Certification Practices Statements announced by the competent authorities according to the Electronic Signatures Act. EV CPS Executive Summary: 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 EV CPS 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. Global CA CPS section 1.4.1: Class 1: This CA or the RA conducts limited verification of the subscriber's name (e.g. the name of an individual or the registered name or universal resource location (URL) of an organization) and e-mail data with a simple procedure. … This CA and RA assure only the uniqueness of the name and e-mail data of subscribers in the database of this CA, and all other information related to subscribers is considered as unverified. Global CA CPS section 4.1.2: After verifying the identity and supporting documents according to the SOP for identity authentication of different levels of assurance, RA should set the personal identification number (PIN) and protection password of subscribers to complete the subscriber registration. Global CA CPS section 4.3.1: (1) Subscribers must pass at least the PIN and password check and verification. After logging on to RA, subscribers should sign the certificate application information with the subscriber private key before delivering it to RA. (2) After verifying the PIN and password of subscribers and checking the integrity of the certificate application information, RA should sign the certificate application information of subscribers with the RA private key if no error is found
Code Signing Subscriber Verification Procedures	Global CA CPS Executive Summary: Only InfoSec Certificates of Level of Assurance Class 3 can be used for code signing. Global CA CPS section 1.4.1 regarding InfoSec Certs of Class 3: A. Method of Identity Authentication: Apart from checking the information of Class 2 certificates, subscribers shall personally apply for the registration. An organization (juristic person) may apply for registration through an agent holding valid authorization documents and documents that can identify his/her identity. When organizations can provide identity documents that can verify their organization status and such documents have been confirmed by the RA, they may apply for registration by e-mail, by fax, or by electronic document containing an electronic signature.
Multi-factor Authentication	All accounts of CA have to use smartcard to login to certificate management system.

	Global CA CPS section 5.2.1: To ensure that one-person acting alone cannot circumvent safeguards, CA responsibilities and authority are divided between multiple roles and individuals. The trust roles and their division of labor of this CA are as follows: (1) Administrator: To take charge of system installation, system management and environment parameter setup. (2) Officer: To take charge of the issuance and revocation of certificates. Global CA CPS section 5.2.2: The number of persons required per task: (1) Administrator: At least two. (2) Officer: At least two. Global CA CPS section 5.2.3: 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	Global CA CPS section 6.7.

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. Did this happen?
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 the SSL server certificate is 4 years and is subject to extension with the approval of PMA when there is a special need. Global CA CPS section 3.3.1: SSL certificates have a validity period no greater than 60 months, but no greater than 39 months after 1 April 2015. - 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. Is this still correct?
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 CIDP Extension	No
Generic names for CAs	No
Lack of Communication With End Users	No