

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

October 8, 2018

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 as of October 8, 2018.**

Dear Members of the Firm,

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, as of October 8, 2018, iTrusChina has:

- disclosed its extended validation SSL (EV SSL) certificate lifecycle management business practices in its:
  - ITRUSCHINATM CERTIFICATION PRACTICE STATEMENT-v1.1; and
  - ITRUSCHINATM CERTIFICATIE POLICY-v1.1

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

- suitable design, and place into operation, 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

October 8, 2018



## 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