Hongkong Post e-Cert
香港郵政電子核證

“Hongkong Post has one root certificate (Subject CN=“Hongkong Post Root CA 1”) that has already been trusted in the Mozilla Root Certificate Program. Since it is approaching to the expiry date of this root certificate, Hongkong Post has planned to rollover this root certificate to two new root certificates (one for issuing SSL certificates and one for issuing non-SSL certificates), and alongside start issuing EV SSL certificates.”

-- General information about CA's associated organization –

Name: **Hongkong Post Certification Authority**

Company Website: **www.eCert.gov.hk (formerly www.hongkongpost.gov.hk)**

CA Email Alias 1: **enquiry@eCert.gov.hk**

CA Email Alias 2: **manho@certizen.com**

Organizational Type : **Government Agency**

Organizational Type (Others) :

Organization Type choices:
- Private Corporation
- Public Corporation
- Government Agency
- Commercial Organization
- International Organization
- Non-Profit Organization
- Academic Institution
- Consortium
- NGO

Geographic Focus: **Hong Kong**

Primary Market / Customer Base:
Hongkong Post is a recognized Certification Authority by virtue of the Electronic Transactions Ordinance (Cap. 553) of Hong Kong SAR of PRC (“ETO”) and offers Hongkong Post Certification Authority (or “Hongkong Post CA”) services to individuals and businesses such as Bureaux and Departments of the Government of Hong Kong SAR, organisations that hold a valid business registration certificate issued by the Government of Hong Kong SAR and statutory bodies of Hong Kong whose existence is recognized by the laws of Hong Kong SAR.

Impact to Mozilla Users:

Hongkong Post has one root certificate (Subject CN="Hongkong Post Root CA 1") that has already been trusted in the Mozilla Root Certificate Program. Since it is approaching to the expiry date of this root certificate, Hongkong Post has planned to rollover this root certificate to two new root certificates (one for issuing SSL certificates and one for issuing non-SSL certificates), and alongside start issuing EV SSL certificates. The following paragraphs explain in more detail.

OVERVIEW OF THE EXISTING ROOT CERTIFICATE "Hongkong Post Root CA 1"

Hongkong Post (or "Hongkong Post CA") currently has one root certificate that has been trusted in Mozilla Root Certificate Program, i.e. subject cn="Hongkong Post Root CA 1" ("Root CA1"). Under this root certificate, there are three valid SubCA certificates, with subject cn="Hongkong Post e-Cert CA 1-10" ("SubCA 1-10"), cn="Hongkong Post e-Cert CA 1-14" ("SubCA 1-14") and cn="Hongkong Post e-Cert CA 1-15" ("SubCA 1-15") respectively.

All end-entity certificates are currently issued by these SubCAs:

- **SubCA 1-10 is currently issuing client certificates that support client authentication, secure email (S/MIME), encrypting files and document signing.**
- **SubCA 1-14 had been used to issue SSL certificates, but already stopped issuing SSL certificates since 1 September 2016.**
- **SubCA 1-15 is currently issuing SSL certificates that is BR compliant and Mozilla CA Policy requirements as well.**

Root CA1 and the three SubCA certificates will expire in 15 May 2023. Customers of our SSL certificates, mainly from Bureaux and Departments of the Government of Hong Kong SAR, are serving over 8 million people of Hong Kong. It is important to renew this root certificate as soon as possible, or no later than the end of 2018.

-- Required and Recommended Practices --

Recommended Practices: https://wiki.mozilla.org/CA/Required_or_Recommended_Practices

Do You, as an official representative of this CA agree to the following Recommended Practices Statement?

I have reviewed Mozilla's lists of Required and Recommended Practices, and confirm that we follow those practices, with clarifications noted in the text box below.

CA's Response to Recommended Practices:

1 Required Practices

1.1 Publicly Available CP and CPS

Hongkong Post CA's CPS(s) are publicly available in URL http://www.eCert.gov.hk/product/cps/ecert/index.html. New version of CPS for the new root certificates is provided in attached information, and will be published in the URL.

1.2 Audit Criteria

Hongkong Post CA continuously completes WebTrust Principles and Criteria for Certification Authorities audit every year. The latest audit report on 28 February 2018 can be found in URL https://cert.webtrust.org/SealFile?seal=2405&file=pdf .

Hongkong Post CA has already completed WebTrust SSL Baseline Requirements Audit Criteria for Certification Authorities. The latest audit report on 28 February 2018 can be found in URL https://cert.webtrust.org/SealFile?seal=2406&file=pdf .

A WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL (Point-in-time) audit as of 31 March 2018 has been completed. The audit report on 30 April 2018 is provided in attached information. Meanwhile, we may issue EV SSL certificates to ourselves and some organizations in connection with us for trial run only. When we do so, we assure to follow the procedure in compliance with the CPS for EV SSL certificate.

1.3 Revocation of Compromised Certificates

In accordance with section 4.9.1 of CPS, we will revoke certificates with private keys that are known, or are suspected, to be compromised, or for which verification of subscriber information is known to be invalid.

1.4 Verifying Domain Name Ownership

In accordance with section 4.2.1 of CPS, we validate the applicant's ownership or control of each FQDN using one or more of the procedures that are reserved in BR 3.2.2.4.2, 3.2.2.4.3 or 3.2.2.4.4.

1.5 Verifying Email Address Control

This root certificate does not have Email trust bit set. Our CPS does not require verification of email address (if any) to be included in SSL certificate.

1.6 DNS names go in SAN

With reference to Appendix B of CPS, DNS names go in SAN.

1.7 OCSP

With reference to Appendix C of CPS, we provide certificate status information via OCSP in compliance with CA/B Forum BR.

1.8 Network Security Controls

We maintain network security controls that meets the Network and Certificate System Security Requirements of CAB Forum.

2 Recommended Practices

2.1 CA Hierarchy

Please refer to the section CA Hierarchy Information below for a graphical or textual description of Hongkong Post CA hierarchy.

2.2 Document Handling of IDNs in CP/CPS

We allow the use of IDNs in certificates. With reference to ??? of CPS, Hongkong Post CA handles the issue of homographic spoofing of IDNs.

2.3 Usage of Appropriate Constraints

This root certificate has SSL trust bit set only.

2.4 Pre-Issuing Linting

We use such tools (certlint/cablint, x509lint, zlint) manually for cross-checking the logic of validation in our certificate issuance system. We are evaluating the impact of integrating them into our system, and may use them in future.

-- Forbidden and Potentially Problematic Practices --

Potentially Problematic Practices:
https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices

Do You, as an official representative of this CA agree to the following 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 clarifications noted in the text box below.

1 Forbidden Practices

1.1 Long-lived Certificates

Our newly issued SSL certificates have a maximum lifetime of 25 months.

1.2 Non-Standard Email Address Prefixes for Domain Ownership Validation

When using email address for domain ownership validation, we conform to BR section 3.2.2.4.4 to use an email address created by pre-pending ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’, or ‘postmaster’ in the local part, followed by the at-sign (“@”), followed by the Authorisation Domain Name, which may be formed by pruning zero or more components from the requested FQDN.

1.3 Issuing End Entity Certificates Directly From Roots

Hongkong Post CA root certificate does not issue end-entity certificates directly.

1.4 Distributing Generated Private Keys in PKCS#12 Files

We do not generate key pairs for SSL certificates.

1.5 Certificates Referencing Local Names or Private IP Addresses

We do not issue SSL certificates referencing local names or reserved IP addresses.

1.6 Issuing SSL Certificates for .int Domains

We do not issue SSL certificates for .int domain names.

1.7 OCSP Responses Signed by a Certificate Under a Different Root

OCSP Responses are always signed by the respective responder certificate issued under the same Hongkong Post CA root certificate.

1.8 Issuance of SHA-1 Certificates

We do not issue new SHA-1 SSL certificates, and all intermediate and end-entity certificates under the two new root certificates are SHA-256 certificates.

2 Potentially Problematic Practices

2.1 Delegation of Domain / Email Validation to Third Parties

We do not delegate domain and email validation to any third parties.

2.2 Allowing External Entities to Operate Subordinate CAs

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.

2.3 Generic Names for CAs

Subject information of the two new root certificates are:

Root CA for issuing non-SSL certificates	Root CA for issuing SSL certificates

CN = Hongkong Post Root CA 2
O = Hongkong Post
L = Hong Kong
S = Hong Kong
C = HK
	CN = Hongkong Post Root CA 3
	O = Hongkong Post
	L = Hong Kong
	S = Hong Kong
	C = HK

Subject information of Subordinate CAs under the two new root certificates are:

CN = Hongkong Post e-Cert CA 2 - 15
O = Hongkong Post
L = Hong Kong
S = Hong Kong
C = HK
	CN = Hongkong Post e-Cert SSL CA 3 - 17
	O = Hongkong Post
	L = Hong Kong
	S = Hong Kong
	C = HK

CN = Hongkong Post e-Cert CA 2 - 17 **O = Hongkong Post** **L = Hong Kong** **S = Hong Kong** **C = HK**	**CN = Hongkong Post e-Cert EV SSL CA 3 - 17** **O = Hongkong Post** **L = Hong Kong** **S = Hong Kong** **C = HK**

2.4 Lack of Communication With End Users

We actively respond to any questions, that subscribers, relying parties or general public might have, via service hotline or email.

2.5 Backdating the notBefore Date

We do not backdate any certificates.

2.6 Issuer Encoding in CRL

The encoding of the Issuer field in our CRL is the same as that of the Issuer in certificates.

- Policies and Practices -

Policy Documentation:
Languages that the CP/CPS and other documents are provided in.

CA Document Repository: **http://www.eCert.gov.hk/product/cps/ecert/index.html**

CP: **http://www.eCert.gov.hk/product/cps/ecert/index.html**

CPS: **http://www.eCert.gov.hk/product/cps/ecert/index.html**

Other Relevant Documents:

Auditor Name: **PwC - PricewaterhouseCoopers International Limited**

Auditor Website: **http://www.pwc.com/**

Auditor Qualifications: **http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx**

Standard Audit URL: **https://cert.webtrust.org/SealFile?seal=2405&file=pdf**

Standard Audit Type: **WebTrust**

Standard Audit Statement Date: **2/28/2018**

BR Audit URL:
If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.

BR Audit Type: **WebTrust**

BR Audit Statement Date: **2/28/2018**

EV SSL Audit URL: **provided in the attached information**
If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.

EV SSL Audit Type: **WebTrust**

EV SSL Audit Statement Date: **30 April 2018**

BR Commitment to Comply:
If requesting Websites trust bit, need section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of the CA/Browser Forum's Baseline Requirements.
We post our commitment to comply with the BRs in URL of CA Document Repository.

BR Self Assessment:
If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_Self-Assessment) to the Bugzilla Bug.
A BR Self-assessment is provided in the attached information of this request.

SSL Verification Procedures:
if Websites trust bit requested...
Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert.
CP/CPS must clearly specify the procedures that the CA employs. Each documented procedure should state which subsection of BR section 3.2.2.4 it is complying with.
Section 4.2.1 of CPS describes the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL certificate.

EV SSL Verification Procedures:
If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate.
The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.

Section 4.2.1, 3.2.2.2 and 3.2.5 of CPS describes the procedure for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organisation to request the EV SSL certificate.

Organization Verification Procedures:
CP/CPS sections that describe identity and organization verification procedures for cert issuance.
We only issue OV and EV SSL certificates. Section 3.2.2.1 and 3.2.5 of CPS describes the procedure for verifying the identity, existence, and authority of the organisation to request the OV SSL certificates.

Email Address Verification Procedures:
if Email trust bit requested...
Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert.
This root certificate does not have Email trust bit set.

Multi-Factor Authentication:
section number of the CP/CPS that states that multi-factor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)
Section 5.2.2 and section 6.5 of CPS describes the multi-person control over the life cycle of activation data such as PINs and passwords for accessing the CA system.

Network Security:
section number(s) of the CP/CPS dealing with Network Security.
Section 6.7 of CPS describes network security controls of Hongkong Post CA's network environment.

-- Technical Information about each Root Certificate --

Provide the following information for each root cert for which you are requesting inclusion or change.

-- Root Certificate #1 --

Root Certificate Name: **Hongkong Post Root CA 3**

- Certificate Data -

Root Certificate Download URL:	**Provided in attached information of this request, “Root CA3 and SubCAs.zip”**
Certificate Issuer Field:	**CN = Hongkong Post Root CA 3** **O = Hongkong Post**

	L = Hong Kong
	S = Hong Kong
	C = HK

SHA-1 Fingerprint:	58:A2:D0:EC:20:52:81:5B:C1:F3:F8:64:02:24:4E:C2:8E:02:4B:02
SHA-256 Fingerprint:	5A:2F:C0:3F:0C:83:B0:90:BB:FA:40:60:4B:09:88:44:6C:76:36:18:3D:F9:84:6E:17:10:1A:44:7F:B8:EF:D6
CRL URL(s):	Root CA: Nil Sub CA: http://crl1.eCert.gov.hk/crl/RootCA3ARL.crl SSL certificate issued by Sub CA “Hongkong Post e-Cert SSL CA 3 - 17”: http://crl1.eCert.gov.hk/crl/eCertSCA3-17CRL1.crl SSL certificate issued by Sub CA “Hongkong Post e-Cert EV SSL CA 3 - 17": http://crl1.ecert.gov.hk/crl/eCertESCA3-17CRL1.crl With reference to sections 4.9.7, 7.2 and Appendix C of CPS, Hongkong Post CA updates and publishes the Certificate Revocation Lists (CRLs) containing information of suspended or revoked SSL certificates 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)).
OCSP URL(s):	Root CA: Nil Sub CA: http://ocsp1.ecert.gov.hk/ SSL certificate issued by Sub CAs “Hongkong Post e-Cert SSL CA 3 - 17” and “Hongkong Post e-Cert EV SSL CA 3 - 17": http://ocsp1.ecert.gov.hk/ With reference to sections 4.9.9, 7.3 and Appendix C of CPS, the OCSP response for that certificate will be updated at the same time when the next Certificate Revocation List is updated and published, except for Extended Validation e-Cert (Server) the respective OCSP response will be updated and published immediately upon the suspension or revocation of that certificate. Furthermore, the OCSP next update date is two days after the current update date.
Mozilla Trust Bits:	Websites
SSL Validation Type:	OV; EV (planned to be launched and its launch date is to be confirmed)
Mozilla EV Policy OID(s):	2.23.140.1.2.2
Root Stores Included In:	The existing root certificate (Subject CN=“Hongkong Post Root CA 1”) has already been trusted in : • Mozilla Root Certificate Program, https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport

	• **Microsoft Trusted Root Certificate Program, https://social.technet.microsoft.com/wiki/contents/articles/31634.microsoft-trusted-root-certificate-program-participants.aspx** • **Apple Trust Store, https://support.apple.com/en-us/HT204132** • **Adobe Approved Trust List, https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html**
Mozilla Applied Constraints:	**No Constraints**
Test Website:	**OV certificate Valid: https://valid-ov.eCert.gov.hk/** **OV certificate Expired: https://expired-ov.eCert.gov.hk/** **OV certificate Revoked: https://revoked-ov.eCert.gov.hk/** **EV certificate Valid: https://valid-ev.eCert.gov.hk/** **EV certificate Expired: https://expired-ev.eCert.gov.hk/** **EV certificate Revoked: https://revoked-ev.eCert.gov.hk/**
Test Results:	**Tested via http://certificate.revocationcheck.com/ , https://github.com/awslabs/certlint , https://github.com/kroeckx/x509lint and https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version** **There is no material errors according to our interpretation.**

- CA Hierarchy Information -

CA Hierarchy:	**NEW ROOT CERTIFICATES "Hongkong Post Root CA 2" and "Hongkong Post Root CA 3"** **For transition of all end-entity certificates to under new PKIs, we plan to separate them into two PKIs of root certificates, i.e. subject cn="Hongkong Post Root CA 2" ("Root CA2") and cn="Hongkong Post Root CA 3" ("Root CA3"). Root CA2 will be used to issue SubCAs that will issue client certificates only. Root CA3 will be used to issue SubCAs that will issue SSL certificates only, including one SubCA that issues SSL certificate and another SubCA that issues EV SSL certificate.** **As we note that the timeline for waiting and vetting our application by Mozilla and other browser vendors may not be guaranteed, we would create a cross-certificate of Root CA3, i.e. subject cn="Hongkong Post Root CA 3" ("XRoot CA3") signed by Root CA1. In other words, for SSL certificates issued under Root CA3, Mozilla Firefox and browsers of other vendors would automatically find the ultimate trust anchor Root CA1. When XRoot CA3 expires or is terminated at our own discretionary, Mozilla Firefox would automatically find the direct trust anchor Root CA3.** **PKI OF "Hongkong Post Root CA 2"**

A) “Hongkong Post Root CA 2” [Note 1]

- **Validity period: 25 years (from 9 May 2015 to 9 May 2040)**
- **Serial number: 68 a5 fd a6 d0 1c 5e 3f cf e4 f9 99 df 7a 6c 6f 39 a9 7f fc**
- **Signature algorithm: SHA256RSA**
- **Key size: 4096 bits**
- **Key usage: Digital Signature, Non-Repudiation, Certificate Signing, CRL Signing**
- **SubCA certificates:**
    - **Hongkong Post e-Cert CA 2-15**
    - **Hongkong Post e-Cert CA 2-17**

B) “Hongkong Post e-Cert CA 2-15” [Note 2]

- **Validity period: 15 years (from 9 May 2015 to 9 May 2030)**
- **Serial number: 00 a8 9f e8 f0 ea e0 a5 51 ff e6 5f c0 85 34 0e a0 d3 4a 08**
- **Signature algorithm: SHA256RSA**
- **Key size: 2048 bits**
- **Key usage: Digital Signature, Non-Repudiation, Certificate Signing, CRL Signing**
- **Path Length Constraint: 0**

C) “Hongkong Post e-Cert CA 2-17” [Note 3]

- **Validity period: 15 years (from 12 August 2017 to 12 August 2032)**
- **Serial number: 29 00 7d 78 98 e1 c0 f0 c7 e2 4c 00 cf 4a eb 31 31 ea 4e ac**
- **Signature algorithm: SHA256RSA**
- **Key size: 2048 bits**
- **Key usage: Digital Signature, Non-Repudiation, Certificate Signing, CRL Signing**
- **Path Length Constraint: 0**

PKI OF “Hongkong Post Root CA 3”

A) “Hongkong Post Root CA 3” [Note 4]

- **Validity period: 25 years (from 3 June 2017 to 3 June 2042)**
- **Serial number: 08 16 5f 8a 4c a5 ec 00 c9 93 40 df c4 c6 ae 23 b8 1c 5a a4**
- **Signature algorithm: SHA256RSA**
- **Key size: 4096 bits**
- **Key usage: Certificate Signing, CRL Signing**
- **SubCA certificates:**

  - “Hongkong Post e-Cert SSL CA 3-17” (“SSL CA 3-17”) (for non-EV SSL)
  - “Hongkong Post e-Cert EVSSL CA 3-17” (“EVSSL CA 3-17”) (for EV SSL)
- Cross-certificate signed by Root CA1:
  - “Hongkong Post Root CA 3” (“XRoot CA3”)[Note 5]

B) “Hongkong Post e-Cert SSL CA 3-17” [Note 6]

- Validity period: 15 years (from 3 June 2017 to 3 June 2032)
- Serial number: 63 fe 03 bd 8b bb 95 12 a4 09 1e d9 3c 5f ed 14 c0 e1 81 d5
- Signature algorithm: SHA256RSA
- Key size: 2048 bits
- Key usage: Certificate Signing, CRL Signing
- Path Length Constraint: 0

C) “Hongkong Post e-Cert EV SSL CA 3-17” [Note 7]

- Validity period: 15 years (from 3 June 2017 to 3 June 3032)
- Serial number: 68 ed 49 dd a3 79 25 92 57 8c 32 51 20 da 22 e9 f1 e1 0b d4
- Signature algorithm: SHA256RSA
- Key size: 2048 bits
- Key usage: Certificate Signing, CRL Signing
- Path Length Constraint: 0

Note 1: For information, Root CA2 was created in 9 May 2015 for two SubCAs. However, it is not prepared for this request.

2: For information, SubCA 2-15 was created at the same time of Root CA2 (i.e. 9 May 2015) for issuance of end-entity certificates other than SSL certificates. It is not prepared for this request.

3: For information, SubCA 2-17 was created on 12 August 2017 for issuance of end-entity certificates other than SSL certificates. It is not prepared for this request.

4: For this request, Root CA3 was created in 3 June 2017 for two SubCAs. See attached information “Root CA3 and SubCAs.zip” for this self-signed CA root certificate.

5: The cross-certificate Root CA3 was created on 12 August 2017, which is signed by our Root CA1. See attached information “Root CA3 and SubCAs.zip” for this cross-certificate.

	6: SSL CA 3-17 was created at the same time of Root CA3 (i.e. 3 June 2017) for issuance of SSL certificates. See attached information “Root CA3 and SubCAs.zip” for this intermediate certificate. **7: EVSSL CA 3-17 was created at the same time of Root CA3 (i.e. 3 June 2017) for issuance of EV SSL certificates. See attached information “Root CA3 and SubCAs.zip” for this intermediate certificate.**
Externally Operated SubCAs:	**All SubCAs are operated internally at premises of Hongkong Post CA. However, for avoidance of doubt, 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 since 1 April 2012.**
Cross-Signing:	**This Root CA does not cross-sign any external SubCAs. On the other hand, for smooth rollover of root certificate, the existing root certificate (Subject CN=“Hongkong Post Root CA 1”) has signed a cross-certificate to this Root CA, named “Hongkong Post Root CA 3”, and posted in CCADB.**
Technical Constraints on Third-party Issuers:	**Third-party Issuers/SubCAs are not supported.**

-- End Root Certificate #1 --