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 Certification Authority 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 the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

Management of iTrusChina is responsible for establishing and maintaining effective controls over its Certification Authority operations, including CA business practices disclosure, CA service integrity (including key and certificate lifecycle management controls) and CA environmental 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 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, as of October 8, 2018, iTrusChina has:

- disclosed its key and certificate lifecycle management business and information privacy practices in its:
  - ITRUSCHINATM CERTIFICATION PRACTICE STATEMENT-v1.1; and
  - ITRUSCHINATM CERTIFICATIE POLICY-v1.1

  and designed such services in accordance with its disclosed practices.
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - subscriber information is properly authenticated (for the registration activities performed by iTrusChina); and
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA's business practice disclosure;
  - 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 v2.1, 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

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

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 OV SSL CA	Signing Key	2048 bits	sha256RSA	A5:3B:5C:9B:B5:AD:92:70:3D:C4:F7:7F:E6:4D:91:3A:23:9F:D3:72:07:3A:48:E2:7A:04:81:58:0A:56:37:C4	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 DV SSL CA	Signing Key	2048 bits	sha256RSA	5F:7E:8B:4A:8C:11:BA:F2:CB:E6:45:9B:47:FD:B6:D5:0C:02:85:C4:A9:94:F4:EE:F2:FE:51:60:AA:0A:B7:8A	vTrus Root CA
vTrus ECC Root CA	Root Key	ECC(384 bits)	sha384ECDSA	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 OV SSL CA	Signing Key	ECC(256 bits)	sha256ECDSA	23:58:1E:F1:92:1D:F2:F9:29:0D:BA:0D:4D:4F:48:A9:7F:98:AE:AE:FB:5E:33:50:B3:F7:05:82:E8:CD:BE:78	vTrus ECC Root CA
vTrus ECC EV SSL CA	Signing Key	ECC(256 bits)	sha256ECDSA	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
vTrus ECC DV SSL CA	Signing Key	ECC(256 bits)	sha256ECDSA	C9:7E:36:CE:BF:15:80:AB:1B:DA:D6:1C:1D:53:B0:5C:75:81:9E:85:D9:37:21:4B:E6:84:C8:59:B2:2D:45:E0	vTrus ECC Root CA