Independent practitioner's assurance report

2020/BJ-XXXX

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 SSL Certification Authority operations for the period from January 9, 2019 to January 8, 2020.

Management's Responsibilities

iTrusChina's management is responsible for the preparation of its assertion in accordance with WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.4.1.

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 prepared, in all material respects, in accordance with WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.4.1.

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 SSL certificate lifecycle management practices and procedures,

(2) evaluating whether the design of practices and procedures complies with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.4.1,

(3) testing and evaluating the operating effectiveness of practices and procedures; 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.

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 have performed no procedures to evaluate the effectiveness of controls at individual subscribers and relying party locations.

Inherent Limitation

We draw attention to the fact that WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.4.1 include certain inherent limitations that can influence the reliability of the information.

Because of the nature and inherent limitations of controls, iTrusChina'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, 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 – SSL Baseline with Network Security - Version 2.4.1.

Emphasis of Matters

Without modifying our conclusion, 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 – SSL Baseline with Network Security - Version 2.4.1, nor the suitability of any of the iTrusChina's services for any customer's intended purpose.

Independent practitioner's assurance report (Continued)

Use of the WebTrust Seal

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

Without modifying our opinion, we draw attention to the fact that 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 – SSL Baseline with Network Security - Version 2.4.1 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 – SSL Baseline with Network Security - Version 2.4.1 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 20, 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, PRC1

March 20, 2020

Dear Members of the Firm,

Assertion by Management of iTrusChina Co.,Ltd. regarding its Disclosure of Business Practices and its Controls over its SSL Certification Authority Services 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 SSL CA services.

Management of iTrusChina Co.,Ltd. ("iTrusChina") is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system controls, SSL CA business practices disclosure and SSL CA service integrity (including key 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 internal 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.

The management of iTrusChina has assessed the controls over its SSL 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 SSL CA services at Mainland China, during the period of January 9, 2019 through January 8, 2020, iTrusChina has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - ITRUSCHINATM CERTIFICATION PRACTICE STATEMENT-v1.3.1; and
  - ITRUSCHINATM CERTIFICATIE POLICY-v1.3

including its commitment to provide SSL CA certificates in conformity with the CA/Browser Forum Requirement on the iTrusChina website, and provided such services in accordance with its disclosed practices.

- maintained effective controls to provide reasonable assurance that:
  - The Certificate Policy and/or Certificate Practices Statement are available on a 24*7 basis and updated annually;
  - Subscriber information is properly collected, authenticated (for the registration activities performed by the CA) and verified;
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - Logical and physical access to CA systems and data is restricted to authorized individuals;
  - The continuity of key and certificate management and operations is maintained;
  - CA systems development, maintenance and operations are properly authorized and performed to maintain CA integrity, and
  - CA's network and certificate system security are properly managed.

in accordance with WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.4.1, including the following:

SSL Baseline Requirement Business Practices Disclosure

SSL Service Integrity

- Key Generation Ceremonies
- Certificate Content and Profile
- Certificate Request Requirements
- Verification Practices
- Certificate Revocation and Status Checking
- Employees and Third Parties
- Data Records
- Audit

CA Environmental Security

Network and Certificate System Security Requirements

- General Protections for the Network and Supporting Systems
- Trusted Roles, Delegated Third Parties, and System Accounts
- Logging, Monitoring, and Alerting
- Vulnerability Detection and Patch Management

iTrusChina Representative

March 20, 2020

Appendix

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

Key Name	Key Type	Key Size	Algorithm	Certificates (SHA256 fingerprint)	Certificate signed by
vTrus Root CA	Root Key	4096 bits	sha256RSA	8A71DE6559336F426C26E53880D00D88A18DA4C6A91F0DCB6194E206C5C96387	vTrus Root CA
vTrus OV SSL CA	Signing Key	2048 bits	sha256RSA	A53B5C9BB5AD92703DC4F77FE64D913A239FD372073A48E27A0481580A5637C4	vTrus Root CA
vTrus EV SSL CA	Signing Key	2048 bits	sha256RSA	F3AA6D712A15F63F8350804979DB542419A61B2B1D22E756C417ABFE8D74A3CA	vTrus Root CA
vTrus DV SSL CA	Signing Key	2048 bits	sha256RSA	5F7E8B4A8C11BAF2CBE6459B47FDB6D50C0285C4A994F4EEF2FE5160AA0AB78A	vTrus Root CA
vTrus ECC Root CA	Root Key	ECC(384 bits)	sha384ECDSA	30FBBA2C32238E2A98547AF97931E550428B9B3F1C8EEB6633DCFA86C5B27DD3	vTrus ECC Root CA
vTrus ECC OV SSL CA	Signing Key	ECC(256 bits)	sha256ECDSA	23581EF1921DF2F9290DBA0D4D4F48A97F98AEAEFB5E3350B3F70582E8CDBE78	vTrus ECC Root CA
vTrus ECC EV SSL CA	Signing Key	ECC(256 bits)	sha256ECDSA	BD30C0D1E7ACB83EFC4F5F6C62F8F3A579BAB27527AFAE666C696C3A867175F1	vTrus ECC Root CA
vTrus ECC DV SSL CA	Signing Key	ECC(256 bits)	sha256ECDSA	C97E36CEBF1580AB1BDAD61C1D53B05C75819E85D937214BE684C859B22D45E0	vTrus ECC Root CA