Bugzilla ID: 408949
Bugzilla Summary: Add Hongkong Post Root Certificates

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	Hongkong Post
Website URL (English version)	http://www.hongkongpost.gov.hk/index.html
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	National Government CA
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?)	Hongkong Post is a government agency and is a recognized CA under the law of Hong Kong Special Administrative Region (HKSAR) of China, and has been issuing digital certificates, under the brand name "e-Cert" to individuals and organizations of HKSAR since January 2000. Hongkong Post CA operations have been outsourced to E-Mice Solutions. This is documented in the CPS and the Management Assertions. The WebTrust audit covers both Hongkong Post and E-Mice CA operations.

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	Hongkong Post Root CA 1	COMPLETE
Cert summary / comments	This root has only one direct subordinate, Hongkong Post e-Cert CA 1, which is the signer key and is used to issue different types of recognized e-Certs to individuals and organizations.	COMPLETE
The root CA certificate URL Download into FireFox and verify	http://www.hongkongpost.gov.hk/product/download/root/img/smartid_rt.cacert	COMPLETE
SHA-1 fingerprint.	D6:DA:A8:20:8D:09:D2:15:4D:24:B5:2F:CB:34:6E:B2:58:B2:8A:58	COMPLETE
Valid from	2003-05-15	COMPLETE

Valid to	2023-05-15	COMPLETE
Cert Version	3	COMPLETE
Modulus length / key length or type of signing key (if ECC)	2048	COMPLETE
CRL • URL • update frequency for end-entity certificates	The direct subordinate CA has the following full-CRL URL: http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1.crl There is also a partitioned-CRL URL for the end-entity e-Certs: http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL2.crl From e-Cert CPS: Appendix C - Hongkong Post Certificate Revocation Lists (CRLs) HKPost updates and publishes the following Certificate Revocation Lists (CRLs) containing information of e-Certs suspended or revoked under this CPS 3 times daily at 09:15, 14:15 and 19:00 Hong Kong Time (i.e. 01:15, 06:15 and 11:00 Greenwich Mean Time (GMT or UTC))	COMPLETE
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation	N/A	COMPLETE
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.)	Basic Constraint: Maximum number of intermediate CAs: 3 This root only has one direct subordinate CA, “Hongkong Post e-Cert CA 1”: http://www.hongkongpost.gov.hk/product/download/root/img/smartid_ca.cacert Cert Hierarchy: Hongkong Post Root CA 1 -> Hongkong Post e-Cert CA 1 -> Hongkong Post e-Cert (Personal) -> Hongkong Post e-Cert (Organisational) -> Hongkong Post e-Cert (Encipherment) -> Hongkong Post e-Cert (Server) -> Hongkong Post Bank-Cert (Bank of East Asia-Corporate) certificate -> Hongkong Post Bank-Cert (Shanghai Commercial Bank-Personal) certificate -> Hongkong Post Bank-Cert (Shanghai Commercial Bank-Corporate) certificate	COMPLETE

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.	Comment #23: "Hongkong Post e-Cert CA 1 issued all end-entity certs directly and there is no subordinate CA under Hongkong Post e-Cert CA 1."	
For subordinate CAs operated by third parties, if any: 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. (For example, contractual 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.) The extent and nature of contractual and technical controls exercised over subordinate CAs, including: a) Whether or not subordinate CAs are constrained to issue certificates only within certain domains. *[We need a technical*	Comment #23: Hongkong Post has appointed E-Mice Solutions (HK) Limited ("E-Mice") as its agent to operate the e-Cert services related to "Hongkong Post Root CA 1" and all its subordinate CA certificates and end-entity certificates. In WebTrust audit report: We have examined the management assertions by the Hongkong Post Certification Authority ("HKPCA") with E-Mice Solutions (HK) Limited ("E-Mice") as an "agent" of HKPCA1 that during the period 1st January 2007 through 31st December 2007, for its e-Cert and Bank-Cert Certification Authority ("CA") operations, HKPCA: In Management Assertions: HKPCA operations have been outsourced to E-Mice Solutions (HK) Limited ("E-Mice") on 27th October 2006 for operating and maintaining the systems and services of HKPCA for a period from 1st April 2007 to 31st March 2011 as disclosed in HKPCA's business practices disclosures. HKPCA with E-Mice as its agent is responsible for the management assertions of the HKPCA operations. HKPCA with E-Mice as its agent is responsible for establishing and maintaining effective controls over its Certification Authority operations, including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified. From e-Cert CPS: 1.2.1.3 HKPost's Right to Subcontract HKPost may subcontract its obligations for performing some or all of the functions required by this CPS and the Subscriber Agreement provided that the subcontractor agrees to undertake to perform those functions and enters into a contract with HKPost to perform the services. In the event that such sub-contracting occurs, HKPost shall	COMPLETE **Note: The operation of this root and all of its subordinate CAs has been outsourced to E-Mice Solutions Limited. This information is provided in the CPS and Management Assertions. The WebTrust audit includes both E-Mice operations and Hongkong Post operations.**

description of how this is typically controlled.] b) Whether or not subordinate CAs can create their own subordinates. *[We need a technical description of how this is typically controlled.]*	remain liable for the performance of the CPS and the Subscriber Agreement as if such sub-contracting had not occurred. From Bank-Cert CPS Preamble: With the Hong Kong SAR Government's decision to outsource the HKPost CA operations, the Hong Kong SAR Government has, through an open tender exercise, awarded a contract ("Contract") to E-Mice Solutions (HK) Limited ("Contractor") on 27 October 2006 for operating and maintaining the systems and services of the HKPost CA as stipulated in this CPS for a period from 1 April 2007 to 31 March 2011. HKPost remains a recognized CA under Section 34 of the Ordinance and the Contractor is an agent of HKPost appointed pursuant to Section 3.2 of the Code of Practice for Recognized Certification Authorities issued by the Government Chief Information Officer under Section 33 of the Ordinance.	
List any other root CAs that have issued cross-signing certificates for this root CA	None	COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites	COMPLETE
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • 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	OV	COMPLETE

an OV certificate.)		
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • 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.	https://www.hongkongpost.gov.hk/	COMPLETE
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	Certification Practice Statement for e-Certs: http://www.hongkongpost.gov.hk/product/cps/ecert/img/cps_en23.pdf This CPS is for: • Hongkong Post e-Cert (Personal) • Hongkong Post e-Cert (Organisational) • Hongkong Post e-Cert (Encipherment) • Hongkong Post e-Cert (Server) CPS for Bank-Cert: http://www.hongkongpost.gov.hk/product/cps/bankcert/img/bank_cps_en14.pdf	COMPLETE
AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the	Audit Type (WebTrust, ETSI etc.): WebTrust Auditor: PricewaterhouseCoopers Auditor Website: http://www.pwc.com/ Audit Document URL(s): http://cert.webtrust.org/SealFile?seal=125&file=pdf	COMPLETE

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.)	https://cert.webtrust.org/ViewSeal?id=125 Audit date: 3/10/2008	

Review CPS sections dealing with subscriber verification (COMPLETE)

- Verify domain check for SSL
    - From e-Cert CPS: 3.1.8.3 Each application for e-Cert (Server) certificates must be accompanied by the following documentation:- a) An authorisation letter bearing the "For and on behalf of" chop and the authorised signature(s) of the Organisation giving authority to the Authorised Representative to make the application and prove the ownership of the domain name to be identified in the e-Cert (Server) certificate;
    - From e-Cert CPS: 3.1.8.6 For Subscriber Organisations to whom an e-Cert (Organisational), e-Cert (Encipherment) or e-Cert (Server) certificate with a 2-year validity period is issued, HKPost will verify again the existence of the Subscriber Organisation, and in the case of e-Cert (Server) the ownership of the domain name identified in the certificate, approximately at the end of the first year of the validity period. HKPost may suspend or revoke the certificates issued to that Subscriber Organisation in accordance with the provisions set out in Section 4.5 (Certificate Revocation) of this CPS if the Subscriber Organisation's existence cannot be attested, or in the case of e-Cert (Server) the ownership of the domain name cannot be attested.
- 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.
    - Not applicable. Hongkong Post is requesting to enable the SSL trust bit only.
        - The CPS does not provide information indicating that the email address in the cert is verified to be owned/controlled by the subscriber.
        - Comment #23: the personal/organisational certificates issued by Hongkong Post CA support email signing, if email address is provided by the applicant in the application of certificate. Hongkong Post CA will verify the name of the subscriber and the organisation name for organisational certificates. Although Hongkong Post CA will not verify the email account associated with the email address in the certificate that is owned by the subscriber, the email recipient can check the certificate of the sender to identify the subject name, and organisation name for organisational certificate, of the email signer to consider to trust the email or not. Therefore, it is also our intention to enable the trust indicator for email signing for the personal/organisational certificates, which are generated by the same Hongkong Post CA root certificate, if that meets Mozilla.
- Verify identity info in code signing certs is that of subscriber
    - Not applicable. Hongkong Post is requesting to enable the SSL trust bit only.

- Make sure it's clear which checks are done for which context (cert usage)
    - The CPS makes the cert context clear.

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

- Long-lived DV certificates
    - All server certs are OV
    - From CPS section 1.2.4: 1 year or 2 year to be selected by the Applicant at the time of application
- Wildcard DV SSL certificates
    - All server certs are OV
- Delegation of Domain / Email validation to third parties
    - **The operation of this root and all of its subordinate CAs has been outsourced to E-Mice Solutions Limited. This information is provided in the CPS and Management Assertions. The CPS covers verifying the ownership of the domain. Only the SSL trust bit is requested, so email validation is not applicable at this time. The WebTrust audit includes both E-Mice operations and Hongkong Post operations.**
- Issuing end entity certificates directly from roots
    - No end entity certs are issued directly from root.
- Allowing external entities to operate unconstrained subordinate CAs
    - **See info above. HKPCA operations have been outsourced to E-Mice Solutions. This is documented in the CPS and the Management Assertions. The WebTrust audit covers E-Mice.**
- Distributing generated private keys in PKCS#12 files
    - According to CPS section 4.4.2: The applicant generates the private key and public key on his/her own devices
- Certificates referencing hostnames or private IP addresses
    - Not found.
- OCSP Responses signed by a certificate under a different root
    - No OCSP
- CRL with critical CIDP Extension
    - Comment #36: "Exactly, our design of full CRL is inline with your recommendation. Our full CRL (http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1.crl) does not carry the CIDP extensions.

Verify Audits (COMPLETE)

(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- 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.
    - N/A
- Review Audit to flag any issues noted in the report
    - No issues noted in audit report.