



INDEPENDENT PRACTITIONER'S ASSURANCE REPORT

2019/BJ-0117

(Page 1 of 3)

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 – Extended Validation SSL operations for the period from October 8th, 2018 to January 8th, 2019 for its keys and certificates listed in the Appendix of iTrus-EV management's assertion.

Management's Responsibility

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 – Extended Validation SSL – Version 1.6.2.](#)

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.

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 and to report our opinion solely to you, as a body, in accordance with our agreed terms of engagement and for no other purpose. We do not assume responsibility towards or accept liability to any other person for the contents of this report.

We conducted our procedures in accordance with International Standard on Assurance Engagements 3000 (Revised) “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 work to form the opinion.



INDEPENDENT PRACTITIONER'S ASSURANCE REPORT (Continued)

A reasonable assurance engagement involves performing procedures to obtain sufficient and appropriate evidence whether the management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.2](#).

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:

- (1) obtaining an understanding of iTrusChina's EV certificate lifecycle management practices and procedures, including its relevant controls over issuance, renewal and revocation of EV certificates,
- (2) evaluating whether the design of practices and procedures complies with CPA Canada [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.2](#),
- (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 subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent Limitation

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, throughout the period October 8th 2018 to January 8th, 2019, iTrusChina management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.2](#).



普华永道

2019/BJ-0117

(Page 3 of 3)

INDEPENDENT PRACTITIONER'S ASSURANCE REPORT (Continued)

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 – Extended Validation SSL – Version 1.6.2](#), nor the suitability of any of the iTrusChina's services for any customer's intended purpose.

Use of the WebTrust seal

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

Purpose and Restriction on Use and Distribution

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.

This report is intended solely for the use of the Management of iTrusChina to submit the report to the related authority in connection with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.2](#), may not be suitable for another purpose and should not be distributed to or used by any other parties for any other purpose.


PricewaterhouseCoopers Zhong Tian LLP Beijing Branch

Beijing, China

April 9, 2019



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/](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

April 9, 2019

Dear Members of the Firm,

Assertion by Management of iTrusChina Co.,Ltd. regarding its Disclosure of Business Practices and its Controls Over its Extended Validation SSL Operations during the period October 8th, 2018 to January 8th, 2019.

iTrusChina Co.,Ltd. (“iTrusChina”) operates the Certification Authority (CA) services known as listed in the **Appendix**, and provides Extended Validation SSL (“CA-EV SSL”) CA services.

The management of iTrusChina Co.,Ltd. (“iTrusChina”) is responsible for establishing and maintaining effective controls over its CA-EV SSL operations, including its CA-EV SSL business practices disclosure, CA-EV SSL service integrity (including key and certificate lifecycle management controls) and CA environmental controls.

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 CA-EV SSL 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-EV SSL services at Mainland China, during the period of October 8th, 2018 through January 8th, 2019, iTrusChina has:

- disclosed its extended validation SSL (EV SSL) certificate lifecycle management business practices in its:
 - [ITRUSCHINATM CERTIFICATION PRACTICE STATEMENT-v1.2](#); and
 - [ITRUSCHINATM CERTIFICATIE POLICY-v1.2](#)

including its commitment to provide CA-EV SSL certificates in conformity with the CA/Browser Forum Guidelines 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;
 - EV subscriber information is properly collected, authenticated (for the registration activities performed by the CA) and verified;
 - The integrity of keys and EV SSL certificates it manages is established and protected throughout their life cycles;

in accordance with [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.2](#), including the following:

Extended Validation SSL Business Practices Disclosure

Extended Validation SSL Services Integrity

- Key Generation Ceremonies
- EV SSL Subscriber and Certificate Content Profiles
- EV SSL Certificate Request Requirements
- Information Verification Requirements
- Certificate Revocation and Status Checking
- Employees and Third Parties
- Data Records
- Audit and Legal

iTrusChina Representative

April 9, 2019



李通振

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	8A:71:DE:65:59:33:6F:42:6C:26:E5:38:80:D0:0D:88:A1:8D:A4:C6:A9:1F:0D:CB:61:94:E2:06:C5:C9:63:87	vTrus Root CA
vTrus EV SSL CA	Signing Key	2048 bits	sha256RSA	F3:AA:6D:71:2A:15:F6:3F:83:50:80:49:79:DB:54:24:19:A6:1B:2B:1D:22:E7:56:C4:17:AB:FE:8D:74:A3:CA	vTrus Root CA
vTrus ECC Root CA	Root Key	ECC(384 bits)	sha384ECD SA	30:FB:BA:2C:32:23:8E:2A:98:54:7A:F9:79:31:E5:50:42:8B:9B:3F:1C:8E:EB:66:33:DC:FA:86:C5:B2:7D:D3	vTrus ECC Root CA
vTrus ECC EV SSL CA	Signing Key	ECC(256 bits)	sha256ECD SA	BD:30:C0:D1:E7:AC:B8:3E:FC:4F:5F:6C:62:F8:F3:A5:79:BA:B2:75:27:AF:AE:66:6C:69:6C:3A:86:71:75:F1	vTrus ECC Root CA

