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

INDEPENDENT ASSURANCE REPORT

To the management of 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 Guangzhou and Foshan, China, throughout the period 1 March 2020 to 28 February 2021 for its CAs as enumerated in Appendix A, GDCA has:

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

- maintained effective controls to provide reasonable assurance that:
  - GDCA's Certification Practice Statement is consistent with its Certificate Policy
  - GDCA provides its services in accordance with its Certificate Policy and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.

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

Certification authority's responsibilities

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 v2.2.

GDCA had disclosed an incident (Bug 1662382) on Mozilla's Bugzilla Platform on 1 September 2020. In the incident, one certificate was mis-issued with an incorrect value put in the organizationName field of the certificate. The mis-issued certificate had been revoked within 24 hours after the mis-issuance, and the cause analysis of the incident and the remediations conducted by GDCA have been illustrated in the process of public discussion. The discussions

of the matter on the public platform had been closed on 5 October 2020.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information,* issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

(1) obtaining an understanding of GDCA's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
(2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

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

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at 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 2020 to 28 February 2021, 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 v2.2.

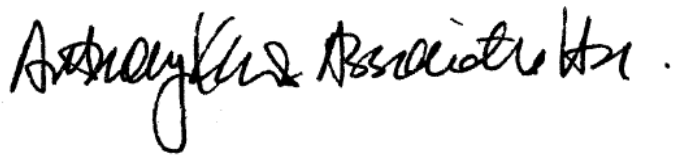
This report does not include any representation as to the quality of GDCA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.2, nor the suitability of any of GDCA's services for any customer's intended purpose.

Use of the WebTrust seal

GDCA's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

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

12 May 2021



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

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	E2C9409F4DCEE89AA17CCF0E3F65C529886A1951	BFFF8FD04433487D6A8AA60C1A29767A9FC2BBB05E420F713A13B992891D3893	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	686223D3A9DFC522D155654D64762589AAB6D074	882E0146D15D3483EE5981E35067F1449E562B89E22ECC3FDF37274EDD314CDA	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	686223D3A9DFC522D155654D64762589AAB6D074	BEC06F55344C3DE4F12CD5D808906CDE275234951BE0176A787E628E2BE7D51F	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A2D739636727D5D1EB6E2812369CF68E4	051C238FAD7C1DC0FCEB4AEF79CAE97FE49A82DA8916A4A0920F307AACD60F81	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A2D739636727D5D1EB6E2812369CF68E4	2F2F008817710A1085B4E6BC5E3335474444D983272E33995A331BE1A4C4FE0A	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	C0F67A5BBE7C08C6AD04BB486145B0F56257A0B3	5600AFB6BAE2A83B66B9CBBE9CEEC8F53E26420A69939A48DCC6D56B99790A63	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5BBE7C08C6AD04BB486145B0F56257A0B3	1E96ABB2D6502B5DCE518EC00B5A1E543349EFD2E3F68BE9ABC1128B256FEDD7	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	7313CE83C60C2AA02692AE3F7B4074B5300B3595	74468180CE564BAD7E812210AF743E85CA96CBA44CF5851FA00082341B2535F5	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	5503AE8E0735A81763DBC9D61E3E639DDDC617D0	99442C8F83A3C5090CA50C1C0B1DE4B32ED418FF0AA7C3240E91230159F3E7BF	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	1E6AEADEF52FBFA8D36CC7C63FDB6C6460DCE341	96A5A2CD39800CFB6A2A830EE52DCF47FBB00FF1B03204DB36915CEA31F13342	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	1E6AEADEF52FBFA8D36CC7C63FDB6C6460DCE341	55324A9832512FC6C99F15BF0E9ED3D6BEB4398CCEE194B7FF849D96D9130D44	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE6180C09990596DD62455F2FFC0EB2717EC	5DB60C2D6B6BECF314477589A3A4FB4CCF84649D69B0B21B3D6B2ABA78BD35FB	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE6180C09990596DD62455F2FFC0EB2717EC	86C6707BBE27CDE1215E25D3F8146A522281E18C45DF2CB8C6FB7A03C1733510	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	116492AEA041621C2084B7D38881D1CD8072C77F	3253412FDAD4523108C098BB0EE0EFEDD7FAFDD00FB30E47C6BBA9FE3E1CDB88	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	827A42A2BE5C08BBADF14CA6EB71B58B1201F329	71A1A38FF485137002DD5CD780B3873DDE146723EE28080ECF3738C7C4FEB1AE	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	28B9AF467654EA51D4B2810E540916D2DEEFF386	FA920C8539428B3CB4BF77BE2532BC6D0DDD97EB664EE8BEA297DAAD147EA76F	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	0B630E582F1B860F85B257B24A3131C4A970A19B	203D73A528847AAA7B4EA16098B048215B311BFB3E24AB27DCD7B15BDF83C1D6	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	0C2556EAFD7A04DDC2AE623909693113 8EBE91D8	E43F7A0BAF943180D7D40FED2E54965BD674DC2C82EFAB2A5108AA3D6664A641	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	FBF66620D2AA7B2C10CB52E259D40A153C11E3F7	13CD63B1F4A3F41914BD7EA3362DBEE075A2291382068616222 97BF643598961	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	0B1C0C1723AD9F26C4928AFC7F77FD1627097831	1DDCBC25FC8E9987B5F425A2131550D38329A663DB08F15BDDDB71F2BF87E200	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	5543FAB389F57FD55AD4FEB1258451E2C86ABEF7	18CDC6E98BE17513D4F12B72FFB8FA7437FD18A21352C2695EB68BB91D0B1BAD	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	49EE724EDA99640CE14480ED731D35FC8D4243C4	F051A99F5630D835FAF6F6D1A50DD92B36A127DF3B12B54317A07630FCDB0307	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	C87CB0D420A5DB5697F29730C88A61899FA5F222	EA152FD132DE4F4E71930A9760517A81DACBBB5F1014D8BD7782AC0CC37E9431	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	BCB2E53526589289 93BC96AC2344456B4644C7BF	08646322AE51E91C8D61D90A2D11F4D3BA6D386A414256B66AD57116934A9EC3	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	55612DF062120F01ECEF127A6E5AC45D0299A22C	AA0E436C04420376287C9AC94A38B975B84DF16F0C630FF079E750DADD03453A	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	428A21F3DD52570A928FC182C4C615B5AEC63EFB	1A404FB498FC8D525DEEAC47299CABA3D4A716D94AD55DFAFCF7B6576AFA6466	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	5BB1FEC68A2F902E21DDCEEDDAAAFB2570F2D067	BA4B5FB3FD54BE90EBBAC6AEBF512D2FC490B1D6397BC4E779F2ED3D34D0D721	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	9F5C6CA8E4A530A57DE3168120EBFCB1C16C0D760	E5AB9FA5362A0F0137C84541B4F6829087307329BE3C05F8BC4A2811159B7BFF	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	1D60F5967C36559221E343DBC8C862D3BBC34684	007B5E81298733CB0FF0EA8D2FBAE9BC554A05EC39576E0D0F2EABDA3289E1E1	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BD90963A7CC81C8E2114AD921F8A30239A3880F8	760F03A6A7F99BA47E42DF456B0E3ED2D8DF9918115797396CE83E95040AF547	GDCA TrustAUTH E5 ROOT

Appendix B

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

Name	Version	Release Date
GDCA CPS	5.4	5 February 2021
GDCA CPS	5.3	1 October 2020
GDCA CPS	5.2	20 August 2020
GDCA CPS	5.1	31 May 2020
GDCA EV CPS	2.3	1 October 2020
GDCA EV CPS	2.2	20 August 2020
GDCA EV CPS	2.1	31 May 2020
GDCA CP	2.5	5 February 2021
GDCA CP	2.4	1 October 2020
GDCA CP	2.3	20 August 2020
GDCA CP	2.2	31 May 2020
GDCA EV CP	2.2	1 October 2020
GDCA EV CP	2.1	20 August 2020
GDCA EV CP	2.0	31 May 2020

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

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 the following CA services:

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

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

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

GDCA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in GDCA management's opinion, in providing its Certification Authority (CA) services at Guangzhou and Foshan, China, throughout the period 1 March 2020 to 28 February 2021, GDCA has:

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

- maintained effective controls to provide reasonable assurance that:
  - GDCA's Certification Practice Statement is consistent with its Certificate Policy
  - GDCA provides its services in accordance with its Certificate Policy and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

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

CA Business Practices Disclosure

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

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services

- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

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 1662382) on Mozilla's Bugzilla Platform on 1 September 2020. In the incident, one certificate was mis-issued with an incorrect value put in the organizationName field of the certificate. The mis-issued certificate had been revoked within 24 hours after the mis-issuance, and the cause analysis of the incident and the remediations conducted by GDCA have been illustrated in the process of public discussion. The discussions of the matter on the public platform had been closed on 5 October 2020.

Ms. Liao Zhimin
Deputy General Manager of Global Digital Cybersecurity Authority Co.,Ltd.
Ke Jiao Road, Nanhai Software Technology Park, Shishan Town, Nanhai District, Foshan City, Guangdong Province.

12 May 2021

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	E2C9409F4DCEE89AA17CCF0E3F65C529886A1951	BFFF8FD04433487D6A8AA60C1A29767A9FC2BBB05E420F713A13B992891D3893	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	686223D3A9DFC522D155654D64762589AAB6D074	882E0146D15D3483EE5981E35067F1449E562B89E22ECC3FDF37274EDD314CDA	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	686223D3A9DFC522D155654D64762589AAB6D074	BEC06F55344C3DE4F12CD5D808906CDE275234951BE0176A787E628E2BE7D51F	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A2D739636727D5D1EB6E2812369CF68E4	051C238FAD7C1DC0FCEB4AEF79CAE97FE49A82DA8916A4A0920F307AACD60F81	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A2D739636727D5D1EB6E2812369CF68E4	2F2F008817710A1085B4E6BC5E3335474444D983272E33995A331BE1A4C4FE0A	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	C0F67A5BBE7C08C6AD04BB486145B0F56257A0B3	5600AFB6BAE2A83B66B9CBBE9CEEC8F53E26420A69939A48DCC6D56B99790A63	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5BBE7C08C6AD04BB486145B0F56257A0B3	1E96ABB2D6502B5DCE518EC00B5A1E543349EFD2E3F68BE9ABC1128B256FEDD7	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	7313CE83C60C2AA02692AE3F7B4074B5300B3595	74468180CE564BAD7E812210AF743E85CA96CBA44CF5851FA00082341B2535F5	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	5503AE8E0735A81763DBC9D61E3E639DDDC617D0	99442C8F83A3C5090CA50C1C0B1DE4B32ED418FF0AA7C3240E91230159F3E7BF	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	1E6AEADEF52FBFA8D36CC7C63FDB6C6460DCE341	96A5A2CD39800CFB6A2A830EE52DCF47FBB00FF1B03204DB36915CEA31F13342	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	1E6AEADEF52FBFA8D36CC7C63FDB6C6460DCE341	55324A9832512FC6C99F15BF0E9ED3D6BEB4398CCEE194B7FF849D96D9130D44	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE6180C09990596DD62455F2FFC0EB2717EC	5DB60C2D6B6BECF314477589A3A4FB4CCF84649D69B0B21B3D6B2ABA78BD35FB	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE6180C09990596DD62455F2FFC0EB2717EC	86C6707BBE27CDE1215E25D3F8146A522281E18C45DF2CB8C6FB7A03C1733510	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	116492AEA041621C2084B7D38881D1CD8072C77F	3253412FDAD4523108C098BB0EE0EFEDD7FAFDD00FB30E47C6BBA9FE3E1CDB88	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	827A42A2BE5C08BBADF14CA6EB71B58B1201F329	71A1A38FF485137002DD5CD780B3873DDE146723EE28080ECF3738C7C4FEB1AE	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	28B9AF467654EA51D4B2810E540916D2DEEFF386	FA920C8539428B3CB4BF77BE2532BC6D0DDD97EB664EE8BEA297DAAD147EA76F	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	0B630E582F1B860F85B257B24A3131C4A970A19B	203D73A528847AAA7B4EA16098B048215B311BFB3E24AB27DCD7B15BDF83C1D6	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	0C2556EAFD7A04DDC2AE623909693113 8EBE91D8	E43F7A0BAF943180D7D40FED2E54965BD674DC2C82EFAB2A5108AA3D6664A641	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	FBF66620D2AA7B2C10CB52E259D40A153C11E3F7	13CD63B1F4A3F41914BD7EA3362DBEE075A2291382068616222297BF643598961	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	0B1C0C1723AD9F26C4928AFC7F77FD1627097831	1DDCBC25FC8E9987B5F425A2131550D38329A663DB08F15BDDDB71F2BF87E200	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	5543FAB389F57FD55AD4FEB1258451E2C86ABEF7	18CDC6E98BE17513D4F12B72FFB8FA7437FD18A21352C2695EB68BB91D0B1BAD	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	49EE724EDA99640CE14480ED731D35FC8D4243C4	F051A99F5630D835FAF6F6D1A50DD92B36A127DF3B12B54317A07630FCDB0307	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	C87CB0D420A5DB5697F29730C88A61899FA5F222	EA152FD132DE4F4E71930A9760517A81DACBBB5F1014D8BD7782AC0CC37E9431	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	BCB2E53526589289 93BC96AC2344456B4644C7BF	08646322AE51E91C8D61D90A2D11F4D3BA6D386A414256B66AD57116934A9EC3	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	55612DF062120F01ECEF127A6E5AC45D0299A22C	AA0E436C04420376287C9AC94A38B975B84DF16F0C630FF079E750DADD03453A	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	428A21F3DD52570A928FC182C4C615B5AEC63EFB	1A404FB498FC8D525DEEAC47299CABA3D4A716D94AD55DFAFCF7B6576AFA6466	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	5BB1FEC68A2F902E21DDCEEDDAAAFB2570F2D067	BA4B5FB3FD54BE90EBBAC6AEBF512D2FC490B1D6397BC4E779F2ED3D34D0D721	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	9F5C6CA8E4A530A57DE3168112EBFCB1C16C0D760	E5AB9FA5362A0F0137C84541B4F6829087307329BE3C05F8BC4A2811159B7BFF	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	1D60F5967C36559221E343DBC8C862D3BBC34684	007B5E81298733CB0FF0EA8D2FBAE9BC554A05EC39576E0D0F2EABDA3289E1E1	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BD90963A7CC81C8E2114AD921F8A30239A3880F8	760F03A6A7F99BA47E42DF456B0E3ED2D8DF9918115797396CE83E95040AF547	GDCA TrustAUTH E5 ROOT

Appendix B

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

Name	Version	Release Date
GDCA CPS	5.4	5 February 2021
GDCA CPS	5.3	1 October 2020
GDCA CPS	5.2	20 August 2020
GDCA CPS	5.1	31 May 2020
GDCA CPS	5.0	20 September 2019
GDCA EV CPS	2.3	1 October 2020
GDCA EV CPS	2.2	20 August 2020
GDCA EV CPS	2.1	31 May 2020
GDCA EV CPS	2.0	20 September 2019
GDCA CP	2.5	5 February 2021
GDCA CP	2.4	1 October 2020
GDCA CP	2.3	20 August 2020
GDCA CP	2.2	31 May 2020
GDCA CP	2.1	20 September 2019
GDCA EV CP	2.2	1 October 2020
GDCA EV CP	2.1	20 August 2020
GDCA EV CP	2.0	31 May 2020
GDCA EV CP	1.9	20 September 2019

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

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，对附件一的数安时代科技股份有限公司（Global Digital Cybersecurity Authority Co., Ltd.，以下简称“GDCA”）于 2020 年 3 月 1 日至 2021 年 2 月 28 日就 GDCA 在中国广州和佛山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，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）中披露了电子认证业务、密钥生命周期管理、证书生命周期管理，以及 CA 环境控制管理

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

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

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

以符合 WebTrust Principles and Criteria for Certification Authorities v2.2。

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

GDCA于2020年9月1日曾于Mozilla Bugzilla公众平台揭漏事件Bug 1662382。于此事件中，一张数字证书因organizationName栏位输入错误發生误签，此张误签的数字证书于24个小时内被GDCA發现并完成吊销。关于此事件的發生根本原因与整改方案，GDCA业已于公众平台阐明，此议题的相关讨论于2020年10月5日结束。

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 v2.2 的规定。

审计师的独立性和质量控制

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

审计师的责任

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

我们相信，我们获取的证据是充分、适当的，为发表鉴证结论提供了基础。

控制的有效性

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

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 2020 年 3 月 1 日至 2021 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 v2.2。

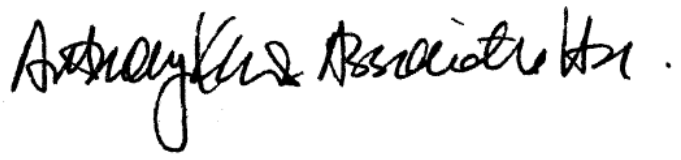
本报告并不包括任何在 WebTrust Principles and Criteria for Certification Authorities v2.2 以外的质量标准声明，或对任何客户对 GDCA 服务的合适性声明。

对 Webtrust 标识的使用

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

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

12 May 2021



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	E2C9409F4DCEE89AA17CCF0E3F65C529886A1951	BFFF8FD04433487D6A8AA60C1A29767A9FC2BBB05E420F713A13B992891D3893	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	686223D3A9DFC522D155654D64762589AAB6D074	882E0146D15D3483EE5981E35067F1449E562B89E22ECC3FDF37274EDD314CDA	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	686223D3A9DFC522D155654D64762589AAB6D074	BEC06F55344C3DE4F12CD5D808906CDE275234951BE0176A787E628E2BE7D51F	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A2D739636727D5D1EB6E2812369CF68E4	051C238FAD7C1DC0FCEB4AEF79CAE97FE49A82DA8916A4A0920F307AACD60F81	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A2D739636727D5D1EB6E2812369CF68E4	2F2F008817710A1085B4E6BC5E3335474444D983272E33995A331BE1A4C4FE0A	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	C0F67A5BBE7C08C6AD04BB486145B0F56257A0B3	5600AFB6BAE2A83B66B9CBBE9CEEC8F53E26420A69939A48DCC6D56B99790A63	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5BBE7C08C6AD04BB486145B0F56257A0B3	1E96ABB2D6502B5DCE518EC00B5A1E543349EFD2E3F68BE9ABC1128B256FEDD7	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	7313CE83C60C2AA02692AE3F7B4074B5300B3595	74468180CE564BAD7E812210AF743E85CA96CBA44CF5851FA00082341B2535F5	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	5503AE8E0735A81763DBC9D61E3E639DDDC617D0	99442C8F83A3C5090CA50C1C0B1DE4B32ED418FF0AA7C3240E91230159F3E7BF	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	1E6AEADEF52FBFA8D36CC7C63FDB6C6460DCE341	96A5A2CD39800CFB6A2A830EE52DCF47FBB00FF1B03204DB36915CEA31F13342	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	1E6AEADEF52FBFA8D36CC7C63FDB6C6460DCE341	55324A9832512FC6C99F15BF0E9ED3D6BEB4398CCEE194B7FF849D96D9130D44	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE6180C09990596DD62455F2FFC0EB2717EC	5DB60C2D6B6BECF314477589A3A4FB4CCF84649D69B0B21B3D6B2ABA78BD35FB	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE6180C09990596DD62455F2FFC0EB2717EC	86C6707BBE27CDE1215E25D3F8146A522281E18C45DF2CB8C6FB7A03C1733510	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	116492AEA041621C2084B7D38881D1CD8072C77F	3253412FDAD4523108C098BB0EE0EFEDD7FAFDD00FB30E47C6BBA9FE3E1CDB88	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	827A42A2BE5C08BBADF14CA6EB71B58B1201F329	71A1A38FF485137002DD5CD780B3873DDE146723EE28080ECF3738C7C4FEB1AE	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	28B9AF467654EA51D4B2810E540916D2DEEFF386	FA920C8539428B3CB4BF77BE2532BC6D0DDD97EB664EE8BEA297DAAD147EA76F	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	0B630E582F1B860F85B257B24A3131C4A970A19B	203D73A528847AAA7B4EA16098B048215B311BFB3E24AB27DCD7B15BDF83C1D6	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	0C2556EAFD7A04DDC2AE623909693113 8EBE91D8	E43F7A0BAF943180D7D40FED2E54965BD674DC2C82EFAB2A5108AA3D6664A641	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	FBF66620D2AA7B2C10CB52E259D40A153C11E3F7	13CD63B1F4A3F41914BD7EA3362DBEE075A2291382068616222297BF643598961	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	0B1C0C1723AD9F26C4928AFC7F77FD1627097831	1DDCBC25FC8E9987B5F425A2131550D38329A663DB08F15BDDDB71F2BF87E200	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	5543FAB389F57FD55AD4FEB1258451E2C86ABEF7	18CDC6E98BE17513D4F12B72FFB8FA7437FD18A21352C2695EB68BB91D0B1BAD	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	49EE724EDA99640CE14480ED731D35FC8D4243C4	F051A99F5630D835FAF6F6D1A50DD92B36A127DF3B12B54317A07630FCDB0307	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	C87CB0D420A5DB5697F29730C88A61899FA5F222	EA152FD132DE4F4E71930A9760517A81DACBBB5F1014D8BD7782AC0CC37E9431	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	BCB2E53526589289 93BC96AC2344456B4644C7BF	08646322AE51E91C8D61D90A2D11F4D3BA6D386A414256B66AD57116934A9EC3	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	55612DF062120F01ECEF127A6E5AC45D0299A22C	AA0E436C04420376287C9AC94A38B975B84DF16F0C630FF079E750DADD03453A	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	428A21F3DD52570A928FC182C4C615B5AEC63EFB	1A404FB498FC8D525DEEAC47299CABA3D4A716D94AD55DFAFCF7B6576AFA6466	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	5BB1FEC68A2F902E21DDCEEDDAAAFB2570F2D067	BA4B5FB3FD54BE90EBBAC6AEBF512D2FC490B1D6397BC4E779F2ED3D34D0D721	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	9F5C6CA8E4A530A57DE3168128EBFCB1C16C0D760	E5AB9FA5362A0F0137C84541B4F6829087307329BE3C05F8BC4A2811159B7BFF	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	1D60F5967C36559221E343DBC8C862D3BBC34684	007B5E81298733CB0FF0EA8D2FBAE9BC554A05EC39576E0D0F2EABDA3289E1E1	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BD90963A7CC81C8E2114AD921F8A30239A3880F8	760F03A6A7F99BA47E42DF456B0E3ED2D8DF9918115797396CE83E95040AF547	GDCA TrustAUTH E5 ROOT

附件二

范围内适用之CP/CPS版本:

Name	Version	Release Date
GDCA CPS	5.4	5 February 2021
GDCA CPS	5.3	1 October 2020
GDCA CPS	5.2	20 August 2020
GDCA CPS	5.1	31 May 2020
GDCA EV CPS	2.3	1 October 2020
GDCA EV CPS	2.2	20 August 2020
GDCA EV CPS	2.1	31 May 2020
GDCA CP	2.5	5 February 2021
GDCA CP	2.4	1 October 2020
GDCA CP	2.3	20 August 2020
GDCA CP	2.2	31 May 2020
GDCA EV CP	2.2	1 October 2020
GDCA EV CP	2.1	20 August 2020
GDCA EV CP	2.0	31 May 2020

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

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（附件一列示了服务所包括的根证书和中级证书），并提供以下电子认证（以下简称“CA”）服务：

- 订户注册
- 电子证书更新
- 电子证书密钥更新
- 电子证书发布
- 电子证书分发
- 电子证书吊銷
- 电子证书状态查询
- 订户密钥和证书管理

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

任何控制都有其固有限制，包括人为失误，以及规避或逾越控制的可能性。因此，即使有效的控制也仅能对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，GDCA 管理层认为，在2020 年3 月1 日至2021 年2 月28 日就GDCA 在中国广州和佛山所提供的电子认证服务期间，GDCA已：

- 於附件二之CP/CPS披露电子认证业务、密钥生命周期管理、证书生命周期管理，以及CA环境控制管理

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

- 通过有效控制机制，以提供以下合理保证：
  - 有效维护所管理的密钥与证书在生命周期中的完整性；
  - 建立并保护所管理的订户密钥和订户证书在生命周期中的完整性；以及
  - 于GDCA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 电子认证审计标准V2.2（WebTrust Principles and Criteria for Certification Authorities v2.2），包括以下内容：

CA业务规则披露

- 电子认证业务规则（CPS）
- 证书策略（CP）

CA业务规则管理

- 证书策略管理
- 电子认证业务规则管理
- CP和CPS的一致性

CA环境控制

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

CA密钥生命周期管理

- CA密钥生成
- CA密钥保管、备份及恢复
- CA公钥发布
- CA密钥用途
- CA密钥归档和销毁
- CA密钥泄露
- CA加密设备生命周期管理

订户密钥生命周期管理

- 订户密钥生成服务
- 智能芯片卡生命週期管理
- 订户密钥管理要求

电子证书生命周期管理

- 用户注册
- 电子证书更新

- 电子证书密钥更新
- 电子证书颁发
- 电子证书发布
- 电子证书撤销
- 电子证书状态查询

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2020年9月1日曾于Mozilla Bugzilla公众平台揭漏事件Bug 1662382。于此事件中，一张数字证书因organizationName栏位输入错误發生误签，此张误签的数字证书于24个小时内被GDCA發现并完成吊销。关于此事件的發生根本原因与整改方案，GDCA业已于公众平台阐明，此议题的相关讨论于2020年10月5日结束。

副总经理 廖智敏
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
2021年5月12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	E2C9409F4DCEE89AA17CCF0E3F65C529886A1951	BFFF8FD04433487D6A8AA60C1A29767A9FC2BBB05E420F713A13B992891D3893	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	686223D3A9DFC522D155654D64762589AAB6D074	882E0146D15D3483EE5981E35067F1449E562B89E22ECC3FDF37274EDD314CDA	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	686223D3A9DFC522D155654D64762589AAB6D074	BEC06F55344C3DE4F12CD5D808906CDE275234951BE0176A787E628E2BE7D51F	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A2D739636727D5D1EB6E2812369CF68E4	051C238FAD7C1DC0FCEB4AEF79CAE97FE49A82DA8916A4A0920F307AACD60F81	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 CodeSigning CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	49FD9E1A2D739636727D5D1EB6E2812369CF68E4	2F2F008817710A1085B4E6BC5E3335474444D983272E33995A331BE1A4C4FE0A	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	C0F67A5BBE7C08C6AD04BB486145B0F56257A0B3	5600AFB6BAE2A83B66B9CBBE9CEEC8F53E26420A69939A48DCC6D56B99790A63	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 SSL CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	C0F67A5BBE7C08C6AD04BB486145B0F56257A0B3	1E96ABB2D6502B5DCE518EC00B5A1E543349EFD2E3F68BE9ABC1128B256FEDD7	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	7313CE83C60C2AA02692AE3F7B4074B5300B3595	74468180CE564BAD7E812210AF743E85CA96CBA44CF5851FA00082341B2535F5	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	5503AE8E0735A81763DBC9D61E3E639DDDC617D0	99442C8F83A3C5090CA50C1C0B1DE4B32ED418FF0AA7C3240E91230159F3E7BF	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	1E6AEADEF52FBFA8D36CC7C63FDB6C6460DCE341	96A5A2CD39800CFB6A2A830EE52DCF47FBB00FF1B03204DB36915CEA31F13342	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	1E6AEADEF52FBFA8D36CC7C63FDB6C6460DCE341	55324A9832512FC6C99F15BF0E9ED3D6BEB4398CCEE194B7FF849D96D9130D44	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE6180C09990596DD62455F2FFC0EB2717EC	5DB60C2D6B6BECF314477589A3A4FB4CCF84649D69B0B21B3D6B2ABA78BD35FB	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Generic CA O = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. C = CN	Signing Key	sha256RSA	2048 bits	D3FEEE6180C09990596DD62455F2FFC0EB2717EC	86C6707BBE27CDE1215E25D3F8146A522281E18C45DF2CB8C6FB7A03C1733510	GDCA TrustAUTH R5 ROOT
CN = GDCA TrustAUTH R4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha256RSA	2048 bits	116492AEA041621C2084B7D38881D1CD8072C77F	3253412FDAD4523108C098BB0EE0EFEDD7FAFDD00FB30E47C6BBA9FE3E1CDB88	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	827A42A2BE5C08BBADF14CA6EB71B58B1201F329	71A1A38FF485137002DD5CD780B3873DDE146723EE28080ECF3738C7C4FEB1AE	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	28B9AF467654EA51D4B2810E540916D2DEEFF386	FA920C8539428B3CB4BF77BE2532BC6D0DDD97EB664EE8BEA297DAAD147EA76F	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	0B630E582F1B860F85B257B24A3131C4A970A19B	203D73A528847AAA7B4EA16098B048215B311BFB3E24AB27DCD7B15BDF83C1D6	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	0C2556EAFD7A04DDC2AE623909693113 8EBE91D8	E43F7A0BAF943180D7D40FED2E54965BD674DC2C82EFAB2A5108AA3D6664A641	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	FBF66620D2AA7B2C10CB52E259D40A153C11E3F7	13CD63B1F4A3F41914BD7EA3362DBEE075A2291382068616222297BF643598961	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	0B1C0C1723AD9F26C4928AFC7F77FD1627097831	1DDCBC25FC8E9987B5F425A2131550D38329A663DB08F15BDDDB71F2BF87E200	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	5543FAB389F57FD55AD4FEB1258451E2C86ABEF7	18CDC6E98BE17513D4F12B72FFB8FA7437FD18A21352C2695EB68BB91D0B1BAD	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	49EE724EDA99640CE14480ED731D35FC8D4243C4	F051A99F5630D835FAF6F6D1A50DD92B36A127DF3B12B54317A07630FCDB0307	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	C87CB0D420A5DB5697F29730C88A61899FA5F222	EA152FD132DE4F4E71930A9760517A81DACBBB5F1014D8BD7782AC0CC37E9431	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	BCB2E53526589289 93BC96AC2344456B4644C7BF	08646322AE51E91C8D61D90A2D11F4D3BA6D386A414256B66AD57116934A9EC3	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	55612DF062120F01ECEF127A6E5AC45D0299A22C	AA0E436C04420376287C9AC94A38B975B84DF16F0C630FF079E750DADD03453A	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	428A21F3DD52570A928FC182C4C615B5AEC63EFB	1A404FB498FC8D525DEEAC47299CABA3D4A716D94AD55DFAFCF7B6576AFA6466	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	5BB1FEC68A2F902E21DDCEEDDAAAFB2570F2D067	BA4B5FB3FD54BE90EBBAC6AEBF512D2FC490B1D6397BC4E779F2ED3D34D0D721	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 CodeSigning CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	9F5C6CA8E4A530A57DE316812EBFCB1C16C0D760	E5AB9FA5362A0F0137C84541B4F6829087307329BE3C05F8BC4A2811159B7BFF	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Generic CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	1D60F5967C36559221E343DBC8C862D3BBC34684	007B5E81298733CB0FF0EA8D2FBAE9BC554A05EC39576E0D0F2EABDA3289E1E1	GDCA TrustAUTH E5 ROOT
CN = GDCA TrustAUTH E4 Primer CA O = Global Digital Cybersecurity Authority Co., Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	BD90963A7CC81C8E2114AD921F8A30239A3880F8	760F03A6A7F99BA47E42DF456B0E3ED2D8DF9918115797396CE83E95040AF547	GDCA TrustAUTH E5 ROOT

附件二

范围内适用之CP/CPS版本:

Name	Version	Release Date
GDCA CPS	5.4	5 February 2021
GDCA CPS	5.3	1 October 2020
GDCA CPS	5.2	20 August 2020
GDCA CPS	5.1	31 May 2020
GDCA CPS	5.0	20 September 2019
GDCA EV CPS	2.3	1 October 2020
GDCA EV CPS	2.2	20 August 2020
GDCA EV CPS	2.1	31 May 2020
GDCA EV CPS	2.0	20 September 2019
GDCA CP	2.5	5 February 2021
GDCA CP	2.4	1 October 2020
GDCA CP	2.3	20 August 2020
GDCA CP	2.2	31 May 2020
GDCA CP	2.1	20 September 2019
GDCA EV CP	2.2	1 October 2020
GDCA EV CP	2.1	20 August 2020
GDCA EV CP	2.0	31 May 2020
GDCA EV CP	1.9	20 September 2019