

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 EV SSL 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 EV SSL 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 EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated for the registration activities performed by BJCA
- suitably designed, and placed into operation, controls to provide reasonable assurance that its EV SSL CA is operated in conformity with CA/Browser Forum Guidelines

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.8.

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 Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.8.

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 Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.8.

This report does not include any representation as to the quality of BJCA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.8., 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 Extended Validation SSL ("EV SSL") CA services.

The management of BJCA is responsible for establishing controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website, EV SSL key lifecycle management controls, EV SSL 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 EV SSL CA services. Based on that assessment, in providing its EV SSL CA services at Beijing, China, as of 19 December 2019, BJCA has:

- disclosed its EV SSL 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 EV SSL 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 EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated for the registration activities performed by BJCA
- suitably designed, and placed into operation, controls to provide reasonable assurance that its EV SSL CA is operated in conformity with CA/Browser Forum Guidelines

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.8.

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 C0A882766A7 FA6AD2749FB 57A7F3E98FB 769C1FA7B09 C2C44D5AE	BJCA Global Root CA1
CN = BJCA EV SSL CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	B8D0A92CC1 D098F5B5E59 AB48344333C 5DC68EBB	6C8C0FE05B0 7DF3EC60248 A44EF5B0786 3D38CB2	115A2A45DB5 20361A2CDF0 A395C4A4BD 8A18902EAA4 036792825F8 46BBB76917	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 SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	279D5CC4300 03053399649 97CFDE6F7A9 6EFA787	92537777459 9ACA7417523 DB15E8A5E5E C30E6C2	E6014777053 41270FD1200 66BBDF26223 E6953C4DB8F A7EA197EAF5 BF8343B25	BJCA Global Root CA2