

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](#) and [Appendix B](#), iTrusChina has:

- disclosed its 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 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 the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.6](#).

Management’s Responsibilities

iTrusChina’s management 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 v2.6](#).

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 (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 - SSL Baseline with Network Security v2.6](#). 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:

1. 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;
2. selectively testing transactions executed in accordance with disclosed 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.

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, 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 - SSL Baseline with Network Security v2.6](#).

Emphasis of Matter

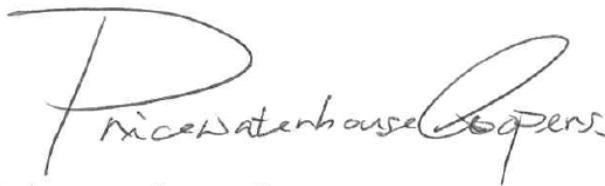
Without modifying our opinion, we draw attention to the fact that this report does not include any representation as to the quality of iTrusChina's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.6](#), nor the 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 - SSL Baseline with Network Security v2.6](#) 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 v2.6](#). We do not assume responsibility towards or accept liability to any other person for the contents of this report.

Use of the WebTrust seal

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.

A handwritten signature in cursive script that reads "PricewaterhouseCoopers".

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 for SSL Baseline Requirements and Network Security 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	8A71DE6 559336F 426C26E 53880D 00D88A 18DA4C 6A91FO DCB6194 E206C5 C96387
1	2	CN = vTrus OV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	23 03 01 e5 d6 9a c8 93 od 62 33 94 ff d2 a0 91 7c oe 7e 7b	RSA Encryption	(2048 bits)	sha256With RSAEncryption	13 December 2023 11:19:22	10 December 2033 11:19:22	e4 72 c3 a7 32 98 7b c2 a1 5b 02 70 87 54 94 71 84 bo fd e6	2CF5539 249A9E3 8FC010E 29FF3E8 046658F 3D030B 9331047 3687FA9 1F8DA4 4CA

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)	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	F3AA6D 712A15F 63F8350 804979D B542419 A61B2B1 D22E756 C417ABF E8D74A 3CA
3	2	CN = vTrus DV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	47 b6 12 of eb d5 e7 25 4c 99 de 1c dc dd 53 5a d3 5f 99 76	RSA Encryption	(2048 bits)	sha256With RSAEncryption	13 December 2023 11:21:40	10 December 2033 11:21:40	63 af fd 9f e6 69 67 19 f5 bf 18 e9 9c fd 75 19 9e 2f fb fe	0A85075 DD6B38 2EAB314 49823D B8BED6 B61A441 714165E 33FACA 42CD9C 8DEC2A
4	2	CN = vTrus FastSSL CA G1 O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	48 15 cb de 3d 2b e0 64 75 f3 79 3f b9 4e 64 a0 73 d2 1b fa	RSA Encryption	(2048 bits)	sha256With RSAEncryption	13 December 2023 11:18:07	10 December 2033 11:18:07	e5 51 97 ea c9 32 02 55 56 8f 20 7e 02 df b8 6d 02 db 6c 32	3B83EB 5D7A9A 5AF0627 5A0A1C1 B35BD5 62622A5 521E269 9F25559 328B882 9058

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
5	2	CN = vTrus YunSSL DV CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	1f f2 f8 8b 5b f9 fd 73 8b ec 90 ab af db 50 1a fe 74 ea da	RSA Encryption	(2048 bits)	sha256With RSAEncryption	13 Decem ber 2023 11:16:17	10 Dece mber 2033 11:16: 17	47 17 f5 bf 9c 28 5d a8 70 25 fa 6a b2 3f 76 ad 96 27 80 c5	A7D7285 843B89 B134F85 2CB52A 6F43193 8257C82 6D699A A806C8 94A0A1C DB847
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 15:26:4 4	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	30FBBA 2C32238 E2A9854 7AF9793 1E55042 8B9B3F1 C8EEB6 633DCF A86C5B 27DD3
6	2	CN = vTrus ECC OV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	46 0a 85 46 79 6f d1 39 ba 62 ed 86 d7 63 46 94 21 29 b7 a4	ECDSA Encryption	ECC(256 bits)	sha384With ECDSAEncryption	13 Decem ber 2023 11:23:5 8	10 Dece mber 2033 11:23: 58	35 f9 ef ce 60 77 6f bb c0 9f 68 27 1a 87 83 04 70 88 15 c6	42E46C4 4874591 2851764 9731457 B6AE20 099D541 BD182C5 497B2E6 7E6FFD 0F6

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
7	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	BD30Co D1E7AC B83EFC 4F5F6C6 2F8F3A5 79BAB27 527AFA E666C69 6C3A867 175F1
8	2	CN = vTrus ECC DV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	14 66 a8 2c bf 01 83 aa 09 3f d2 28 of ac 3c oe 39 fo 29 40	ECDSA Encryption	ECC(256 bits)	sha384With ECDSAEncryption	13 December 2023 11:25:48	10 December 2033 11:25:48	fc 88 bd 89 dc 68 of 0c 83 09 05 1e 4a 20 24 e3 27 0c b4 75	4D391FC 790BD7 02CAD3 CCBCoB 025C5C DD88C6 FDF274 DCF5FB D3F027 A80C2C 7E5

Appendix B – IN-SCOPE CAs FOR NETWORK SECURITY 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	4e cf 53 2a 91 cd 68 44 cd c6 83 9b 66 11 0a b2 d2 d9 31 9b	RSA Encryption	(2048 bits)	sha256WithRSAEncryption	14 October 2021 11:24:59	14 October 2041 11:24:59	4b c4 32 db 71 97 3e da ea 94 c7 19 92 3c c8 09 65 23 88 1b	B5C3EFC7BA547B66318C23C93E0FB18301DB84ADA233B19C9F2F26F5D64C3559
2	2	CN = vTrus Time Stamping CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	13 ac 9f of 9b 2f e2 10 e0 6a 96 88 8c 4e ee 1c 49 04 oe a4	RSA Encryption	(4096 bits)	sha256WithRSAEncryption	14 October 2021 11:28:32	14 October 2041 11:28:32	31 0b da ae 5d 96 43 f7 cb 13 11 ba 48 f7 00 ad dd 5a 29 ff	F7291D1E8BCC7583AC3FA83977C6C5EBC784A118A397647A9FC37EF85E14DF5C

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 SSL Certification Authority Services 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 A](#) and [Appendix B](#) and provides SSL CA services.

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

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 Certification Authority (CA) services in Mainland China, throughout the period from January 9, 2023 to January 8, 2024, iTrusChina has:

- disclosed its 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 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 systems 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 the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.6](#).



iTrusChina Representative

March 27, 2024



Appendix A – In-Scope CAs for SSL Baseline Requirements and Network Security 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 FoDCB6194E 206C5C96387
1	2	CN = vTrus OV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	23 03 01 e5 d6 9a c8 93 od 62 33 94 ff d2 a0 91 7c 0e 7e 7b	RSA Encryption	(2048 bits)	sha256With RSAEncryption	13 Decem ber 2023 11:19:22	10 Dece mber 2033 11:19:22	e4 72 c3 a7 32 98 7b c2 a1 5b 02 70 87 54 94 71 84 b0 fd e6	2CF5539249A 9E38FC010E2 9FF3E804665 8F3D030B93 310473687FA 91F8DA44CA
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 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	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	47 b6 12 of eb d5 e7 25 4c 99 de 1c dc dd 53 5a d3 5f 99 76	RSA Encryption	(2048 bits)	sha256With RSAEncrypt ion	13 Decem ber 2023 11:21:4 0	10 Dece mber 2033 11:21: 40	63 af fd 9f e6 69 67 19 f5 bf 18 e9 9c fd 75 19 9e 2f fb fe	0A85075DD6 B382EAB3144 9823DB8BED 6B61A4417141 65E33FACA42 CD9C8DEC2A
4	2	CN = vTrus FastSSL CA G1 O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	48 15 cb de 3d 2b e0 64 75 f3 79 3f b9 4e 64 a0 73 d2 1b fa	RSA Encryption	(2048 bits)	sha256With RSAEncrypt ion	13 Decem ber 2023 11:18:0 7	10 Dece mber 2033 11:18: 07	e5 51 97 ea c9 32 02 55 56 8f 20 7e 02 df b8 6d 02 db 6c 32	3B83EB5D7A 9A5AF06275A 0A1C1B35BD5 62622A5521E 2699F255593 28B8829058
5	2	CN = vTrus YunSSL DV CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	1f f2 f8 8b 5b f9 fd 73 8b ec 90 ab af db 50 1a fe 74 ea da	RSA Encryption	(2048 bits)	sha256With RSAEncrypt ion	13 Decem ber 2023 11:16:17	10 Dece mber 2033 11:16: 17	47 17 f5 bf 9c 28 5d a8 70 25 fa 6a b2 3f 76 ad 96 27 80 c5	A7D7285843B 89B134F852C B52A6F43193 8257C826D69 9AA806C894 AoA1CDB847
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(3 84 bits)	sha384With ECDSAEncr yption	31 July 2018 15:26:4 4	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 238E2A98547 AF97931E550 428B9B3F1C8 EEB6633DCF A86C5B27DD 3
6	2	CN = vTrus ECC OV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	46 0a 85 46 79 6f d1 39 ba 62 ed 86 d7 63 46 94 21 29 b7 a4	ECDSA Encryption	ECC(2 56 bits)	sha384With ECDSAEncr yption	13 Decem ber 2023 11:23:5 8	10 Dece mber 2033 11:23: 58	35 f9 ef ce 60 77 6f bb c0 9f 68 27 1a 87 83 04 70 88 15 c6	42E46C44874 591285176497 31457B6AE20 099D541BD18 2C5497B2E67 E6FFD0F6

7	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(2 56 bits)	sha256With ECDSAEncr yption	31 July 2018 15:39:2 0	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	BD30CoD1E7 ACB83EFC4F 5F6C62F8F3A 579BAB27527 AFAE666C69 6C3A867175F 1
8	2	CN = vTrus ECC DV SSL CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	14 66 a8 2c bf 01 83 aa 09 3f d2 28 of ac 3c oe 39 fo 29 40	ECDSA Encryption	ECC(2 56 bits)	sha384With ECDSAEncr yption	13 Decem ber 2023 11:25:4 8	10 Dece mber 2033 11:25: 48	fc 88 bd 89 dc 68 of oc 83 09 05 1e 4a 20 24 e3 27 oc b4 75	4D391FC790B D702CAD3CC BCoBo25C5C DD88C6FDF2 74DCF5FBD3 Fo27A80C2C7 E5

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	4e cf 53 2a 91 cd 68 44 cd c6 83 9b 66 11 0a b2 d2 d9 31 9b	RSA Encryption	(2048 bits)	sha256With RSAEncryption	14 October 2021 11:24:59	14 October 2041 11:24:59	4b c4 32 db 71 97 3e da ea 94 c7 19 92 3c c8 09 65 23 88 1b	B5C3EFC7BA 547B66318C2 3C93E0FB183 01DB84ADA2 33B19C9F2F2 6F5D64C3559
2	2	CN = vTrus Time Stamping CA O = iTrusChina Co.,Ltd. C = CN	CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	13 ac 9f of 9b 2f e2 10 eo 6a 96 88 8c 4e ee 1c 49 04 oe a4	RSA Encryption	(4096 bits)	sha256With RSAEncryption	14 October 2021 11:28:32	14 October 2041 11:28:32	31 0b da ae 5d 96 43 f7 cb 13 11 ba 48 f7 00 ad dd 5a 29 ff	F7291D1E8BC C7583AC3FA8 3977C6C5EBC 784A118A397 647A9FC37EF 85E14DF5C