CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)

Introduction must include:
1) CA's Legal Name: Government of Hong Kong SAR, Hongkong Post, Certizen
2) Root certificates in scope: Hongkong Post Root CA 1; Hongkong Post Root CA 3
3) Version of the BR used: CA Baseline Requirement 1.5.5
4) Document version used: HK Post CA CPS OID:1.3.6.1.4.1.16030.1.7.1 [**Note:** This version of CPS re-formats the current CPS for e-Cert (Server) in accordance to RFC3647, but had not yet been disclosed and made available to the public at the time of submission of this self-assessment. Furthermore, this self-assessment covers the practice of issuing EV SSL certificate, which had not yet been rolled out to production.]
5) If you intend to submit your self-assessment with statements such as "will add/update in our next version of CP/CPS", indicate when you plan to provide the updated documents.
Note: When you are doing your BR Self Assessment, if you find that the required information is not currently in your CP/CPS documents, then you may indicate what your CA currently does, how it is currently documented, that the next version of your CP/CPS will contain this information, and when the next version of your CP/CPS will be available.

BR Section Number	List the specific documents and section numbers of those documents which meet the requirements of each BR section	Explain how the CA's listed documents meet the requirements of each BR section.
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*	Section 1.2	Provides document history with previous revision of the CPS.
1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*		The CPS is up to date and the stated practices are fully implemented
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. *Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.*	Appendix E	With effect from the date of this CPS, no Registration Authority for Hongkong Post e-Cert is appointed
2.1. Repositories *Provide the direct URLs to the CA's repositories*	Section 2.1	The link to the HKPCA repository is stated in that section. It is http://www.hongkongpost.gov.hk

2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." *--> Copy the specific text that is used into the explanation in this row. (in English)*	Section 2.2	Under the Ordinance, HKPost maintains a Repository that contains a list of accepted certificates issued under this CPS
2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." *--> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.*		valid-ov.hongkongpost.gov.hk revoked-ov.hongkongpost.gov.hk expired-ov.hongkongpost.hk valid-ev.hongkongpost.gov.hk revoked-ev.hongkongpost.gov.hk expired-ev.hongkongpost.gov.hk
2.3. Time or frequency of publication *Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.*	Section 2.3	Upon approval of an updated CPS by HKPost, the CPS changes will be effective upon publication by HKPost in the HKPost CA web site at http://www.hongkongpost.gov.hk
2.4. Access controls on repositories *Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.*	Section 2.4	The Repository is maintained in a location that is viewable on-line and is protected from unauthorised access.
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	Section 3.2.2	The certificate validation methods used by Hongkong Post CA are described in Section 3.2.2 CPS
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	Section 3.2.2	The certificate validation methods used by Hongkong Post CA are described in Section 3.2.2 CPS
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, *indicate how your CP/CPS meets the requirements in this section of the BRs.*		Application of Hongkong Post e-Cert is currently restricted to bureau and departments of HKSAR Government, statutory bodies under the law of HKSAR, and companies registered in HK.

3.2.2.4 Validation of Domain Authorization or Control *Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation.* ***It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.***	Section 4.2.1	The certificate validation methods used by Hongkong Post CA are described in Section 4.2.1 CPS
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	N/A	N/A
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Section 4.2.1	
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Section 4.2.1	
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Section 4.2.1	
3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Section 4.2.1	
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	N/A	N/A
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	N/A	N/A
3.2.2.4.8 IP Address If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	N/A	N/A

3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	N/A	N/A
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	N/A	N/A
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, *indicate how your CA meets the requirements in this section of the BRs.*	N/A	IP Addresss not listed in HKP CA's certificates
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then *indicate how your CA meets the requirements in this seciton of the BRs.*	Appendix B	Certificates are not allow with (*) in a CN or subjectAltName of type DNS-ID, e.g. "*.local", "*.com", "*.com.hk"
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*	Section 4.2.1	The issuance procedure defines which data sources are considered Reliable Data Sources. It also requires the CA staff to verify that records are still valid before relying on them.
3.2.2.8 CAs MUST check and process CAA records *Indicate your CA's understanding that this section is a requirement as of September 8, 2017, and how your CA meets the requirements in this section of the BRs.*	Section 4.2.1	HKPost will check the Certification Authority Authorisation record(s) (“CAA Record”) published for the domain name(s) to be identified in the certificate.
3.2.3. Authentication of Individual Identity	Section 3.2.3	The Applicant is required to present his HKID Card for identity verification
3.2.5. Validation of Authority	Section 3.2.5	
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	Section 3.2.6	
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	Section 4.1.1	An Authorised Representative of Applicant that hold a valid business registration certificate issued by the Government of the Hong Kong SAR, statutory bodies of Hong Kong whose existence is recognized by the laws of Hong Kong, or bureaux, departments or agencies of Government of HKSAR may submit a certificate application to HKPost.
4.1.2. Enrollment Process and Responsibilities	Section 4.1.2	
4.2. Certificate application processing	Section 4.2	

4.2.1 Re-use of validation information is limited to 825 days *Indicate your CA's understanding that this is a requirement as of March 1, 2018, and indicate how your CA meets the requirements of this section.*	Section 3.2.2.1 and 4.6.1	1. Validity period of Hongkong Post SSL cert are no longer than 25 months. 2. Renewal of Hongkong Post SSL cert need to submit related documents again.
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.*	Section 4.2.1	HKPost will check the CAA Record published for the domain name(s) to be identified in the certificate. , It also validated the Applicant's ownership or control of each Fully-Qualified Domain Name ("FQDN") listed in the e-Cert (Server) certificate.
4.2.2. Approval or Rejection of Certificate Applications	Section 4.2.2	
4.3.1. CA Actions during Certificate Issuance	Section 4.3.1	
4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking certificates.*	Section 4.9.1	The reasons are listed in Section 4.9.1 CPS
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking subordinate CA certificates.*	Section 4.9.1	
4.9.2. Who Can Request Revocation	Section 4.9.2	
4.9.3. Procedure for Revocation Request	Section 4.9.3	
4.9.5. Time within which CA Must Process the Revocation Request	Section 4.9.5	
4.9.7. CRL Issuance Frequency *Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.*	Section 4.9.7	
4.9.9. On-line Revocation/Status Checking Availability	Section 4.9.9	
4.9.10. On-line Revocation Checking Requirements *Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.*	Section 4.9.10	HKPost OCSP supoort GET. It will be updated 3 times daily and is prevent errounious return of "good" status.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	Section 4.9.11	No stipulation in CPS, but we will provide advice to customer upon request
4.10.1. Operational Characteristics	Section 4.10.1	
4.10.2. Service Availability	Section 4.10.2	
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS	Section 5	
5.2.2. Number of Individuals Required per Task	Section 5.2.2	
5.3.1. Qualifications, Experience, and Clearance Requirements	Section 5.3.1	
5.3.3. Training Requirements and Procedures	Section 5.3.3	
5.3.4. Retraining Frequency and Requirements	Section 5.3.4	
5.3.7. Independent Contractor Controls	Section 5.3.7	
5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section.*	Section 5.4.1	

5.4.3. Retention Period for Audit Logs	Section 5.4.3	
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	Section 5.4.8	
5.5.2. Retention Period for Archive	Section 5.5.2	
5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	Section 5.7.1	
6.1.1. Key Pair Generation	Section 6.1.1	
6.1.2. Private Key Delivery to Subscriber	Section 6.1.2	Applicant’s Private key will be generated by the Applicant
6.1.5. Key Sizes	Section 6.1.5	The HKPost signing key pair is 2048-bit RSA. Subscriber key pair is 2048-bit RSA.
6.1.6. Public Key Parameters Generation and Quality Checking	Section 6.1.6	Signing key generation, storage, and signing operations performed by HKPost are conducted within a hardware cryptographic module
6.1.7. Key Usage Purposes	Section 6.1.7	
6.2. Private Key Protection and Cryptographic Module Engineering Controls	Section 6.2	
6.2.5. Private Key Archival	Section 6.2.5	All Private Keys will not be archived.
6.2.6. Private Key Transfer into or from a Cryptographic Module	Section 6.2.6	
6.2.7. Private Key Storage on Cryptographic Module	Section 6.2.7	HKPost Private Keys are created in a crypto module validated to at least FIPS 140-1 Level 3.
6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days *Indicate how your CA meets the requirements of this section.*	Section 6.3.2	
6.5.1. Specific Computer Security Technical Requirements The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance. *Indicate how your CA meets the requirements of this section.*	Section 6.5.1	
7.1. Certificate profile CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG. *Indicate how your CA meets the requirements of this section.*	Appendix B	
7.1.1. Version Number(s)	Appendix B	All certificates referred to in this CPS are issued in the X.509 version 3 format
7.1.2. Certificate Content and Extensions; Application of RFC 5280	Appendix B	
7.1.2.1 Root CA Certificate	Appendix B	
7.1.2.2 Subordinate CA Certificate	Appendix B	
7.1.2.3 Subscriber Certificate	Appendix B	
7.1.2.4 All Certificates	Appendix B	
7.1.2.5 Application of RFC 5280	Appendix B	
7.1.3. Algorithm Object Identifiers	Appendix B	

7.1.4. Name Forms	Appendix B	
7.1.4.1 Issuer Information	Appendix B	
7.1.4.2 Subject Information - Subscriber Certificates	Appendix B	
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	Appendix B	
7.1.5. Name Constraints *Indicate your CA's understanding of Mozilla's requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section.*	Appendix B	
7.1.6. Certificate Policy Object Identifier	Appendix B	
7.1.6.1 Reserved Certificate Policy Identifiers	Appendix B	
7.1.6.2 Root CA Certificates	Appendix B	
7.1.6.3 Subordinate CA Certificates	Appendix B	
7.1.6.4 Subscriber Certificates	Appendix B	
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	Section 8	
8.1. Frequency or circumstances of assessment The period during which the CA issues Certificates SHALL be dividied into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration. For new CA Certificates: The point-in-time readiness assessment SHAL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*	Section 8.1	Compliance audits and assessments are performed at least once in every 12 months.
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	Section 8.2	
8.4. Topics covered by assessment	Section 8.4	
8.6. Communication of results	Section 8.6	

Also indicate your understanding and compliance with Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps). .... The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information: - name of the company being audited; - name and address of the organization performing the audit; - Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope; - audit criteria (with version number) that were used to audit each of the certificates; - a list of the CA policy documents (with version numbers) referenced during the audit; - whether the audit is for a period of time or a point in time; - the start date and end date of the period, for those that cover a period of time; - the point-in-time date, for those that are for a point in time; - the date the report was issued (which will necessarily be after the end date or point-in-time date); and - For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers). "		
8.7. Self-Audits	Section 8.7	
9.6.1. CA Representations and Warranties	Section 9.6.1	
9.6.3. Subscriber Representations and Warranties	Section 9.6.3	
9.8. Limitations of liability	Section 9.8	
9.9.1. Indemnification by CAs	Section 9.9	
9.16.3. Severability	Section 9.16.3	