



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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 2024 to 9 March 2025 for its CAs as enumerated in Appendix A, BJCA has:

- disclosed its SSL certificate life cycle management business practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the BJCA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
 - SSL certificate 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 – SSL Baseline v2.8](#).

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 – SSL Baseline v2.8](#).

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.



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* 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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of BJCA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- (2) selectively testing transactions executed in accordance with disclosed SSL 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 2024 to 9 March 2025, 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 – SSL Baseline v2.8](#).

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 – SSL Baseline v2.8](#), nor the suitability of any of BJCA's services for any customer's intended purpose.



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

Use of the WebTrust seal

BJCA's use of the WebTrust for Certification Authorities – SSL Baseline 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.



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL

20 May 2025

DFK INTERNATIONAL



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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	D5EC8D7B4CB0A882766A7FA79F4E7E8CB9D6BAE77831003216A	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	979E3DDE6F6661DACF9B488980BE268DD69CD7B	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



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

CN = BJCA Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	642C5F6D522 989CC0E6A34 B7EEF782CD5 156927D	73CFC180589F 52980B5265F4 2CE609B472A 16705	9677A7E2ACB 3F5BA75AD9B CEE3C18A4C4 84DAF891B81 7F0AC713923 E4337EA56	BJCA Global Root CA1
CN = BJCA EV Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	033DCCDFE44 04249018EE1C EB18310A438 6F8959	9B8D9769786 8141938D1AA 5F189AF6344B B5F118	418D2B75C8B 44B3A20FC93 F55D7006158 CC8C0F1A9C1 A8C5E8C902A ACF36B308	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	BB4F167A205 8F9AC81D1A4 0E557AC1D48 8121EBC	BFEFB8E857E5 1A7D53AC4B0 CB230D2507B B9224C	64FF2BFC836 D5980F58605F D80029F499B 805610E10467 B9DCCC0D32 7E0AF561	BJCA Global Root CA1
CN = BJCA Global Root CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha384ECDSA	384 bits	D24AB1517F0 6F0D1821F4E6 E5FAB83FC48 D4B091	F42786EB6EB8 6D88316702F BBA66A45300 AA7AA6	574DF6931E2 78039667B720 AFDC1600FC2 7EB66DD3092 979FB7385648 7212882	BJCA Global Root CA2
CN = BJCA EV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	279D5CC4300 030533996499 7CFDE6F7A96 EFA787	925377774599 ACA7417523D B15E8A5E5EC 30E6C2	E60147770534 1270FD12006 68BDF26223E 6953C4DB8FA 7EA197EAF5B	BJCA Global Root CA2
CN = BJCA OV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	CA1C62CFE81 50616C7FE01B 45C2108EB3B 92E3E8	387EBE6C0015 EA74B9EF4269 4C9EBB617E9 71D61	3A1A4BD6A62 468578DBC91 DC24705B276 A837CC18B6B EF1FF3F6ED0F E6326302	BJCA Global Root CA2
CN = BJCA IV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	6B39D730F3D 8570AA47F74 6D8699BF378 212F0E3	07C381DFC16 F3CC389F4628 302E64BADCA 112C33	2F9F41114DC ADC30784E40 FEF7D6EE063 A9BE7A363DE 5737E88FA111 8671505E	BJCA Global Root CA2
CN = BJCA DV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	DE37D665C8F CAF8063B2B9 726B06E75E15 37A25D	BA0866235B8 CA2DAE7E564 95DEB0664BB 67ADDAC	3F5CB1531CB 1223AABFB70 872DC43D2D D6CC3D2823E 96B458A9F8A 7EC0265946	BJCA Global Root CA2



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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	1.0.11	3 March 2025
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.10	27 August 2024
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.9	1 March 2024
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.11	3 March 2025
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.10	27 August 2024
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.9	1 March 2024



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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.

The management of BJCA is responsible for establishing and maintaining effective controls over its SSL CA operations, its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and 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, 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 CA services at locations as enumerated in Appendix C, throughout the period 10 March 2024 to 9 March 2025, BJCA has:

- disclosed its SSL certificate life cycle management business practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the BJCA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
 - SSL certificate subscriber information is properly authenticated (for the registration activities performed by BJCA)
- 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 – SSL Baseline – v2.8](#).

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

20 May 2025



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	C5EFEDCCD88 D21C648E4E3 D7142EA7169 3E59801	D5EC8D7B4CB A79F4E7E8CB 9D6BAE77831 003216A	F3896F88FE7C 0A882766A7F A6AD2749FB5 7A7F3E98FB76 9C1FA7B09C2 C44D5AE	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 A395C4A4BD8 A18902EAA40 36792825F846 BBD76917	BJCA Global Root CA1
CN = BJCA OV SSL CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	979E3DDE6F6 661DACF9B48 8980BE268DD D69CD7B	0A22BC3871D 1402BDD48CD B0EA46969F3E 40DCF1	0A6BC3E2024 AC462F5D72B E436AE61D03 3978EA8DDB6 3D4C5D62149 15E69049B	BJCA Global Root CA1
CN = BJCA IV SSL CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	DFBC24E9910 BDD34AC2D2 0F394C6EE1B9 B526036	19B542B7B97 422418E28FAE 255F98F9436E AE49B	D70C597009A F3A3A37BDFA BEA0C64108C 7B83CD6C204 2E8FF178A3EE 8FE0CAE8	BJCA Global Root CA1
CN = BJCA DV SSL CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	0DBC8F111BA 0C205422C38 A16A882C993 AF231CF	70B2B43140A 8209FE368647 6E455482E559 1FB30	B408D6C8209 7121694B9B65 48C5B494459 4C081134F36 C5BE88D74FA 34759D91	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	234C1318B9C D20E7DF1337 5CB49C609CA 4B1F2BE	64D1D686B88 A70B2784E43F 74172105AB4 053C2A	245B753A631 DD7A5A5B0D 3E6DFECA459 9C7A1C93D71 CBA04ED7BC8 1D3986303F	BJCA Global Root CA1
CN = BJCA Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	642C5F6D522 989CC0E6A34 B7EEF782CD5 156927D	73CFC180589F 52980B5265F4 2CE609B472A 16705	9677A7E2ACB 3F5BA75AD9B CEE3C18A4C4 84DAF891B81 7F0AC713923 E4337EA56	BJCA Global Root CA1

CN = BJCA EV Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	033DCCDFE449B8D9769786 04249018EE1C8141938D1AA EB18310A4385F189AF6344B 6F8959B5F118	418D2B75C8B 44B3A20FC93 F55D7006158 CC8C0F1A9C1 A8C5E8C902A ACF36B308	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	BB4F167A205BFEB8E857E5 8F9AC81D1A41A7D53AC4B0 0E557AC1D48CB230D2507B 8121EBCB9224C	64FF2BFC836 D5980F58605F D80029F499B 805610E10467 B9DCCC0D32 7E0AF561	BJCA Global Root CA1
CN = BJCA Global Root CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha384ECDSA	384 bits	D24AB1517F0F42786EB6EB8 6F0D1821F4E66D88316702F E5FAB83FC48BBA66A45300 D4B091AA7AA6	574DF6931E2 78039667B720 AFDC1600FC2 7EB66DD3092 979FB7385648 7212882	BJCA Global Root CA2
CN = BJCA EV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	279D5CC4300925377774599 030533996499ACA7417523D 7CFDE6F7A96B15E8A5E5EC EFA78730E6C2	E60147770534 1270FD12006 6BBDF26223E 6953C4DB8FA 7EA197EAF5B F8343B25	BJCA Global Root CA2
CN = BJCA OV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	CA1C62CFE81387EBE6C0015 50616C7FE01BEA74B9EF4269 45C210BEB3B4C9EBB617E9 92E3E871D61	3A1A4BD6A62 468578DBC91 DC24705B276 A837CC18B6B EF1FF3F6ED0F E6326302	BJCA Global Root CA2
CN = BJCA IV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	6B39D730F3D07C381DFC16 8570AA47F74F3CC389F4628 6D8699BF378302E64BADCD 212F0E3112C33	2F9F41114DC ADC30784E40 FEF7D6EE063 A9BE7A363DE 5737E88FA111 8671505E	BJCA Global Root CA2
CN = BJCA DV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	DE37D665C8FBA0866235B8 CAF8063B2B9CA2DAE7E564 726B06E75E1595DEB0664BB 37A25D67ADDAC	3F5CB1531CB 1223AABFB70 872DC43D2D D6CC3D2823E 96B458A9F8A 7EC0265946	BJCA Global Root CA2

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	1.0.11	3 March 2025
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.10	27 August 2024
Beijing Certificate Authority Co., Ltd. Global Certification Practice Statement	1.0.9	1 March 2024
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.11	3 March 2025
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.10	27 August 2024
Beijing Certificate Authority Co., Ltd. Global Certificate Policy	1.0.9	1 March 2024



Appendix C

Locations in-scope:

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



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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 所列北京数字认证股份有限公司（以下简称“BJCA”）于 2024 年 3 月 10 日至 2025 年 3 月 9 日期间于附件表 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 SSL 证书生命周期业务规则，包括承诺遵循 CA/Browser 论坛的相关指引提供 SSL 证书服务，并依据披露的业务规则提供相关服务
- 通过有效控制机制，以提供以下合理保证：
 - 建立并保护所管理的密钥和 SSL 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 SSL 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 – SSL Baseline v2.8](#)。

BJCA 的责任

BJCA 的管理层负责确保管理阶层认定，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 – SSL Baseline v2.8](#) 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。本所采用国际质量管理标准 (ISQM) 1，即 *执行财务报表审计或审阅或其他保证或相关服务*



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

业务的公司的质量管理，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 SSL 证书生命周期管理，包括 SSL 证书发放、更新和吊销，并了解 BJCA 的网络和证书系统安全是否符合 CA/Browser 论坛的相应要求；
- (2) 选择测试业务操作是否遵守了所披露的 SSL 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 2024 年 3 月 10 日至 2025 年 3 月 9 日期间的电子认证服务的管理阶层认定在所有重大方面符合 [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline v2.8](#)。

本报告并不包括任何在 [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline v2.8](#) 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。



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

对 Webtrust 标识的使用

在 BJCA 网站上的 WebTrust SSL BR 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。



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL

20 May 2025

DFK INTERNATIONAL



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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	D5EC8D7B4CB0A882766A7FA79F4E7E8CB9D6BAE77831003216A	F3896F88FE7C0A882766A7FA6AD2749FB57A7F3E98FB769C1FA7B09C2C44D5AE	BJCA Global Root CA1
CN = BJCA EV SSL CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	B8D0A92CC1D098F5B5E59AB48344333C5DC68EBB	6C8C0FE05B07DF3EC60248A44EF5B07863D38CB2	115A2A45DB520361A2CDF0A395C4A48BD8A18902EAA4036792825F846BBD76917	BJCA Global Root CA1
CN = BJCA OV SSL CA1 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	2048 bits	979E3DDE6F6661DACF9B488980BE268DD69CD7B	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 Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	642C5F6D522989CC0E6A34B7EEF782CD5156927D	73CFC180589F52980B5265F42CE609B472A16705	9677A7E2ACB3F5BA75AD9BCEE3C18A4C484DAF891B817F0AC713923E4337EA56	BJCA Global Root CA1



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

CN = BJCA EV Code Signing CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	033DCCDFE449B8D9769786 04249018EE1C8141938D1AA EB18310A4385F189AF6344B 6F8959B5F118	418D2B75C8B 44B3A20FC93 F55D7006158 CC8C0F1A9C1 A8C5E8C902A ACF36B308	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	BB4F167A205BFEB8E857E5 8F9AC81D1A41A7D53AC4B0 0E557AC1D48CB230D2507B 8121EBCB9224C	64FF2BFC836 D5980F58605F D80029F499B 805610E10467 B9DCCC0D32 7E0AF561	BJCA Global Root CA1
CN = BJCA Global Root CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha384ECDSA	384 bits	D24AB1517F0F42786EB6EB8 6F0D1821F4E66D88316702F E5FAB83FC48BBA66A45300 D4B091AA7AA6	574DF6931E2 78039667B720 AFDC1600FC2 7EB66DD3092 979FB7385648 7212882	BJCA Global Root CA2
CN = BJCA EV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	279D5CC4300925377774599 030533996499ACA7417523D 7CFDE6F7A96B15E8A5E5EC EFA78730E6C2	E60147770534 1270FD12006 6B8DF26223E 6953C4DB8FA 7EA197EAF5B F8343B25	BJCA Global Root CA2
CN = BJCA OV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	CA1C62CFE81387EBE6C0015 50616C7FE01BEA74B9EF4269 45C2108EB3B4C9EBB617E9 92E3E871D61	3A1A4BD6A62 468578DBC91 DC24705B276 A837CC18B6B EF1FF3F6ED0F E6326302	BJCA Global Root CA2
CN = BJCA IV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	6B39D730F3D07C381DFC16 8570AA47F74F3CC389F4628 6D8699BF378302E64BAD4 212F0E3112C33	2F9F41114DC ADC30784E40 FEF7D6EE063 A9BE7A363DE 5737E88FA111 8671505E	BJCA Global Root CA2
CN = BJCA DV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	DE37D665C8FBA0866235B8 CAF8063B2B9CA2DAE7E564 726B06E75E1595DEB0664BB 37A25D67ADDAC	3F5CB1531CB 1223AABFB70 872DC43D2D D6CC3D2823E 96B458A9F8A 7EC0265946	BJCA Global Root CA2



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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	1.0.11	2025年3月3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	1.0.10	2024年8月27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	1.0.9	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	1.0.11	2025年3月3日
北京数字认证股份有限公司全球认证体系证书策略	1.0.10	2024年8月27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



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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 CA 所包括的根证书和中级证书)，并提供 SSL CA 电子认证服务。

BJCA 的管理阶层负责针对 SSL CA 服务建立并维护有效的控制，包括：SSL CA 业务规则披露、SSL CA 密钥生命周期管理和 SSL CA 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 2024 年 3 月 10 日至 2025 年 3 月 9 日就 BJCA 在附件表 C 所列地点提供 CA 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 SSL 证书生命周期业务规则，包括承诺遵循 CA/Browser 论坛的相关指引提供 SSL 证书服务，并依据披露的业务规则提供相关服务
- 通过有效控制机制，以提供以下合理保证：
 - 建立并保护所管理的密钥和订户 SSL 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 SSL 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 – SSL Baseline – v2.8](#)。

总经理 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
2025 年 5 月 20 日



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	D5EC8D7B4CB0A79F4E7E8CB9D6BAE77831003216A	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	979E3DDE6F6661DACF9B488980BE268DD69CD7B	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 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	033DCCDFE449B8D976978644B3A20FC9304249018EE1C8141938D1AAF55D7006158EB18310A4385F189AF6344BCC8C0F1A9C16F8959B5F118A8C5E8C902AACF36B308	BJCA Global Root CA1
CN = BJCA TimeStamp CA1 G2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256RSA	4096 bits	BB4F167A2058F9AC81D1A40E557AC1D488121EBC	BJCA Global Root CA1
CN = BJCA Global Root CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Root Key	sha384ECDSA	384 bits	D24AB1517F06F0D1821F4E6E5FAB83FC48D4B091	BJCA Global Root CA2
CN = BJCA EV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	279D5CC43000305339964997CFDE6F7A96EFA787	BJCA Global Root CA2
CN = BJCA OV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	CA1C62CFE8150616C7FE01B45C210BEB3B92E3E8	BJCA Global Root CA2
CN = BJCA IV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	6B39D730F3D8570AA47F746D8699BF378212F0E3	BJCA Global Root CA2
CN = BJCA DV SSL CA2 O = BEIJING CERTIFICATE AUTHORITY C = CN	Signing Key	sha256ECDSA	256 bits	DE37D665C8FCAF8063B2B9726B06E75E1537A25D	BJCA Global Root CA2

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	1.0.11	2025年3月3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	1.0.10	2024年8月27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	1.0.9	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	1.0.11	2025年3月3日
北京数字认证股份有限公司全球认证体系证书策略	1.0.10	2024年8月27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

附件表 C

范围内地点:

地点	功能
中国北京 (北)	数据中心, 管理支持
中国北京 (南)	数据中心