Print this page

Mozilla - CA Program

Case Information

Case Number	00000314	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Government of Hong Kong (SAR), Hongkong Post, Certizen	**Request Status**	In Detailed CP/CPS Review

Additional Case Information

Subject	Include Hongkong Post Root CA 3 root	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1464306

General information about CA's associated organization

CA Email Alias 1	enquiry@hongkongpost.gov.hk		
CA Email Alias 2			
Company Website	https://www.ecert.gov.hk/	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Hong Kong	**Verified?**	Verified
Primary Market / Customer Base	Bureaux and Departments of the Government of Hong Kong SAR are serving over 8 million people of Hong Kong.	**Verified?**	Verified
Impact to Mozilla Users	Root Renewal	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and Recommended Practices, and confirm that we follow those

			practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	1. Publicly Available CP and CPS: CPS section 2 1.1 Revision Table, updated annually: Server CPS section 1.2 1.2 CAA Domains listed in CP/CPS: Server CPS section 4.2.1 1.3 BR Commitment to Comply statement in CP/CPS: Server CPS Preamble and section 4.2.1 2. Audit Criteria: Server CPS section 8 3. Revocation of Compromised Certificates: Server CPS section 4.9.1 4. Verifying Domain Name Ownership: Server CPS section 4.2.1 5. Verifying Email Address Control: N/A 6. DNS names go in SAN: Server CPS section 3.1 and Appendix B 7. OCSP: Server CPS Appendix C - OCSP SHALL NOT respond "Good" for unissued certs: 8. Network Security Controls: Server CPS section 6.7	**Verified?**	Verified

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's lists of Forbidden and Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	1. Long-lived Certificates: Server CPS sections 4.6.1, 6.3.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: Server CPS section 4.2.1 3. Issuing End Entity Certificates Directly From Roots: Server CPS section 6.1.7 4. Distributing Generated Private Keys in PKCS#12 Files: Server CPS section 3.2.1 5. Certificates Referencing Local Names or Private IP Addresses: CPS section 4.2.1 6. Issuing SSL Certificates for .int Domains: CPS section 4.2.1 7. OCSP Responses Signed by a Certificate Under a Different Root: Server CPS Appendix C 8. Issuance of SHA-1 Certificates: Server CPS Appendix B 9. Delegation of Domain / Email Validation to Third Parties: CPS section	**Verified?**	Verified

4.2.1

Root Case Record # 1

Root Case Information

Root Certificate Name	Hongkong Post Root CA 3	**Root Case No**	R00000621
Request Status	In Detailed CP/CPS Review	**Case Number**	00000314

Certificate Data

Certificate Issuer Common Name	Hongkong Post Root CA 3
O From Issuer Field	Hongkong Post
OU From Issuer Field	
Valid From	2017 Jun 03
Valid To	2042 Jun 03
Certificate Serial Number	08165F8A4CA5EC00C99340DFC4C6AE23B81C5AA4
Subject	CN=Hongkong Post Root CA 3; OU=; O=Hongkong Post; C=HK
Signature Hash Algorithm	SHA256WithRSA
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	58A2D0EC2052815BC1F3F86402244EC28E024B02
SHA-256 Fingerprint	5A2FC03F0C83B090BBFA40604B0988446C7636183DF9846E17101A447FB8EFD6
Subject + SPKI SHA256	8ADF99FED163C7809331E00788A9311612373EE392E3E43D59628B50139E7127
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	Hongkong Post plans to rollover their currently-included "Hongkong Post Root CA 1" root (bug #408949) to two new roots, this "Hongkong Post Root CA 3" root for SSL (OV and EV) cert issuance and the other root for non-SSL cert issuance.	**Verified?**	Verified

Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8980482	**Verified?**	Verified
CRL URL(s)	http://crl1.hongkongpost.gov.hk/crl/RootCA3ARL.crl http://crl1.hongkongpost.gov.hk/crl/eCertESCA3-17CRL1.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp1.hongkongpost.gov.hk	**Verified?**	Verified
Mozilla Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included In		**Verified?**	Not Applicable
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://valid-ev.ecert.gov.hk/	**Verified?**	Verified
Test Website - Expired	https://expired-ev.hongkongpost.gov.hk		
Test Website - Revoked	https://revoked-ev.hongkongpost.gov.hk		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/valid-ev.ecert.gov.hk No errors.	**Verified?**	Verified
CA/Browser Forum Lint Test	https://bugzilla.mozilla.org/attachment.cgi?id=8980483 "Tested via ... https://github.com/awslabs/certlint ... There is no material errors according to our interpretation."	**Verified?**	Verified
Test Website Lint Test	https://bugzilla.mozilla.org/attachment.cgi?id=8980483 "Tested via ... https://github.com/kroeckx/x509lint ... There is no material errors according to our interpretation."	**Verified?**	Verified
EV Tested	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	Server CPS section 7.3 and Appendix B. Offline Root: Hongkong Post Root CA 3 SubCAs: Hongkong Post e-Cert SSL CA 3 - 17 Hongkong Post e-Cert EV SSL CA 3 - 17	**Verified?**	Verified
Externally Operated SubCAs	The Government of the Hong Kong SAR has appointed Certizen Limited ("Certizen") as an agent of Hongkong Post CA on 13 October 2011 for operating and maintaining the systems and services of Hongkong Post CA from 1 April 2012. As such, Hongkong Post CA with Certizen as the agent is responsible for the management of all its Root CAs and Subordinate CAs. There is no other external entities allowed to operate any Subordinate CAs of Hongkong Post CA.	**Verified?**	Verified
Cross Signing	Server CPS section 1.3.1: "Under this CPS, HKPost performs the functions and assumes the obligations of a CA. HKPost is the only CA authorised to issue certificates under this CPS."	**Verified?**	Verified

Technical Constraint on 3rd party Issuer	CPS Appendix E - List of Registration Authorities for the Hongkong Post e-Cert, if any "With effect from the date of this CPS, no Registration Authority for Hongkong Post e-Cert is appointed."	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are provided in English. e-Cert (Server) CPS for old root: https://www.hongkongpost.gov.hk/product/cps/ecert/img/server_cps_en2.pdf The new CPS that has this new "Hongkong Post Root CA 3" root has not been officially published yet, so it is attached to the Bugzilla Bug.	**Verified?**	Verified
CA Document Repository	https://www.hongkongpost.gov.hk/product/cps/ecert/index.html	**Verified?**	Verified
CP Doc Language	English		
CP	https://bug1464306.bmoattachments.org/attachment.cgi?id=8980476	**Verified?**	Verified
CP Doc Language	English		
CPS	https://bug1464306.bmoattachments.org/attachment.cgi?id=8980476	**Verified?**	Verified
Other Relevant Documents	All historical assessment reports available here: https://www.ogcio.gov.hk/en/our_work/regulation/eto/ca/disclosure_records/hkpost/disclosure_records_hkpost_01.html	**Verified?**	Verified
Auditor	PwC - PricewaterhouseCoopers International Limited	**Verified?**	Verified
Auditor Location	Hong Kong	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2405&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	2/28/2018	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2406&file=pdf	**Verified?**	Verified
BR Audit Type		**Verified?**	Verified

BR Audit Statement Date	2/28/2018	**Verified?**	Verified
EV SSL Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8980478	**Verified?**	Verified
EV SSL Audit Type	WebTrust	**Verified?**	Verified
EV SSL Audit Statement Date	4/30/2018	**Verified?**	Verified
BR Commitment to Comply	Server CPS PREAMBLE	**Verified?**	Verified
BR Self Assessment	https://bug1464306.bmoattachments.org/attachment.cgi?id=8980480	**Verified?**	Verified
SSL Verification Procedures	Server CPS section 4.2.1	**Verified?**	Verified
EV SSL Verification Procedures	Server CPS sections 1.3.3, 3.2.2.2, 3.2.5	**Verified?**	Verified
Organization Verification Procedures	Server CPS sections 3.2.2, 3.2.3, 3.2.5, 4.1, 4.2.1	**Verified?**	Verified
Email Address Verification Procedures	N/A	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	Server CPS section 6.5.1	**Verified?**	Verified
Network Security	Server CPS section 6.7	**Verified?**	Verified