

## 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 2021 to 31 July 2022 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 v2.5](#).

CFCA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures do 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 v2.5](#).

### **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 2021 to 31 July 2022, 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 v2.5](#).

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 v2.5](#), nor the suitability of any of CFCA's services for any customer's intended purpose.

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

- CFCA was aware of the incident ([Bug 1741497](#)) reported on Mozilla's Bugzilla Platform on 16 November 2021. In the incident, audit statements were past due for the root certificate of CFCA EV ROOT because the corresponding links were not available yet for public disclosure of the audit statements in time before the due date via the regular approach with the issuing body. The routine auditing works had been accomplished, audit statements were prepared, and the content of the audit statements had been disclosed on Mozilla's Bugzilla Platform on 4 January 2022 and the official website of CFCA alternatively for this situation. The corresponding links were obtained from the regular issuing body for public disclosure of the audit statements afterwards on 16 June 2022 as disclosed in the same thread of Mozilla's Bugzilla Platform.
- CFCA was informed on 1 June 2022 the incident ([Bug 1771482](#)) reported on Mozilla's Bugzilla Platform on 27 May 2022. In the incident, one certificate was mis-issued with incorrect values put in the postalCode and streetAddress fields of the certificate. The mis-issued certificate had been revoked on 2 June 2022 after the mis-issuance, and the cause analysis of the incident and the remediations conducted by CFCA have been illustrated in the process of public discussions. The discussions of the matter on the public platform had been closed on 19 August 2022.
- CFCA was informed on 11 June 2022 the incident ([Bug 1778035](#)) reported on Mozilla's Bugzilla Platform on 4 July 2022. In the incident, the status of a revoked certificate was mis-reported via the OCSP service of the CA. The incorrect response was investigated and the cause analysis of the incident and the remediations conducted by CFCA have been illustrated in the process of public discussions. The system component was updated on 16 June 2022 to solve the issue according to the discussions of the matter on the public platform.

#### 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

24 October 2022



## 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	e3fe2dfd28d0 0bb5bab6a2c4 bf06aa058c93f b2f	5CC3D78E4E1 D5E45547A04 E6873E64F90C F9536D1CCC2 EF800F355C4C 5FD70FD	CFCA EV ROOT
CN = CFCA EV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	5508e2dccc95 6d1f5ddeb347 e8e916c6c045 77c4	CC7253EBDE9 F7E92CBA297 B5BADED1B22 E5CEACA525E 201B4DC410F 4F3504B5E	CFCA EV ROOT
CN = CFCA OV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	66b3effb5495 87e9aca59656 aee67ded3ad0 43d1	F07BBBDE076 F9B40C57CC4 BEFEDE97CA1 F53B9AE147F0 35D284CBF53 F3432FB8	CFCA EV ROOT

## Appendix B

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

Name	Version	Date
<a href="#">Certification Practice Statement of CFCA Global-Trust System CFCA</a>	4.3	July 2022
<a href="#">Certification Practice Statement of CFCA Global-Trust System CFCA</a>	4.2	July 2021
<a href="#">Certification Practice Statement of CFCA Identity CA System</a>	1.5	July 2021

## 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 2021 to 31 July 2022, CFCA has:

- disclosed its SSL certificate life cycle management business practices in its Certification Practice Statement (CP/CPS) 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 v2.5](#).

CFCA has disclosed the following matters publicly on Mozilla's Bugzilla's Platform during the audit period:

Bug ID	Summary	Opened	Closed	Resolution
1741497	Overdue Audit Statements 2021	16 November 2021	-	Fixed but thread not closed yet
1771482	Precertificate with postalCode and streetAddress swapped	27 May 2022	19 August 2022	Fixed
1778035	The wrong status of OCSP	4 July 2022	-	Fixed but thread not closed yet



Ms. \_\_\_\_\_



President and General Manager of China Financial Certification Authority Co., Ltd.  
20-3, Pingyuanli, Caishikou South Avenue, Xi Cheng District, Beijing, China

24 October 2022



**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	e3fe2dfd28d0 0bb5bab6a2c4 bf06aa058c93f b2f	5CC3D78E4E1 D5E45547A04 E6873E64F90C F9536D1CCC2 EF800F355C4C 5FD70FD	CFCA EV ROOT
CN = CFCA EV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	5508e2dcc95 6d1f5ddeb347 e8e916c6c045 77c4	CC7253EBDE9 F7E92CBA297 B5BADED1B22 E5CEACA525E 201B4DC410F 4F3504B5E	CFCA EV ROOT
CN = CFCA OV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	66b3effb5495 87e9aca59656 aee67ded3ad0 43d1	F07BBBDE076 F9B40C57CC4 BEFEDE97CA1 F53B9AE147F0 35D284CBF53 F3432FB8	CFCA EV ROOT

CFCA



## Appendix B

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

Name	Version	Date
<a href="#">Certification Practice Statement of CFCA Global-Trust System CFCA</a>	4.3	July 2022
<a href="#">Certification Practice Statement of CFCA Global-Trust System CFCA</a>	4.2	July 2021
<a href="#">Certification Practice Statement of CFCA Identity CA System</a>	1.5	July 2021

## 独立鉴证报告

( 注意：本中文报告只作参考。正文请参阅英文报告。 )

致：中金金融认证中心有限公司管理阶层

我们接受委托，对附件表 A 所列中金金融认证中心有限公司（简称“CFCA”）于 2021 年 8 月 1 日至 2022 年 7 月 31 日期间于中国北京及成都运营的电子认证服务其管理阶层认定执行了合理保证的鉴证业务。根据管理阶层认定，CFCA 已：

- 在附件表 B 列举的中国金融认证中心全球信任体系电子认证业务规则（CP/CPS）中披露了 SSL 证书生命周期业务规则，包括承诺遵循 CA/Browser 论坛的相关指引提供 SSL 证书服务，并依据披露的业务规则提供相关服务
- 通过有效控制机制，以提供以下合理保证：
  - 建立并保护所管理的密钥和 SSL 证书在生命周期中的完整性；以及
  - 于 CFCA 所执行的注册操作恰当地鉴定 SSL 证书申请者的信息
- 通过有效控制机制，以提供以下合理保证：
  - 对 CA 系统和数据的逻辑和物理访问仅限于授权的个人；
  - 保持密钥和证书管理操作的连续性；以及
  - CA 系统的开发，维护和操作得到适当的授权和执行，以维持 CA 系统的完整
- 通过有效控制机制，以提供合理保证确保符合 CA/Browser 论坛（CA/Browser Forum）发布的网络及证书系统安全规范（Network and Certificate System Security Requirements）

以符合 [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5](#)。

CFCA 未托管其私钥，未提供订户密钥生成服务，亦未提供证书挂起服务。据此，我们的审计程序未延伸至相关标准的有关控制。

## CFCA 的责任

CFCA 的管理层负责确保管理层认定，包括其陈述的客观性以及认定中描述的 CFCA 所提供的服务能够符合 [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5](#) 的规定。

## 审计师的独立性和质量控制

我们保持独立性并遵守国际道德委员会针对会计人员发布的职业会计师道德准则 ( Code of Ethics for Professional Accountants ) 规定的道德要求，该准则是建立在正直、客观、专业能力和谨慎、保密和职业行为的基本原则之上。我们公司遵循国际标准要求的质量控制 1 ( International Standard on Quality Control 1 )，并据此维护全面的质量控制体系，包括符合道德要求、专业标准和适用法律法规要求的文件化的政策和程序。

## 审计师的责任

我们的职责是在执行鉴证工作的基础上对 CFCA 的管理层认定发表结论。我们根据国际审计与鉴证准则理事会发布的国际鉴证业务准则第 3000 号 “历史财务信息审计或审阅以外的鉴证业务” 的规定执行了鉴证工作。此准则要求我们计划并执行相应的审计程序以获取所有重大方面和对管理层认定的合理保证，包括：

- (1) 了解 CFCA SSL 证书生命周期管理，包括 SSL 证书发放、更新和吊销，并了解 CFCA 的网络和证书系统安全是否符合 CA/Browser 论坛的相应要求；
- (2) 选择测试业务操作是否遵守了所披露的 SSL 证书生命周期管理；
- (3) 测试和评估控制活动执行的有效性；以及
- (4) 执行其他我们认为必要的鉴证程序。

我们相信，我们获取的证据是充分、适当的，为发表鉴证结论提供了基础。

## 控制的有效性

CFCA 的内部控制的有效性和重要性，及其对用户及相关依赖方的控制风险评估所产生的影响，取决于控制间的相互作用以及其他存在于每个用户和相关依赖方的因素。我们并没有对用户和依赖方所负责的控制的有效性进行任何评估工作。

## 固有限制

由于内部控制体系本身的限制，CFCA 满足上述要求的能力可能会受到影响，例如：控制可能未达到预防、发现或纠正错误、舞弊、对系统或信息的未授权访问，或违反内外部制度或规定的要求。此外，风险的变化可能会影响本评估报告在将来时间的参考价值。

## 结论

我们认为，CFCA 于 2021 年 8 月 1 日至 2022 年 7 月 31 日期间的电子认证服务的管理阶层认定在所有重大方面符合 [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5](#)。

本报告并不包括任何在 [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5](#) 以外的质量标准声明，或对客户对 CFCA 服务的合适性声明。

在不修改意见的情况下，我们在程序中注意到以下事项：

- CFCA 获悉 2021 年 11 月 16 日在 Mozilla 的 Bugzilla 平台上报告的事件 [Bug 1741497](#)。在该事件中，CFCA EV ROOT 的根证书的审计报告过期，因为尚未能按往例由负责公布报告的机构取得相应的链接，在截止日期前及时公示审计报告。例行审计工作当时已经完成，审计报告已编制完成，审计报告内容已于 2022 年 1 月 4 日在 Mozilla 的 Bugzilla 平台和 CFCA 官方网站上披露。相应的链接是从 2022 年 6 月 16 日之后方从公开披露审计报告的机构获得，如 Mozilla 的 Bugzilla 平台的同一讨论序列所披露的。
- CFCA 于 2022 年 6 月 1 日获通知 Mozilla Bugzilla 公众平台于 5 月 27 日通报了事件 [Bug 1771482](#)。于此事件中，一张数字证书因 postalCode 与 streetAddress 栏位输入错误发生误签，此张误签的数字证书于 6 月 2 日完成吊销。关于此事件的发生根本原因与整改方案，CFCA 业已于公众平台阐明，此议题的相关讨论于 2022 年 8 月 19 日结束。
- CFCA 于 2022 年 6 月 11 日获通知 Mozilla Bugzilla 公众平台于 7 月 4 日通报了事件 [Bug 1778035](#)。于此事件中，某已完成吊销的数字证书经 OCSP 服务查询证书效力获得错误的信息；关于此事件的发生根本原因与整改方案，CFCA 业已于公众平台阐明；经调查后，系统于 6 月 16 日进行了更新，修正了相关问题。

## 对 Webtrust 标识的使用

在 CFCA 网站上的 WebTrust SSL BR 电子认证标识是本报告内容的一种符号表示，它并不是为了也不应被认为是对本报告的更新或任何进一步的保证。

# AKAM

2105 Wing On Ctr, 111 Connaught Rd, HK

Anthony KAM  
& associates ltd  
certified public accountants  
爾孝財會計師行有限公司

+852 2246 6888 info@akamcpa.com

# AKAM

Anthony Kam & Associates Ltd.

2105 Wing On Ctr, 111 Connaught Road, HK SAR, China

24 October 2022

*Anthony Kam & Associates Ltd.*

## 附件表 A

本鉴证报告内包括的密钥与证书列举如下:

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	e3fe2dfd28d0 0bb5bab6a2c4 bf06aa058c93f b2f	5CC3D78E4E1 D5E45547A04 E6873E64F90C F9536D1CCC2 EF800F355C4C 5FD70FD	CFCA EV ROOT
CN = CFCA EV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	5508e2dccc95 6d1f5ddeb347 e8e916c6c045 77c4	CC7253EBDE9 F7E92CBA297 B5BADED1B22 E5CEACA525E 201B4DC410F 4F3504B5E	CFCA EV ROOT
CN = CFCA OV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	66b3effb5495 87e9aca59656 aee67ded3ad0 43d1	F07BBBDE076 F9B40C57CC4 BEFEDE97CA1 F53B9AE147F0 35D284CBF53 F3432FB8	CFCA EV ROOT

## 附件表 B

适用范围内的电子认证业务规则（CPS）和证书政策（CP）版本:

Name	Version	Date
<a href="#">中国金融认证中心全球信任体系电子认证业务规则</a>	4.3	July 2022
<a href="#">中国金融认证中心全球信任体系电子认证业务规则</a>	4.2	July 2021
<a href="#">中国金融认证中心 IdentityCA 体系电子认证业务规则</a>	1.5	July 2021

## CFCA 电子认证服务的管理阶层认定报告

( 本中文报告只作参考，正文请参阅英文报告 )

中金金融认证中心有限公司 ( 以下简称 “ CFCA ” ) 运营电子认证服务机构 ( 以下简称 “ CA ” ，附件表 A 列举了 CA 所包括的根证书和中级证书 ) ，并提供电子认证服务。

CFCA 管理层已对所提供的电子认证服务的业务规则披露及控制进行评估。基于此评估，CFCA 管理层认为，在 2021 年 8 月 1 日至 2022 年 7 月 31 日就 CFCA 在中国北京及成都提供 CA 服务期间，CFCA 已：

- 在附件表 B 列举的中国金融认证中心全球信任体系电子认证业务规则 ( CP/CPS ) 中披露了 SSL 证书生命周期业务规则，包括承诺遵循 CA/Browser 论坛的相关指引提供 SSL 证书服务，并依据披露的业务规则提供相关服务
- 通过有效控制机制，以提供以下合理保证：
  - 建立并保护所管理的密钥和订户 SSL 证书在生命周期中的完整性；以及
  - 于 CFCA 所执行的注册操作恰当地鉴定 SSL 证书申请者的信息；
- 通过有效控制机制，以提供以下合理保证：
  - 对 CA 系统和数据的逻辑和物理访问仅限于授权的个人；
  - 保持密钥和证书管理操作的连续性；以及
  - CA 系统的开发，维护和操作得到适当的授权和执行，以维持 CA 系统的完整；
- 通过有效控制机制，以提供合理保证确保符合 CA/Browser 论坛发布的网络及证书系统安全规范

以符合 [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5](#)。

CFCA 已于 Mozilla 的 Bugzilla 平台披露本次审计期间有关的下列事项：

Bug ID	Summary	Opened	Closed	Resolution
1741497	Overdue Audit Statements 2021	16 November 2021	-	Fixed but thread not closed yet
1771482	Precertificate with postalCode and streetAddress swapped	27 May 2022	19 August 2022	Fixed
1778035	The wrong status of OCSP	4 July 2022	-	Fixed but thread not closed yet





董事长兼总经理

中金金融认证中心有限公司  
中国北京市西城区菜市口南大街平原里 20-3

2022 年 10 月 24 日



附件表 A

本认定报告内包括的密钥与证书列举如下:

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	e3fe2dfd28d0 0bb5bab6a2c4 bf06aa058c93f b2f	5CC3D78E4E1 D5E45547A04 E6873E64F90C F9536D1CCC2 EF800F355C4C 5FD70FD	CFCA EV ROOT
CN = CFCA EV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	5508e2dccc95 6d1f5ddeb347 e8e916c6c045 77c4	CC7253EBDE9 F7E92CBA297 B5BADED1B22 E5CEACA525E 201B4DC410F 4F3504B5E	CFCA EV ROOT
CN = CFCA OV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	66b3effb5495 87e9aca59656 aee67ded3ad0 43d1	F07BBBDE076 F9B40C57CC4 BEFEDE97CA1 F53B9AE147F0 35D284CBF53 F3432FB8	CFCA EV ROOT

附件表 B

适用范围内的电子认证业务规则 ( CPS ) 和证书政策 ( CP ) 版本:

Name	Version	Date
<a href="#">中国金融认证中心全球信任体系电子认证业务规则</a>	4.3	July 2022
<a href="#">中国金融认证中心全球信任体系电子认证业务规则</a>	4.2	July 2021
<a href="#">中国金融认证中心 IdentityCA 体系电子认证业务规则</a>	1.5	July 2021

