Bugzilla ID: 448794
Bugzilla Summary: Add Chunghwa Telecom eCA 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.

General Information	Data
CA Name	Chunghwa Telecom (CHT)
Website URL (English version)	http://www.cht.com.tw/CHTFinalE/Web/ http://publicca.hinet.net/index.htm
Organizational type	Commercial
Primary market / customer base	Chunghwa Telecom (CHT) chiefly provides telecommunication and information-related services. A public corporation, CHT is the largest integrated telecommunication operator in Taiwan.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	ePKI Root Certification Authority CN is not set. OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd.
Cert summary / comments	This root, eCA, is the highest CA in the hierarchical structure of ePKI, Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI). This eCA root has two internally-operated subordinate CAs: CHTCA and Public CA. The CHTCA is the internal CA of Chunghwa Telecom (CHT) which signs certificates for CHT employees. The Public CA signs certificates for CHT clients. In the eCA CPS the term cross-certificate means a certificate used to establish a trust relationship between two CAs. Within the ePKI the cross-certificate is intended to mean subordinate CA. All subordinate CAs are operated by the Data Communication Business Group, which is a division of Chunghwa Telecom. Email from Nien Hua on 11/18/2008: "Within the ePKI the cross-certificate is intended to mean subordinate CA. All subordinate CAs are operated by the Data Communication Business Group, which is a division of Chunghwa Telecom."
The root CA certificate URL	http://epki.com.tw/download/ROOTeCA.cer http://210.71.154.6/download/ROOTeCA.cer

SHA-1 fingerprint.	67:65:0d:f1:7e:8e:7e:5b:82:40:a4:f4:56:4b:cf:e2:3d:69:c6:f0
Valid from	2004-12-19
Valid to	2034-12-19
Cert Version	3
Modulus length	4096
Test website	https://epki.com.tw/index_en.htm
CRL URL update frequency for end-entity certificates	eCA CARL: http://epki.com.tw/repository/CRL/CA.crl http://210.71.154.6/repository/CRL/CA.crl Next update for CARL is 24 hours. http://repository.publicca.hinet.net/crl/complete.crl Next update for CRLs of end-entity certs is 48 hours.
OCSP Responder URL	http://ocsp.publicca.hinet.net/OCSP/ocsp PublicCA, a sub-CA of this root, supports OCSP. The AIA extension of any EE certificate issued by PublicCA contains the URL of the OCSP responder. The database behind the OCSP responder will be updated immediately to reflect end-entity revocation.
List or description of subordinate CAs operated by the CA organization associated with the root CA.	eCA has two internally operated subordinate CAs: CHTCA and Public CA. The CHTCA is the internal CA of Chunghwa Telecom (CHT) which signs certificates for CHT employees. The Public CA signs certificates for CHT clients. http://publicca.hinet.net/chtca_en.htm The Chunghwa Telecom Certification Authority (CHTCA) is the Level 1 Subordinate CA of Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI), and is responsible for issuance and management of the certification of Chunghwa Telecom's employees or application software in the Infrastructure. http://publicca.hinet.net/publica_en.htm The PublicCA is the Level 1 Subordinate CA of Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI), and is responsible for issuance and management of the certification of natural person, organization, and equipment or application software in the Infrastructure. PublicCA cannot issue subordinate CA certificates because it's PathLengthConstraint=0. Subscribers may use the certificates for internet order placing, internet banking, internet tax filing, secure transmission, data encryption, and identity certification, among others.
For subordinate CAs operated by third parties, if any:	There are currently no sub-CAs operated by third parties. ePKI CP Section 1.3.3, Subordinate Certification Authority" "Establishment of subordinate CA shall follow relevant CP regulations, set up contact window to be responsible for interoperable work between eCA and its subordinate CA.

	CPS: The eCA is responsible for the processing of firsthand certificate applications and revocations. There is no need to set up a Registration Authority (RA) of eCA. The eCA accepts the applications from the subject CAs and authenticates them. From CHT: All subordinate CAs are operated by the Data Communication Business Group, which is a division of our company (Chunghwa Telecom). In addition, we have a Policy Management Authority (PMA) which is formed by management-level persons to supervise the operation of the subordinate CAs.
List any other root CAs that have issued cross-signing certificates for this root CA	The eCA has not been used to cross-sign another root CA in another PKI domain, and there are currently no plans to do so. However the CPS includes a significant amount of information about how a cross-signed CA would need to follow the CPS and be audited. Email from Nien Hua on 11/18/2008: "Within the ePKI the cross-certificate is intended to mean subordinate CA. All subordinate CAs are operated by the Data Communication Business Group, which is a division of Chunghwa Telecom."
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites Email Code From Nien Hua Cheng in reply in Bugzilla 11/3/08: The authentication procedure please read PublicCA CPS ,relevant section as below 3.1.5 Resolution procedures for naming disputes 3.1.8 Organization identity verification 3.1.10 Equipment or application software verification procedure Our government maintaining a legal organization database, so we can check the organization status (alive or suspend) online. Our company also provides DNS register service in Taiwan therefore we have a lot of organization data to verify the application information or using whois function. If our customers apply an SSL certificate, they must provide an email address in the application form, After the authentication procedure finish, they will receive an email from PublicCA then they must use the information of this email to finish the certificate acceptance. From Nien Hua Cheng in email 3/3/08: CHTCA is the enterprise CA for Chunghwa Telecom. Therefore, CHTCA will only issues certificates to employees or servers of Chunghwa Telecom. CHTCA will not issue server certificates for non-CHT domains. However, the CA certificate of CHTCA itself does not have a Name Constraints extension to enforce this. Due to the limitation of our CA

	software, we can not include a NameConstraints extension in the subordinate CA certificate. However, our company policy will only allow our RA staffs, which are our employee, to approve server certificates for CHT domains. The compliance of our staffs to our company policy is periodically reviewed by auditors at least once per year. Both CHTCA and Public CA can issue certificates containing Subject Name in non-Latin character sets. In cases where locality names, organization names, organizational unit names, or common names in Subject Name field contain strings outside of the scope of ASN.1 PrintableString, the strings will be encoded as UTF8 strings and their ASN.1 Tags will be UTF8String. For SSL certificates, we believe our Public CA is capable to encode Internationalized Domain Name as UTF8String in the common name (CN) sub-field of the Subject Name field. However, we have not yet encounter a subscriber who request to include Internationalized Domain Name in SSL certificate. We do have issued many certificates to end users whose subject names contain traditional Chinese character (in UTF8 encoding of course). If you are interested, we will be glad to provide some example certificates.
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV From CPS: 3.1.8 Authentication of Organization Identity eCA examines the existence of the organization, meanwhile verifies the official document, representative identity and the representative's authority of representing the organization. The organization representative is required to apply the certificate in person. From CHT: "We do not issue DV certificates. All the RDNs (C, O, OU, CN) in the subject DN have to be officially registered name. That is they are all OV certificates."
EV policy OID(s)	Not EV
CP/CPS	http://210.71.154.6/repository_en.htm ePKI CP (English Version) http://210.71.154.6/download/ePKI_CP_V1_2004.pdf Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure Version 1.0 October 2004 eCA CPS (English Version) http://210.71.154.6/download/eCA_CPS_english.pdf The ePKI Root Certification Authority Certification Practice Statement (eCA CPS) is stipulated following the Certificate Policy (CP) for the Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI). Complying with the bylaws of the Taiwan Digital Signature Act PublicCA CPS (English Version)

	http://210.71.154.6/download/PublicCA%20CPS%20English%20version1.3.pdf Public Certification Authority Certification Practice Statement of Chunghwa Telecom
AUDIT	Audit Type: WebTrust for CA Auditor: SunRise CPAs' Firm, a member firm of DFK international. Auditor Website: http://www.dfk.com/ Audit: https://cert.webtrust.org/ViewSeal?id=695 (2008.10.31)

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify domain check for SSL
    - eCA CPS section 3.1.8:
      "For a certificate to be used for SSL-enabled servers, the registrant shall prove its ownership of the domain(s) referenced in the certificate or its authorization from the domain owner to act on the owner's behalf. The Subject CA shall take reasonable measures to verify that the registrant has registered the domain(s) referenced in the certificate or has been authorized by the domain owner to act on the owner's bhalf; For instance, the Subject CA will verify the ownership of the domain name by checking against an internal or publicly available database."
    - From CHT: "Our company also provides DNS register service in Taiwan therefore we have a lot of organization data to verify the application information or using whois function."
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - eCA CPS section 3.1.8: "For a certificate issued to be used for digitally signing and/or encrypting email messages, the registrant shall prove its ownership of the email address or its authorization from the email address owner to act on the email address owner's behalf. The Subject CA shall take reasonable measures to verify that the registrant controls the email account associated with the email address referenced in the certificate or has been authorized by the email address owner to act on the address owner's behalf"
    - From CHT: "After the authentication procedure finish, they will receive an email from PublicCA then they must use the information of this email to finish the certificate acceptance."
- Verify identity info in code signing certs is that of subscriber
    - Identity is verified as per CPS section 3.1.8 and 3.1.9.

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- 1.1 Long-lived DV certificates
    - All of their SSL certs are OV.
- 1.2 Wildcard DV SSL certificates

    - All of their SSL certs are OV.
- 1.3 Issuing end entity certificates directly from roots
    - Root is offline, end-entity certs issued through subordinate CAs
- 1.4 Allowing external entities to operate unconstrained subordinate CAs
    - All subordinate CAs are operated by the Data Communication Business Group, which is a division of Chunghwa Telecom.
- 1.5 Distributing generated private keys in PKCS#12 files
    - private keys are generated by the subscribers
- 1.6 Certificates referencing hostnames or private IP addresses
    - CHT does not issue Certificates referencing hostnames or private IP addresses to their customers.
- 1.7 OCSP Responses signed by a certificate under a different root
    - The OCSP responder's certificate is issued by the subordinate CA itself, and therefore its certificate is under the same root.
- 1.8 CRL with critical CIDP Extension
    - CRL and CARL both imported without error into Firefox.

Verify Audits

- Validate contact info in report, call to verify that they did indeed issue this report.
    - Posted on WebTrust site
- For EV CA's, verify current WebTrust EV Audit done.
    - Not EV
- Review Audit to flag any issues noted in the report
    - No issues noted in the report