日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL

19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

INDEPENDENT ASSURANCE REPORT

To the management of iTrusChina Co., Ltd. ("iTrusChina"):

We have been engaged, in a reasonable assurance engagement, to report on iTrusChina management's assertion that for its Certification Authority ("CA") operations at locations as enumerated in Appendix C, throughout the period 9 January 2024 to 8 January 2025 for its CAs as enumerated in Appendix A, iTrusChina has:

- disclosed its SSL certificate life cycle management business practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B, 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 certificate subscriber information is properly authenticated

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline, v2.8.

Without modified our opinion, we noted the following matters during our procedures:

- iTrusChina was notified that it may have issued certificates where the Applicant's Private Key has been previously disclosed as having been compromised. An incident processing thread (Bug 1927384) on Mozilla's Bugzilla Platform created on 27 October 2024 for remediations of the mis-issued certificates. All remediation actions have been accomplished on 18 November 2024 and the processing thread has been closed on 28 January 2025;

- iTrusChina was notified that it did not respond to CPR of mis-issuance addressed in (Bug 1927384) within 24 hours. An incident processing thread (Bug 1927675) on Mozilla's Bugzilla Platform created on 28 October 2024 for remediations of the issue. All remediation actions have been accomplished on 25 November 2024 and the processing thread has been closed on 2 December 2024;

19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

- iTrusChina was notified on 16 July 2024 that two revoked certificates were listed in CRL with reason code 7, which is not defined in RFC 5280. An incident processing thread (Bug 1907949) on Mozilla's Bugzilla Platform created on 15 July 2024 for remediations of the issue. All remediation actions have been accomplished on 23 August 2024 and the processing thread has been closed on 28 August 2024.

- iTrusChina was notified that it lacks the 2018 KGC report and audit report coverage for the period from 31 July 2018 to 7 Oct 2018, which is considered a violation of the Section 6.1.1.1 and 8.1 of TLS Baseline Requirements. An incident processing thread (Bug 1923279) on Mozilla's Bugzilla Platform created on 8 October 2024 for remediations of the issue. All remediation actions have been accomplished on 25 November 2024 and the processing thread has been closed on 2 December 2024.

Certification authority's responsibilities

iTrusChina's management is responsible for its 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, v2.8.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* 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.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information,* issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

(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 business 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.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at iTrusChina and their effect on assessments of control

19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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 limitations

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

Opinion

In our opinion, throughout the period 9 January 2024 to 8 January 2025, iTrusChina management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline, v2.8.

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, v2.8, nor the suitability of any of iTrusChina's services for any customer's intended purpose.

Use of the WebTrust seal

iTrusChina's use of the WebTrust for Certification Authorities – SSL Baseline 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.

日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL

28 March 2025

DFK INTERNATIONAL

日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL

19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

Appendix A

The list of keys and certificates covered in the report is as follow:

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	Root Key	sha256RSA	4096 bits	54627063F1758443588ED11620B1C6AC1ABCF689	8A71DE6559336F426C26E53880D00D88A18DA4C6A91F0DCB6194E206C5C96387	vTrus Root CA
CN = vTrus DV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256RSA	2048 bits	63AFFD9FE6696719F5BF18E99CFD75199E2FFBFE	0A85075DD6B382EAB31449823DB8BED6B61A441714165E33FACA42CD9C8DEC2A	vTrus Root CA
CN = vTrus OV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256RSA	2048 bits	E472C3A732987BC2A15B0270875494718 4B0FDE6	2CF5539249A9E38FC010E29FF3E8046658F3D030B93310473687FA91F8DA44CA	vTrus Root CA
CN = vTrus EV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256RSA	2048 bits	F072D934393548A4BA5D1173DADF07E3CB118400	F3AA6D712A15F63F8350804979DB542419A61B2B1D22E756C417ABFE8D74A3CA	vTrus Root CA
CN = vTrus YunSSL DV CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256RSA	2048 bits	4717F5BF9C285DA87025FA6AB23F76AD962780C5	A7D7285843B89B134F852CB52A6F431938257C826D699AA806C894A0A1CDB847	vTrus Root CA
CN = vTrus FastSSL CA G1 O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256RSA	2048 bits	E55197EAC9320255568F207E02DFB86D02DB6C32	3B83EB5D7A9A5AF06275A0A1C1B35BD562622A5521E2699F25559328B8829058	vTrus Root CA

日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL

19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	Root Key	sha384ECDSA	384 bits	9839CDBED8B28CF7B2ABE1AD24AF7B7CA1DB1FCF	30FBBA2C32238E2A98547AF97931E550428B9B3F1C8EEB6633DCFA86C5B27DD3	vTrus ECC Root CA
CN = vTrus ECC DV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	FC88BD89DC680F0C8309051E4A2024E3270CB475	4D391FC790BD702CAD3CCBC0B025C5CDD88C6FDF274DCF5FBD3F027A80C2C7E5	vTrus ECC Root CA
CN = vTrus ECC OV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	35F9EFCE60776FBBC09F68271A878304708815C6	42E46C4487459128517649731457B6AE20099D541BD182C5497B2E67E6FFD0F6	vTrus ECC Root CA
CN = vTrus ECC EV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256ECDSA	256 bits	BF16C125066118616BE13019083F7E542703B75B	BD30C0D1E7ACB83EFC4F5F6C62F8F3A579BAB27527AFAE666C696C3A867175F1	vTrus ECC Root CA

日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL

19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

Appendix B

Applicable versions of Certification Practice Statement (CPS) and Certificate Policy (CP) in-scope:

Name	Version	Date
iTrusChina Global-Trust Certification Practice Statement	1.5.7	24 September 2024
iTrusChina Global-Trust Certification Practice Statement	1.5.6	22 August 2024
iTrusChina Global-Trust Certification Practice Statement	1.5.5	10 July 2024
iTrusChina Global-Trust Certification Practice Statement	1.5.4	28 March 2024
iTrusChina Global-Trust Certification Practice Statement	1.5.3	15 December 2023
iTrusChina Global-Trust Certificate Policy	1.5.7	24 September 2024
iTrusChina Global-Trust Certificate Policy	1.5.6	22 August 2024
iTrusChina Global-Trust Certificate Policy	1.5.5	10 July 2024
iTrusChina Global-Trust Certificate Policy	1.5.4	28 March 2024
iTrusChina Global-Trust Certificate Policy	1.5.3	15 December 2023

日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL

19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

Appendix C

Locations in-scope:

Location	Function
Beijing (North), China	Administration and datacenter facility
Beijing (South), China	Secure site hosting backup materials

MANAGEMENT'S ASSERTION

iTrusChina Co., Ltd. ("iTrusChina") operates the Certification Authority (CA) services known as CAs in Appendix A.

The management of iTrusChina is responsible for establishing and maintaining effective controls over its SSL CA operations, 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.

iTrusChina management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in iTrusChina management's opinion, in providing its CA services at locations as enumerated in Appendix C, throughout the period 9 January 2024 to 8 January 2025, iTrusChina has:

- disclosed its SSL certificate life cycle management business practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B, 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 certificate 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 authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline - v2.8.

Without modified our opinion, we noted the following matters during our procedures:

- iTrusChina was notified that it may have issued certificates where the Applicant's Private Key has been previously disclosed as having been compromised. An incident processing thread (Bug 1927384) on Mozilla's Bugzilla Platform created on 27 October 2024 for remediations of the mis-issued certificates. All remediation actions have been accomplished on 18 November 2024 and the processing thread has been closed on 28 January 2025;
- iTrusChina was notified that it did not respond to CPR of mis-issuance addressed in (Bug 1927384) within 24 hours. An incident processing thread (Bug 1927675) on Mozilla's Bugzilla Platform created on 28 October 2024 for remediations of the issue. All remediation actions have been accomplished on 25 November 2024 and the processing thread has been closed on 2 December 2024;

- iTrusChina was notified on 16 July 2024 that two revoked certificates were listed in CRL with reason code 7, which is not defined in RFC 5280. An incident processing thread (Bug 1907949) on Mozilla's Bugzilla Platform created on 15 July 2024 for remediations of the issue. All remediation actions have been accomplished on 23 August 2024 and the processing thread has been closed on 28 August 2024.

- iTrusChina was notified that it lacks the 2018 KGC report and audit report coverage for the period from 31 July 2018 to 7 Oct 2018, which is considered a violation of the Section 6.1.1.1 and 8.1 of TLS Baseline Requirements. An incident processing thread (Bug 1923279) on Mozilla's Bugzilla Platform created on 8 October 2024 for remediations of the issue. All remediation actions have been accomplished on 25 November 2024 and the processing thread has been closed on 2 December 2024.

Mr. Yanzhao Li

Chief Security Officer of iTrusChina Co., Ltd.
Room 401A, Building 4, Yard 7, Shangdi 8th RD, Haidian District, Beijing, China.

28 March 2025

Appendix A

The list of keys and certificates covered in the management's assertion is as follow:

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = vTrus Root CA O = iTrusChina Co.,Ltd. C = CN	Root Key	sha256RSA	4096 bits	54627063F1758443588ED11620B1C6AC1ABCF689	8A71DE6559336F426C26E53880D00D88A18DA4C6A91F0DCB6194E206C5C96387	vTrus Root CA
CN = vTrus DV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256RSA	2048 bits	63AFFD9FE6696719F5BF18E99CFD75199E2FFBFE	0A85075DD6B382EAB31449823DB8BED6B61A441714165E33FACA42CD9C8DEC2A	vTrus Root CA
CN = vTrus OV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256RSA	2048 bits	E472C3A732987BC2A15B0270875494718 4B0FDE6	2CF5539249A9E38FC010E29FF3E8046658F3D030B93310473687FA91F8DA44CA	vTrus Root CA
CN = vTrus EV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256RSA	2048 bits	F072D934393548A4BA5D1173DADF07E3CB118400	F3AA6D712A15F63F8350804979DB542419A61B2B1D22E756C417ABFE8D74A3CA	vTrus Root CA
CN = vTrus YunSSL DV CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256RSA	2048 bits	4717F5BF9C285DA87025FA6AB23F76AD962780C5	A7D7285843B89B134F852CB52A6F431938257C826D699AA806C894A0A1CDB847	vTrus Root CA
CN = vTrus FastSSL CA G1 O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256RSA	2048 bits	E55197EAC9320255568F207E02DFB86D02DB6C32	3B83EB5D7A9A5AF06275A0A1C1B35BD562622A5521E2699F25559328B8829058	vTrus Root CA
CN = vTrus ECC Root CA O = iTrusChina Co.,Ltd. C = CN	Root Key	sha384ECDSA	384 bits	9839CDBED8B28CF7B2ABE1AD24AF7B7CA1DB1FCF	30FBBA2C32238E2A98547AF97931E550428B9B3F1C8EEB6633DCFA86C5B27DD3	vTrus ECC Root CA

CN = vTrus ECC DV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	FC88BD89DC680F0C8309051E4A2024E3270CB475	4D391FC790BD702CAD3CCBC0B025C5CDD88C6FDF274DCF5FBD3F027A80C2C7E5	vTrus ECC Root CA
CN = vTrus ECC OV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha384ECDSA	256 bits	35F9EFCE60776FBBC09F68271A878304708815C6	42E46C4487459128517649731457B6AE20099D541BD182C5497B2E67E6FFD0F6	vTrus ECC Root CA
CN = vTrus ECC EV SSL CA O = iTrusChina Co.,Ltd. C = CN	Signing Key	sha256ECDSA	256 bits	BF16C125066118616BE13019083F7E542703B75B	BD30C0D1E7ACB83EFC4F5F6C62F8F3A579BAB27527AFAE666C696C3A867175F1	vTrus ECC Root CA

Appendix B

Applicable versions of Certification Practice Statement (CPS) and Certificate Policy (CP) in-scope:

Name	Version	Date
iTrusChina Global-Trust Certification Practice Statement	1.5.7	24 September 2024
iTrusChina Global-Trust Certification Practice Statement	1.5.6	22 August 2024
iTrusChina Global-Trust Certification Practice Statement	1.5.5	10 July 2024
iTrusChina Global-Trust Certification Practice Statement	1.5.4	28 March 2024
iTrusChina Global-Trust Certification Practice Statement	1.5.3	15 December 2023
iTrusChina Global-Trust Certificate Policy	1.5.7	24 September 2024
iTrusChina Global-Trust Certificate Policy	1.5.6	22 August 2024
iTrusChina Global-Trust Certificate Policy	1.5.5	10 July 2024
iTrusChina Global-Trust Certificate Policy	1.5.4	28 March 2024
iTrusChina Global-Trust Certificate Policy	1.5.3	15 December 2023

Appendix C

Locations in-scope:

Location	Function
Beijing (North), China	Administration and datacenter facility
Beijing (South), China	Secure site hosting backup materials