Global Digital Cybersecurity Authority Co., Ltd.
Ke Jiao Rd, Nanhai Software Technology Park,
Shishan Town, Nanhai District
Foshan, China

Report of Independent Accountant on Assessment of the Assertion by the management of Global Digital Cybersecurity Authority Co., Ltd. ("GDCA")

To: Mr. Liu Qiang
General Manager, Global Digital Cybersecurity Authority Co., Ltd.

We have been engaged, in a reasonable assurance engagement, to report on the accompanying Global Digital Cybersecurity Authority Co., Ltd. ("GDCA") Webtrust management's assertion that for its Certification Authority (CA) operations at GuangZhou and FoShan, China, throughout the period 1 March 2016 to 28 February 2017 for its Root and Subordinate CAs listed in the appendix of the management's assertion, GDCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
  - Certification Practice Statement Version 4.4 (https://www.gdca.com.cn/export/sites/default/customer_service/.content/attachments/1.GDCA-CPS-V4.4.pdf); and
  - Certificate Policy Version 1.5 (https://www.gdca.com.cn/export/sites/default/customer_service/.content/attachments/1.GDCA-CP-V1.5.pdf)

- 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;
  - subscriber information is properly authenticated (for the registration activities performed by GDCA); and
  - subordinate CA certificate requests are accurate, authenticated, and approved (GDCA does not have any subordinate CA)

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;

INDEPENDENT ASSURANCE REPORT (CONTINUED)
Global Digital Cybersecurity Authority Co., Ltd.

- 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 V2.0 (http://www.webtrust.org/homepage-documents/item54279.pdf).

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 V2.0.

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 behavior.

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;

INDEPENDENT ASSURANCE REPORT (CONTINUED)
Global Digital Cybersecurity Authority Co., Ltd.

(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 2016 to 28 February 2017, 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 V2.0.

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 V2.0, 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.

INDEPENDENT ASSURANCE REPORT (CONTINUED)
Global Digital Cybersecurity Authority Co., Ltd.

Restriction on Use and Distribution

Our report is intended solely for the use of GDCA to submit the report to the related authority in connection with the WebTrust Principles and Criteria for Certification Authorities V2.0, and may not be suitable for another purpose. This report is not intended to be, and should not be distributed to or used, for any other purpose.

PricewaterhouseCoopers Zhong Tian LLP
Shanghai, China
14 April 2017

普华永道

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

对数安时代科技股份有限公司管理层认定发表的独立鉴证报告
（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总经理刘镪先生

我们接受委托，对后附的数安时代科技股份有限公司（Global Digital Cybersecurity Authority Co., Ltd.，简称“GDCA”）于 2016 年 3 月 1 日至 2017 年 2 月 28 日止期间于中国广州和佛山运营的电子认证服务管理层认定执行了合理保证的鉴证业务。根据管理层认定，GDCA：

- 披露 SSL 证书生命周期管理业务规则于：
  - 电子认证业务规则（CPS） V4.4（https://www.gdca.com.cn/export/sites/default/customer_service/.content/attachments/1.GDCA-CPS-V4.4.pdf）；以及
  - 证书策略（CP）V1.5（https://www.gdca.com.cn/export/sites/default/customer_service/.content/attachments/1.GDCA-CP-V1.5.pdf）。

- 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；
  - 恰当地鉴定（GDCA 所执行的注册操作）订户证书申请者的信息；以及
  - 下级 CA 证书请求是准确、经鉴定并通过批准的。（GDCA 无任何下级子 CA）

- 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 V2.0（Trust Services Principles and Criteria for Certification Authorities V2.0）（http://www.webtrust.org/homepage-documents/item54279.pdf）

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电子认证审计标准V2.0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） 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。

独立鉴证报告（续）
数安时代科技股份有限公司

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 2016 年 3 月 1 日至 2017 年 2 月 28 日止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 电子认证审计标准 V2.0。

本报告并不包括任何在 WebTrust 电子认证审计标准 V2.0 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。

使用和分发限制

本报告仅供GDCA根据WebTrust电子认证审计标准V2.0的要求而向有关机构提交时使用，不适用于任何其他目的。除了将本报告副本提供给WebTrust以外，本报告非为其他目的编制，也不能为其他目的分发或使用。

普华永道中天会计师事务所（特殊普通合伙）

中国上海市
2017年4月14日

Global Digital Cybersecurity Authority Co., Ltd.

Addr: Global Digital Cybersecurity Authority Co.,Ltd. Ke Jiao Rd, Nanhai Software Technology Park, Shishan Town,
Nanhai District, Foshan City,
Guangdong Province
Zip: 528225
Tel: (0757) 86681781
Fax: (0757) 86682880
https://www.gdca.com.cn

PricewaterhouseCoopers Zhong Tian LLP
11th Floor
PricewaterhouseCoopers Center
2 Corporate Avenue
202 Hu Bin Road, Huangpu District
Shanghai 200021, PRC

14 April, 2017

Dear Sirs,

Assertion of Management as to the Disclosure of Business Practices and Controls Over the Certification Authority Operations during the period from 1 March, 2016 through 28 February, 2017

Global Digital Cybersecurity Authority Co., Ltd. ("GDCA") operates the Certification Authority (CA) services known as its Root and Subordinate CAs (please refer to the appendix), and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

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, certificate lifecycle management controls, and subordinate CA 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 2016 to 28 February 2017, GDCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
  - Certification Practice Statement Version 4.4 (https://www.gdca.com.cn/export/sites/default/customer_service/.content/attachments/1.GDCA-CPS-V4.4.pdf); and
  - Certificate Policy Version 1.5 (https://www.gdca.com.cn/export/sites/default/customer_service/.content/attachments/1.GDCA-CP-V1.5.pdf)

- 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;
  - subscriber information is properly authenticated (for the registration activities performed by GDCA); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- 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 v2.0 (http://www.webtrust.org/homepage-documents/item54279.pdf), 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

Certificate Lifecycle Management Controls

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

Mr. Liu Qiang
General Manager of Global Digital Cybersecurity Authority Co., Ltd.

Company Chop

Appendix

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	Certificates (Thumbprint)	Certificate Signed by
GDCA TrustAUTH R5 ROOT	Root Key	sha256RSA	4096 bits	e2 c9 40 9f 4d ce e8 9a a1 7c cf 0e 3f 65 c5 29 88 6a 19 51	0f 36 38 5b 81 1a 25 c3 9b 31 4e 83 ca e9 34 66 70 cc 74 b4	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 EV CodeSigning CA	Signing Key	sha256RSA	2048 bits	68 62 23 d3 a9 df c5 22 d1 55 65 4d 64 76 25 89 aa b6 d0 74	d5 6c 4f fb 6d c9 d1 c2 6d 98 a0 57 2a 75 24 80 71 cf 72 9d	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 Extended Validation CodeSigning CA	Signing Key	sha256RSA	2048 bits	68 62 23 d3 a9 df c5 22 d1 55 65 4d 64 76 25 89 aa b6 d0 74	ac e9 a0 22 fa 09 38 5a d3 a3 e7 9c af 34 fe 39 58 50 a4 82	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 CodeSigning CA	Signing Key	sha256RSA	2048 bits	49 fd 9e 1a 2d 73 96 36 72 7d 5d 1e b6 e2 81 23 69 cf 68 e4	fc 6d cb 06 a5 5b ff 76 83 64 27 5b 29 d6 4f 7c 3a a9 cf b4	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 CodeSigning CA	Signing Key	sha256RSA	2048 bits	49 fd 9e 1a 2d 73 96 36 72 7d 5d 1e b6 e2 81 23 69 cf 68 e4	b0 5c 15 74 ab 17 c5 5f 15 fc 1e 42 21 dd f9 27 76 54 47 bb	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 OV SSL CA	Signing Key	sha256RSA	2048 bits	c0 f6 7a 5b be 7c 08 c6 ad 04 bb 48 61 45 b0 f5 62 57 a0 b3	c3 4a d6 45 d5 79 1c 5f 22 e7 33 d7 53 47 08 15 85 75 6c 2d	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 SSL CA	Signing Key	sha256RSA	2048 bits	c0 f6 7a 5b be 7c 08 c6 ad 04 bb 48 61 45 b0 f5 62 57 a0 b3	f0 2b cb 1e 1e 56 56 73 59 80 c1 53 df 0d 43 62 92 4f 4c 10	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 DV SSL CA	Signing Key	sha256RSA	2048 bits	73 13 ce 83 c6 0c 2a a0 26 92 ae 3f 7b 40 74 b5 30 0b 35 95	30 18 4a 5b 92 4e 67 9e 7a 91 32 93 17 d0 56 0f 58 7e 69 7b	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 IV SSL CA	Signing Key	sha256RSA	2048 bits	55 03 ae 8e 07 35 a8 17 63 db c9 d6 1e 3e 63 9d dd c6 17 d0	78 ae a8 51 a3 1b 0f 04 9a f0 2c d0 f2 ad 91 40 60 4f a7 a3	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 EV SSL	Signing Key	sha256RSA	2048 bits	1e 6a ea de f5 2f bf a8 d3 6c c7 c6	c6 7a 61 4f 23 42 18 b7 9f be 91 40	GDCA TrustAUTH R5 ROOT

CA				3f db 6c 64 60 dc e3 41	c0 33 dc aa 73 2a 5c 4f	
GDCA TrustAUTH R4 Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	1e 6a ea de f5 2f bf a8 d3 6c c7 c6 3f db 6c 64 60 dc e3 41	20 ec 59 23 96 51 de c2 37 0d fd d0 75 97 6d c8 8c 01 32 7b	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 Generic CA	Signing Key	sha256RSA	2048 bits	d3 fe ee 61 80 c0 99 90 59 6d d6 24 55 f2 ff c0 eb 27 17 ec	6f ed 83 eb e1 83 cc 71 d0 ed e1 2a e8 77 e0 df 98 96 1f 24	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 Generic CA	Signing Key	sha256RSA	2048 bits	d3 fe ee 61 80 c0 99 90 59 6d d6 24 55 f2 ff c0 eb 27 17 ec	08 ef 1f 76 9a d6 10 ac a6 14 70 dd db 35 c5 d0 25 15 9d b5	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 Primer CA	Signing Key	sha256RSA	2048 bits	11 64 92 ae a0 41 62 1c 20 84 b7 d3 88 81 d1 cd 80 72 c7 7f	14 c2 b3 3b bf 6e bd 84 fc a7 01 54 13 eb d0 43 3e 17 1a 98	GDCA TrustAUTH R5 ROOT
数安时代 R5 根 CA	Root Key	sha256RSA	4096 bits	82 7a 42 a2 be 5c 08 bb ad f1 4c a6 eb 71 b5 8b 12 01 f3 29	23 eb 1b a4 64 71 a1 e7 e9 f2 db 57 01 fe f8 f2 f8 0c aa e9	数安时代 R5 根 CA
数安时代 R4 EV 服务器证书 CA	Signing Key	sha256RSA	2048 bits	28 b9 af 46 76 54 ea 51 d4 b2 81 0e 54 09 16 d2 de ef f3 86	0d 9d 15 af 72 5b eb a2 27 c4 29 43 23 10 c5 53 b7 b8 9b d3	数安时代 R5 根 CA
数安时代 R4 OV 服务器证书 CA	Signing Key	sha256RSA	2048 bits	0b 63 0e 58 2f 1b 86 0f 85 b2 57 b2 4a 31 31 c4 a9 70 a1 9b	93 92 5b 05 17 30 05 86 fd 2c 45 eb 18 6e 00 9e b9 75 a5 d0	数安时代 R5 根 CA
数安时代 R4 DV 服务器证书 CA	Signing Key	sha256RSA	2048 bits	0c 25 56 ea fd 7a 04 dd c2 ae 62 39 09 69 31 13 8e be 91 d8	01 ad 04 cd e1 05 56 23 4a f6 6f a0 e6 64 f3 a6 18 80 4d f5	数安时代 R5 根 CA
数安时代 R4 IV 服务器证书 CA	Signing Key	sha256RSA	2048 bits	fb f6 66 20 d2 aa 7b 2c 10 cb 52 e2 59 d4 0a 15 3c 11 e3 f7	10 b8 fb 9a d2 50 32 6a ee fb 05 ad da 9d 3a 2b bb bd 5d bf	数安时代 R5 根 CA
数安时代 R4 代码签名证书 CA	Signing Key	sha256RSA	2048 bits	0b 1c 0c 17 23 ad 9f 26 c4 92 8a fc 7f 77 fd 16 27 09 78 31	4f be 54 bc 70 8e b1 2a 11 86 dd 79 aa ff e7 95 f8 ad c6 e9	数安时代 R5 根 CA
数安时代 R4 普通订户证书	Signing Key	sha256RSA	2048 bits	55 43 fa b3 89 f5 7f d5	07 33 29 cb 53 b1 86 36	数安时代 R5 根 CA

CA				5a d4 fe b1 25 84 51 e2 c8 6a be f7	25 38 1b fb 48 a0 43 a7 b1 fe 28 6f	
数安时代 R4 基础订户证书 CA	Signing Key	sha256RSA	2048 bits	49 ee 72 4e da 99 64 0c e1 44 80 ed 73 1d 35 fc 8d 42 43 c4	e5 da 52 2d 5f 38 7a 6e 72 49 5e 66 a4 be ba 0f 24 f2 59 dc	数安时代 R5 根 CA
GDCA TrustAUTH E5 ROOT	Root Key	sha384ECDSA	384 bits	c8 7c b0 d4 20 a5 db 56 97 f2 97 30 c8 8a 61 89 9f a5 f2 22	eb 46 6c d3 75 65 f9 3c de 10 62 cd 8d 98 26 ed 23 73 0f 12	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 EV SSL CA	Signing Key	sha384ECDSA	256 bits	bc b2 e5 35 26 58 92 89 93 bc 96 ac 23 44 45 6b 46 44 c7 bf	1f ae a7 c3 5e 84 b9 5a 55 f6 c7 d7 fd 2f e5 21 ea 77 72 59	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 OV SSL CA	Signing Key	sha384ECDSA	256 bits	55 61 2d f0 62 12 0f 01 ec ef 12 7a 6e 5a c4 5d 02 99 a2 2c	50 15 62 d8 1b a2 40 27 1b ee 06 d2 b3 7f 5b 35 cb 9d 8c b8	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 DV SSL CA	Signing Key	sha384ECDSA	256 bits	42 8a 21 f3 dd 52 57 0a 92 8f c1 82 c4 c6 15 b5 ae c6 3e fb	8e 9b 9a db f5 ec c4 6b 05 76 82 2e de 5e 80 d1 57 6b 5d 7c	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 IV SSL CA	Signing Key	sha384ECDSA	256 bits	5b b1 fe c6 8a 2f 90 2e 21 dd ce ed da aa fb 25 70 f2 d0 67	a8 45 2b fc 20 f9 de b6 9b 8b 3f 29 73 e0 a3 b3 6f 82 eb 5b	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 CodeSigning CA	Signing Key	sha384ECDSA	256 bits	9f 5c 6c a8 e4 a5 30 a5 7d e3 16 81 2e bf cb 1c 16 c0 d7 60	10 6a 4e 5d ca 05 92 28 e4 ff 89 52 66 53 a4 64 7d 57 ee 63	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 Generic CA	Signing Key	sha384ECDSA	256 bits	1d 60 f5 96 7c 36 55 92 21 e3 43 db c8 c8 62 d3 bb c3 46 84	fd 63 ba 6e e7 89 f6 0a 16 72 b5 b3 3a 29 7d 71 71 65 54 ee	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 Primer CA	Signing Key	sha384ECDSA	256 bits	bd 90 96 3a 7c c8 1c 8e 21 14 ad 92 1f 8a 30 23 9a 38 80 f8	5f 42 a4 4d c8 ca 12 df ae 1c 29 92 1f 47 3e 3b be 8b d4 2c	GDCA TrustAUTH E5 ROOT

数安时代科技股份有限公司

地址：数安时代科技股份有限公司，
广东省佛山市南海区狮山镇南海软件科技园
科教路
邮编：528225
电话：(0757) 86681781
传真：(0757) 86682880
https://www.gdca.com.cn

普华永道中天会计师事务所（特殊普通合伙）
中国上海市黄浦区湖滨路202号
企业天地2号楼
普华永道中心11楼

2017 年 4 月 14 日

致：普华永道中天会计师事务所（特殊普通合伙）：

就 2016 年 3 月 1 日到 2017 年 2 月 28 日期间电子认证服务的管理层认定报告
（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
- 电子证书撤销
- 电子证书状态查询

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，证书生命周期管理，以及下级 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 2016 年 3 月 1 日至 2017 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：

- 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环境控制管理于：

- 电子认证业务规则（CPS）V4.4（https://www.gdca.com.cn/export/sites/default/customer_service/.content/attachments/1.GDCA-CPS-V4.4.pdf）；以及
- 证书策略（CP）V1.5（https://www.gdca.com.cn/export/sites/default/customer_service/.content/attachments/1.GDCA-CP-V1.5.pdf）。

- 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；
- 恰当地鉴定（GDCA 所执行的注册操作）订户证书申请者的信息；以及
- 下级 CA 证书请求是准确、经鉴定并通过批准的。

- 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 V2.0（Trust Services Principles and Criteria for Certification Authorities V2.0）（http://www.webtrust.org/homepage-documents/item54279.pdf），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

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

刘镭
数安时代科技股份有限公司总经理

公司盖章

附件

下表列示本认定报告所包括的密钥和证书：

密钥名称	密钥种类	密钥算法	密钥长度	密钥 ID	证书指纹	证书签发者
GDCA TrustAUTH R5 ROOT	Root Key	sha256 RSA	4096 bits	e2 c9 40 9f 4d ce e8 9a a1 7c cf 0e 3f 65 c5 29 88 6a 19 51	0f 36 38 5b 81 1a 25 c3 9b 31 4e 83 ca e9 34 66 70 cc 74 b4	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 EV CodeSigning CA	Signing Key	sha256 RSA	2048 bits	68 62 23 d3 a9 df c5 22 d1 55 65 4d 64 76 25 89 aa b6 d0 74	d5 6c 4f fb 6d c9 d1 c2 6d 98 a0 57 2a 75 24 80 71 cf 72 9d	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 Extended Validation CodeSigning CA	Signing Key	sha256 RSA	2048 bits	68 62 23 d3 a9 df c5 22 d1 55 65 4d 64 76 25 89 aa b6 d0 74	ac e9 a0 22 fa 09 38 5a d3 a3 e7 9c af 34 fe 39 58 50 a4 82	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 CodeSigning CA	Signing Key	sha256 RSA	2048 bits	49 fd 9e 1a 2d 73 96 36 72 7d 5d 1e b6 e2 81 23 69 cf 68 e4	fc 6d cb 06 a5 5b ff 76 83 64 27 5b 29 d6 4f 7c 3a a9 cf b4	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 CodeSigning CA	Signing Key	sha256 RSA	2048 bits	49 fd 9e 1a 2d 73 96 36 72 7d 5d 1e b6 e2 81 23 69 cf 68 e4	b0 5c 15 74 ab 17 c5 5f 15 fc 1e 42 21 dd f9 27 76 54 47 bb	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 OV SSL CA	Signing Key	sha256 RSA	2048 bits	c0 f6 7a 5b be 7c 08 c6 ad 04 bb 48 61 45 b0 f5 62 57 a0 b3	c3 4a d6 45 d5 79 1c 5f 22 e7 33 d7 53 47 08 15 85 75 6c 2d	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 SSL CA	Signing Key	sha256 RSA	2048 bits	c0 f6 7a 5b be 7c 08 c6 ad 04 bb 48 61 45 b0 f5 62 57 a0 b3	f0 2b cb 1e 1e 56 56 73 59 80 c1 53 df 0d 43 62 92 4f 4c 10	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 DV SSL CA	Signing Key	sha256 RSA	2048 bits	73 13 ce 83 c6 0c 2a a0 26 92 ae 3f 7b 40 74 b5 30 0b 35 95	30 18 4a 5b 92 4e 67 9e 7a 91 32 93 17 d0 56 0f 58 7e 69 7b	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 IV SSL CA	Signing Key	sha256 RSA	2048 bits	55 03 ae 8e 07 35 a8 17 63 db c9 d6 1e 3e 63 9d dd c6 17 d0	78 ae a8 51 a3 1b 0f 04 9a f0 2c d0 f2 ad 91 40 60 4f a7 a3	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 EV SSL	Signing Key	sha256 RSA	2048 bits	1e 6a ea de f5 2f bf a8 d3 6c c7 c6	c6 7a 61 4f 23 42 18 b7 9f be 91 40	GDCA TrustAUTH R5 ROOT

CA				3f db 6c 64 60 dc e3 41	c0 33 dc aa 73 2a 5c 4f	
GDCA TrustAUTH R4 Extended Validation SSL CA	Signing Key	sha256 RSA	2048 bits	1e 6a ea de f5 2f bf a8 d3 6c c7 c6 3f db 6c 64 60 dc e3 41	20 ec 59 23 96 51 de c2 37 0d fd d0 75 97 6d c8 8c 01 32 7b	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 Generic CA	Signing Key	sha256 RSA	2048 bits	d3 fe ee 61 80 c0 99 90 59 6d d6 24 55 f2 ff c0 eb 27 17 ec	6f ed 83 eb e1 83 cc 71 d0 ed e1 2a e8 77 e0 df 98 96 1f 24	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 Generic CA	Signing Key	sha256 RSA	2048 bits	d3 fe ee 61 80 c0 99 90 59 6d d6 24 55 f2 ff c0 eb 27 17 ec	08 ef 1f 76 9a d6 10 ac a6 14 70 dd db 35 c5 d0 25 15 9d b5	GDCA TrustAUTH R5 ROOT
GDCA TrustAUTH R4 Primer CA	Signing Key	sha256 RSA	2048 bits	11 64 92 ae a0 41 62 1c 20 84 b7 d3 88 81 d1 cd 80 72 c7 7f	14 c2 b3 3b bf 6e bd 84 fc a7 01 54 13 eb d0 43 3e 17 1a 98	GDCA TrustAUTH R5 ROOT
数安时代 R5 根 CA	Root Key	sha256 RSA	4096 bits	82 7a 42 a2 be 5c 08 bb ad f1 4c a6 eb 71 b5 8b 12 01 f3 29	23 eb 1b a4 64 71 a1 e7 e9 f2 db 57 01 fe f8 f2 f8 0c aa e9	数安时代 R5 根 CA
数安时代 R4 EV 服务器证书 CA	Signing Key	sha256 RSA	2048 bits	28 b9 af 46 76 54 ea 51 d4 b2 81 0e 54 09 16 d2 de ef f3 86	0d 9d 15 af 72 5b eb a2 27 c4 29 43 23 10 c5 53 b7 b8 9b d3	数安时代 R5 根 CA
数安时代 R4 OV 服务器证书 CA	Signing Key	sha256 RSA	2048 bits	0b 63 0e 58 2f 1b 86 0f 85 b2 57 b2 4a 31 31 c4 a9 70 a1 9b	93 92 5b 05 17 30 05 86 fd 2c 45 eb 18 6e 00 9e b9 75 a5 d0	数安时代 R5 根 CA
数安时代 R4 DV 服务器证书 CA	Signing Key	sha256 RSA	2048 bits	0c 25 56 ea fd 7a 04 dd c2 ae 62 39 09 69 31 13 8e be 91 d8	01 ad 04 cd e1 05 56 23 4a f6 6f a0 e6 64 f3 a6 18 80 4d f5	数安时代 R5 根 CA
数安时代 R4 IV 服务器证书 CA	Signing Key	sha256 RSA	2048 bits	fb f6 66 20 d2 aa 7b 2c 10 cb 52 e2 59 d4 0a 15 3c 11 e3 f7	10 b8 fb 9a d2 50 32 6a ee fb 05 ad da 9d 3a 2b bb bd 5d bf	数安时代 R5 根 CA
数安时代 R4 代码签名证书 CA	Signing Key	sha256 RSA	2048 bits	0b 1c 0c 17 23 ad 9f 26 c4 92 8a fc 7f 77 fd 16 27 09 78 31	4f be 54 bc 70 8e b1 2a 11 86 dd 79 aa ff e7 95 f8 ad c6 e9	数安时代 R5 根 CA
数安时代 R4 普通订户证书	Signing Key	sha256 RSA	2048 bits	55 43 fa b3 89 f5 7f d5	07 33 29 cb 53 b1 86 36	数安时代 R5 根 CA

CA				5a d4 fe b1 25 84 51 e2 c8 6a be f7	25 38 1b fb 48 a0 43 a7 b1 fe 28 6f	
数安时代 R4 基础订户证书 CA	Signing Key	sha256 RSA	2048 bits	49 ee 72 4e da 99 64 0c e1 44 80 ed 73 1d 35 fc 8d 42 43 c4	e5 da 52 2d 5f 38 7a 6e 72 49 5e 66 a4 be ba 0f 24 f2 59 dc	数安时代 R5 根 CA
GDCA TrustAUTH E5 ROOT	Root Key	sha384 ECDSA	384 bits	c8 7c b0 d4 20 a5 db 56 97 f2 97 30 c8 8a 61 89 9f a5 f2 22	eb 46 6c d3 75 65 f9 3c de 10 62 cd 8d 98 26 ed 23 73 0f 12	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 EV SSL CA	Signing Key	sha384 ECDSA	256 bits	bc b2 e5 35 26 58 92 89 93 bc 96 ac 23 44 45 6b 46 44 c7 bf	1f ae a7 c3 5e 84 b9 5a 55 f6 c7 d7 fd 2f e5 21 ea 77 72 59	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 OV SSL CA	Signing Key	sha384 ECDSA	256 bits	55 61 2d f0 62 12 0f 01 ec ef 12 7a 6e 5a c4 5d 02 99 a2 2c	50 15 62 d8 1b a2 40 27 1b ee 06 d2 b3 7f 5b 35 cb 9d 8c b8	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 DV SSL CA	Signing Key	sha384 ECDSA	256 bits	42 8a 21 f3 dd 52 57 0a 92 8f c1 82 c4 c6 15 b5 ae c6 3e fb	8e 9b 9a db f5 ec c4 6b 05 76 82 2e de 5e 80 d1 57 6b 5d 7c	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 IV SSL CA	Signing Key	sha384 ECDSA	256 bits	5b b1 fe c6 8a 2f 90 2e 21 dd ce ed da aa fb 25 70 f2 d0 67	a8 45 2b fc 20 f9 de b6 9b 8b 3f 29 73 e0 a3 b3 6f 82 eb 5b	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 CodeSigning CA	Signing Key	sha384 ECDSA	256 bits	9f 5c 6c a8 e4 a5 30 a5 7d e3 16 81 2e bf cb 1c 16 c0 d7 60	10 6a 4e 5d ca 05 92 28 e4 ff 89 52 66 53 a4 64 7d 57 ee 63	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 Generic CA	Signing Key	sha384 ECDSA	256 bits	1d 60 f5 96 7c 36 55 92 21 e3 43 db c8 c8 62 d3 bb c3 46 84	fd 63 ba 6e e7 89 f6 0a 16 72 b5 b3 3a 29 7d 71 71 65 54 ee	GDCA TrustAUTH E5 ROOT
GDCA TrustAUTH E4 Primer CA	Signing Key	sha384 ECDSA	256 bits	bd 90 96 3a 7c c8 1c 8e 21 14 ad 92 1f 8a 30 23 9a 38 80 f8	5f 42 a4 4d c8 ca 12 df ae 1c 29 92 1f 47 3e 3b be 8b d4 2c	GDCA TrustAUTH E5 ROOT