普华永道

Independent practitioner's assurance report

2020/BJ-0096

To the management of iTrusChina Co., Ltd ("iTrusChina"):

We have been engaged to perform a reasonable assurance engagement on the accompanying management's assertion of iTrusChina Co., Ltd ("iTrusChina") for its Certification Authority operations for the period from January 9, 2019 to January 8, 2020.

Management's Responsibilities

iTrusChina'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 – Version 2.2.

Our Independence and Quality Control

We have complied with the independence and other ethical requirement of the International Code of Ethics for Professional Accountants (including International Independence Standards) 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.

Our 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.

Practitioner's Responsibilities

It is our responsibility to express an opinion on the accompanying management's assertion of iTrusChina based on our work performed.

We conducted our work in accordance with the International Standard on Assurance Engagements 3000 (Revised) "Assurance Engagements Other Than Audits or Reviews of Historical Financial Information". This standard requires that we plan and perform our work to form the opinion.

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence whether the management's assertion of iTrusChina is fairly stated, in all material respects, in accordance with WebTrust Principles and Criteria for Certification Authorities – Version 2.2.

The extent of procedures selected depends on the practitioner's judgment and our assessment of the engagement risk. Within the scope of our work, we performed amongst others the following procedures:

Independent practitioner's assurance report (Continued)

(1) obtaining an understanding of iTrusChina'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.

The relative effectiveness and significance of specific controls at iTrusChina 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 subscribers and relying party locations. We do not provide any assurance on the effectiveness of controls at individual subscribers and relying party locations.

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

Inherent Limitation

We draw attention to the fact that WebTrust Principles and Criteria for Certification Authorities – Version 2.2 includes certain inherent limitations that can influence the reliability of the information.

For example, controls may not prevent, or detect and correct, error, fraud, unauthorised 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, the accompanying management's assertion of iTrusChina, for the period from January 9, 2019 to January 8, 2020, is fairly stated, in all material respects, in accordance with WebTrust Principles and Criteria for Certification Authorities – Version 2.2.

Emphasis of Matter

Without modifying our opinion, we draw attention to the fact that this report does not include any representation as to the quality of iTrusChina's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Version 2.2, nor the suitability of any of the iTrusChina's services for any customer's intended purpose.

Independent practitioner's assurance report (Continued)

Other Matter

iTrusChina'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.

Purpose and Restriction on Use and Distribution

The accompanying management's assertion of iTrusChina was prepared for obtaining and displaying the WebTrust Seal [1] on its website using WebTrust Principles and Criteria for Certification Authorities – Version 2.2 designed for this purpose. As a result, the accompanying management's assertion of iTrusChina may not be suitable for another purpose. This report is intended solely for the Management of iTrusChina in connection with obtaining and displaying the WebTrust Seal on its website after submitting the report to the related authority in connection with the WebTrust Principles and Criteria for Certification Authorities – Version 2.2 and should not be distributed to or used by any other parties for any other purpose. We do not assume responsibility towards or accept liability to any other person for the contents of this report.

PricewaterhouseCoopers Zhong Tian LLP Beijing Branch

Beijing, China

March 25, 2020

1 The maintenance and integrity of the iTrusChina website is the responsibility of the directors. The work carried out by the assurance provider does not involve consideration of these matters and, accordingly, the assurance provider accepts no responsibility for any differences between the accompanying assertion by the management of iTrusChina on which the assurance report was issued or the assurance report that was issued and the information presented on the website.

iTrusChina Co.,Ltd.
Room 401A, Building 4, Yard 7, Shangdi 8th RD
Haidian District, Beijing.
Tel: 010-50947500
Fax: 010-50947517/50947516
Http://www.itrus.com.cn/

PricewaterhouseCoopers Zhong Tian LLP, Beijing Branch
26/F Tower A
Beijing Fortune Plaza, 7 DongsanhuanZhong Road
Chaoyang District, Beijing 100020, PRC

March 25, 2020

Dear Sirs,

Assertion by Management of iTrusChina Co., Ltd. regarding its Disclosure of Business Practices and its Controls over its Certification Authority Operations during the period of January 9, 2019 through January 8, 2020.

iTrusChina Co.,Ltd. ("iTrusChina") operates the Certification Authority (CA) services known as listed in the **Appendix**, and provides the following CA services:

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

Management of iTrusChina 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 iTrusChina's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of iTrusChina has assessed its disclosures of its certificate practices and

controls over its CA services. The key and certificates covered in our assessment are listed in the **Appendix** of this letter. Based on that assessment, in iTrusChina management's opinion, in providing its CA services at Mainland China, during the period of January 9, 2019 through January 8, 2020, iTrusChina has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - ITRUSCHINATM CERTIFICATION PRACTICE STATEMENT-v1.3.1; and
  - ITRUSCHINATM CERTIFICATIE POLICY-v1.3
- maintained effective controls to provide reasonable assurance that:
  - ITRUSCHINATM CERTIFICATION PRACTICE STATEMENT-v1.3.1 is consistent with its ITRUSCHINATM CERTIFICATIE POLICY-v1.3
  - iTrusChina provides its services in accordance with its ITRUSCHINATM CERTIFICATIE POLICY-v1.3 and ITRUSCHINATM CERTIFICATION PRACTICE STATEMENT-v1.3.1
- 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 iTrusChina); 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 lifecycle management operations is maintained; and
  - CA system development, maintenance and operations are properly authorized and performed to maintain CA system integrity

in accordance with WebTrust Principles and Criteria for Certification Authorities – Version 2.2, including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

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

CA Environmental Controls

- Security Management

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

CA Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

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

iTrusChina does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

iTrusChina Representative

March 25, 2020

Appendix

The list of keys and certificates covered in the management assessment is as follow:

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
1	1	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	43 e3 71 13 d8 b3 59 14 5d b7 ce 8c fd 35 fd 6f bc 05 8d 45	rsaEncryption	(4096 bits)	sha256WithRSAEncryption	31 July 2018 15:24:05	31 July 2043 15:24:05	54 62 70 63 f1 75 84 43 58 8e d1 16 20 b1 c6 ac 1a bc f6 89	8A71DE6559336F426C26E53880D00D88A18DA4C6A91F0DCB6194E206C5C96387
2	1	CN = vTrus OV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	1f a4 3d 72 63 5e 7b f3 81 35 ee f3 9c cf c9 dd c3 47 79 86	rsaEncryption	(2048 bits)	sha256WithRSAEncryption	31 July 2018 15:33:57	31 July 2038 15:33:57	e4 72 c3 a7 32 98 7b c2 a1 5b 02 70 87 54 94 71 84 b0 fd e6	A53B5C9BB5AD92703DC4F77FE64D913A239FD372073A48E27A0481580A5637C4
2	2	CN = vTrus EV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	7d 74 6e a3 6e 21 36 27 0e 8f c2 e2 45 6d 22 9c b9 0c 80 b7	rsaEncryption	(2048 bits)	sha256WithRSAEncryption	31 July 2018 15:31:06	31 July 2038 15:31:06	f0 72 d9 34 39 35 48 a4 ba 5d 11 73 da df 07 e3 cb 11 84 00	F3AA6D712A15F63F8350804979DB542419A61B2B1D22E756C417ABFE8D74A3CA

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
2	3	CN = vTrus DV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	56 63 e4 e2 e8 4a ad 4f 80 af a0 fe 14 ab 78 4f ec 00 0c 9b	rsaEncryption	(2048 bits)	sha256WithRSAEncryption	31 July 2018 15:35:45	31 July 2038 15:35:45	63 af fd 9f e6 69 67 19 f5 bf 18 e9 9c fd 75 19 9e 2f fb fe	5F7E8B4A8C11BAF2CBE6459B47FDB6D50C0285C4A994F4EEF2FE5160AA0AB78A
3	1	CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	6e 6a bc 59 aa 53 be 98 39 67 a2 d2 6b a4 3b e6 6d 1c d6 da	ecdsaEncryption	ECC(384 bits)	sha384WithECDSAEncryption	31 July 2018 15:26:44	31 July 2043 15:26:44	98 39 cd be d8 b2 8c f7 b2 ab e1 ad 24 af 7b 7c a1 db 1f cf	30FBBA2C32238E2A98547AF97931E550428B9B3F1C8EEB6633DCFA86C5B27DD3
4	1	CN = vTrus ECC OV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	6d a1 64 f1 2f ab 56 2c eb 17 3c 46 bc aa 9f a9 0b ee d2 46	ecdsaEncryption	ECC(256 bits)	sha256WithECDSAEncryption	31 July 2018 15:41:18	31 July 2038 15:41:18	35 f9 ef ce 60 77 6f bb c0 9f 68 27 1a 87 83 04 70 88 15 c6	23581EF1921DF2F9290DBA0D4D4F48A97F98AEAEFB5E3350B3F70582E8CDBE78

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
4	2	CN = vTrus ECC EV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	30 22 82 d6 6d f3 b3 7a 7f 5b f3 73 d4 ae 8e 7c 5c 12 53 76	ecdsaEncryption	ECC(256 bits)	sha256WithECDSAEncryption	31 July 2018 15:39:20	31 July 2038 15:39:21	bf 16 c1 25 06 61 18 61 6b e1 30 19 08 3f 7e 54 27 03 b7 5b	BD30C0D1E7ACB83EFC4F5F6C62F8F3A579BAB27527AFAE666C696C3A867175F1
4	3	CN = vTrus ECC DV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	17 ba 09 a8 1f 8e 36 83 68 c2 5e 5e 1c e3 a5 f2 84 83 9d ed	ecdsaEncryption	ECC(256 bits)	sha256WithECDSAEncryption	31 July 2018 15:43:31	31 July 2038 15:43:32	fc 88 bd 89 dc 68 0f 0c 83 09 05 1e 4a 20 24 e3 27 0c b4 75	C97E36CEBF1580AB1BDAD61C1D53B05C75819E85D937214BE684C859B22D45E0