AKAM
Anthony KAM
& associates ltd
certified public accountants
阙孝财会计师行有限公司
2105 Wing On Ctr, 111 Connaught Rd, HK
+852 2246 6888
info@akamcpa.com

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 business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - BJCA Global Certification Practice Statement v1.0.1; and
  - BJCA Global Certificate Policy v1.0.1
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - BJCA's Certification Practice Statement is consistent with its Certificate Policy; and
  - BJCA provides its services in accordance with its Certificate Policy and Certification Practice Statement
- suitably designed, and placed into operation, 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; and
  - subscriber information is properly authenticated for the registration activities performed by BJCA
- suitably designed, and placed into operation, 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.

BJCA does not escrow its CA keys and does not provide certificate suspension services. Accordingly, our procedures does not extend to controls that would address those criteria.

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 v2.2.

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

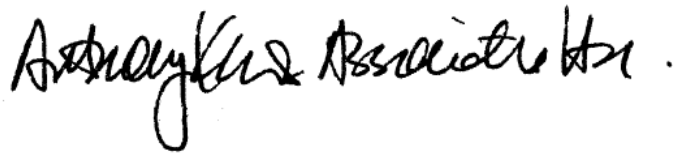
In our opinion, as of 19 December 2019, BJCA management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.

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 v2.2, 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 the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management

The management of BJCA is responsible for establishing controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, and 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 disclosures of its certificate practices and controls over its CA services. Based on that assessment, in BJCA management's opinion, in providing its CA services at Beijing, China, as of December 19, 2019, BJCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
    - BJCA Global Certification Practice Statement v1.0.1; and
    - BJCA Global Certificate Policy v1.0.1

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - BJCA's Certification Practice Statement is consistent with its Certificate Policy;
    - BJCA provides its services in accordance with its Certificate Policy and Certification Practice Statement

- suitably designed, and placed into operation, 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; and
    - subscriber information is properly authenticated for the registration activities performed by BJCA

- suitably designed, and placed into operation, 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 authorised and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2, including the following:

- CA Business Practices Management
  - Certificate Policy Management
  - Certification Practice Statement Management
  - CP and CPS Consistency
- CA Environmental Controls
  - Security Management
  - Asset Classification and Management
  - Personnel Security
  - Physical & Environmental Security
  - Operations Management
  - System Access Management
  - System Development and 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
  - Integrated Circuit Card (ICC) Lifecycle Management
  - Requirements for Subscriber Key Management Lifecycle Management Controls
- Certificate Lifecycle Management Controls
  - Subscriber Registration
  - Certificate Renewal
  - Certificate Rekey
  - Certificate Issuance
  - Certificate Distribution
  - Certificate Revocation
  - Certificate Validation

BJCA does not escrow its CA keys and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

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	C5EFEDCCD88D21C648E4E3D7142EA71693E59801	D5EC8D7B4CBA79F4E7E8CB9D6BAE77831003216A	F3896F88FE7C0A882766A7FA6AD2749FB57A7F3E98FB769C1FA7B09C2C44D5AE	BJCA Global Root CA1
CN = BJCA EV SSL CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	B8D0A92CC1D098F5B5E59AB48344333C5DC68EBB	6C8C0FE05B07DF3EC60248A44EF5B07863D38CB2	115A2A45DB520361A2CDF0A395C4A4BD8A18902EAA4036792825F846BBD76917	BJCA Global Root CA1
CN = BJCA OV SSL CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	979E3DDE6F6661DACF9B488980BE268DDD69CD7B	0A22BC3871D1402BDD48CDB0EA46969F3E40DCF1	0A6BC3E2024AC462F5D72BE436AE61D033978EA8DDB63D4C5D6214915E69049B	BJCA Global Root CA1
CN = BJCA IV SSL CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	DFBC24E9910BDD34AC2D20F394C6EE1B9B526036	19B542B7B97422418E28FAE255F98F9436EAE49B	D70C597009AF3A3A37BDFABEA0C64108C7B83CD6C2042E8FF178A3EE8FE0CAE8	BJCA Global Root CA1
CN = BJCA DV SSL CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	0DBC8F111BA0C205422C38A16A882C993AF231CF	70B2B43140A8209FE3686476E455482E5591FB30	B408D6C82097121694B9B6548C5B4944594C081134F36C5BE88D74FA34759D91	BJCA Global Root CA1
CN = BJCA EV Code Signing CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	42B1C3B38CC8881366A44AF5A664359C9BB35B0D	B4C6A05E0F646876C6E567D3C3EE874DDD4A4411	B6352ACC11ECCCFE449023D88C3C038082DE78829CB7C33DD5017FE95852AECA	BJCA Global Root CA1
CN = BJCA Code Signing CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	0C4AEE56B17C40E52715104FC71D1DE3F0E5ED1D	CCC406B5CBCC3ECC73ACA5E8A1737A9E0187739A	47D98649B0ABE9F8C8596BEBD95AF3316300506E156C1968E39C95AE83BD70D5	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	234C1318B9CD20E7DF13375CB49C609CA4B1F2BE	64D1D686B88A70B2784E43F74172105AB4053C2A	245B753A631DD7A5A5B0D3E6DFECA4599C7A1C93D71CBA04ED7BC81D3986303F	BJCA Global Root CA1

CN = BJCA Generic CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	BA6DE37E301FFBEF4147C92436694D4ED2709BCF	52FDCAACF3B8D86CD9A1720A929D6EAF5D2FF41F	19D0FE660DBC0FA948CF45918E48DEFB8396C4026903BC19FE4F91552DFF4DC9	BJCA Global Root CA1
CN = BJCA Global Root CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha384ECDSA	384 bits	D24AB1517F06F0D1821F4E6E5FAB83FC48D4B091	F42786EB6EB86D883167020AFDC1600FBBA66A45300AA7AA6	574DF6931E278039667B720AFDC1600FC27EB66DD3092979FB73856487212882	BJCA Global Root CA2
CN = BJCA EV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	279D5CC4300030533996499797CFDE6F7A96EFA787	92537777459 9ACA7417523DB15E8A5E5EC30E6C2	E601477705341270FD120066BBDF26223E6953C4DB8FA7EA197EAF5BF8343B25	BJCA Global Root CA2
CN = BJCA OV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	CA1C62CFE8150616C7FE01B45C210BEB3B92E3E8	387EBE6C0015EA74B9EF42694C9EBB617E971D61	3A1A4BD6A62468578DBC91DC24705B276A837CC18B6BEF1FF3F6ED0FE6326302	BJCA Global Root CA2
CN = BJCA IV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	6B39D730F3D8570AA47F746D8699BF378212F0E3	07C381DFC16F3CC389F4628302E64BADC4112C33	2F9F41114DCADC30784E40FEF7D6EE063A9BE7A363DE5737E88FA1118671505E	BJCA Global Root CA2
CN = BJCA DV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	DE37D665C8FCAF8063B2B9726B06E75E1537A25D	BA0866235B8CA2DAE7E56495DEB0664BB67ADDAC	3F5CB1531CB1223AABFB70872DC43D2DD6CC3D2823E96B458A9F8A7EC0265946	BJCA Global Root CA2
CN = BJCA EV Code Signing CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	EFB3DD847B269B4439CF60B3AB2B7937BF7B5836	6AEF680994841CAF84F1C89FBCDE33BD35FFE6EC	E97960A1A1740CAD61D0ED6A5BDBE4E946D11E6EBDB093D668AB9BB004F78BB3	BJCA Global Root CA2
CN = BJCA Code Signing CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	1B0A1719C7D94CE62343BB49E4BA377CA68916FB	C19E2F1F91545CF2F9FFB997EDD7BE5460BA031B	FC6C124D84F7EDFF00F0EEF6FE54E832114A74D131E075932A6FF03D6E575AAB	BJCA Global Root CA2
CN = BJCA TimeStamp CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	F61EF80F24B8785FD2D39FA278A6D5803A62EC83	A85F45588C2B58D7F6F44C2A60780A5C45195B89	353D175D25D53E850FF336271E1A7C0DC072AF8E0092BCAB6B9BC39E0FABAE09	BJCA Global Root CA2

CN = BJCA Generic CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	E3E3802981D2E3E845B7F7DDF8E344C02B4E203E	B5039623282F5FCA39D83D500A51A11EBB54EEAB	B4CDCF2F4A1141CFE604F7D50627C96F882AAB95C1D3B7A4ABB24615DB157D17	BJCA Global Root CA2
CN = BJCA Global Root CA3 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha256RSA	4096 bits	746FBA42408008EA5D266E968ADDBF840583D2DF	3ECFEB8B92CFDCC7F3502E11887C065AD46BE798	AAA048773350488832AABDA6954B33EE28BB2773DD851AB3C4F6F1D2F9F3777B	BJCA Global Root CA3
CN = BJCA DocSign CA3 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	C388C0F97985D4883F9F99C5CE541371A89D5FD0	57ED82AF3348C76BF1363575DE45F32E92872704	20F06D387FB129121713B4EF93A82A436FD9E615233A3C444891CDACB95D5EC7	BJCA Global Root CA3