pwc 羅兵咸永道

Independent practitioner's assurance report

To the Management of iTrusChina Co., Ltd ("iTrusChina")

Scope

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 (CA) operations in Beijing, China, for the period from January 9, 2022 to January 8, 2023 for its CAs as enumerated in **Appendix A**, iTrusChina has:

- disclosed SSL certificate lifecycle management business practices in its:
  - iTrusChina Global-Trust Certification Practice Statement v1.4.9; and
  - iTrusChina Global-Trust Certificate Policy v1.4.7,

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the iTrusChina website, and provided such services in accordance with its disclosed practices,
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by iTrusChina),
- 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 management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity,
- and for its CAs as enumerated in **Appendix A** and **Appendix B,** maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum,

in accordance with WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.6.

Management's Responsibilities

The management of iTrusChina is responsible for the management's 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 – SSL Baseline with Network Security - Version 2.6.

Our Independence and Quality Management

We have complied with the independence and other ethical requirements 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 Management 1, which requires the firm to design, implement and operate a system of quality management including policies or 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 management's assertion of iTrusChina based on our work performed.

We conducted our work in accordance with 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 as to whether the management's assertion of iTrusChina is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.6. 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:

- obtaining an understanding of iTrusChina's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of iTrusChina's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management business practices;
- testing and evaluating the operating effectiveness of the controls; and
- 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 subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber 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

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, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any opinion based on our findings to future periods is subject to the risk that changes may alter the validity of such opinion.

Opinion

In our opinion, the management's assertion of iTrusChina, for the period from January 9, 2022 to January 8, 2023, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.6.

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 – SSL Baseline with Network Security - Version 2.6, nor the suitability of any of the iTrusChina's services for any customer's intended purpose.

Other Matter

ITrusChina's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security 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.

pwc

羅兵咸永道

Purpose and Restriction on Use

The management's assertion of iTrusChina was prepared for obtaining and displaying the WebTrust Seal on iTrusChina website[1] using the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.6 designed for this purpose. As a result, the 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 iTrusChina 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 2.6. We do not assume responsibility towards or accept liability to any other person for the contents of this report.

PricewaterhouseCoopers
Certified Public Accountants

Hong Kong, 28 March 2023

1 The maintenance and integrity of the iTrusChina website is the responsibility of the directors of iTrusChina. 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 management's assertion of iTrusChina on which the assurance report was issued or the assurance report that was issued and the information presented on the website.

Appendix A – IN-SCOPE CAs FOR SSL BASELINE REQUIREMENTS AND NETWORKSECURITY REQUIREMENTS

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	RSA Encryption	(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
1	2	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	RSA Encryption	(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 bo fd e6	A53B5C9BB5AD92703DC4F77FE64D913A239FD372073A48E27A0481580A5637C4

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
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	RSA Encryption	(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	F3AA6D712A15F63F835080497 9DB542419A61B2B1D22E756C417ABFE8D74A3CA
3	2	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	RSA Encryption	(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

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
2	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	ECDSA Encryption	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	2	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	ECDSA Encryption	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
5	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	ECDSA Encryption	ECC (256 bits)	sha256WithECDSAEncryption	31 July 2018 15:39:20	31 July 2038 15:39:20	bf 16 c1 25 06 61 18 61 6b e1 30 19 08 3f 7e 54 27 03 b7 5b	BD30C0D1E7ACB83EFC4F5F6C62F8F3A579BAB27527AFAE666C696C3A867175F1
6	2	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	ECDSA Encryption	ECC (256 bits)	sha256WithECDSAEncryption	31 July 2018 15:43:31	31 July 2038 15:43:31	fc 88 bd 89 dc 68 0f 0c 83 09 05 1e 4a 20 24 e3 27 0c b4 75	C97E36CEBF1580AB1BDAD61C1D53B05C75819E85D937214BE684C859B22D45E0

Appendix B – IN-SCOPE CAs FOR NETWORKSECURITY REQUIREMENTS ONLY

CA #	Cert#	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
1	2	CN = vTrus Document Signing CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	4ecf532a91cd6844cdc6839b66110ab2d2d9319b	RSA Encryption	(2048 bits)	sha256WithRSAEncryption	14 October 2021 11:24:59	14 October 2041 11:24:59	4bc432db71973edaea94c719923cc8096523881b	B5C3EFC7BA547B66318C23C93E0FB18301DB84ADA233B19C9F2F26F5D64C3559
2	2	CN = vTrus Time Stamping CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	13ac9f0f9b2fe210e06a96888c4eee1c49040ea4	RSA Encryption	(4096 bits)	sha256WithRSAEncryption	14 October 2021 11:28:32	14 October 2041 11:28:32	310bdaae5d9643f7cb1311ba48f700addd5a29ff	F7291D1E8BCC7583AC3FA83977C6C5EBC784A118A397647A9FC37EF85E14DF5C

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

PricewaterhouseCoopers Limited
22/F Prince's Building
Central
Hong Kong

March 28, 2023

Dear Sirs,

Assertion by Management of iTrusChina Co., Ltd. regarding its Disclosure of Business Practices and its Controls over its SSL Certification Authority Services throughout the period of January 9, 2022 to January 8, 2023.

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

The management of iTrusChina has assessed its disclosures of its certificate practices and controls over its SSL CA services. The key and certificates covered in our assessment are listed in the **Appendix A** of this letter. Based on that assessment, in providing its SSL CA services in Mainland China, throughout the period of January 9, 2022 to January 8, 2023, iTrusChina has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - iTrusChina Global-Trust Certification Practice Statement v1.4.9; and
  - iTrusChina Global-Trust Certificate Policy v1.4.7

  including its commitment to provide SSL 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 integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by iTrusChina)
- 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 management operations is maintained;

and

- CA systems development, maintenance and operations are properly authorized and performed to maintain CA integrity

and, for the list of roots and other CAs in scope for Network Security Requirements listed in the **Appendix A** and **Appendix B**:

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

In accordance with WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.6.

iTrusChina Representative

March 28, 2023

Appendix A – IN-SCOPE CAs FOR SSL BASELINE REQUIREMENTS AND NETWORKSECURITY REQUIREMENTS

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	RSA Encryption	(4096 bits)	sha256With RSAEncryption	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	8A71DE65593 36F426C26E5 3880D00D88 A18DA4C6A91 F0DCB6194E 206C5C96387
1	2	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	RSA Encryption	(2048 bits)	sha256With RSAEncryption	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	A53B5C9BB5 AD92703DC4 F77FE64D913 A239FD37207 3A48E27A048 1580A5637C4
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	RSA Encryption	(2048 bits)	sha256With RSAEncryption	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	F3AA6D712A1 5F63F835080 4979DB54241 9A61B2B1D22 E756C417ABF E8D74A3CA

3	2	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	RSA Encryption	(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
2	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	ECDSA Encryption	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	2	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 ob ee d2 46	ECDSA Encryption	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
5	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	ECDSA Encryption	ECC(256 bits)	sha256WithECDSAEncryption	31 July 2018 15:39:20	31 July 2038 15:39:20	bf 16 c1 25 06 61 18 61 6b e1 30 19 08 3f 7e 54 27 03 b7 5b	BD30C0D1E7ACB83EFC4F5F6C62F8F3A579BAB27527AFAE666C696C3A867175F1

6	2	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	ECDSA Encryption	ECC(256 bits)	sha256With ECDSAEncryption	31 July 2018 15:43:31	31 July 2038 15:43:31	fc 88 bd 89 dc 68 of 0c 83 09 05 1e 4a 20 24 e3 27 0c b4 75	C97E36CEBF1580AB1BDAD61C1D53B05C75819E85D937214BE684C859B22D45E0

Appendix B – IN-SCOPE CAs FOR NETWORKSECURITY REQUIREMENTS ONLY

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
1	2	CN = vTrus Document Signing CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	4ecf532a91cd6844cdc6839b66110ab2d2d9319b	RSA Encryption	(2048 bits)	sha256WithRSAEncryption	14 October 2021 11:24:59	14 October 2041 11:24:59	4bc432db71973edaea94c719923cc8096523881b	B5C3EFC7BA547B66318C23C93E0FB18301DB84ADA233B19C9F2F26F5D64C3559
2	2	CN = vTrus Time Stamping CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	13ac9f0f9b2fe210e06a96888c4eee1c49040ea4	RSA Encryption	(4096 bits)	sha256WithRSAEncryption	14 October 2021 11:28:32	14 October 2041 11:28:32	310bdaae5d9643f7cb1311ba48f700addd5a29ff	F7291D1E8BCC7583AC3FA83977C6C5EBC784A118A397647A9FC37EF85E14DF5C