

Independent practitioner's assurance report

To the Management of Hongkong Post Certification Authority:

Scope

We have been engaged to perform a reasonable assurance engagement on the accompanying [management's assertion](#) of Hongkong Post Certification Authority ("HKPCA") with Certizen Limited ("Certizen") as its agent in providing its Certification Authority ("CA") operations in the Hong Kong Special Administrative Region of the People's Republic of China for the period from 1 January 2024 to 31 December 2024 for its CAs as enumerated in [Appendix C](#), HKPCA with Certizen as its agent has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statements ("CPS") referenced in [Appendix D](#).
- maintained effective controls to provide reasonable assurance that:
 - HKPCA provides its services in accordance with its CPS,
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated (for the registration activities performed by HKPCA with Certizen as its agent); and
 - subordinate CA certificate requests are accurate, authenticated, and approved,
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorised individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA system development, maintenance, and operations are properly authorised and performed to maintain CA system integrity,

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

HKPCA makes use of external registration authorities for specific subscriber registration activities as disclosed in HKPCA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.

HKPCA does not escrow its CA keys. Accordingly, our procedures did not extend to controls that would address those criteria.

Management’s Responsibilities

The management of HKPCA with Certizen as its agent is responsible for the management’s assertion, including the fairness of its presentation, and the provision of its described services in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Our Independence and Quality Management

We have complied with the independence and other ethical requirements of the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our firm applies International Standard on Quality Management 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner’s Responsibilities

It is our responsibility to express an opinion on the management’s assertion based on our work performed.

We conducted our procedures in accordance with International Standard on Assurance Engagements 3000 (Revised) “Assurance Engagements Other Than Audits or Reviews of Historical Financial Information”, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our work to form the opinion.

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence whether the management’s assertion of HKPCA (with Certizen as its agent) is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#). The extent of procedures selected depends on the practitioner’s judgment and our assessment of the engagement risk. Within the scope of our work, we performed amongst others the following procedures:

- obtaining an understanding of HKPCA’s key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
- selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
- testing and evaluating the operating effectiveness of the controls; and
- performing such other procedures as we considered necessary in the circumstances.

The relative effectiveness and significance of specific controls at HKPCA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Inherent Limitation

Because of the nature and inherent limitations of controls, HKPCA (with Certizen as its agent)'s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any opinion based on our findings to future periods is subject to the risk that changes may alter the validity of such opinion.

Opinion

In our opinion, the management's assertion of HKPCA with Certizen as its agent, for the period from 1 January 2024 to 31 December 2024, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Emphasis of Matter

This report does not include any representation as to the quality of HKPCA (with Certizen as its agent)'s services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), nor the suitability of any of HKPCA (with Certizen as its agent)'s services for any customer's intended purpose.

Our opinion is not modified in respect of this matter.

Other Matters

We noted the following other matters during our procedures:

The certificate for the Hongkong Post Root CA 1 (Appendix C Root CA #1) CA expired on 15 May 2023 and was not renewed.

HKPCA's management has disclosed five incidents (see [Appendix B](#)) during the period from 1 January 2024 to 31 December 2024. The remedial actions and the root causes of these incidents undertaken by HKPCA have been posted publicly in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum.

Our opinion is not modified in respect of these matters.

Purpose and Restriction on Use

The management's assertion was prepared for obtaining and displaying the WebTrust Seal on HKPCA website¹ using the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#) designed for this purpose. As a result, the management's assertion of HKPCA (with Certizen as its agent) may not be suitable for another purpose. This report is intended solely for management of HKPCA in connection with obtaining and displaying the WebTrust Seal on its website after submitting the report to the related authority in connection with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Our report is not to be used for any other purpose. We do not assume responsibility towards or accept liability to any other parties for the contents of this report.

Use of the WebTrust seal

HKPCA's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.



PricewaterhouseCoopers
Certified Public Accountants

Hong Kong, 24 February 2025

¹ The maintenance and integrity of the HKPCA website is the responsibility of the Management of HKPCA; the work carried out by the assurance provider does not involve consideration of these matters and, accordingly, the assurance provider accepts no responsibility for any differences between the accompanying management's assertion of HKPCA on which the assurance report was issued or the assurance report that was issued and the information presented on the website.



Appendix A – Auditor’s information

Auditor Name	Address
PricewaterhouseCoopers	22/F Prince's Building, Central, Hong Kong



Appendix B – Publicly disclosed incidents during the period from 1 January 2024 to 31 December 2024

Bugzilla ID	Disclosure	Publicly Disclosed Link
1887888	Hongkong Post: Delayed revocation of TLS certificates with basicConstraints not marked as critical	Bugzilla Ticket Link
1887008	Hongkong Post: TLS certificates with basicConstraints not marked as critical	Bugzilla Ticket Link
1886722	Hongkong Post: Delayed response to CPR	Bugzilla Ticket Link
1886665	Hongkong Post: Delayed revocation of TLS certificates with Certificate Policies extension problem	Bugzilla Ticket Link
1886406	Hongkong Post: TLS certificates with Certificate Policies extension that does not assert http scheme	Bugzilla Ticket Link



Appendix C – In Scope CA

Full Name of CA:
Hongkong Post Certification Authority

List of HKPCA's Root CA:

Reference	Root CA Name	Remarks
1	Hongkong Post Root CA 1	Valid from 15 May 2003 and expired on 15 May 2023
<u>Subject DN</u> C=HK, O=Hongkong Post, CN=Hongkong Post Root CA 1 <u>SHA-1 Thumbprint</u> D6DAA8208D09D2154D24B52FCB346EB258B28A58 <u>SHA-256 Thumbprint</u> F9E67D336C51002AC054C632022D66DDA2E7E3FFF10AD061ED31D8BBB410CFB2		
2	Hongkong Post Root CA 2	Valid from 5 September 2015
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 2 <u>SHA-1 Thumbprint</u> DE010808E41EC41930D44095F8FE596B582C8CA2 <u>SHA-256 Thumbprint</u> 3945E08A8D4A0554B7605A7B355B10188E3EF842C76A805C54E3657C4D041AAA		
3	Hongkong Post Root CA 3	Valid from 3 June 2017
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 <u>SHA-1 Thumbprint</u> 58A2D0EC2052815BC1F3F86402244EC28E024B02 <u>SHA-256 Thumbprint</u> 5A2FC03FoC83B090BBFA40604B0988446C7636183DF9846E17101A447FB8EFD6		

List of HKPCA's Subordinate CA:

Reference	Subordinate CA Name	Remarks
1	Hongkong Post e-Cert CA 1 - 10	Revoked on 9 January 2010
<u>Subject DN</u> C=HK, O=Hongkong Post, CN=Hongkong Post e-Cert CA 1 - 10 <u>SHA-1 Thumbprint</u> 8E7DC57B719EF6EDAFE371DC932E3BD7DA86C27A <u>SHA-256 Thumbprint</u> 44E24932FB1CD30DD94B20C2FoF3B7B9EB33B5C3BFC9344BC47A5167BFBD2A13		
2	Hongkong Post e-Cert CA 1 - 10	Issuance of SSL subscriber certificate was terminated from 1 January 2016 and expired on 15 May 2023
<u>Subject DN</u> C=HK, O=Hongkong Post, CN=Hongkong Post e-Cert CA 1 - 10 <u>SHA-1 Thumbprint</u> 3C8C897A8067713565626201E9EB20262E1D58CB <u>SHA-256 Thumbprint</u> 5274CC53BC061F9F984430F401A9D3BA35A20CEEBC8E8E6DFA71B269A7C640D2		
3	Hongkong Post e-Cert CA 1 - 14	Issuance of SSL subscriber certificate was terminated from 1 September 2016 and expired on 15 May 2023
<u>Subject DN</u> C=HK, O=Hongkong Post, CN=Hongkong Post e-Cert CA 1 - 14 <u>SHA-1 Thumbprint</u> 7DE6BE6FD505A861C3C81C7F1D467315C664A928 <u>SHA-256 Thumbprint</u> 14422A1BD5A91EDBA7397B8698922369B6AF6984FF87ACF6139DAA919E795A14		
4	Hongkong Post e-Cert CA 1 - 15	Issuance of SSL subscriber certificate was terminated from 1 July 2019 and expired on 15 May 2023
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 1 - 15 <u>SHA-1 Thumbprint</u> A19DF5F1BFB89686AF985667C4F80E8A09DDFD36 <u>SHA-256 Thumbprint</u> 5CB9E9DE32B187E40BA14FDF200FDA62C7B4FBF88D64F77CE02DD6EBE6BCC1B0		
5	Hongkong Post e-Cert CA 2 - 15	Valid from 5 September 2015
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 2 - 15		

Reference	Subordinate CA Name	Remarks
<u>SHA-1 Thumbprint</u> 893FF8AFFC3738A49816EE0D134C9929E55BF747 <u>SHA-256 Thumbprint</u> 3271139D13EFEF47B348CD2436CE43A02E9B77E1D99318A3B9C751FC937F6230		
6	Hongkong Post e-Cert CA 2 - 17	Valid from 12 August 2017
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 2 - 17 <u>SHA-1 Thumbprint</u> 8745EFDfE96260F27014CCE8C8B98E7882A89B50 <u>SHA-256 Thumbprint</u> CBB56EAEFD6FECDE2408F2F9CE8C324CDDBD3D967A5D76A9A22E81FF89B516AF		
7	Hongkong Post e-Cert CA 2 - 19	Valid from 29 July 2019
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 2 - 19 <u>SHA-1 Thumbprint</u> FA3E35B01455216190505b21f14D7A97CAAE413 <u>SHA-256 Thumbprint</u> 5BFF0E9BCE3B75D36EA46E0746174C034885606CBE46228ED0AE9E5782583FB2		
8	Hongkong Post e-Cert SSL CA 3 - 17	Valid from 3 June 2017 for issuance of non-EV SSL certificate
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert SSL CA 3 - 17 <u>SHA-1 Thumbprint</u> 92797871DC6A0B6EE1417BB657D7ED6FC6F975EB <u>SHA-256 Thumbprint</u> 69ECDBC3147F581DFDCB522D9DEFB260B26784AD4955C74E6A52522CCC4C4408		

9	Hongkong Post e-Cert EV SSL CA 3 - 17	Valid from 3 June 2017 for issuance of EV SSL certificate
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert EV SSL CA 3 - 17 <u>SHA-1 Thumbprint</u> 6CA9BB1B3BAEF67D6D5414132A7EFB212836639E <u>SHA-256 Thumbprint</u> C18D53BF9864DD09BCBCACFD672E2566D4C81F6889E36DF5DD425C04211D0763		
10	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 12 August 2017
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 <u>SHA-1 Thumbprint</u> DoD535192598FCA8B68789EDCEF1EA51B3A898A5 <u>SHA-256 Thumbprint</u> ABFA404ECEEA854381ABE294AC829440E0133E077911A67E1293CF111AC43C44		
11	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and valid from 12 August 2017 and expired on 15 May 2023
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 <u>SHA-1 Thumbprint</u> 97FC47E174E2AA5332321DCFF6077A19F04387F0 <u>SHA-256 Thumbprint</u> 176AEBF2972BD6F47179EDE3DE63848B1543B45AE2954BEA45185B152537B9C4		
12	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 27 July 2022
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 <u>SHA-1 Thumbprint</u> 881700C3346CBA89A8C1C5C44A584A8441319944 <u>SHA-256 Thumbprint</u> F8F6037491861C069D3BB442B78A3DB4049EE7787B7C2841A7BA6966B5272F2C		

13	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and valid from 27 July 2022 and expired on 15 May 2023
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 <u>SHA-1 Thumbprint</u> 3069BCFC8DDoAFBAABA5CA81D23CCC6413131F6F <u>SHA-256 Thumbprint</u> 5544A24FEB21F681F1987D30EoAF5C49E9F9FFFD5550A889B40B1EC9CC81E667		
14	Hongkong Post Root CA 3	Cross-certificate issued by GlobalSign root CA “GlobalSign Root CA - R3” and valid from 16 November 2022 to establish a trust relationship from Hongkong Post Root CA 3 to GlobalSign Root CA - R3
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 <u>SHA-1 Thumbprint</u> AFoF1F7AFBD02E3DDE39BD0B646CF97B7D122408 <u>SHA-256 Thumbprint</u> 00482341B104AoDE6EoF1D508DB84CB514F7494FE04982133A5C750136C55DC8		

Appendix D - List of HKPCA's Certification Practice Statements

Document Names	Version
CPS for e-Cert (Personal), e-Cert (Organisational) and e-Cert (Encipherment)	OID = 1.3.6.1.4.1.16030.1.1.49 (valid from 21 December 2023) OID = 1.3.6.1.4.1.16030.1.1.50 (valid from 15 March 2024) OID = 1.3.6.1.4.1.16030.1.1.51 (valid from 25 July 2024) OID = 1.3.6.1.4.1.16030.1.1.52 (valid from 28 August 2024) ^
CPS for e-Cert (Server)	OID = 1.3.6.1.4.1.16030.1.7.19 (valid from 21 December 2023) OID = 1.3.6.1.4.1.16030.1.7.20 (valid from 22 March 2024) OID = 1.3.6.1.4.1.16030.1.7.21 (valid from 25 July 2024) OID = 1.3.6.1.4.1.16030.1.7.22 (valid from 15 August 2024) ^
CPS for e-Cert (Organisational Role)	OID = 1.3.6.1.4.1.16030.1.3.15 (valid from 21 December 2023) OID = 1.3.6.1.4.1.16030.1.3.16 (valid from 25 July 2024) OID = 1.3.6.1.4.1.16030.1.3.17 (valid from 21 August 2024) ^
CPS for Bank-Cert (Personal), Bank-Cert (Corporate) and Bank-Cert (Bank)	OID = 1.3.6.1.4.1.16030.1.2.17 (valid from 1 December 2022) OID = 1.3.6.1.4.1.16030.1.2.18 (valid from 15 March 2024) OID = 1.3.6.1.4.1.16030.1.2.19 (valid from 25 July 2024) OID = 1.3.6.1.4.1.16030.1.2.20 (valid from 21 August 2024) ^
CPS for g-Cert (Individual) g-Cert (Functional Unit)	OID = 1.3.6.1.4.1.16030.1.8.10 (valid from 21 December 2023) OID = 1.3.6.1.4.1.16030.1.8.11 (valid from 25 July 2024) ^
CPS for iAM Smart-Cert	OID = 1.3.6.1.4.1.16030.1.9.2 (valid from 1 November 2022) OID = 1.3.6.1.4.1.16030.1.9.3 (valid from 11 July 2024) OID = 1.3.6.1.4.1.16030.1.9.4 (valid from 25 July 2024) ^

^ Latest CPS version

PricewaterhouseCoopers
22/F Prince's Building
Central
Hong Kong

24 February 2025

Dear Sirs,

**Assertion by Management as to the Disclosure of Business Practices and Controls
over the Hongkong Post Certification Authority Operations during the period from
1 January 2024 through 31 December 2024**

The Postmaster General operates the Certification Authority (“CA”) services known as Hongkong Post Certification Authority (“HKPCA”) through its Root CAs and Subordinate CAs referenced in Appendix A and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate validation
- Subscriber key generation and management
- Subordinate CA certification

The management of HKPCA with Certizen Limited (“Certizen”) as its agent is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its [website](#), CA business practice management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to HKPCA’s Certification Authority operations.

Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of HKPCA with Certizen as its agent has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in management's opinion, HKPCA with Certizen as its agent, in providing its CA services in the Hong Kong Special Administrative Region of the People's Republic of China, throughout the period from 1 January 2024 to 31 December 2024, HKPCA with Certizen as its agent has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statements (“CPS”) referenced in Appendix B,
- maintained effective controls to provide reasonable assurance that:
 - HKPCA provides its service in accordance with its CPS referenced in Appendix B,
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated (for the registration activities performed by HKPCA with Certizen as its agent); and
 - subordinate CA certificate requests are accurate, authenticated, and approved,
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity,

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (“CPS”)

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security

- Operations Management
- System Access Management
- System Development, Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

HKPCA makes use of external registration authorities for specific subscriber registration activities as disclosed in HKPCA's business practices. Accordingly, our assertion does not extend to the controls exercised by these external registration authorities.

HKPCA does not escrow its CA keys. Accordingly, our assertion does not extend to controls that would address those criteria.

The certificate for the Hongkong Post Root CA 1 (Appendix A Root CA #1) CA expired

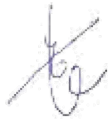
on 15 May 2023 and was not renewed.

HKPCA has disclosed five incidents (see Appendix C) during the period from 1 January 2024 to 31 December 2024. The remedial actions and the root causes of these incidents undertaken by HKPCA have been posted publicly in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum.

Yours faithfully,



(Lilian MAK)
for Postmaster General



(Eva CHAN)
for Certizen Limited

Appendix A

Full Name of CA:

Hongkong Post Certification Authority

List of HKPCA's Root CA:

Reference	Root CA Name	Remarks
1	Hongkong Post Root CA 1	Valid from 15 May 2003 and expired on 15 May 2023
<u>Subject DN</u> C=HK, O=Hongkong Post, CN=Hongkong Post Root CA 1 <u>SHA-1 Thumbprint</u> D6DAA8208D09D2154D24B52FCB346EB258B28A58 <u>SHA-256 Thumbprint</u> F9E67D336C51002AC054C632022D66DDA2E7E3FFF10AD061ED31D8BBB410C FB2		
2	Hongkong Post Root CA 2	Valid from 5 September 2015
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 2 <u>SHA-1 Thumbprint</u> DE010808E41EC41930D44095F8FE596B582C8CA2 <u>SHA-256 Thumbprint</u> 3945E08A8D4A0554B7605A7B355B10188E3EF842C76A805C54E3657C4D041AA A		
3	Hongkong Post Root CA 3	Valid from 3 June 2017
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 <u>SHA-1 Thumbprint</u> 58A2D0EC2052815BC1F3F86402244EC28E024B02 <u>SHA-256 Thumbprint</u> 5A2FC03F0C83B090BBFA40604B0988446C7636183DF9846E17101A447FB8EFD6		

List of HKPCA's Subordinate CA:

Reference	Subordinate CA Name	Remarks
1	Hongkong Post e-Cert CA 1 - 10	Revoked on 9 January 2010
<u>Subject DN</u> C=HK, O=Hongkong Post, CN=Hongkong Post e-Cert CA 1 - 10 <u>SHA-1 Thumbprint</u> 8E7DC57B719EF6EDAFE371DC932E3BD7DA86C27A <u>SHA-256 Thumbprint</u> 44E24932FB1CD30DD94B20C2F0F3B7B9EB33B5C3BFC9344BC47A5167BFBD2A13		
2	Hongkong Post e-Cert CA 1 - 10	Issuance of SSL subscriber certificate was terminated from 1 January 2016 and expired on 15 May 2023
<u>Subject DN</u> C=HK, O=Hongkong Post, CN=Hongkong Post e-Cert CA 1 - 10 <u>SHA-1 Thumbprint</u> 3C8C897A8067713565626201E9EB20262E1D58CB <u>SHA-256 Thumbprint</u> 5274CC53BC061F9F984430F401A9D3BA35A20CEEBC8E8E6DFA71B269A7C640D2		
3	Hongkong Post e-Cert CA 1 - 14	Issuance of SSL subscriber certificate was terminated from 1 September 2016 and expired on 15 May 2023
<u>Subject DN</u> C=HK, O=Hongkong Post, CN=Hongkong Post e-Cert CA 1 - 14 <u>SHA-1 Thumbprint</u> 7DE6BE6FD505A861C3C81C7F1D467315C664A928 <u>SHA-256 Thumbprint</u> 14422A1BD5A91EDBA7397B8698922369B6AF6984FF87ACF6139DAA919E795A14		

4	Hongkong Post e-Cert CA 1 - 15	Issuance of SSL subscriber certificate was terminated from 1 July 2019 and expired on 15 May 2023
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 1 - 15</p> <p><u>SHA-1 Thumbprint</u> A19DF5F1BFB89686AF985667C4F80E8A09DDFD36</p> <p><u>SHA-256 Thumbprint</u> 5CB9E9DE32B187E40BA14FDF200FDA62C7B4FBF88D64F77CE02DD6EBE6BC C1B0</p>		
5	Hongkong Post e-Cert CA 2 - 15	Valid from 5 September 2015
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 2 - 15</p> <p><u>SHA-1 Thumbprint</u> 893FF8AFFC3738A49816EE0D134C9929E55BF747</p> <p><u>SHA-256 Thumbprint</u> 3271139D13EFEF47B348CD2436CE43A02E9B77E1D99318A3B9C751FC937F6230</p>		
6	Hongkong Post e-Cert CA 2 - 17	Valid from 12 August 2017
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 2 - 17</p> <p><u>SHA-1 Thumbprint</u> 8745EFD6FE96260F27014CCE8C8B98E7882A89B50</p> <p><u>SHA-256 Thumbprint</u> CBB56EAEFD6FECDE2408F2F9CE8C324CDDBD3D967A5D76A9A22E81FF89B516AF</p>		
7	Hongkong Post e-Cert CA 2 - 19	Valid from 29 July 2019
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 2 - 19</p> <p><u>SHA-1 Thumbprint</u> FA3E35B01455216190505b21f14D7A97CAAE413</p> <p><u>SHA-256 Thumbprint</u> 5BFF0E9BCE3B75D36EA46E0746174C034885606CBE46228ED0AE9E5782583FB2</p>		

8	Hongkong Post e-Cert SSL CA 3 - 17	Valid from 3 June 2017 for issuance of non-EV SSL certificate
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert SSL CA 3 - 17</p> <p><u>SHA-1 Thumbprint</u> 92797871DC6A0B6EE1417BB657D7ED6FC6F975EB</p> <p><u>SHA-256 Thumbprint</u> 69ECDBC3147F581DFDCB522D9DEFB260B26784AD4955C74E6A52522CCC4C4408</p>		
9	Hongkong Post e-Cert EV SSL CA 3 - 17	Valid from 3 June 2017 for issuance of EV SSL certificate
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert EV SSL CA 3 - 17</p> <p><u>SHA-1 Thumbprint</u> 6CA9BB1B3BAEF67D6D5414132A7EFB212836639E</p> <p><u>SHA-256 Thumbprint</u> C18D53BF9864DD09BCBCACFD672E2566D4C81F6889E36DF5DD425C04211D0763</p>		
10	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 12 August 2017
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> D0D535192598FCA8B68789EDCEF1EA51B3A898A5</p> <p><u>SHA-256 Thumbprint</u> ABFA404ECEEA854381ABE294AC829440E0133E077911A67E1293CF111AC43C44</p>		

11	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and valid from 12 August 2017 and expired on 15 May 2023
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> 97FC47E174E2AA5332321DCFF6077A19F04387F0</p> <p><u>SHA-256 Thumbprint</u> 176AEBF2972BD6F47179EDE3DE63848B1543B45AE2954BEA45185B152537B9C4</p>		
12	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 27 July 2022
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> 881700C3346CBA89A8C1C5C44A584A8441319944</p> <p><u>SHA-256 Thumbprint</u> F8F6037491861C069D3BB442B78A3DB4049EE7787B7C2841A7BA6966B5272F2C</p>		
13	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and valid from 27 July 2022 and expired on 15 May 2023
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> 3069BCFC8DD0AFBAABA5CA81D23CCC6413131F6F</p> <p><u>SHA-256 Thumbprint</u> 5544A24FEB21F681F1987D30E0AF5C49E9F9FFFD5550A889B40B1EC9CC81E667</p>		

14	Hongkong Post Root CA 3	Cross-certificate issued by GlobalSign root CA “GlobalSign Root CA - R3” and valid from 16 November 2022 to establish a trust relationship from Hongkong Post Root CA 3 to GlobalSign Root CA - R3
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> AF0F1F7AFBD02E3DDE39BD0B646CF97B7D122408</p> <p><u>SHA-256 Thumbprint</u> 00482341B104A0DE6E0F1D508DB84CB514F7494FE04982133A5C750136C55DC8</p>		

Appendix B

List of HKPCA's Certification Practice Statements:

Document Names	Version
CPS for e-Cert (Personal), e-Cert (Organisational) and e-Cert (Encipherment)	OID = 1.3.6.1.4.1.16030.1.1.49 (valid from 21 December 2023) OID = 1.3.6.1.4.1.16030.1.1.50 (valid from 15 March 2024) OID = 1.3.6.1.4.1.16030.1.1.51 (valid from 25 July 2024) OID = 1.3.6.1.4.1.16030.1.1.52 (valid from 28 August 2024) ^
CPS for e-Cert (Server)	OID = 1.3.6.1.4.1.16030.1.7.19 (valid from 21 December 2023) OID = 1.3.6.1.4.1.16030.1.7.20 (valid from 22 March 2024) OID = 1.3.6.1.4.1.16030.1.7.21 (valid from 25 July 2024) OID = 1.3.6.1.4.1.16030.1.7.22 (valid from 15 August 2024) ^
CPS for e-Cert (Organisational Role)	OID = 1.3.6.1.4.1.16030.1.3.15 (valid from 21 December 2023) OID = 1.3.6.1.4.1.16030.1.3.16 (valid from 25 July 2024) OID = 1.3.6.1.4.1.16030.1.3.17 (valid from 21 August 2024) ^
CPS for Bank-Cert (Personal), Bank-Cert (Corporate) and Bank-Cert (Bank)	OID = 1.3.6.1.4.1.16030.1.2.17 (valid from 1 December 2022) OID = 1.3.6.1.4.1.16030.1.2.18 (valid from 15 March 2024) OID = 1.3.6.1.4.1.16030.1.2.19 (valid from 25 July 2024) OID = 1.3.6.1.4.1.16030.1.2.20 (valid from 21 August 2024) ^
CPS for g-Cert (Individual) g-Cert (Functional Unit)	OID = 1.3.6.1.4.1.16030.1.8.10 (valid from 21 December 2023) OID = 1.3.6.1.4.1.16030.1.8.11 (valid from 25 July 2024) ^
CPS for iAM Smart-Cert	OID = 1.3.6.1.4.1.16030.1.9.2 (valid from 1 November 2022) OID = 1.3.6.1.4.1.16030.1.9.3 (valid from 11 July 2024) OID = 1.3.6.1.4.1.16030.1.9.4 (valid from 25 July 2024) ^

^ Latest CPS version

Appendix C

Publicly disclosed incidents

Bugzilla ID	Disclosure	Publicly Disclosed Link
1887888	Hongkong Post: Delayed revocation of TLS certificates with basicConstraints not marked as critical	Bugzilla Ticket Link
1887008	Hongkong Post: TLS certificates with basicConstraints not marked as critical	Bugzilla Ticket Link
1886722	Hongkong Post: Delayed response to CPR	Bugzilla Ticket Link
1886665	Hongkong Post: Delayed revocation of TLS certificates with Certificate Policies extension problem	Bugzilla Ticket Link
1886406	Hongkong Post: TLS certificates with Certificate Policies extension that does not assert http scheme	Bugzilla Ticket Link