AKAM
Anthony KAM
& associates ltd
certified public accountants
阙孝财会计师行有限公司
2105 Wing On Ctr, 111 Connaught Rd, HK
+852 2246 6888
info@akamcpa.com

INDEPENDENT ASSURANCE REPORT

To the management of China Financial Certification Authority Co., Ltd. ("CFCA"):

We have been engaged, in a reasonable assurance engagement, to report on CFCA management's assertion that for its Certification Authority ("CA") operations at Beijing and Chengdu, China, throughout the period 1 August 2019 to 31 July 2020 for its CAs as enumerated in Appendix A, CFCA 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 CFCA 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

- 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 v2.4.1.

CFCA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures does not extend to controls that would address those criteria.

Certification authority's responsibilities

CFCA'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 with Network Security v2.4.1.

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 Control 1, 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 CFCA'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 CFCA'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 CFCA 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 limitations

Because of the nature and inherent limitations of controls, CFCA'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 1 August 2019 to 31 July 2020, CFCA 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 with Network Security v2.4.1.

Without modified our opinion above, we noted that CFCA disclosed an incident (Bug 1608333) on Mozilla's Bugzilla Platform on 9 January 2020. In the incident, two certificates were mis-issued in the testing process by a testing engineer. The two mis-issued certificates had been revoked within two hours after mis-issuance, and the root cause analysis of the incident and the remediations conducted by CFCA have been illustrated in the process of public discussion. The discussions of the matter on the public platform had been closed on 17 January 2020.

We have noted any instance possible non-compliance that are relevant to the CAs enumerated in Appendix A. CFCA's assertion noted all instances possible non-compliance, addressed by CFCA, during the engagement period, regardless of the particular CAs enumerated in Appendix A.

This report does not include any representation as to the quality of CFCA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1, nor the suitability of any of CFCA's services for any customer's intended purpose.

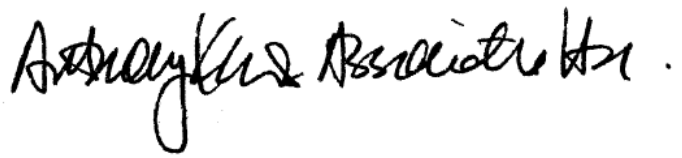
Use of the WebTrust seal

CFCA'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.

AKAM

Anthony Kam & Associates Ltd.
2105 Wing On Ctr, 111 Connaught Road, HK SAR, China

21 October 2020



AKAM
Anthony KAM
& associates ltd
certified public accountants
阙孝财会计师行有限公司
2105 Wing On Ctr, 111 Connaught Rd, HK
+852 2246 6888
info@akamcpa.com

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 = CFCA EV ROOT O = China Financial Certification Authority C = CN	Root Key	sha256RSA	4096 bits	e3fe2dfd28d00bb5bab6a2c4bf06aa058c93fb2f	5CC3D78E4E1D5E45547A04E6873E64F90CF9536D1CCC2EF800F355C4C5FD70FD	CFCA EV ROOT
CN = CFCA EV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	5508e2dccc956d1f5ddeb347e8e916c6c04577c4	CC7253EBDE9F7E92CBA297B5BADED1B22E5CEACA525E201B4DC410F4F3504B5E	CFCA EV ROOT
CN = CFCA OV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	66b3effb549587e9aca59656aee67ded3ad043d1	F07BBBDE076F9B40C57CC4BEFEDE97CA1F53B9AE147F035D284CBF53F3432FB8	CFCA EV ROOT
CN = CFCA Identity CA O = China Financial Certification Authority C = CN	Root Key	sha256RSA	4096 bits	c0ac76a2d35dfff6cd16005b38a77f557d85596c	0566635F27C08FB06292264B8B4EDCB370801A2F586D6A7840D4140312FD5A24	CFCA Identity CA
CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	9c44f4bf378f460b5991e5b6d81c0e77bc9af272	FFB85C26308A961351249EA641F659D49F639E91DAED9C92D046CCDCECC93D2F	CFCA Identity CA

AKAM
Anthony KAM
& associates ltd
certified public accountants
阙孝财会计师行有限公司
2105 Wing On Ctr, 111 Connaught Rd, HK
+852 2246 6888
info@akamcpa.com

Appendix B

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

Name	Version	Date
Certification Practice Statement of CFCA Global-Trust System CFCA	4.0	June 2019
Certification Practice Statement of CFCA Identity CA System	1.4	July 2020
Certification Practice Statement of CFCA Identity CA System	1.3	July 2019
CFCA Certificate Policy	3.1	November 2018

CFCA MANAGEMENT'S ASSERTION

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

CFCA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in CFCA management's opinion, in providing its CA services at Beijing and Chengdu, China, throughout the period 1 August 2019 to 31 July 2020, CFCA 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 CFCA 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 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
- 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 v2.4.1.

CFCA had disclosed an incident (Bug 1608333) on Mozilla's Bugzilla Platform on 9 January 2020. In the incident, two certificates were mis-issued in the testing process by a testing engineer. The two mis-issued certificates had been revoked within two hours after mis-issuance, and the root cause analysis of the incident and the remediations conducted by CFCA have been illustrated in the process of public discussion. The discussions of the matter on the public platform had been closed on 17 January 2020.

Ms. _____

President and General Manager of China Financial Certification Authority Co., Ltd.

20-3, Pingyuaali, Caishikou South Avenue, Xi Cheng District, Beijing, China

21 October 2020

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 = CFCA EV ROOT O = China Financial Certification Authority C = CN	Root Key	sha256RSA	4096 bits	e3fe2dfd28d00bb5bab6a2c4bf06aa058c93fb2f	5CC3D78E4E1D5E45547A04E6873E64F90CF9536D1CCC2EF800F355C4C5FD70FD	CFCA EV ROOT
CN = CFCA EV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	5508e2dccc956d1f5ddeb347e8e916c6c04577c4	CC7253EBDE9F7E92CBA297B5BADED1B22E5CEACA525E201B4DC410F4F3504B5E	CFCA EV ROOT
CN = CFCA OV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	66b3effb549587e9aca59656aee67ded3ad043d1	F07BBBDE076F9B40C57CC4BEFEDE97CA1F53B9AE147F035D284CBF53F3432FB8	CFCA EV ROOT
CN = CFCA Identity CA O = China Financial Certification Authority C = CN	Root Key	sha256RSA	4096 bits	c0ac76a2d35dfff6cd16005b38a77f557d85596c	0566635F27C08FB06292264B8B4EDCB370801A2F586D6A7840D4140312FD5A24	CFCA Identity CA
CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	9c44f4bf378f460b5991e5b6d81c0e77bc9af272	FFB85C26308A961351249EA641F659D49F639E91DAED9C92D046CCDCECC93D2F	CFCA Identity CA

Appendix B

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

Name	Version	Date
Certification Practice Statement of CFCA Global-Trust System CFCA	4.0	June 2019
Certification Practice Statement of CFCA Identity CA System	1.4	July 2020
Certification Practice Statement of CFCA Identity CA System	1.3	July 2019
CFCA Certificate Policy	3.1	November 2018