



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 Global Digital Cybersecurity Authority Co.,Ltd. ("GDCA"):

We have been engaged, in a reasonable assurance engagement, to report on GDCA management's assertion that for its Certification Authority ("CA") operations at locations as enumerated in Appendix C, throughout the period 1 March 2024 to 28 February 2025 for its CAs as enumerated in Appendix A, GDCA has:

- disclosed its Extended Validation SSL ("EV 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 EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the GDCA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL certificate subscriber information is properly authenticated

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

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

GDCA had disclosed an incident ([Bug 1888060](#)) on Mozilla's Bugzilla Platform on 26 March 2024. In the incident, GDCA had issued 20 SSL/TLS certificates from 15 September to 8 October 2023 with the Basic Constraints extension included but not set as Critical, the affected certificates including 12 OV certificates, 7 DV certificates, and 1 EV certificate. As of 5:10PM, 2 April 2024 (UTC+8), all these certificates had either been revoked or expired. After the mis-issuance, the cause analysis of the incident and the remediations conducted by GDCA have been illustrated in the process of public discussion. The matter on the public platform has been closed on 5 March 2025.

GDCA had disclosed an incident ([Bug 1889062](#)) on Mozilla's Bugzilla Platform on 2 April 2024. In the incident, As noted in [Bug 1888060](#), GDCA had issued 20 SSL/TLS certificates with Non-critical Basic Constraints extension from 15 September to 8 October 2023, and as of 5:10PM, 2 April 2024 (UTC+8), all the certificates had either been revoked or expired. There were 13 certificates which had not been revoked within 5 days since receiving the Certificate Problem Report, leading to a violation of Baseline Requirements 4.9.1.1. After the revocations delayed, the cause analysis of the derived incident and the remediations conducted by GDCA have been illustrated in the process of public discussion. The matter on the public platform has been closed on 2 April 2025.

Certification authority's responsibilities

GDCA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).



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

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 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 GDCA's EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
- (2) selectively testing transactions executed in accordance with disclosed EV 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 GDCA 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, GDCA'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 1 March 2024 to 28 February 2025, GDCA management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

This report does not include any representation as to the quality of GDCA's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#), nor the suitability of any of GDCA'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

GDCA's use of the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL 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 report is as follow:

Key Name	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = GDCA TrustAUTH R5 ROOT O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Root Key	sha256RSA	4096 bits	E2C9409F 4DCEE89A A17CCF0E 3F65C529 886A1951	BFFF8FD0443 3487D6A8AA6 0C1A29767A9 FC2BBB05E42 0F713A13B99 2891D3893	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 EV CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	686223D3 A9DFC522 D155654D 64762589 AAB6D074	882E0146D15 D3483EE5981 E35067F1449 E562B89E22E CC3FDF37274 EDD314CDA	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Extended Validation CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	686223D3 A9DFC522 D155654D 64762589 AAB6D074	BEC06F55344 C3DE4F12CD5 D808906CDE2 75234951BE0 176A787E628 E2BE7D51F	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A 2D739636 727D5D1E B6E28123 69CF68E4	051C238FAD7 C1DC0FCEB4A EF79CAE97FE 49A82DA8916 A4A0920F307 AACD60F81	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A 2D739636 727D5D1E B6E28123 69CF68E4	2F2F0088177 10A1085B4E6 BC5E3335474 444D983272E 33995A331BE 1A4C4FE0A	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 OV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5B BE7C08C6 AD04BB48 6145B0F5 6257A0B3	5600AFB6BAE 2A83B66B9CB BE9CEEC8F53 E26420A6993 9A48DCC6D56 B99790A63	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5B BE7C08C6 AD04BB48 6145B0F5 6257A0B3	1E96ABB2D65 02B5DCE518E C00B5A1E543 349EFD2E3F6 8BE9ABC1128 B256FEDD7	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 DV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	7313CE83 C60C2AA0 2692AE3F 7B4074B5 300B3595	74468180CE5 64BAD7E8122 10AF743E85C A96CBA44CF5 851FA000823 41B2535F5	GDCA TrustAUTH R5 ROOT



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 = GDCA TrustAUTH R4 IV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	5503AE8E 0735A817 63DBC9D6 1E3E639D DDC617D0	99442C8F83A 3C5090CA50C 1C0B1DE4B32 ED418FF0AA7 C3240E91230 159F3E7BF	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 EV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	1E6AEADE F52FBFA8 D36CC7C6 3FDB6C64 60DCE341	96A5A2CD398 00CFB6A2A83 0EE52DCF47F BB00FF1B032 04DB36915CE A31F13342	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Extended Validation SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	1E6AEADE F52FBFA8 D36CC7C6 3FDB6C64 60DCE341	55324A98325 12FC6C99F15 BF0E9ED3D6B EB4398CCEE1 94B7FF849D9 6D9130D44	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE61 80C09990 596DD624 55F2FFC0 EB2717EC	5DB60C2D6B6 BECF3144775 89A3A4FB4CC F84649D69B0 B21B3D6B2AB A78BD35FB	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE61 80C09990 596DD624 55F2FFC0 EB2717EC	86C6707BBE2 7CDE1215E25 D3F8146A522 281E18C45DF 2CB8C6FB7A0 3C1733510	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	116492AE A041621C 2084B7D3 8881D1CD 8072C77F	3253412FDAD 4523108C098 BB0EE0EFEDD 7FAFDD00FB3 0E47C6BBA9F E3E1CDB88	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Plus EV CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	4A5D70FA 0E1FFC31 1F6D5834 064DE635 D0475180	3B39A01EB6D D0C0E870359 F01AFB66665 E0D5C240802 91A0769D7F0 FB4BB0E4E	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 TimeStamp CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	E5F795D3 4860FFB7 02F17810 50FFD10D FB735803	4FBCDFC8184 C41523CEBA5 8A4F3BAFD36 ECADACC11EC A148AA24C77 4C8E4B47B	GDCA TrustAUTH R5 ROOT



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 = 数安时代 R5 根 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha256RSA	4096 bits	827A42A2 BE5C08BB ADF14CA6 EB71B58B 1201F329	71A1A38FF48 5137002DD5C D780B3873DD E146723EE28 080ECF3738C 7C4FEB1AE	数安时代R5 根 CA
CN = 数安时代 R4 EV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	28B9AF46 7654EA51 D4B2810E 540916D2 DEEFF386	FA920C85394 28B3CB4BF77 BE2532BC6D0 DDD97EB664E E8BEA297DAA D147EA76F	数安时代R5 根 CA
CN = 数安时代 R4 OV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0B630E58 2F1B860F 85B257B2 4A3131C4 A970A19B	203D73A5288 47AAA7B4EA1 6098B048215 B311BFB3E24 AB27DCD7B15 BDF83C1D6	数安时代R5 根 CA
CN = 数安时代 R4 DV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0C2556EA FD7A04DD C2AE6239 09693113 8EBE91D8	E43F7A0BAF9 43180D7D40F ED2E54965BD 674DC2C82EF AB2A5108AA3 D6664A641	数安时代R5 根 CA
CN = 数安时代 R4 IV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	FBF66620 D2AA7B2C 10CB52E2 59D40A15 3C11E3F7	13CD63B1F4A 3F41914BD7E A3362DBEE07 5A229138206 86162229BF 643598961	数安时代R5 根 CA
CN = 数安时代 R4 代码签名证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0B1C0C17 23AD9F26 C4928AFC 7F77FD16 27097831	1DDCBC25FC8 E9987B5F425 A2131550D38 329A663DB08 F15BDDDB71F 2BF87E200	数安时代R5 根 CA
CN = 数安时代 R4 普通订户证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	5543FAB3 89F57FD5 5AD4FEB1 258451E2 C86ABEF7	18CDC6E98BE 17513D4F12B 72FFB8FA743 7FD18A21352 C2695EB68BB 91D0B1BAD	数安时代R5 根 CA
CN = 数安时代 R4 基础订户证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49EE724E DA99640C E14480ED 731D35FC 8D4243C4	F051A99F563 0D835FAF6F6 D1A50DD92B3 6A127DF3B12 B54317A0763 0FCDB0307	数安时代R5 根CA



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 = GDCA TrustAUTH E5 ROOT O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha384ECDSA	384 bits	C87CB0D4 20A5DB56 97F29730 C88A6189 9FA5F222	EA152FD132D E4F4E71930A 9760517A81D ACBBB5F1014 D8BD7782AC0 CC37E9431	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 EV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BCB2E535 26589289 93BC96AC 2344456B 4644C7BF	08646322AE5 1E91C8D61D9 0A2D11F4D3B A6D386A4142 56B66AD5711 6934A9EC3	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 OV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	55612DF0 62120F01 ECEEF127A 6E5AC45D 0299A22C	AA0E436C044 20376287C9A C94A38B975B 84DF16F0C63 0FF079E750D ADD03453A	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 DV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	428A21F3 DD52570A 928FC182 C4C615B5 AEC63EFB	1A404FB498F C8D525DEEAC 47299CABA3D 4A716D94AD5 5DFAFCF7B65 76AFA6466	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 IV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	5BB1FEC6 8A2F902E 21DDCEED DAAAFB25 70F2D067	BA4B5FB3FD5 4BE90EBBAC6 AEBF512D2FC 490B1D6397B C4E779F2ED3 D34D0D721	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	9F5C6CA8 E4A530A5 7DE31681 2EBFCB1C 16C0D760	E5AB9FA5362 A0F0137C845 41B4F682908 7307329BE3C 05F8BC4A281 1159B7BFF	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	1D60F596 7C365592 21E343DB C8C862D3 BBC34684	007B5E81298 733CB0FF0EA 8D2FBAE9BC5 54A05EC3957 6E0D0F2EABD A3289E1E1	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BD90963A 7CC81C8E 2114AD92 1F8A3023 9A3880F8	760F03A6A7F 99BA47E42DF 456B0E3ED2D 8DF99181157 97396CE83E9 5040AF547	GDCA TrustAUTH E5 ROOT



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 = GDCA TLS ROOT R52 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha256RSA	4096 bits	C1C376BF 8554B5BC 7485FCBA B3C583CE D9F5BF8B	77AE39E8D12 4F6BC747C74 FA8DA2AE089 358C4930566 ED736914467 2D74C6471	GDCA TLS ROOT R52
CN = GDCA TLS OV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	20E9D874 315D922D 5593310D 8997A43B 3F17C041	6C12CD82419 0D6ADD67E25 8F74FC7DFAE 4A4A37151BB FE1B50D9FBC ED296E720	GDCA TLS ROOT R52
CN = GDCA TLS EV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	73BB9BD3 D57E6455 A03EBBF8 7F5320D8 EBF21D17	998C68E2C65 106EBBF9AD6 F39CC4478B9 A23D5D71EEC AB51A643067 E49E0A285	GDCA TLS ROOT R52
CN = GDCA TLS DV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	29312D4F 17B4E721 ACAB9DA7 1AFE439E A80B3080	AC54B851E73 83961B1D649 35BA59DA920 B3DB7EE5734 B22250184FA 95C08C15A	GDCA TLS ROOT R52
CN = GDCA TLS ROOT E52 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha384ECDSA	384 bits	069953CD EE29468A 9548584F 43635AEE 0AF13904	D50FDF57D3C EC20EE91256 A4A6DA768C3 6A510DFE577 1F23EF4B183 3290BF012	GDCA TLS ROOT E52
CN = GDCA TLS OV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	175CF6CE 6D73FA04 4C3F7E74 EB71838C 0033BB84	9194B7C0D00 571592962AE 4F6F1302837 362FE09B038 98EBFCCDB84 5E6F861E8	GDCA TLS ROOT E52
CN = GDCA TLS EV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	9ED918C1 C15E3D68 EDED2F57 046E3DE2 BBD1959A	BD488893767 ABBF139ED36 76840EA5CD4 544171DDBEF 3C67B6AD4E9 A3BA45AA7	GDCA TLS ROOT E52
CN = GDCA TLS DV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	A353DDE7 18C8E3BB A047EBD5 7395ABC0 79F2D4DA	0E114041712 89F7214FD9F 817E01D7170 2394BBB57EF 678F9AC6881 022816235	GDCA TLS ROOT E52



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	Release Date
GDCA CPS	6.2	28 February 2025
GDCA CPS	6.1	15 April 2024
GDCA CPS	6.0	31 August 2023
GDCA EV CPS	3.0	28 February 2025
GDCA EV CPS	2.9	15 April 2024
GDCA EV CPS	2.8	8 May 2023
GDCA CP	3.3	28 February 2025
GDCA CP	3.2	15 April 2024
GDCA CP	3.1	31 August 2023
GDCA EV CP	2.9	28 February 2025
GDCA EV CP	2.8	15 April 2024
GDCA EV CP	2.7	8 May 2023



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
Guangzhou City, Guangdong, China	Administration and Support
Foshan City (West), Guangdong, China	Datacenter Facility
Foshan City (East), Guangdong, China	Datacenter Facility



GDCA MANAGEMENT'S ASSERTION

Global Digital Cybersecurity Authority Co.,Ltd. ("GDCA") operates the Certification Authority (CA) services known as CAs in Appendix A, and provides Extended Validation SSL ("EV SSL") CA services.

The management of GDCA is responsible for establishing and maintaining effective controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website, EV SSL key lifecycle management controls, EV SSL certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to GDCA's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

GDCA management has assessed its disclosures of its EV SSL practices and controls over its EV SSL CA services. Based on that assessment, in GDCA management's opinion, in providing its EV SSL CA services at locations as enumerated in Appendix C, throughout the period 1 March 2024 to 28 February 2025, GDCA has:

- disclosed its EV SSL certificate lifecycle management business practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B, including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on the GDCA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL certificate subscriber information is properly authenticated

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.8.](#)

GDCA 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.

GDCA had disclosed an incident (Bug 1888060) on Mozilla's Bugzilla Platform on 26 March 2024. In the incident, GDCA had issued 20 SSL/TLS certificates from 15 September to 8 October 2023 with the Basic Constraints extension included but not set as Critical, the affected certificates including 12 OV certificates, 7 DV certificates, and 1 EV certificate. As of 5:10PM, 2 April 2024 (UTC+8), all these certificates had either been revoked or expired. After the mis-issuance, the cause analysis of the incident and the remediations conducted by GDCA have been illustrated in the process of public discussion. The matter on the public platform has been closed on 5 March 2025.

GDCA had disclosed an incident (Bug 1889062) on Mozilla's Bugzilla Platform on 2 April 2024. In the incident, As noted in Bug 1888060, GDCA had issued 20 SSL/TLS certificates with Non-critical Basic Constraints extension from 15 September to 8 October 2023, and as of 5:10PM, 2 April 2024 (UTC+8), all the certificates had either been revoked or expired. There were 13 certificates which had not been revoked within 5 days since receiving the Certificate Problem Report, leading to a violation of Baseline Requirements 4.9.1.1. After the revocations delayed, the cause analysis of the derived incident and the remediations conducted by GDCA have been illustrated in the process of public discussion. The matter on the public platform has been closed on 2 April 2025.



数安时代科技股份有限公司
Global Digital Cybersecurity Authority Co., Ltd.

Mr. Xiao Qiang

General Manager of Global Digital Cybersecurity Authority Co., Ltd.

Ke Jiao Road, Nanhai Software Technology Park, Shishan Town, Nanhai District, Foshan City, Guangdong Province.

20 May 2025



Appendix A

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

Key Name	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = GDCA TrustAUTH R5 ROOT O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Root Key	sha256RSA	4096 bits	E2C9409F 4DCEE89A A17CCF0E 3F65C529 886A1951	BFFF8FD0443 3487D6A8AA6 0C1A29767A9 FC2BBB05E42 0F713A13B99 2891D3893	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 EV CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	686223D3 A9DFC522 D155654D 64762589 AAB6D074	882E0146D15 D3483EE5981 E35067F1449 E562B89E22E CC3FDF37274 EDD314CDA	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Extended Validation CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	686223D3 A9DFC522 D155654D 64762589 AAB6D074	BEC06F55344 C3DE4F12CD5 D808906CDE2 75234951BE0 176A787E628 E2BE7D51F	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A 2D739636 727D5D1E B6E28123 69CF68E4	051C238FAD7 C1DC0FCEB4A EF79CAE97FE 49A82DA8916 A4A0920F307 AACD60F81	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A 2D739636 727D5D1E B6E28123 69CF68E4	2F2F0088177 10A1085B4E6 BC5E3335474 444D983272E 33995A331BE 1A4C4FE0A	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 OV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5B BE7C08C6 AD04BB48 6145B0F5 6257A0B3	5600AFB6BAE 2A83B66B9CB BE9CEEC8F53 E26420A6993 9A48DCC6D56 B99790A63	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5B BE7C08C6 AD04BB48 6145B0F5 6257A0B3	1E96ABB2D65 02B5DCE518E C00B5A1E543 349EFD2E3F6 8BE9ABC1128 B256FEDD7	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 DV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	7313CE83 C60C2AA0 2692AE3F 7B4074B5 300B3595	74468180CE5 64BAD7E8122 10AF743E85C A96CBA44CF5 851FA000823 41B2535F5	GDCA TrustAUTH R5 ROOT

CN = GDCA TrustAUTH R4 IV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	5503AE8E 0735A817 63DBC9D6 1E3E639D DDC617D0	99442C8F83A 3C5090CA50C 1C0B1DE4B32 ED418FF0AA7 C3240E91230 159F3E7BF	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 EV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	1E6AEADE F52FBFA8 D36CC7C6 3FDB6C64 60DCE341	96A5A2CD398 00CFB6A2A83 0EE52DCF47F BB00FF1B032 04DB36915CE A31F13342	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Extended Validation SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	1E6AEADE F52FBFA8 D36CC7C6 3FDB6C64 60DCE341	55324A98325 12FC6C99F15 BFOE9ED3D6B EB4398CCEE1 94B7FF849D9 6D9130D44	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE61 80C09990 596DD624 55F2FFC0 EB2717EC	5DB60C2D6B6 BECF3144775 89A3A4FB4CC F84649D69B0 B21B3D6B2AB A78BD35FB	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE61 80C09990 596DD624 55F2FFC0 EB2717EC	86C6707BBE2 7CDE1215E25 D3F8146A522 281E18C45DF 2CB8C6FB7A0 3C1733510	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	116492AE A041621C 2084B7D3 8881D1CD 8072C77F	3253412FDAD 4523108C098 BB0EE0EFEDD 7FAFDD00FB3 0E47C6BBA9F E3E1CDB88	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Plus EV CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	4A5D70FA 0E1FFC31 1F6D5834 064DE635 D0475180	3B39A01EB6D D0C0E870359 F01AFB66665 E0D5C240802 91A0769D7F0 FB4BB0E4E	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 TimeStamp CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	E5F795D3 4860FFB7 02F17810 50FFD10D FB735803	4FBCDFC8184 C41523CEBA5 8A4F3BAFD36 ECADACC11EC A148AA24C77 4C8E4B47B	GDCA TrustAUTH R5 ROOT
CN = 数安时代 R5 根 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha256RSA	4096 bits	827A42A2 BE5C08BB ADF14CA6 EB71B58B 1201F329	71A1A38FF48 5137002DD5C D780B3873DD E146723EE28 080ECF3738C 7C4FEB1AE	数安时代R5 根 CA

CN = 数安时代 R4 EV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	28B9AF46 7654EA51 D4B2810E 540916D2 DEEFF386	FA920C85394 28B3CB4BF77 BE2532BC6D0 DDD97EB664E E8BEA297DAA D147EA76F	数安时代R5 根 CA
CN = 数安时代 R4 OV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0B630E58 2F1B860F 85B257B2 4A3131C4 A970A19B	203D73A5288 47AAA7B4EA1 6098B048215 B311BFB3E24 AB27DCD7B15 BDF83C1D6	数安时代R5 根 CA
CN = 数安时代 R4 DV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0C2556EA FD7A04DD C2AE6239 09693113 8EBE91D8	E43F7A0BAF9 43180D7D40F ED2E54965BD 674DC2C82EF AB2A5108AA3 D6664A641	数安时代R5 根 CA
CN = 数安时代 R4 IV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	FBF66620 D2AA7B2C 10CB52E2 59D40A15 3C11E3F7	13CD63B1F4A 3F41914BD7E A3362DBEE07 5A229138206 861622297BF 643598961	数安时代R5 根 CA
CN = 数安时代 R4 代码签名证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0B1C0C17 23AD9F26 C4928AFC 7F77FD16 27097831	1DDCBC25FC8 E9987B5F425 A2131550D38 329A663DB08 F15BDDDB71F 2BF87E200	数安时代R5 根 CA
CN = 数安时代 R4 普通订户证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	5543FAB3 89F57FD5 5AD4FEB1 258451E2 C86ABEF7	18CDC6E98BE 17513D4F12B 72FFB8FA743 7FD18A21352 C2695EB68BB 91D0B1BAD	数安时代R5 根 CA
CN = 数安时代 R4 基础订户证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49EE724E DA99640C E14480ED 731D35FC 8D4243C4	F051A99F563 0D835FAF6F6 D1A50DD92B3 6A127DF3B12 B54317A0763 0FCDB0307	数安时代R5 根CA
CN = GDCA TrustAUTH E5 ROOT O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha384ECDSA	384 bits	C87CB0D4 20A5DB56 97F29730 C88A6189 9FA5F222	EA152FD132D E4F4E71930A 9760517A81D ACBBB5F1014 D8BD7782AC0 CC37E9431	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 EV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BCB2E535 26589289 93BC96AC 2344456B 4644C7BF	08646322AE5 1E91C8D61D9 0A2D11F4D3B A6D386A4142 56B66AD5711 6934A9EC3	GDCA TrustAUTH E5 ROOT

CN = GDCA TrustAUTH E4 OV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	55612DF0 62120F01 ECEF127A 6E5AC45D 0299A22C	AA0E436C044 20376287C9A C94A38B975B 84DF16F0C63 0FF079E750D ADD03453A	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 DV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	428A21F3 DD52570A 928FC182 C4C615B5 AEC63EFB	1A404FB498F C8D525DEEAC 47299CABA3D 4A716D94AD5 5DFAFCF7B65 76AFA6466	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 IV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	5BB1FEC6 8A2F902E 21DDCEED DAAAFB25 70F2D067	BA4B5FB3FD5 4BE90EBBAC6 AEBF512D2FC 490B1D6397B C4E779F2ED3 D34D0D721	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	9F5C6CA8 E4A530A5 7DE31681 2EBFCB1C 16C0D760	E5AB9FA5362 A0F0137C845 41B4F682908 7307329BE3C 05F8BC4A281 1159B7BFF	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	1D60F596 7C365592 21E343DB C8C862D3 BBC34684	007B5E81298 733CB0FF0EA 8D2FBAE9BC5 54A05EC3957 6E0D0F2EABD A3289E1E1	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BD90963A 7CC81C8E 2114AD92 1F8A3023 9A3880F8	760F03A6A7F 99BA47E42DF 456B0E3ED2D 8DF99181157 97396CE83E9 5040AF547	GDCA TrustAUTH E5 ROOT
CN = GDCA TLS ROOT R52 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha256RSA	4096 bits	C1C376BF 8554B5BC 7485FCBA B3C583CE D9F5BF8B	77AE39E8D12 4F6BC747C74 FA8DA2AE089 358C4930566 ED736914467 2D74C6471	GDCA TLS ROOT R52
CN = GDCA TLS OV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	20E9D874 315D922D 5593310D 8997A43B 3F17C041	6C12CD82419 0D6ADD67E25 8F74FC7DFAE 4A4A37151BB FE1B50D9FBC ED296E720	GDCA TLS ROOT R52



CN = GDCA TLS EV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	73BB9BD3 D57E6455 A03EBBF8 7F5320D8 EBF21D17	998C68E2C65 106EBBF9AD6 F39CC4478B9 A23D5D71EEC AB51A643067 E49E0A285	GDCA TLS ROOT R52
CN = GDCA TLS DV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	29312D4F 17B4E721 ACAB9DA7 1AFE439E A80B3080	AC54B851E73 83961B1D649 35BA59DA920 B3DB7EE5734 B22250184FA 95C08C15A	GDCA TLS ROOT R52
CN = GDCA TLS ROOT E52 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha384ECDSA	384 bits	069953CD EE29468A 9548584F 43635AEE 0AF13904	D50FDF57D3C EC20EE91256 A4A6DA768C3 6A510DFE577 1F23EF4B183 3290BF012	GDCA TLS ROOT E52
CN = GDCA TLS OV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	175CF6CE 6D73FA04 4C3F7E74 EB71838C 0033BB84	9194B7C0D00 571592962AE 4F6F1302837 362FE09B038 98EBFCCDB84 5E6F861E8	GDCA TLS ROOT E52
CN = GDCA TLS EV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	9ED918C1 C15E3D68 EDED2F57 046E3DE2 BBD1959A	BD488893767 ABBF139ED36 76840EA5CD4 544171DDBEF 3C67B6AD4E9 A3BA45AA7	GDCA TLS ROOT E52
CN = GDCA TLS DV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	A353DDE7 18C8E3BB A047EBD5 7395ABC0 79F2D4DA	0E114041712 89F7214FD9F 817E01D7170 2394BBB57EF 678F9AC6881 022816235	GDCA TLS ROOT E52

Appendix B

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

Name	Version	Release Date
GDCA CPS	6.2	28 February 2025
GDCA CPS	6.1	15 April 2024
GDCA CPS	6.0	31 August 2023
GDCA EV CPS	3.0	28 February 2025
GDCA EV CPS	2.9	15 April 2024
GDCA EV CPS	2.8	8 May 2023
GDCA CP	3.3	28 February 2025
GDCA CP	3.2	15 April 2024
GDCA CP	3.1	31 August 2023
GDCA EV CP	2.9	28 February 2025
GDCA EV CP	2.8	15 April 2024
GDCA EV CP	2.7	8 May 2023



Appendix C

Locations in-scope:

Location	Function
Guangzhou City, Guangdong, China	Administration and Support
Foshan City (West), Guangdong, China	Datacenter Facility
Foshan City (East), Guangdong, 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：数安时代科技股份有限公司管理阶层

我们接受委托，对附件一列数安时代科技股份有限公司 (Global Digital Cybersecurity Authority Co., Ltd. ，以下简称 “GDCA”) 于 2024 年 3 月 1 日至 2025 年 2 月 28 日期间于附件三所列地点运营的电子认证 (“CA”) 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，GDCA 已：

- 在附件二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 EV 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 EV 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 EV SSL 证书在生命周期中的完整性；以及
 - 于 GDCA 所执行的注册操作恰当地鉴定 EV 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 – Extended Validation SSL v1.8](#) 。

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

GDCA 于 2024 年 3 月 26 日披露了 Mozilla Bugzilla 平台上的一起事件 ([Bug 1888060](#)) 。在该事件中，GDCA 在 2023 年 9 月 15 日至 10 月 8 日期间颁发了 20 个 SSL/TLS 证书，证书包括了基本约束扩展，但未设置为关键，受影响的证书包括 12 个 OV 证书、7 个 DV 证书和 1 个 EV 证书。截至 2024 年 4 月 2 日下午 5:10 (UTC+8) ，所有这些证书均已被撤销或过期。错发事件发生后，GDCA 对事件原因的分析和整改措施已在公众讨论过程中得到



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

阐述。此事於公共平台上的討論於2025 年 3月 5日關閉。

GDCA 于 2024 年 4 月 2 日披露了 Mozilla Bugzilla 平台上的一起事件 ([Bug 1889062](#))。在该事件中，如 [Bug 1888060](#) 中所述，GDCA 在 2023 年 9 月 15 日至 10 月 8 日期间颁发了 20 个带有非关键基本约束扩展的 SSL/TLS 证书，截至 2024 年 4 月 2 日下午 5 点 10 分 (UTC+8)，所有证书已被撤销或过期。然而，有 13 个证书在收到证书问题报告后 5 天内尚未吊销，导致违反了基线要求 4.9.1.1。撤销延誤的衍生事件發生后，原因分析以及 GDCA 采取的补救措施已在公众讨论过程中得到阐述。此事於公共平台上的討論於 2025 年 4 月 2 日關閉。

GDCA 的责任

GDCA 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 GDCA 所提供的服务能够符合 [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#) 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 GDCA 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 GDCA EV SSL 证书生命周期管理，包括 EV SSL 证书发放、更新和吊销；
- (2) 选择测试业务操作是否遵守了所披露的 EV 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

GDCA 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



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

由于内部控制体系本身的限制，GDCA 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，GDCA 于 2024 年 3 月 1 日至 2025 年 2 月 28 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 – Extended Validation SSL v1.8](#)。

本报告并不包括任何 [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#) 以外的质量标准声明，或对客户对 GDCA 服务的合适性声明。

对 Webtrust 标识的使用

在 GDCA 网站上的 WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL 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

附件一

本认定报告内包括的密钥与证书列举如下:

Key Name	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = GDCA TrustAUTH R5 ROOT O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Root Key	sha256RSA	4096 bits	E2C9409F 4DCEE89A A17CCF0E 3F65C529 886A1951	BFFF8FD0443 3487D6A8AA6 0C1A29767A9 FC2BBB05E42 0F713A13B99 2891D3893	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 EV CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	686223D3 A9DFC522 D155654D 64762589 AAB6D074	882E0146D15 D3483EE5981 E35067F1449 E562B89E22E CC3FDF37274 EDD314CDA	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Extended Validation CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	686223D3 A9DFC522 D155654D 64762589 AAB6D074	BEC06F55344 C3DE4F12CD5 D808906CDE2 75234951BE0 176A787E628 E2BE7D51F	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A 2D739636 727D5D1E B6E28123 69CF68E4	051C238FAD7 C1DC0FCEB4A EF79CAE97FE 49A82DA8916 A4A0920F307 AACD60F81	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A 2D739636 727D5D1E B6E28123 69CF68E4	2F2F0088177 10A1085B4E6 BC5E3335474 444D983272E 33995A331BE 1A4C4FE0A	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 OV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5B BE7C08C6 AD04BB48 6145B0F5 6257A0B3	5600AFB6BAE 2A83B66B9CB BE9CEEC8F53 E26420A6993 9A48DCC6D56 B99790A63	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5B BE7C08C6 AD04BB48 6145B0F5 6257A0B3	1E96ABB2D65 02B5DCE518E C00B5A1E543 349EFD2E3F6 8BE9ABC1128 B256FEDD7	GDCA TrustAUTH R5 ROOT



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 = GDCA TrustAUTH R4 DV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	7313CE83 C60C2AA0 2692AE3F 7B4074B5 300B3595	74468180CE5 64BAD7E8122 10AF743E85C A96CBA44CF5 851FA000823 41B2535F5	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 IV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	5503AE8E 0735A817 63DBC9D6 1E3E639D DDC617D0	99442C8F83A 3C5090CA50C 1C0B1DE4B32 ED418FF0AA7 C3240E91230 159F3E7BF	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 EV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	1E6AEADE F52FBFA8 D36CC7C6 3FDB6C64 60DCE341	96A5A2CD398 00CFB6A2A83 0EE52DCF47F BB00FF1B032 04DB36915CE A31F13342	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Extended Validation SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	1E6AEADE F52FBFA8 D36CC7C6 3FDB6C64 60DCE341	55324A98325 12FC6C99F15 BF0E9ED3D6B EB4398CCEE1 94B7FF849D9 6D9130D44	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE61 80C09990 596DD624 55F2FFC0 EB2717EC	5DB60C2D6B6 BECF3144775 89A3A4FB4CC F84649D69B0 B21B3D6B2AB A78BD35FB	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE61 80C09990 596DD624 55F2FFC0 EB2717EC	86C6707BBE2 7CDE1215E25 D3F8146A522 281E18C45DF 2CB8C6FB7A0 3C1733510	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	116492AE A041621C 2084B7D3 8881D1CD 8072C77F	3253412FDAD 4523108C098 BB0EE0EFEDD 7FAFDD00FB3 0E47C6BBA9F E3E1CDB88	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Plus EV CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	4A5D70FA 0E1FFC31 1F6D5834 064DE635 D0475180	3B39A01EB6D D0C0E870359 F01AFB66665 E0D5C240802 91A0769D7F0 FB4BB0E4E	GDCA TrustAUTH R5 ROOT



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 = GDCA TrustAUTH R4 TimeStamp CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	E5F795D3 4860FFB7 02F17810 50FFD10D FB735803	4FBCDFC8184 C41523CEBA5 8A4F3BAFD36 ECADACC11EC A148AA24C77 4C8E4B47B	GDCA TrustAUTH R5 ROOT
CN = 数安时代 R5 根 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha256RSA	4096 bits	827A42A2 BE5C08BB ADF14CA6 EB71B58B 1201F329	71A1A38FF48 5137002DD5C D780B3873DD E146723EE28 080ECF3738C 7C4FEB1AE	数安时代R5 根 CA
CN = 数安时代 R4 EV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	28B9AF46 7654EA51 D4B2810E 540916D2 DEEFF386	FA920C85394 28B3CB4BF77 BE2532BC6D0 DDD97EB664E E8BEA297DAA D147EA76F	数安时代R5 根 CA
CN = 数安时代 R4 OV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0B630E58 2F1B860F 85B257B2 4A3131C4 A970A19B	203D73A5288 47AAA7B4EA1 6098B048215 B311BFB3E24 AB27DCD7B15 BDF83C1D6	数安时代R5 根 CA
CN = 数安时代 R4 DV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0C2556EA FD7A04DD C2AE6239 09693113 8EBE91D8	E43F7A0BAF9 43180D7D40F ED2E54965BD 674DC2C82EF AB2A5108AA3 D6664A641	数安时代R5 根 CA
CN = 数安时代 R4 IV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	FBF66620 D2AA7B2C 10CB52E2 59D40A15 3C11E3F7	13CD63B1F4A 3F41914BD7E A3362DBEE07 5A229138206 861622297BF 643598961	数安时代R5 根 CA
CN = 数安时代 R4 代码签名证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0B1C0C17 23AD9F26 C4928AFC 7F77FD16 27097831	1DDCBC25FC8 E9987B5F425 A2131550D38 329A663DB08 F15BDDDB71F 2BF87E200	数安时代R5 根 CA
CN = 数安时代 R4 普通订户证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	5543FAB3 89F57FD5 5AD4FEB1 258451E2 C86ABEF7	18CDC6E98BE 17513D4F12B 72FFB8FA743 7FD18A21352 C2695EB68BB 91D0B1BAD	数安时代R5 根 CA



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 = 数安时代 R4 基础订户证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49EE724E DA99640C E14480ED 731D35FC 8D4243C4	F051A99F563 0D835FAF6F6 D1A50DD92B3 6A127DF3B12 B54317A0763 0FCDB0307	数安时代R5 根CA
CN = GDCA TrustAUTH E5 ROOT O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha384ECDSA	384 bits	C87CB0D4 20A5DB56 97F29730 C88A6189 9FA5F222	EA152FD132D E4F4E71930A 9760517A81D ACBBB5F1014 D8BD7782AC0 CC37E9431	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 EV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BCB2E535 26589289 93BC96AC 2344456B 4644C7BF	08646322AE5 1E91C8D61D9 0A2D11F4D3B A6D386A4142 56B66AD5711 6934A9EC3	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 OV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	55612DF0 62120F01 ECEFF127A 6E5AC45D 0299A22C	AA0E436C044 20376287C9A C94A38B975B 84DF16F0C63 0FF079E750D ADD03453A	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 DV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	428A21F3 DD52570A 928FC182 C4C615B5 AEC63EFB	1A404FB498F C8D525DEEAC 47299CABA3D 4A716D94AD5 5DFAFCF7B65 76AFA6466	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 IV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	5BB1FEC6 8A2F902E 21DDCEED DAAAFB25 70F2D067	BA4B5FB3FD5 4BE90EBBAC6 AEBF512D2FC 490B1D6397B C4E779F2ED3 D34D0D721	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	9F5C6CA8 E4A530A5 7DE31681 2EBFCB1C 16C0D760	E5AB9FA5362 A0F0137C845 41B4F682908 7307329BE3C 05F8BC4A281 1159B7BFF	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	1D60F596 7C365592 21E343DB C8C862D3 BBC34684	007B5E81298 733CB0FF0EA 8D2FBAE9BC5 54A05EC3957 6E0D0F2EABD A3289E1E1	GDCA TrustAUTH E5 ROOT



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 = GDCA TrustAUTH E4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BD90963A 7CC81C8E 2114AD92 1F8A3023 9A3880F8	760F03A6A7F 99BA47E42DF 456B0E3ED2D 8DF99181157 97396CE83E9 5040AF547	GDCA TrustAUTH E5 ROOT
CN = GDCA TLS ROOT R52 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha256RSA	4096 bits	C1C376BF 8554B5BC 7485FCBA B3C583CE D9F5BF8B	77AE39E8D12 4F6BC747C74 FA8DA2AE089 358C4930566 ED736914467 2D74C6471	GDCA TLS ROOT R52
CN = GDCA TLS OV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	20E9D874 315D922D 5593310D 8997A43B 3F17C041	6C12CD82419 0D6ADD67E25 8F74FC7DFAE 4A4A37151BB FE1B50D9FBC ED296E720	GDCA TLS ROOT R52
CN = GDCA TLS EV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	73BB9BD3 D57E6455 A03EBBF8 7F5320B8 EBF21D17	998C68E2C65 106EBBF9AD6 F39CC4478B9 A23D5D71EEC AB51A643067 E49E0A285	GDCA TLS ROOT R52
CN = GDCA TLS DV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	29312D4F 17B4E721 ACAB9DA7 1AFE439E A80B3080	AC54B851E73 83961B1D649 35BA59DA920 B3DB7EE5734 B22250184FA 95C08C15A	GDCA TLS ROOT R52
CN = GDCA TLS ROOT E52 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha384ECDSA	384 bits	069953CD EE29468A 9548584F 43635AEE 0AF13904	D50FDF57D3C EC20EE91256 A4A6DA768C3 6A510DFE577 1F23EF4B183 3290BF012	GDCA TLS ROOT E52
CN = GDCA TLS OV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	175CF6CE 6D73FA04 4C3F7E74 EB71838C 0033BB84	9194B7C0D00 571592962AE 4F6F1302837 362FE09B038 98EBFCCDB84 5E6F861E8	GDCA TLS ROOT E52



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 = GDCA TLS EV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	9ED918C1 C15E3D68 EDED2F57 046E3DE2 BBD1959A	BD488893767 ABBF139ED36 76840EA5CD4 544171DDBEF 3C67B6AD4E9 A3BA45AA7	GDCA TLS ROOT E52
CN = GDCA TLS DV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	A353DDE7 18C8E3BB A047EBD5 7395ABC0 79F2D4DA	0E114041712 89F7214FD9F 817E01D7170 2394BBB57EF 678F9AC6881 022816235	GDCA TLS ROOT E52



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

附件二

范围内适用之CP/CPS版本:

Name	Version	Release Date
GDCA CPS	6.2	28 February 2025
GDCA CPS	6.1	15 April 2024
GDCA CPS	6.0	31 August 2023
GDCA EV CPS	3.0	28 February 2025
GDCA EV CPS	2.9	15 April 2024
GDCA EV CPS	2.8	8 May 2023
GDCA CP	3.3	28 February 2025
GDCA CP	3.2	15 April 2024
GDCA CP	3.1	31 August 2023
GDCA EV CP	2.9	28 February 2025
GDCA EV CP	2.8	15 April 2024
GDCA EV CP	2.7	8 May 2023



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

附件三

范围内地点:

地点	功能
中国广州市	管理与支持
中国广东佛山(西)	数据中心
中国广东佛山(东)	数据中心



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。)

数安时代科技股份有限公司 (Global Digital Cybersecurity Authority Co., Ltd.，以下简称“GDCA”) 运营电子认证服务机构 (“CA”)，提供增强验证SSL(Extended Validation SSL，“EV SSL”)电子认证服务，附件一列示了服务所包括的根证书和中级证书。

GDCA 的管理阶层负责针对EV SSL CA服务建立并维护有效的控制，包括：披露EV SSL CA业务规则，EV SSL CA密钥生命周期管理，EV SSL CA证书生命周期管理，订户EV 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GDCA 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。

GDCA 管理层已对所提供的EV SSL CA服务的业务规则披露及控制进行评估。基于此评估，GDCA 管理层认为，在2024 年3月1日至2025 年2月28日就GDCA 在附件三所列地点提供EV SSL CA服务期间，GDCA已：

- 於附件二之CP/CPS披露EV SSL证书生命周期管理措施，包括承诺遵循 CA/Browser 论坛 (CA/Browser Forum) 的相关指引提供EV SSL 证书服务，并依据披露的业务实践提供相关服务
- 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EV SSL证书在生命周期中的完整性；以及
 - 于 GDCA 所执行的注册操作恰当地鉴定 EV 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 – Extended Validation SSL – Version 1.8](#)。

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

GDCA 于 2024 年 3 月 26 日披露了 Mozilla Bugzilla 平台上的一起事件 ([Bug 1888060](#))。在该事件中，GDCA 在 2023 年 9 月 15 日至 10 月 8 日期间颁发了 20 个 SSL/TLS证书，证书包括了基本约束扩展，但未设置为关键，受影响的证书包括 12 个 OV 证书、7 个 DV 证书和 1 个 EV 证书。截至 2024 年 4 月 2 日下午 5:10 (UTC+8)，所有这些证书均已被撤销或过期。错发事件发生后，GDCA对事件原因的分析和整改措施已在公众讨论过程中得到阐述。此事於公共平台上的討論於2025 年 3月5日關閉。

GDCA 于 2024 年 4 月 2 日披露了 Mozilla Bugzilla 平台上的一起事件 ([Bug 1889062](#))。在该事件中，如 [Bug 1888060](#) 中所述，GDCA 在 2023 年 9 月 15 日至 10 月 8 日期间颁发了 20 个带有非关键基本约束扩展的 SSL/TLS



证书，截至2024年4月2日下午5点10分（UTC+8），所有证书已被撤销或过期。然而，有 13 个证书在收到证书问题报告后 5 天内尚未吊销，导致违反了基线要求 4.9.1.1。撤销延误的衍生事件发生后，原因分析以及GDCA采取的补救措施已在公众讨论过程中得到阐述。此事於公共平台上的討論於2025 年 4月 2日關閉。

总经理 肖强

数安时代科技股份有限公司

中国广东省佛山市南海区狮山镇南海软件科技园 科教路

2025年5月20日

附件一

本认定报告内包括的密钥与证书列举如下:

Key Name	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = GDCA TrustAUTH R5 ROOT O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Root Key	sha256RSA	4096 bits	E2C9409F 4DCEE89A A17CCF0E 3F65C529 886A1951	BFFF8FD0443 3487D6A8AA6 0C1A29767A9 FC2BBB05E42 0F713A13B99 2891D3893	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 EV CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	686223D3 A9DFC522 D155654D 64762589 AAB6D074	882E0146D15 D3483EE5981 E35067F1449 E562B89E22E CC3FDF37274 EDD314CDA	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Extended Validation CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	686223D3 A9DFC522 D155654D 64762589 AAB6D074	BEC06F55344 C3DE4F12CD5 D808906CDE2 75234951BE0 176A787E628 E2BE7D51F	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A 2D739636 727D5D1E B6E28123 69CF68E4	051C238FAD7 C1DC0FCEB4A EF79CAE97FE 49A82DA8916 A4A0920F307 AACD60F81	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A 2D739636 727D5D1E B6E28123 69CF68E4	2F2F0088177 10A1085B4E6 BC5E3335474 444D983272E 33995A331BE 1A4C4FE0A	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 OV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5B BE7C08C6 AD04BB48 6145B0F5 6257A0B3	5600AFB6BAE 2A83B66B9CB BE9CEEC8F53 E26420A6993 9A48DCC6D56 B99790A63	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5B BE7C08C6 AD04BB48 6145B0F5 6257A0B3	1E96ABB2D65 02B5DCE518E C00B5A1E543 349EFD2E3F6 8BE9ABC1128 B256FEDD7	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 DV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	7313CE83 C60C2AA0 2692AE3F 7B4074B5 300B3595	74468180CE5 64BAD7E8122 10AF743E85C A96CBA44CF5 851FA000823 41B2535F5	GDCA TrustAUTH R5 ROOT



CN = GDCA TrustAUTH R4 IV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	5503AE8E 0735A817 63DBC9D6 1E3E639D DDC617D0	99442C8F83A 3C5090CA50C 1C0B1DE4B32 ED418FF0AA7 C3240E91230 159F3E7BF	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 EV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	1E6AEADE F52FBFA8 D36CC7C6 3FDB6C64 60DCE341	96A5A2CD398 00CFB6A2A83 0EE52DCF47F BB00FF1B032 04DB36915CE A31F13342	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Extended Validation SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	1E6AEADE F52FBFA8 D36CC7C6 3FDB6C64 60DCE341	55324A98325 12FC6C99F15 BFOE9ED3D6B EB4398CCEE1 94B7FF849D9 6D9130D44	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE61 80C09990 596DD624 55F2FFC0 EB2717EC	5DB60C2D6B6 BECF3144775 89A3A4FB4CC F84649D69B0 B21B3D6B2AB A78BD35FB	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE61 80C09990 596DD624 55F2FFC0 EB2717EC	86C6707BBE2 7CDE1215E25 D3F8146A522 281E18C45DF 2CB8C6FB7A0 3C1733510	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	116492AE A041621C 2084B7D3 8881D1CD 8072C77F	3253412FDAD 4523108C098 BB0EE0EFEDD 7FAFDD00FB3 0E47C6BBA9F E3E1CDB88	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Plus EV CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	4A5D70FA 0E1FFC31 1F6D5834 064DE635 D0475180	3B39A01EB6D D0C0E870359 F01AFB66665 E0D5C240802 91A0769D7F0 FB4BB0E4E	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 TimeStamp CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	E5F795D3 4860FFB7 02F17810 50FFD10D FB735803	4FBCDFC8184 C41523CEBA5 8A4F3BAFD36 ECADACC11EC A148AA24C77 4C8E4B47B	GDCA TrustAUTH R5 ROOT
CN = 数安时代 R5 根 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha256RSA	4096 bits	827A42A2 BE5C08BB ADF14CA6 EB71B58B 1201F329	71A1A38FF48 5137002DD5C D780B3873DD E146723EE28 080ECF3738C 7C4FEB1AE	数安时代R5 根 CA

CN = 数安时代 R4 EV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	28B9AF46 7654EA51 D4B2810E 540916D2 DEEFF386	FA920C85394 28B3CB4BF77 BE2532BC6D0 DDD97EB664E E8BEA297DAA D147EA76F	数安时代R5 根 CA
CN = 数安时代 R4 OV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0B630E58 2F1B860F 85B257B2 4A3131C4 A970A19B	203D73A5288 47AAA7B4EA1 6098B048215 B311BFB3E24 AB27DCD7B15 BDF83C1D6	数安时代R5 根 CA
CN = 数安时代 R4 DV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0C2556EA FD7A04DD C2AE6239 09693113 8EBE91D8	E43F7A0BAF9 43180D7D40F ED2E54965BD 674DC2C82EF AB2A5108AA3 D6664A641	数安时代R5 根 CA
CN = 数安时代 R4 IV 服务器证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	FBF66620 D2AA7B2C 10CB52E2 59D40A15 3C11E3F7	13CD63B1F4A 3F41914BD7E A3362DBEE07 5A229138206 861622297BF 643598961	数安时代R5 根 CA
CN = 数安时代 R4 代码签名证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	0B1C0C17 23AD9F26 C4928AFC 7F77FD16 27097831	1DDCBC25FC8 E9987B5F425 A2131550D38 329A663DB08 F15BDDDB71F 2BF87E200	数安时代R5 根 CA
CN = 数安时代 R4 普通订户证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	5543FAB3 89F57FD5 5AD4FEB1 258451E2 C86ABEF7	18CDC6E98BE 17513D4F12B 72FFB8FA743 7FD18A21352 C2695EB68BB 91D0B1BAD	数安时代R5 根 CA
CN = 数安时代 R4 基础订户证书 CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49EE724E DA99640C E14480ED 731D35FC 8D4243C4	F051A99F563 0D835FAF6F6 D1A50DD92B3 6A127DF3B12 B54317A0763 0FCDB0307	数安时代R5 根CA
CN = GDCA TrustAUTH E5 ROOT O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha384ECDSA	384 bits	C87CB0D4 20A5DB56 97F29730 C88A6189 9FA5F222	EA152FD132D E4F4E71930A 9760517A81D ACBBB5F1014 D8BD7782AC0 CC37E9431	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 EV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BCB2E535 26589289 93BC96AC 2344456B 4644C7BF	08646322AE5 1E91C8D61D9 0A2D11F4D3B A6D386A4142 56B66AD5711 6934A9EC3	GDCA TrustAUTH E5 ROOT

CN = GDCA TrustAUTH E4 OV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	55612DF0 62120F01 ECEF127A 6E5AC45D 0299A22C	AA0E436C044 20376287C9A C94A38B975B 84DF16F0C63 0FF079E750D ADD03453A	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 DV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	428A21F3 DD52570A 928FC182 C4C615B5 AEC63EFB	1A404FB498F C8D525DEEAC 47299CABA3D 4A716D94AD5 5DFAFCF7B65 76AFA6466	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 IV SSL CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	5BB1FEC6 8A2F902E 21DDCEED DAAAFB25 70F2D067	BA4B5FB3FD5 4BE90EBBAC6 AEBF512D2FC 490B1D6397B C4E779F2ED3 D34D0D721	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	9F5C6CA8 E4A530A5 7DE31681 2EBFCB1C 16C0D760	E5AB9FA5362 A0F0137C845 41B4F682908 7307329BE3C 05F8BC4A281 1159B7BFF	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	1D60F596 7C365592 21E343DB C8C862D3 BBC34684	007B5E81298 733CB0FF0EA 8D2FBAE9BC5 54A05EC3957 6E0D0F2EABD A3289E1E1	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BD90963A 7CC81C8E 2114AD92 1F8A3023 9A3880F8	760F03A6A7F 99BA47E42DF 456B0E3ED2D 8DF99181157 97396CE83E9 5040AF547	GDCA TrustAUTH E5 ROOT
CN = GDCA TLS ROOT R52 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha256RSA	4096 bits	C1C376BF 8554B5BC 7485FCBA B3C583CE D9F5BF8B	77AE39E8D12 4F6BC747C74 FA8DA2AE089 358C4930566 ED736914467 2D74C6471	GDCA TLS ROOT R52
CN = GDCA TLS OV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	20E9D874 315D922D 5593310D 8997A43B 3F17C041	6C12CD82419 0D6ADD67E25 8F74FC7DFAE 4A4A37151BB FE1B50D9FBC ED296E720	GDCA TLS ROOT R52



CN = GDCA TLS EV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	73BB9BD3 D57E6455 A03EBBF8 7F5320D8 EBF21D17	998C68E2C65 106EBBF9AD6 F39CC4478B9 A23D5D71EEC AB51A643067 E49E0A285	GDCA TLS ROOT R52
CN = GDCA TLS DV CA R42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384RSA	3072 bits	29312D4F 17B4E721 ACAB9DA7 1AFE439E A80B3080	AC54B851E73 83961B1D649 35BA59DA920 B3DB7EE5734 B22250184FA 95C08C15A	GDCA TLS ROOT R52
CN = GDCA TLS ROOT E52 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Root Key	sha384ECDSA	384 bits	069953CD EE29468A 9548584F 43635AEE 0AF13904	D50FDF57D3C EC20EE91256 A4A6DA768C3 6A510DFE577 1F23EF4B183 3290BF012	GDCA TLS ROOT E52
CN = GDCA TLS OV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	175CF6CE 6D73FA04 4C3F7E74 EB71838C 0033BB84	9194B7C0D00 571592962AE 4F6F1302837 362FE09B038 98EBFCCDB84 5E6F861E8	GDCA TLS ROOT E52
CN = GDCA TLS EV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	9ED918C1 C15E3D68 EDED2F57 046E3DE2 BBD1959A	BD488893767 ABBF139ED36 76840EA5CD4 544171DDBEF 3C67B6AD4E9 A3BA45AA7	GDCA TLS ROOT E52
CN = GDCA TLS DV CA E42 O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	384 bits	A353DDE7 18C8E3BB A047EBD5 7395ABC0 79F2D4DA	0E114041712 89F7214FD9F 817E01D7170 2394BBB57EF 678F9AC6881 022816235	GDCA TLS ROOT E52

附件二

范围内适用之CP/CPS版本:

Name	Version	Release Date
GDCA CPS	6.2	28 February 2025
GDCA CPS	6.1	15 April 2024
GDCA CPS	6.0	31 August 2023
GDCA EV CPS	3.0	28 February 2025
GDCA EV CPS	2.9	15 April 2024
GDCA EV CPS	2.8	8 May 2023
GDCA CP	3.3	28 February 2025
GDCA CP	3.2	15 April 2024
GDCA CP	3.1	31 August 2023
GDCA EV CP	2.9	28 February 2025
GDCA EV CP	2.8	15 April 2024
GDCA EV CP	2.7	8 May 2023



附件三

范围内地点:

地点	功能
中国广州市	管理与支持
中国广东佛山(西)	数据中心
中国广东佛山(东)	数据中心