AKAM

2105 Wing On Ctr, 111 Connaught Rd, HK

Anthony KAM
& associates ltd
certified public accountants
阚孝财会计师行有限公司

+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 locations as enumerated in Appendix C, throughout the period 10 March 2023 to 9 March 2024 for its CAs as enumerated in Appendix A, BJCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B

- maintained effective 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

- 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; and
  - subscriber information is properly authenticated

- 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.

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 v2.2.2.

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) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

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

Relative effectiveness of controls

The relative effectiveness and significance of specific 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 effectiveness of 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, throughout the period 10 March 2023 to 9 March 2024, 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 v2.2.2.

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 v2.2.2, nor the suitability of any of BJCA's services for any customer's intended purpose.

Use of the WebTrust seal

BJCA'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.

AKAM
Anthony Kam & Associates Ltd.
2105 Wing On Ctr, 111 Connaught Road, HK SAR, China

9 May 2024

Anthony Kam & Associates Ltd.

Appendix A

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 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 Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	642C5F6D522989CC0E6A34B7EEF782CD5156927D	73CFC180589F52980B5265F42CE609B472A16705	9677A7E2ACB3F5BA75AD9BCEE3C18A4C484DAF891B817F0AC713923E4337EA56	BJCA Global Root CA1
CN = BJCA EV Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	033DCCDFE4404249018EE1CEB18310A4386F8959	9B8D97697868141938D1AA5F189AF6344BB5F118	418D2B75C8B44B3A20FC93F55D7006158CC8C0F1A9C1A8C5E8C902AACF36B308	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	BB4F167A2058F9AC81D1A40E557AC1D488121EBC	BFEFB8E857E51A7D53AC4B0CB230D2507BB9224C	64FF2BFC836D5980F58605FD80029F499B805610E10467B9DCCC0D327E0AF561	BJCA Global Root CA1
CN = BJCA Global Root CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha384ECDSA	384 bits	D24AB1517F06F0D1821F4E6E5FAB83FC48D4B091	F42786EB6EB86D88316702FBBA66A45300AA7AA6	574DF6931E278039667B720AFDC1600FC27EB66DD3092979FB73856487212882	BJCA Global Root CA2

CN = BJCA EV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	279D5CC43000305339964997CFDE6F7A96EFA787	925377774599ACA7417523DB15E8A5E5EC30E6C2	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 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

CN = BJCA TimeStamp CA3 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 Bits	CC6510A42D4051CC2592F4B5603C7387B357C86B	858802F88DC692BDA15D814ACBA604A565B6B3E5	FD225061F3DAECB3A9EA149D60AF9AC8947EF398AA2433227003170B7BD48455	BJCA Global Root CA3
CN = BJCA Global Root CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	SM3WithSM2	256 Bits	6F40AC08D2DF5FBAF614A0CDBD6855AA890238E7	5860EE6465E8FD28DD37245028AA27B99FCD9F64	AA486528A63D0017D2C7077B567FC2875B4BB266783CD8A58B726F9AC297201F	BJCA Global Root CA4
CN = BJCA EV SSL CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	614DC72F2D5C02F77F7E48BABC27DF560202E866	EEF2D3D6D5503BE2248BC715AFD15EB05C547272	8109F5D475FDD4FE0D82D638CFDAF7FB06D98CF0EF367374FC2D239C0EDC60FD	BJCA Global Root CA4
CN = BJCA SSL CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	2B72EBA676D6E9BAC6EDE4669149C421C94C5A26	786B502AAE7FEB8EE06AE83FC0BED3686C808FE5	B66617BEA8B9ED4D202B0C66585F2F6BF6CA49420253B24EA50D0A7206AA53A1	BJCA Global Root CA4
CN = BJCA EV Code Signing CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	563EA4B9A416675F348FC13CC16DECA8FEF15B80	8BC104AA61EC71D23054049987C1F60BF07C2F3F	740C7A3532D3DCB68D92504F9A2F22FF22F0356B43CA40C3BD17B7F72CB4AD0C	BJCA Global Root CA4

CN = BJCA Code Signing CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	DF761348EB2F4B1D1C9813E6058D45E9B963CFE6	08DEF2549B201B111D20810B1C1804329888F68A	3E9C87D3B6106A48B785856473C0F69554CCB99F888EF99995A91797F84AE6BA	BJCA Global Root CA4
CN = BJCA TimeStamp CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	055D6EBF9057E9F2647044A89B28BDD5854AAA4A	8661CEC355A7AAE0A20ADCE380678FAF93798A69	A7AF1DF1294C3895AF434AE0F0CFC6CBDDEE76FEDC80C5AA14289E410D6C48BD	BJCA Global Root CA4
CN = BJCA Generic CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	90756CD78B5AFD1CDD9E737DEF9DA971EC235DAC	0ED7B0FD27D88855D85CA3545F87605BE3DF409C	A605330C3FB5C0EAC3D67EF4D87819280B8BC11220FDF4659708C64B45ED4551	BJCA Global Root CA4
CN = BJCA DocSign CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	B481FE5D9E3C11F74A7E2FA1FB24C9C59C99B240	C59E85D3B56A92F31062D7FFAECE5DB05E60E229	F339C5073B4F523350B3BA04ACFB099EFE3229F80DDA8085D7A30B63615349C6	BJCA Global Root CA4

Appendix B

Applicable versions of Certification Practice Statement (CPS) and Certificate Policy (CP) in-scope:

Name	Version	Date
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.9	1 March 2024
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.8	13 September 2023
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.7	10 August 2023
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.6	25 July 2022
Beijing Certificate Authority Co., Ltd. SM2 Global-Trust System Certification Practice Statement	1.0.6	1 March 2024
Beijing Certificate Authority Co., Ltd. SM2 Global-Trust System Certification Practice Statement	1.0.5	23 February 2023
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.9	1 March 2024
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.8	13 September 2023
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.7	10 August 2023
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.6	25 July 2022
Beijing Certificate Authority Co., Ltd. SM2 Global-Trust System Certificate Policy	1.0.6	1 March 2024
Beijing Certificate Authority Co., Ltd. SM2 Global-Trust System Certificate Policy	1.0.5	23 February 2023

Appendix C

Locations in-scope:

Location	Function
Beijing (North), China	Datacenter Facility, Administration and Support
Beijing (South), China	Datacenter Facility

BJCA MANAGEMENT'S ASSERTION

BEIJING CERTIFICATE AUTHORITY Co., Ltd. ("BJCA") operates the Certification Authority (CA) services known as CAs in Appendix A, 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 and maintaining effective 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, even effective controls can only provide reasonable assurance with respect to BJCA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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 Certification Authority (CA) services at locations as enumerated in Appendix C, throughout the period 10 March 2023 to 9 March 2024, BJCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B

- maintained effective controls to provide reasonable assurance that:
    - BJCA's applicable versions of Certification Practice Statement are consistent with its applicable versions of Certificate Policy; and
    - BJCA provides its services in accordance with its Certificate Policy and Certification Practice Statement
- 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; and
    - subscriber information is properly authenticated
- 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 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 v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

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

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.

林雪焰

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

9 May 2024

北京数字认证股份有限公司
100000047850

Appendix A

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 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 Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	642C5F6D522989CC0E6A34B7EEF782CD5156927D	73CFC180589F52980B5265F42CE609B472A16705	9677A7E2ACB3F5BA75AD9BCEE3C18A4C484DAF891B817F0AC713923E4337EA56	BJCA Global Root CA1
CN = BJCA EV Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	033DCCDFE4404249018EE1CEB18310A4386F8959	9B8D97697868141938D1AA5F189AF6344BB5F118	418D2B75C8B44B3A20FC93F55D7006158CC8C0F1A9C1A8C5E8C902AACF36B308	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	BB4F167A2058F9AC81D1A40E557AC1D488121EBC	BFEFB8E857E51A7D53AC4B0CB230D2507BB9224C	64FF2BFC836D5980F58605FD80029F499B805610E10467B9DCCC0D327E0AF561	BJCA Global Root CA1
CN = BJCA Global Root CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha384ECDSA	384 bits	D24AB1517F06F0D1821F4E6E5FAB83FC48D4B091	F42786EB6EB86D88316702FBBA66A45300AA7AA6	574DF6931E278039667B720AFDC1600FC27EB66DD3092979FB73856487212882	BJCA Global Root CA2

CN = BJCA EV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	279D5CC4300030533996499 7CFDE6F7A96EFA787	925377774599ACA7417523DB15E8A5E5EC30E6C2	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 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

CN = BJCA TimeStamp CA3 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 Bits	CC6510A42D4051CC2592F4B5603C7387B357C86B	858802F88DC692BDA15D814ACBA604A565B6B3E5	FD225061F3DAECB3A9EA149D60AF9AC8947EF398AA2433227003170B7BD48455	BJCA Global Root CA3
CN = BJCA Global Root CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	SM3WithSM2	256 Bits	6F40AC08D2DF5FBAF614A0CDBD6855AA890238E7	5860EE6465E8FD28DD37245028AA27B99FCD9F64	AA486528A63D0017D2C7077B567FC2875B4BB266783CD8A58B726F9AC297201F	BJCA Global Root CA4
CN = BJCA EV SSL CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	614DC72F2D5C02F77F7E48BABC27DF560202E866	EEF2D3D6D5503BE2248BC715AFD15EB05C547272	8109F5D475FDD4FE0D82D638CFDAF7FB06D98CF0EF367374FC2D239C0EDC60FD	BJCA Global Root CA4
CN = BJCA SSL CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	2B72EBA676D6E9BAC6EDE4669149C421C94C5A26	786B502AAE7FEB8EE06AE83FC0BED3686C808FE5	B66617BEA8B9ED4D202B0C66585F2F6BF6CA49420253B24EA50D0A7206AA53A1	BJCA Global Root CA4
CN = BJCA EV Code Signing CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	563EA4B9A416675F348FC13CC16DECA8FEF15B80	8BC104AA61EC71D23054049987C1F60BF07C2F3F	740C7A3532D3DCB68D92504F9A2F22FF22F0356B43CA40C3BD17B7F72CB4AD0C	BJCA Global Root CA4
CN = BJCA Code Signing CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	DF761348EB2F4B1D1C9813E6058D45E9B963CFE6	08DEF2549B201B111D20810B1C1804329888F68A	3E9C87D3B6106A48B785856473C0F69554CCB99F888EF99995A91797F84AE6BA	BJCA Global Root CA4

CN = BJCA TimeStamp CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	055D6EBF9057E9F2647044A89B28BDD5854AAA4A	8661CEC355A7AAE0A20ADCE380678FAF93798A69	A7AF1DF1294C3895AF434AE0F0CFC6CBDDEE76FEDC80C5AA14289E410D6C48BD	BJCA Global Root CA4
CN = BJCA Generic CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	90756CD78B5AFD1CDD9E737DEF9DA971EC235DAC	0ED7B0FD27D88855D85CA3545F87605BE3DF409C	A605330C3FB5C0EAC3D67EF4D87819280B8BC11220FDF4659708C64B45ED4551	BJCA Global Root CA4
CN = BJCA DocSign CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	B481FE5D9E3C11F74A7E2FA1FB24C9C59C99B240	C59E85D3B56A92F31062D7FFAECE5DB05E60E229	F339C5073B4F523350B3BA04ACFB099EFE3229F80DDA8085D7A30B63615349C6	BJCA Global Root CA4

Appendix B

Applicable versions of Certification Practice Statement (CPS) and Certificate Policy (CP) in-scope:

Name	Version	Date
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.9	1 March 2024
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.8	13 September 2023
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.7	10 August 2023
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.6	25 July 2022
Beijing Certificate Authority Co., Ltd. SM2 Global-Trust System Certification Practice Statement	1.0.6	1 March 2024
Beijing Certificate Authority Co., Ltd. SM2 Global-Trust System Certification Practice Statement	1.0.5	23 February 2023
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.9	1 March 2024
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.8	13 September 2023
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.7	10 August 2023
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.6	25 July 2022
Beijing Certificate Authority Co., Ltd. SM2 Global-Trust System Certificate Policy	1.0.6	1 March 2024
Beijing Certificate Authority Co., Ltd. SM2 Global-Trust System Certificate Policy	1.0.5	23 February 2023

Appendix C

Locations in-scope:

Location	Function
Beijing (North), China	Datacenter Facility, Administration and Support
Beijing (South), China	Datacenter Facility

AKAM

Anthony KAM
& associates ltd
certified public accountants
阚孝财会计师行有限公司

2105 Wing On Ctr, 111 Connaught Rd, HK +852 2246 6888 info@akamcpa.com

独立鉴证报告

（注意：本中文报告只作参考。正文请参阅英文报告。）

致：北京数字认证股份有限公司管理阶层

我们接受委托，对附件表 A 的北京数字认证股份有限公司（以下简称“BJCA”）于 2023 年 3 月 10 日至 2024 年 3 月 9 日就 BJCA 在附件表 C 所列地点运营的电子认证服务其管理阶层认定执行了合理保证的鉴证业务。根据管理阶层认定，BJCA 已：

- 在附件表 B 列举的认证体系电子认证业务规则（CPS）和认证体系证书策略（CP）中披露了电子认证业务、密钥生命周期管理、证书生命周期管理，以及 CA 环境控制管理

- 通过有效控制机制，以提供以下合理保证：
  - BJCA 的 CPS 与 CP 相符；
  - BJCA 遵循 CP 和 CPS 提供电子认证服务

- 通过有效控制机制，以提供以下合理保证：
  - 有效维护所管理的密钥与证书在生命周期中的完整性；
  - 建立并保护所管理的订户密钥和订户证书在生命周期中的完整性；以及
  - 于 BJCA 所执行的注册操作恰当地鉴定证书申请者的信息

- 通过有效控制机制，以提供以下合理保证：
  - 对 CA 系统和数据的逻辑和物理访问仅限于授权的个人；
  - 保持密钥和证书管理操作的连续性；以及
  - CA 系统的开发，维护和操作得到适当的授权和执行，以维持 CA 系统的完整

以符合 WebTrust Principles and Criteria for Certification Authorities v2.2.2。

BJCA 未托管其私钥，亦未提供证书挂起服务。据此，我们的程序未延伸至相关标准的有关控制。

BJCA 的责任

BJCA 的管理层负责确保管理层认定，包括其陈述的客观性以及认定中描述的 BJCA 所提供的服务能够符合 WebTrust Principles and Criteria for Certification Authorities v2.2.2 的规定。

审计师的独立性和质量控制

我们保持独立性并遵守国际道德委员会针对会计人员发布的职业会计师道德准则（*Code of Ethics for Professional Accountants*）规定的道德要求，该准则是建立在正直、客观、专业能力和谨慎、保密和职业行为的基本原则之上。我们公司遵循国际标准要求的质量控制 1（*International Standard on Quality Control 1*），并据此维护全面的质量控制体系，包括符合道德要求、专业标准和适用法律法规要求的文件化的政策和程序。

审计师的责任

我们的职责是在执行鉴证工作的基础上对 BJCA 的管理层认定发表结论。我们根据国际审计与鉴证准则理事会发布的国际鉴证业务准则第 3000 号 *"历史财务信息审计或审阅以外的鉴证业务"* 的规定执行了鉴证工作。此准则要求我们计划并执行相应的审计程序以获取所有重大方面和对管理层认定的合理保证，包括：

(1) 了解 BJCA 密钥和证书生命周期管理及对密钥和证书完整性的控制措施，包括订户和依赖方信息的真实性和保密性，密钥和证书生命周期管理的连续性，以及系统开发、运维的完整性；
(2) 选择测试业务操作是否遵守了所披露的证书生命周期管理；
(3) 测试和评估控制活动执行的有效性；以及
(4) 执行其他我们认为必要的鉴证程序。

我们相信，我们获取的证据是充分、适当的，为发表鉴证结论提供了基础。

控制的有效性

BJCA 的内部控制的有效性和重要性，及其对用户及相关依赖方的控制风险评估所产生的影响，取决于控制间的相互作用以及其他存在于每个用户和相关依赖方的因素。我们并没有对用户和依赖方所负责的控制的有效性进行任何评估工作。

固有限制

由于内部控制体系本身的限制，BJCA 满足上述要求的能力可能会受到影响，例如：控制可能未达到预防、发现或纠正错误、舞弊、对系统或信息的未授权访问，或违反内外部制度或规定的要求。此外，风险的变化可能会影响本评估报告在将来时间的参考价值。

结论

我们认为，BJCA 于 2023 年 3 月 10 日至 2024 年 3 月 9 日期间的电子认证服务的管理层认定在所有重大方面符合 WebTrust Principles and Criteria for Certification Authorities v2.2.2。

本报告并不包括任何在 WebTrust Principles and Criteria for Certification Authorities v2.2.2 以外的质量标准声明，或对任何客户对 BJCA 服务的合适性声明。

对 Webtrust 标识的使用

在 BJCA 网站上的 WebTrust 电子认证标识是本报告内容的一种符号表示，它并不是为了也不应被认为是对本报告的更新或任何进一步的保证。

AKAM
Anthony Kam & Associates Ltd.
2105 Wing On Ctr, 111 Connaught Road, HK SAR, China

9 May 2024

Anthony Kam & Associates Ltd.

附件表 A

本认定报告内包括的密钥与证书列举如下:

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 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 Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	642C5F6D522989CC0E6A34B7EEF782CD5156927D	73CFC180589F52980B5265F42CE609B472A16705	9677A7E2ACB3F5BA75AD9BCEE3C18A4C484DAF891B817F0AC713923E4337EA56	BJCA Global Root CA1
CN = BJCA EV Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	033DCCDFE4404249018EE1CEB18310A4386F8959	9B8D97697868141938D1AA5F189AF6344BB5F118	418D2B75C8B44B3A20FC93F55D7006158CC8C0F1A9C1A8C5E8C902AACF36B308	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	BB4F167A2058F9AC81D1A40E557AC1D488121EBC	BFEFB8E857E51A7D53AC4B0CB230D2507BB9224C	64FF2BFC836D5980F58605FD80029F499B805610E10467B9DCCC0D327E0AF561	BJCA Global Root CA1
CN = BJCA Global Root CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha384ECDSA	384 bits	D24AB1517F06F0D1821F4E6E5FAB83FC48D4B091	F42786EB6EB86D88316702FBBA66A45300AA7AA6	574DF6931E278039667B720AFDC1600FC27EB66DD3092979FB73856487212882	BJCA Global Root CA2

CN = BJCA EV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	279D5CC4300030533996499 7CFDE6F7A96EFA787	925377774599ACA7417523DB15E8A5E5EC30E6C2	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 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

CN = BJCA TimeStamp CA3 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 Bits	CC6510A42D4051CC2592F4B5603C7387B357C86B	858802F88DC692BDA15D814ACBA604A565B6B3E5	FD225061F3DAECB3A9EA149D60AF9AC8947EF398AA2433227003170B7BD48455	BJCA Global Root CA3
CN = BJCA Global Root CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	SM3WithSM2	256 Bits	6F40AC08D2DF5FBAF614A0CDBD6855AA890238E7	5860EE6465E8FD28DD37245028AA27B99FCD9F64	AA486528A63D0017D2C7077B567FC2875B4BB266783CD8A58B726F9AC297201F	BJCA Global Root CA4
CN = BJCA EV SSL CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	614DC72F2D5C02F77F7E48BABC27DF560202E866	EEF2D3D6D5503BE2248BC715AFD15EB05C547272	8109F5D475FDD4FE0D82D638CFDAF7FB06D98CF0EF367374FC2D239C0EDC60FD	BJCA Global Root CA4
CN = BJCA SSL CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	2B72EBA676D6E9BAC6EDE4669149C421C94C5A26	786B502AAE7FEB8EE06AE83FC0BED3686C808FE5	B66617BEA8B9ED4D202B0C66585F2F6BF6CA49420253B24EA50D0A7206AA53A1	BJCA Global Root CA4
CN = BJCA EV Code Signing CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	563EA4B9A416675F348FC13CC16DECA8FEF15B80	8BC104AA61EC71D23054049987C1F60BF07C2F3F	740C7A3532D3DCB68D92504F9A2F22FF22F0356B43CA40C3BD17B7F72CB4AD0C	BJCA Global Root CA4

CN = BJCA Code Signing CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	DF761348EB2F4B1D1C9813E6058D45E9B963CFE6	08DEF2549B201B111D20810B1C1804329888F68A	3E9C87D3B6106A48B785856473C0F69554CCB99F888EF99995A91797F84AE6BA	BJCA Global Root CA4
CN = BJCA TimeStamp CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	055D6EBF9057E9F2647044A89B28BDD5854AAA4A	8661CEC355A7AAE0A20ADCE380678FAF93798A69	A7AF1DF1294C3895AF434AE0F0CFC6CBDDEE76FEDC80C5AA14289E410D6C48BD	BJCA Global Root CA4
CN = BJCA Generic CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	90756CD78B5AFD1CDD9E737DEF9DA971EC235DAC	0ED7B0FD27D88855D85CA3545F87605BE3DF409C	A605330C3FB5C0EAC3D67EF4D87819280B8BC11220FDF4659708C64B45ED4551	BJCA Global Root CA4
CN = BJCA DocSign CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	B481FE5D9E3C11F74A7E2FA1FB24C9C59C99B240	C59E85D3B56A92F31062D7FFAECE5DB05E60E229	F339C5073B4F523350B3BA04ACFB099EFE3229F80DDA8085D7A30B63615349C6	BJCA Global Root CA4

附件表B

范围内适用之CP/CPS版本:

名称	版本	发布日期
北京数字认证股份有限公司全球认证体系电子认证业务规则	1.0.9	2024年3月1日
北京数字认证股份有限公司全球认证体系电子认证业务规则	1.0.8	2023年9月13日
北京数字认证股份有限公司全球认证体系电子认证业务规则	1.0.7	2023年8月10日
北京数字认证股份有限公司全球认证体系电子认证业务规则	1.0.6	2022年7月25日
北京数字认证股份有限公司SM2全球信任体系电子认证业务规则	1.0.6	2024年3月1日
北京数字认证股份有限公司SM2全球信任体系电子认证业务规则	1.0.5	2023年2月23日
北京数字认证股份有限公司全球认证体系证书策略	1.0.9	2024年3月1日
北京数字认证股份有限公司全球认证体系证书策略	1.0.8	2023年9月13日
北京数字认证股份有限公司全球认证体系证书策略	1.0.7	2023年8月10日
北京数字认证股份有限公司全球认证体系证书策略	1.0.6	2022年7月25日
北京数字认证股份有限公司SM2全球信任体系证书策略	1.0.6	2024年3月1日
北京数字认证股份有限公司SM2全球信任体系证书策略	1.0.5	2023年2月23日

附件表 C

范围内地点:

地点	**功能**
中国北京 (北)	数据中心, 管理与支持
中国北京 (南)	数据中心

BJCA 电子认证服务的管理阶层认定报告

（本中文报告只作参考，正文请参阅英文报告）

北京数字认证股份有限公司（以下简称 “ BJCA” ）运营电子认证服务机构（以下简称“CA” ，附件表 A 列举了服务所包括的根证书和中级证书），并提供以下电子认证服务：

- 订户注册
- 证书更新
- 证书密钥更新
- 证书发布
- 证书分发
- 证书吊销
- 证书验证
- 订户密钥和证书管理

BJCA 的管理层负责针对 CA 服务建立并维护有效的控制，包括：CA 业务规则披露、CA 业务规则管理、CA 环境控制、CA 密钥生命周期管理、订户密钥生命周期管理、以及证书生命周期管理。这些控制包括监控机制及为纠正已识别的缺陷所采取的改进措施。

任何控制都有其固有限制，包括人为失误，以及规避或逾越控制的可能性。因此，即使有效的控制也仅能对 BJCA 运营的电子认证服务提供合理保证。此外，由于控制环境的变化，控制的有效性可能随时间而发生变化。

BJCA 管理层已对所提供的电子认证服务的业务规则披露及控制进行评估。基于此评估，BJCA 管理层认为，在 2023 年 3 月 10 日至 2024 年 3 月 9 日就 BJCA 在附件表 C 所列地点提供电子认证服务期间，BJCA 已：

- 在附件表 B 列举的北京数字认证股份有限公司认证体系电子认证业务规则（CPS）和北京数字认证股份有限公司认证体系证书策略（CP）中披露了电子认证业务、密钥生命周期管理、证书生命周期管理，以及 CA 环境控制管理

- 通过有效控制机制，以提供以下合理保证：
  - BJCA 的 CPS 与 CP 相符；以及

- BJCA 遵循 CP 和 CPS 提供电子认证服务；

- 通过有效控制机制，以提供以下合理保证：
  - 有效维护所管理的密钥与证书在生命周期中的完整性；
  - 建立并保护所管理的订户密钥和订户证书在生命周期中的完整性；以及
  - 于 BJCA 所执行的注册操作恰当地鉴定证书申请者的信息；

- 通过有效控制机制，以提供以下合理保证：
  - 对 CA 系统和数据的逻辑和物理访问仅限于授权的个人；
  - 保持密钥和证书管理操作的连续性；以及
  - CA 系统的开发，维护和操作得到适当的授权和执行，以维持 CA 系统的完整；

以符合 WebTrust Principles and Criteria for Certification Authorities v2.2.2，包括以下内容：

- **CA 业务规则披露**
  - 电子认证业务规则（CPS）
  - 证书策略（CP）

- **CA 业务规则管理**
  - 证书策略管理
  - 电子认证业务规则管理
  - CP 和 CPS 的一致性

- **CA 环境控制**
  - 安全管理
  - 资产分类与管理
  - 人员安全
  - 物理及环境安全
  - 运营管理
  - 系统访问管理
  - 系统开发与维护管理
  - 业务持续性管理
  - 监控与合规管理
  - 审计日志管理

- **CA 密钥生命周期管理**
  - CA 密钥生成
  - CA 密钥存储、备份和恢复
  - CA 公钥分发
  - CA 密钥使用
  - CA 密钥归档和销毁
  - CA 密钥泄露
  - CA 密码设备生命周期管理

- **订户密钥生命周期管理**
  - 订户密钥生成服务
  - 智能芯片卡生命周期管理
  - 订户密钥管理控制要求

- **证书生命周期管理**
  - 订户注册
  - 证书更新
  - 证书密钥更新
  - 证书发布
  - 证书分发
  - 证书吊销
  - 证书验证

BJCA 未托管其私钥，亦未提供证书挂起服务。因此，我们的认定报告未延伸至相关标准的有关控制。

总经理 林雪焰 林雪焰
北京数字认证股份有限公司
中国北京市海淀区北四环西路 68 号 1501 号
2024 年 5 月 9 日

证股份有限公司
110000004785

附件表 A

本认定报告内包括的密钥与证书列举如下:

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 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 Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	642C5F6D522989CC0E6A34B7EEF782CD5156927D	73CFC180589F52980B5265F42CE609B472A16705	9677A7E2ACB3F5BA75AD9BCEE3C18A4C484DAF891B817F0AC713923E4337EA56	BJCA Global Root CA1
CN = BJCA EV Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	033DCCDFE4404249018EE1CEB18310A4386F8959	9B8D97697868141938D1AA5F189AF6344BB5F118	418D2B75C8B44B3A20FC93F55D7006158CC8C0F1A9C1A8C5E8C902AACF36B308	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	BB4F167A2058F9AC81D1A40E557AC1D488121EBC	BFEFB8E857E51A7D53AC4B0CB230D2507BB9224C	64FF2BFC836D5980F58605FD80029F499B805610E10467B9DCCC0D327E0AF561	BJCA Global Root CA1
CN = BJCA Global Root CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha384ECDSA	384 bits	D24AB1517F06F0D1821F4E6E5FAB83FC48D4B091	F42786EB6EB86D88316702FBBA66A45300AA7AA6	574DF6931E278039667B720AFDC1600FC27EB66DD3092979FB73856487212882	BJCA Global Root CA2

CN = BJCA EV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	279D5CC4300030533996499 7CFDE6F7A96EFA787	925377774599ACA7417523DB15E8A5E5EC30E6C2	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 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

CN = BJCA TimeStamp CA3 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 Bits	CC6510A42D4051CC2592F4B5603C7387B357C86B	858802F88DC692BDA15D814ACBA604A565B6B3E5	FD225061F3DAECB3A9EA149D60AF9AC8947EF398AA2433227003170B7BD48455	BJCA Global Root CA3
CN = BJCA Global Root CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	SM3WithSM2	256 Bits	6F40AC08D2DF5FBAF614A0CDBD6855AA890238E7	5860EE6465E8FD28DD37245028AA27B99FCD9F64	AA486528A63D0017D2C7077B567FC2875B4BB266783CD8A58B726F9AC297201F	BJCA Global Root CA4
CN = BJCA EV SSL CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	614DC72F2D5C02F77F7E48BABC27DF560202E866	EEF2D3D6D5503BE2248BC715AFD15EB05C547272	8109F5D475FDD4FE0D82D638CFDAF7FB06D98CF0EF367374FC2D239C0EDC60FD	BJCA Global Root CA4
CN = BJCA SSL CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	2B72EBA676D6E9BAC6EDE4669149C421C94C5A26	786B502AAE7FEB8EE06AE83FC0BED3686C808FE5	B66617BEA8B9ED4D202B0C66585F2F6BF6CA49420253B24EA50D0A7206AA53A1	BJCA Global Root CA4
CN = BJCA EV Code Signing CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	563EA4B9A416675F348FC13CC16DECA8FEF15B80	8BC104AA61EC71D23054049987C1F60BF07C2F3F	740C7A3532D3DCB68D92504F9A2F22FF22F0356B43CA40C3BD17B7F72CB4AD0C	BJCA Global Root CA4
CN = BJCA Code Signing CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	DF761348EB2F4B1D1C9813E6058D45E9B963CFE6	08DEF2549B201B111D20810B1C1804329888F68A	3E9C87D3B6106A48B785856473C0F69554CCB99F888EF99995A91797F84AE6BA	BJCA Global Root CA4

CN = BJCA TimeStamp CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	055D6EBF9057E9F2647044A89B28BDD5854AAA4A	8661CEC355A7AAE0A20ADCE380678FAF93798A69	A7AF1DF1294C3895AF434AE0F0CFC6CBDDEE76FEDC80C5AA14289E410D6C48BD	BJCA Global Root CA4
CN = BJCA Generic CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	90756CD78B5AFD1CDD9E737DEF9DA971EC235DAC	0ED7B0FD27D88855D85CA3545F87605BE3DF409C	A605330C3FB5C0EAC3D67EF4D87819280B8BC11220FDF4659708C64B45ED4551	BJCA Global Root CA4
CN = BJCA DocSign CA4 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	SM3WithSM2	256 Bits	B481FE5D9E3C11F74A7E2FA1FB24C9C59C99B240	C59E85D3B56A92F31062D7FFAECE5DB05E60E229	F339C5073B4F523350B3BA04ACFB099EFE3229F80DDA8085D7A30B63615349C6	BJCA Global Root CA4

附件表 B

适用范围内的电子认证业务规则（CPS）和证书政策（CP）版本:

名称	版本	发布日期
北京数字认证股份有限公司全球认证体系电子认证业务规则	1.0.9	2024年3月1日
北京数字认证股份有限公司全球认证体系电子认证业务规则	1.0.8	2023年9月13日
北京数字认证股份有限公司全球认证体系电子认证业务规则	1.0.7	2023年8月10日
北京数字认证股份有限公司全球认证体系电子认证业务规则	1.0.6	2022年7月25日
北京数字认证股份有限公司SM2全球信任体系电子认证业务规则	1.0.6	2024年3月1日
北京数字认证股份有限公司SM2全球信任体系电子认证业务规则	1.0.5	2023年2月23日
北京数字认证股份有限公司全球认证体系证书策略	1.0.9	2024年3月1日
北京数字认证股份有限公司全球认证体系证书策略	1.0.8	2023年9月13日
北京数字认证股份有限公司全球认证体系证书策略	1.0.7	2023年8月10日
北京数字认证股份有限公司全球认证体系证书策略	1.0.6	2022年7月25日
北京数字认证股份有限公司SM2全球信任体系证书策略	1.0.6	2024年3月1日
北京数字认证股份有限公司SM2全球信任体系证书策略	1.0.5	2023年2月23日

附件表 C

范围内地点:

地点	**功能**
中国北京 (北)	数据中心, 管理与支持
中国北京 (南)	数据中心