

INDEPENDENT ASSURANCE REPORT

To the management of BEIJING CERTIFICATE AUTHORITY Co., Ltd. (“BJCA”):

We have been engaged, in a reasonable assurance engagement, to report on BJCA management’s assertion that for its Certification Authority (CA) operations at Beijing, China, as of 19 December 2019 for its CAs as enumerated in the Appendix of the management’s assertion, BJCA has:

- disclosed its Publicly Trusted Code Signing (“PT CS”) certificate life cycle management business practices in its:
 - [BJCA Global Certification Practice Statement v1.0.1](#); and
 - [BJCA Global Certificate Policy v1.0.1](#)including its commitment to provide PT CS certificates in conformity with the CA/Browser Forum Guidelines on the BJCA website, and provided such services in accordance with its disclosed practices
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - the integrity of keys and PT CS certificates it manages is established and protected throughout their lifecycles; and
 - PT CS subscriber information is properly authenticated for the registration activities performed by BJCA
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - requests for PT CS Timestamp Authority certificates are properly authenticated; and
 - certificates issued to PT CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum
- suitably designed, and placed into operation, controls to provide reasonable assurance that its PT CS Timestamp Authority is operated in conformity with CA/Browser Forum Guidelines

in accordance with the WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates – Version 1.0.1.

Certification authority’s responsibilities

BJCA’s management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates – Version 1.0.1.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* 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.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *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 procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- (1) obtaining an understanding of BJCA'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;
- (2) evaluating the suitability of the design of the controls; and
- (3) performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of BJCA's controls, individually or in the aggregate.

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

Suitability of controls

The suitability of the design of the controls at BJCA 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 suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

In our opinion, as of 19 December 2019, BJCA management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates - Version 1.0.1.

This report does not include any representation as to the quality of BJCA's services beyond those covered by the WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates - Version 1.0.1, nor the suitability of any of BJCA's services for any customer's intended purpose.

AKAM

Anthony Kam & Associates Ltd.

2105 Wing On Centre, 111 Connaught Road, Central, Hong Kong, China

19 December 2019



BJCA MANAGEMENT'S ASSERTION

BEIJING CERTIFICATE AUTHORITY Co., Ltd. ("BJCA") operates the Certification Authority (CA) services known as CAs in Appendix and provides Publicly Trusted Code Signing("PT CS") CA services.

The management of BJCA is responsible for establishing controls over its PT CS CA operations, including its PT CS CA business practices disclosure on its website, PT CS key lifecycle management controls, PT CS certificate lifecycle management, PT CS Timestamp Authority 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, controls placed into operation can only provide reasonable assurance with respect to BJCA's Certification Authority operations.

BJCA management has assessed its controls over its PT CS CA services. Based on that assessment, in providing its PT CS CA services at Beijing, China, as of 19 December 2019, BJCA has:

- disclosed its PT CS certificate lifecycle management business practices in its:
 - [BJCA Global Certification Practice Statement v1.0.1](#); and
 - [BJCA Global Certificate Policy v1.0.1](#),

including its commitment to provide PT CS certificates in conformity with the CA/Browser Forum Guidelines on the BJCA website, and provided such services in accordance with its disclosed practices

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - the integrity of keys and PT CS certificates it manages is established and protected throughout their lifecycles; and
 - PT CS subscriber information is properly authenticated for the registration activities performed by BJCA
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - requests for PT CS Timestamp Authority certificates are properly authenticated; and
 - certificates issued to PT CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum
- suitably designed, and placed into operation, controls to provide reasonable assurance that its PT CS Timestamp Authority is operated in conformity with CA/Browser Forum Guidelines

in accordance with the WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates – Version 1.0.1.

Mr. Xueyan Lin _____
CEO of BEIJING CERTIFICATE AUTHORITY Co., Ltd.
1501, No. 68 North Fourth Ring Road West, Haidian District, Beijing, China.



Appendix

The list of keys and certificates covered in the management's assertion is as follow:

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA1 Certificate Thumbprints	SHA256 Certificate Thumbprints	Certificate Signed by
CN = BJCA Global Root CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha256RSA	4096 bits	C5EFEDCCD8 8D21C648E4E 3D7142EA716 93E59801	D5EC8D7B4C BA79F4E7E8C B9D6BAE7783 1003216A	F3896F88FE7 COA882766A7 FA6AD2749FB 57A7F3E98FB 769C1FA7B09 C2C44D5AE	BJCA Global Root CA1
CN = BJCA EV Code Signing CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	42B1C3B38CC 8881366A44A F5A664359C9 BB35B0D	B4C6A05E0F6 46876C6E567 D3C3EE874D DD4A4411	B6352ACC11E CCCCFE449023 D88C3C03808 2DE78829CB7 C33DD5017FE 95852AECA	BJCA Global Root CA1
CN = BJCA Code Signing CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	0C4AEE56B17 C40E5271510 4FC71D1DE3F 0E5ED1D	CCC406B5CB CC3ECC73AC A5E8A1737A9 E0187739A	47D98649B0A BE9F8C8596B EBD95AF3316 300506E156C 1968E39C95A E83BD70D5	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	234C1318B9C D20E7DF1337 5CB49C609CA 4B1F2BE	64D1D686B88 A70B2784E43 F74172105AB 4053C2A	245B753A631 DD7A5A5B0D 3E6DFECA459 9C7A1C93D7 1CBA04ED7B C81D3986303 F	BJCA Global Root CA1
CN = BJCA Global Root CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha384ECDSA	384 bits	D24AB1517F0 6F0D1821F4E 6E5FAB83FC4 8D4B091	F42786EB6EB 86D88316702 FBBA66A4530 0AA7AA6	574DF6931E2 78039667B72 0AFDC1600FC 27EB66DD309 2979FB73856 487212882	BJCA Global Root CA2
CN = BJCA EV Code Signing CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	EFB3DD847B2 69B4439CF60 B3AB2B7937B F7B5836	6AEF6809948 41CAF84F1C8 9FBCDE33BD3 5FFE6EC	E97960A1A17 40CAD61D0E D6A5BDBE4E 946D11E6EBD B093D668AB9 BB004F78BB3	BJCA Global Root CA2
CN = BJCA Code Signing CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	1B0A1719C7D 94CE62343BB 49E4BA377CA 68916FB	C19E2F1F915 45CF2F9FFB9 97EDD7BE546 0BA031B	FC6C124D84F 7EDFF00F0EEF 6FE54E832114 A74D131E075 932A6FF03D6 E575AAB	BJCA Global Root CA2
CN = BJCA TimeStamp CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	F61EF80F24B8 785FD2D39FA 278A6D5803A 62EC83	A85F45588C2 B58D7F6F44C 2A60780A5C4 5195B89	353D175D25 D53E850FF33 6271E1A7C0D C072AF8E009 2BCAB6B9BC3 9E0FABAE09	BJCA Global Root CA2