

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. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.) | Commercial |
| Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?) | 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 | Status / Notes |
|-------------------------|--|----------------|
| Certificate Name | ePKI Root Certification Authority | COMPLETE |
| Cert summary / comments | <p>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.</p> <p>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.</p> | COMPLETE |

| | | |
|--|---|----------|
| | <p>Email from Nien Hua on 11/18/2008:</p> <p>--</p> <p>eCA didn't issue cross-certificate to another PKI domain and ePKI doesn't have any plan issue a cross-certificate to another domain.</p> <p>In theory cross-certificate rootCA may issue certificate to another rootCA ,so it would be better if you post the statement as below:</p> <p>"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."</p> <p>--</p> | |
| <p>The root CA certificate URL</p> <p>Download into FireFox and verify</p> | <p>Certificate HTTP URL (on CA website):</p> <p>http://epki.com.tw/download/ROOTeCA.cer</p> <p>http://210.71.154.6/download/ROOTeCA.cer</p> | COMPLETE |
| SHA-1 fingerprint. | 67:65:0d:f1:7e:8e:7e:5b:82:40:a4:f4:56:4b:cf:e2:3d:69:c6:f0 | COMPLETE |
| Valid from | 2004-12-19 | COMPLETE |
| Valid to | 2034-12-19 | COMPLETE |
| Cert Version | 3 | COMPLETE |
| Modulus length / key length or type of signing key (if ECC) | 4096 | COMPLETE |
| <p>CRL</p> <ul style="list-style-type: none"> • URL • update frequency for end-entity certificates | <p>eCA CRL:</p> <p>http://210.71.154.6/repository/CRL/CA.crl</p> <p>Successfully downloaded into Firefox.</p> <p>From CPS:</p> <p>4.4.10 CARL Issuance Frequency</p> <p>CARLs shall be issued once each day. The updated CARL shall be published in the repository.</p> | COMPLETE |
| <p>OCSP (if applicable)</p> <ul style="list-style-type: none"> • OCSP Responder URL | <p>The Root CA (eCA) only provides the CARL (Certification Authority Revocation List), which is essentially a CRL but its file size is very small.</p> | COMPLETE |

| | | |
|---|--|----------|
| <ul style="list-style-type: none"> Max time until OCSP responders updated to reflect end-entity revocation | <p>PublicCA does support OCSP. The AIA extension of any EE certificate issued by PublicCA contains the URL of the OCSP responder. Currently, the URL of the OCSP responder is http://ocsp.publicca.hinet.net/OCSP/ocsp . The database behind the OCSP responder will be updated immediately to reflect end-entity revocation.</p> | |
| <p>List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.)</p> <p>For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.</p> | <p>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.</p> <p>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.</p> <p>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, equipment or application software in the Infrastructure.</p> <p>PublicCA can not issue subordinate CA certificates because it's PathLengthConstraint=0.</p> <p>Subscribers may use the certificates for internet order placing, internet banking, internet tax filing, secure transmission, data encryption, and identity certification, among others.</p> | COMPLETE |
| <p>For subordinate CAs operated by third parties, if any:</p> <p>General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.</p> <p>(For example, contractual</p> | <p>There are currently no sub-CAs operated by third parties.</p> <p>From 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.</p> <p>From 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</p> | COMPLETE |

| | | |
|---|---|-----------------|
| <p>arrangements should require third-party subordinates to operate in accordance with some CPS/CP. Technical arrangements might include name constraints, not allowing them to create their own subordinates, etc.)</p> | <p>applications from the subject CAs and authenticates them.</p> <p>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.</p> | |
| <p>List any other root CAs that have issued cross-signing certificates for this root CA</p> | <p>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.</p> <p>From CPS: 1.3.5.1 Usage of Issued Certificates The eCA issues two kinds of certificates: the self-signed certificate and cross-certificate. The self-signed certificate is used to establish the trust anchor of ePKI. The cross-certificate is used to build the trust relationship between interoperable CAs and helps in the certificate path processing within or without a PKI domain.</p> <p>The subject of a cross-certificate is one CA, which interoperates with the eCA. This kind of CA is termed as Subject CA. The Subject CA will be more than one CA. The Subject CAs will include the Level 1 subordinate CAs within ePKI as well as the CAs from without. There is also a Subject CA's public key in the cross-certificate. Anyone can use the cross-certificate to verify the signature of the certificate and Certification Authority Revocation List (CARL) issued by the eCA.</p> <p>The policies for cross-signed CAs are described in the ePKI CP and in the eCA CPS.</p> <p>ePKI CP section 2.7.4, Audit Scope: "The audit scope is stipulated as follows: (1) CA follows CPS operation (2) CPS conforms to CP stipulations</p> | <p>COMPLETE</p> |

| | | |
|---|--|----------|
| | <p>(3) Auditors can audit relevant operation units of CA such as the RA. In the event CA and its subordinate CA sign cross-certificate agreement the audit scope should include whether the subordinate CA conforms to stipulations of the cross-certificate agreement.”</p> <p>From eCA CPS: Complying with the bylaws of the Taiwan Digital Signature Act, the eCA CPS delineates how eCA proceeds according to the Fourth Assurance Level (High) to issue and manage the cross certificates of subject CAs.</p> <p>From the CPS: Chunghwa Telecom will designate a third party to conduct the eCA external audit operation. The third party shall audit in accordance with the eCA’s operation.</p> | |
| <p>Requested Trust Bits One or more of:</p> <ul style="list-style-type: none"> • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing) | <p>Websites Email Code</p> <p>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.</p> <p>Both CHTCA and Public CA can issued 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.</p> | COMPLETE |

| | | |
|---|--|----------|
| | <p>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.</p> <p>Vrom 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. If our authentication procedure didn't work well ,we will take legal responsibility please see the section 2.2.1.2 Indemnity exemption</p> | |
| <p>If SSL certificates are issued within the hierarchy rooted at this root CA certificate:</p> <ul style="list-style-type: none"> Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber. (This is commonly referred to as an OV | <p>OV</p> <p>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.</p> <p>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."</p> | COMPLETE |

| | | |
|---|--|----------|
| certificate.) | | |
| If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates. | Not EV | COMPLETE |
| <p>Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable.</p> <ul style="list-style-type: none"> For SSL certificates this should also include URLs of one or more web servers using the certificate(s). There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. Note: mainly interested in SSL, so OK if no email example. | <p>Sample Cert: http://ra.publicca.hinet.net/SSLQueryCert/SSLQueryCert.jsp?TID=08HD730009</p> | COMPLETE |
| <p>CP/CPS</p> <ul style="list-style-type: none"> Certificate Policy URL Certificate Practice Statement(s) (CPS) URL <p>(English or available in English translation)</p> | <p>http://210.71.154.6/repository_en.htm</p> <p>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</p> <p>eCA CPS (English Version) http://210.71.154.6/download/eCA_CPS_english.pdf</p> <p>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</p> <p>PublicCA CPS (English Version) http://210.71.154.6/download/PublicCA%20CPS%20English%20version1.3.pdf</p> | COMPLETE |

| | | |
|---|--|---|
| | Public Certification Authority Certification Practice Statement of Chunghwa Telecom Version 1.3 April 2008 | |
| AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the “audit report and management assertions” document available from the webtrust.org site or elsewhere.) | <p>Audit Type (WebTrust, ETSI etc.): WebTrust for CA</p> <p>Auditor: SunRise CPAs’ Firm, a member firm of DFK international.</p> <p>Auditor Website: http://www.dfk.com/</p> <p>Audit Document URL(s): https://cert.webtrust.org/ViewSeal?id=695</p> | <p>COMPLETE</p> <p>Audit dated October 31, 2008</p> |

Review CPS sections dealing with subscriber verification (COMPLETE)

- 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 behalf; 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.
- Make sure it’s clear which checks are done for which context (cert usage)
 - It’s clear.

Flag Problematic Practices (COMPLETE)

(http://wiki.mozilla.org/CA:Problematic_Practices)

- [1.1 Long-lived DV certificates](#)
 - CHT does 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.
- [1.2 Wildcard DV SSL certificates](#)
 - CHT does 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.
- [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 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.
- [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 CDP Extension](#)
 - eCA CRL successfully downloaded into Firefox

Verify Audits (COMPLETE)

- 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