

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, 2023 to January 8, 2024 for its CAs as enumerated in [Appendix A](#), iTrusChina has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in its:
 - [iTrusChina Global-Trust Certification Practice Statement v1.5](#); and [iTrusChina Global-Trust Certificate Policy v1.5](#);
 - [iTrusChina Global-Trust Certification Practice Statement v1.5.1](#); and [iTrusChina Global-Trust Certificate Policy v1.5.1](#);
 - [iTrusChina Global-Trust Certification Practice Statement v1.5.2](#); and [iTrusChina Global-Trust Certificate Policy v1.5.2](#); and
 - [iTrusChina Global-Trust Certification Practice Statement v1.5.3](#); and [iTrusChina Global-Trust Certificate Policy v1.5.3](#),including its commitment to provide 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 integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated (for the registration activities performed by iTrusChina),

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

Management's Responsibilities

iTrusChina's management is responsible for the management 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 v1.8](#).

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 (ISQM) 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 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 – Extended Validation SSL v1.8](#). 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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
2. selectively testing transactions executed in accordance with disclosed EV SSL certificate lifecycle management practices;

3. testing and evaluating the operating effectiveness of the controls; and
4. 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, 2023 to January 8, 2024, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

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 – Extended Validation SSL v1.8](#), nor the suitability of any of the iTrusChina's services for any customer's intended purpose.

Purpose and Restriction on Use of the report

The management's assertion of iTrusChina was prepared for obtaining and displaying the WebTrust Seal on iTrusChina website¹ using the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#) 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 – Extended Validation SSL v1.8](#).

Our report is not to be used for any other purpose. We do not assume responsibility towards or accept liability to any other parties for the contents of this report.

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.



PricewaterhouseCoopers
Certified Public Accountants

Hong Kong, 27 March 2024

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

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	8A71DE6 559336F 426C26E 53880D 00D88A 18DA4C 6A91Fo DCB6194 E206C5 C96387
1	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 oc 80 b7	RSA Encryption	(2048 bits)	sha256With RSAEncryption	31 July 2018 15:31:06	31 July 2038 15:31:06	fo 72 d9 34 39 35 48 a4 ba 5d 11 73 da df 07 e3 cb 11 84 00	F3AA6D 712A15F 63F8350 804979D B542419 A61B2B1 D22E756 C417ABF E8D74A 3CA

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)	sha384With ECDSAEncryption	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	30FBBA2C32238E2A98547AF97931E550428B9B3F1C8EEB6633DCF A86C5B27DD3
2	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)	sha256With ECDSAEncryption	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	BD30CoD1E7ACB83EFC4F5F6C62F8F3A579BAB27527AFAE666C696C3A867175F1

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

PricewaterhouseCoopers
22/F Prince's Building
Central
Hong Kong

March 27, 2024

Dear Sirs,

Assertion by Management of iTrusChina Co., Ltd. regarding its Disclosure of Business Practices and its Controls over its Extended Validation SSL Operations throughout the period from January 9, 2023 to January 8, 2024.

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

The management of iTrusChina is responsible for establishing and maintaining effective controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its [website](#), EV SSL key lifecycle management controls, and EV SSL 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 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.

Management of iTrusChina has assessed its disclosures of its certificate practices and controls over its EV 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 EV SSL Certification Authority (CA) services in Mainland China, throughout the period from January 9, 2023 to January 8, 2024, iTrusChina has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in its:
 - [iTrusChina Global-Trust Certification Practice Statement v1.5](#); and [iTrusChina Global-Trust Certificate Policy v1.5](#)
 - [iTrusChina Global-Trust Certification Practice Statement v1.5.1](#); and [iTrusChina Global-Trust Certificate Policy v1.5.1](#)
 - [iTrusChina Global-Trust Certification Practice Statement v1.5.2](#); and [iTrusChina Global-Trust Certificate Policy v1.5.2](#)
 - [iTrusChina Global-Trust Certification Practice Statement v1.5.3](#); and [iTrusChina Global-Trust Certificate Policy v1.5.3](#)

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

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).



iTrusChina Representative
March 27, 2024

Appendix – In-Scope CAs

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	8A71DE6559 336F426C26 E53880D00 D88A18DA4 C6A91FoDC B6194E206C 5C96387
1	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 oc 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	F3AA6D712A 15F63F8350 804979DB54 2419A61B2B1 D22E756C41 7ABFE8D74 A3CA
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)	sha384With ECDSAEncryption	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	30FBBA2C32 238E2A9854 7AF97931E55 0428B9B3F1 C8EEB6633 DCFA86C5B 27DD3
2	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)	sha256With ECDSAEncryption	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	BD30CoD1E 7ACB83EFC4 F5F6C62F8F 3A579BAB27 527AFAE666 C696C3A867 175F1