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 as enumerated in Appendix C, throughout the period 1 August 2022 to 31 July 2023 for its CAs as enumerated in Appendix A, CFCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement (CP/CPS) as enumerated in Appendix B

- maintained effective controls to provide reasonable assurance that:
  - CFCA's Certification Practice Statement is consistent with its Certificate Policy
  - CFCA provides its services in accordance with its Certificate Policy and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
  - 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 v2.2.2.

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 v2.2.2.

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 key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
(2) selectively testing transactions executed in accordance with disclosed key and 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 2022 to 31 July 2023, 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 v2.2.2.

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 v2.2.2, 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:

- A reporter had disclosed an incident (Bug 1838371) on Mozilla's Bugzilla Platform on 13 June 2023. In the incident, the reporter found a certificate with an OrganizationName which could not match the name of the domain owner was issued. CFCA explained the mismatch of the OrganizationName coming from the understanding of the agent applicant role in the registration process. According to the understanding of the registration department, the name of the agent applicant can be placed in the OrganizationName field of the

certificate as an expression of the accurate business relationship, which is not commonly recognized as a correct practice for certificate issuance. After communications with the audit practitioner, CFCA agreed on the mismatch as an issue of certificate inaccuracy which needs remediations. The remediations shall then commence with proposal drafted in the incident thread (Bug 1838371) on Mozilla's Bugzilla Platform.

- A reporter had disclosed an incident (Bug 1771482) on Mozilla's Bugzilla Platform on 27 May 2022. In the incident, the reporter found the pre-certificate issued by CFCA that seems to have the postalCode and the streetAddress fields swapped. The incident had been acknowledged, processed, and closed on 15 August 2022 in this audit period as disclosed in the thread on Mozilla's Bugzilla Platform aforementioned.

- CFCA found the OCSP issue and reported it as an incident (Bug 1778035) on 4 July 2022 while processing the incident (Bug 1771482) on Mozilla's Bugzilla Platform. In the incident, CFCA found OCSP cache data was not synchronized after a system update applied, which would lead to an incorrect OCSP status response. The incident had been acknowledged, processed, and closed on 19 April 2023 in this audit period as disclosed in the thread on Mozilla's Bugzilla Platform aforementioned.

- The incident (Bug 1784820) derived from the incident (Bug 1752685) had been reported 14 August 2022 on Mozilla's Bugzilla Platform. In the incident, delayed reporting of ICA certificate issuance was addressed. The incident had been acknowledged, processed, and closed on 30 June 2023 in this audit period as disclosed in the thread on Mozilla's Bugzilla Platform aforementioned.

- The incident (Bug 1793053) derived from the incident (Bug 1752685) had been reported 30 September 2022 on Mozilla's Bugzilla Platform. In the incident, ICA certificate of CFCA was found no EKU field allocated. The incident had been acknowledged, processed, and closed on 30 June 2023 in this audit period as disclosed in the thread on Mozilla's Bugzilla Platform aforementioned.

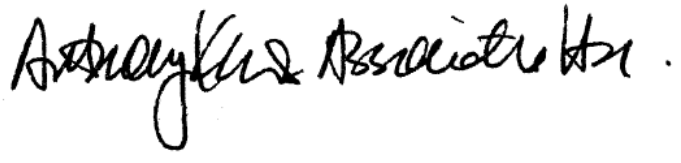
- The incident (Bug 1793059) derived from the incident (Bug 1752685) had been reported 30 September 2022 on Mozilla's Bugzilla Platform. In the incident, the delay of ICA certificate revocation was addressed. The incident had been acknowledged, processed, and closed on 30 June 2023 in this audit period as disclosed in the thread on Mozilla's Bugzilla Platform aforementioned.

Use of the WebTrust seal

CFCA's use of the WebTrust for Certification Authorities 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

27 October 2023



AKAM
Anthony KAM
& associates ltd
certified public accountants
阚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 DV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	55200db47d29fe2c6dcf9dd31cbf015aa7dc81bd	DA738A474EE7473C9699ECBA8EB5F483ADA967988185A05975C4BA0C01B39559	CFCA EV ROOT
CN = CFCA Identity CA O = China Financial Certification Authority C = CN	Root Key	sha256RSA	4096 bits	c0ac76a2d35dfff6cd16005b38a77f557d85596c	FFB85C26308A961351249EA641F659D49F639E91DAED9C92D046CCDCECC93D2F	CFCA Identity CA
CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	9c44f4bf378f460b5991e5b6d81c0e77bc9af272	0566635F27C08FB06292264B8B4EDCB370801A2F586D6A7840D4140312FD5A24	CFCA Identity CA

Appendix B

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

Name	Version	Date
CFCA Certificate Policy and Certification Practice Statement for Global Trusted System	4.4	November 2022
Certification Practice Statement of CFCA Global-Trust System CFCA	4.3	July 2022

AKAM
Anthony KAM
& associates ltd
certified public accountants
阚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 C

Locations in-scope:

Location	Function
Beijing (North), China	Datacenter Facility
Beijing (South), China	Datacenter Facility
Beijing (Central), China	Administration and Support
Chengdu, China	Registrations and Customer Services

CFCA MANAGEMENT'S ASSERTION

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

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of CFCA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, and 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 CFCA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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 Certification Authority (CA) services at locations as enumerated in Appendix C, throughout the period 1 August 2022 to 31 July 2023, CFCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B

- maintained effective controls to provide reasonable assurance that:
    - CFCA's applicable versions of Certification Practice Statement are consistent with its applicable versions of Certificate Policy; and
    - CFCA provides its services in accordance with its Certificate Policy and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
    - 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

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

A reporter had disclosed an incident (Bug 1838371) on Mozilla's Bugzilla Platform on 13 June 2023. In the incident, the reporter found a certificate with an OrganizationName which could not match the name of the domain owner was issued.

A reporter had disclosed an incident (Bug 1771482) on Mozilla's Bugzilla Platform on 27 May 2022. In the incident, the reporter found the pre-certificate issued by CFCA that seems to have the postalCode and the streetAddress fields swapped. The incident had been acknowledged, processed, and closed on 15 August 2022 in this audit period as disclosed in the thread on Mozilla's Bugzilla Platform aforementioned.

CFCA found the OCSP issue and reported it as an incident (Bug 1778035) on 4 July 2022 while processing the incident (Bug 1771482) on Mozilla's Bugzilla Platform. In the incident, CFCA found OCSP cache data was not synchronized after a system update applied, which would lead to an incorrect OCSP status response. The incident had been acknowledged, processed, and closed on 19 April 2023 in this audit period as disclosed in the thread on Mozilla's Bugzilla Platform aforementioned.

The incident (Bug 1784820) derived from the incident (Bug 1752685) had been reported 14 August 2022 on Mozilla's Bugzilla Platform. In the incident, delayed reporting of ICA certificate issuance was addressed. The incident had been acknowledged, processed, and closed on 30 June 2023 in this audit period as disclosed in the thread on Mozilla's Bugzilla Platform aforementioned.

The incident (Bug 1793053) derived from the incident (Bug 1752685) had been reported 30 September 2022 on Mozilla's Bugzilla Platform. In the incident, ICA certificate of CFCA was found no EKU field allocated. The incident had been acknowledged, processed, and closed on 30 June 2023 in this audit period as disclosed in the thread on Mozilla's Bugzilla Platform aforementioned.

The incident (Bug 1793059) derived from the incident (Bug 1752685) had been reported 30 September 2022 on Mozilla's Bugzilla Platform. In the incident, the delay of ICA certificate revocation was addressed. The incident had been acknowledged, processed, and closed on 30 June 2023 in this audit period as disclosed in the thread on Mozilla's Bugzilla Platform aforementioned.

Ms. _____

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

27 October 2023

CFCA
中国金融认证中心

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 DV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	55200db47d29fe2c6dcf9dd31cbf015aa7dc81bd	DA738A474EE7473C9699ECBA8EB5F483ADA967988185A05975C4BA0C01B39559	CFCA EV ROOT
CN = CFCA Identity CA O = China Financial Certification Authority C = CN	Root Key	sha256RSA	4096 bits	c0ac76a2d35dfff6cd16005b38a77f557d85596c	FFB85C26308A961351249EA641F659D49F639E91DAED9C92D046CCDCECC93D2F	CFCA Identity CA
CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	9c44f4bf378f460b5991e5b6d81c0e77bc9af272	0566635F27C08FB06292264B8B4EDCB370801A2F586D6A7840D4140312FD5A24	CFCA Identity CA

Appendix B

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

Name	Version	Date
CFCA Certificate Policy and Certification Practice Statement for Global Trusted System	4.4	November 2022
Certification Practice Statement of CFCA Global-Trust System CFCA	4.3	July 2022

Appendix C

Locations in-scope:

Location	Function
Beijing (North), China	Datacenter Facility
Beijing (South), China	Datacenter Facility
Beijing (Central), China	Administration and Support
Chengdu, China	Registrations and Customer Services

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

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 的中金金融认证中心有限公司（简称 “CFCA” ）于 2022 年 8 月 1 日至 2023 年 7 月 31 日就 CFCA 在附件表 C 所列地点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）中披露了电子认证业务、密钥生命周期管理、证书生命周期管理，以及 CA 环境控制管理

- 通过有效控制机制，以提供以下合理保证：
  - CFCA 的 CPS 与 CP 相符；
  - CFCA 遵循 CP 和 CPS 提供电子认证服务

- 通过有效控制机制，以提供以下合理保证：
  - 有效维护所管理的密钥与证书在生命周期中的完整性；
  - 建立并保护所管理的订户密钥和订户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

以符合 WebTrust Principles and Criteria for Certification Authorities v2.2.2。

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 v2.2.2 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 密钥和证书生命周期管理及对密钥和证书完整性的控制措施，包括订户和依赖方信息的真实性和保密性，密钥和证书生命周期管理的连续性，以及系统开发、运维的完整性；
(2) 选择测试业务操作是否遵守了所披露的证书生命周期管理；
(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 2022 年 8 月 1 日至 2023 年 7 月 31 日期间的电子认证服务的管理层认定在所有重大方面符合 WebTrust Principles and Criteria for Certification Authorities v2.2.2。

本报告并不包括任何在 WebTrust Principles and Criteria for Certification Authorities v2.2.2 以外的质量标准声明，或对任何客户对 CFCA 服务的合适性声明。

- 2023 年 6 月 13 日，一名通报者在 Mozilla 的 Bugzilla 平台上披露了一起事件（Bug 1838371）。在事件中，通报者发现颁发的证书的组织名称与域名所有者的名称不匹配。CFCA 解释 OrganizationName 的不匹配是由于对代理申请人在注册过程中的角色的理解所致。根据注册部门的理解，可以将代理申请者的姓名放在证书的 OrganizationName 字段中，作为准确商务关系的表达，而这通常不被认为是证书颁发的正确做法。在与审计员沟通后，CFCA 同意将不匹配视为证书不准确的问题，需要纠正。补救措施应从 Mozilla 的 Bugzilla 平台上的事件线程（Bug 1838371）中起草的提案开始。

- 2022 年 5 月 27 日，一名通报者在 Mozilla 的 Bugzilla 平台上披露了一起事件（Bug 1771482）。在事件中，通报者发现了 CFCA 颁发的预证书，将邮政编码和街道地址字段互换了。该事件已于 2022 年 8 月 15 日在本审计週期内得到确认、处理和关闭，一如上述 Mozilla Bugzilla 平台上的帖子中所述。

- CFCA 发现了 OCSP 问题，并于 2022 年 7 月 4 日在 Mozilla 的 Bugzilla 平台上处理事件（Bug 1771482）时将其报告为事件（Bug 1778035）。在事件中，CFCA 发现 OCSP 缓存数据在应用系统更新后未同步，这将导致不正确的 OCSP 证书状态响应。该事件已于 2023 年 4 月 19 日在本审计期内得到确认、处理和关闭，一如上述 Mozilla Bugzilla 平台上的帖子中所述。

- 源自事件（Bug 1752685）的事件（Bug 1793053）已于 2022 年 8 月 14 日在 Mozilla 的 Bugzilla 平台上通报。在这一事件中，ICA 证书颁发的延迟通报得到了处置。该事件已于 2023 年 6 月 30 日在本审计期内得到确认、处理和关闭，一如上述 Mozilla 的 Bugzilla 平台上的帖子所披露的那样。

- 源自事件（Bug 1752685）的事件（Bug 1793053）已于 2022 年 9 月 30 日在 Mozilla 的 Bugzilla 平台上通报。在这一事件中，ICA 证书的 EKU 栏目未被配置。该事件已于 2023 年 6 月 30 日在本审计期内得到确认、处理和关闭，一如上述 Mozilla 的 Bugzilla 平台上的帖子所披露的那样。

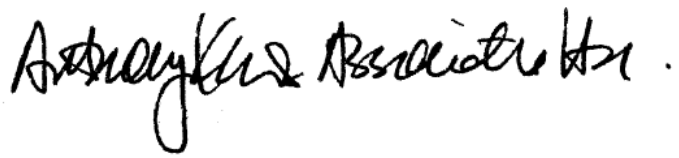
- 源自事件（Bug 1752685）的事件（Bug 1793059）已于 2022 年 9 月 30 日在 Mozilla 的 Bugzilla 平台上通报。在这一事件中，ICA 证书吊销的延迟通报得到了处置。该事件已于 2023 年 6 月 30 日在本审计期内得到确认、处理和关闭，一如上述 Mozilla 的 Bugzilla 平台上的帖子所披露的那样。

对 Webtrust 标识的使用

在 CFCA 网站上的 WebTrust 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
Anthony Kam & Associates Ltd.
2105 Wing On Ctr, 111 Connaught Road, HK SAR, China

27 October 2023



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

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	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 DV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	55200db47d29fe2c6dcf9dd31cbf015aa7dc81bd	DA738A474EE7473C9699ECBA8EB5F483ADA967988185A05975C4BA0C01B39559	CFCA EV ROOT
CN = CFCA Identity CA O = China Financial Certification Authority C = CN	Root Key	sha256RSA	4096 bits	c0ac76a2d35dfff6cd16005b38a77f557d85596c	FFB85C26308A961351249EA641F659D49F639E91DAED9C92D046CCDCECC93D2F	CFCA Identity CA
CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	9c44f4bf378f460b5991e5b6d81c0e77bc9af272	0566635F27C08FB06292264B8B4EDCB370801A2F586D6A7840D4140312FD5A24	CFCA Identity CA

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
CFCA Certificate Policy and Certification Practice Statement for Global Trusted System	4.4	November 2022
Certification Practice Statement of CFCA Global-Trust System CFCA	4.3	July 2022

附件表 C

范围中的地点:

位置	功能
北京 (北), 中国	数据中心
北京 (南), 中国	数据中心
北京 (中), 中国	行政支持
成都, 中国	註册与客户服务

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 列举了服务所包括的根证书和中级证书），并提供以下电子认证服务：

- 订户注册
- 证书更新
- 证书密钥更新
- 证书发布
- 证书分发
- 证书吊销
- 证书验证

CFCA 的管理层负责针对 CA 服务建立并维护有效的控制，包括：CA 业务规则披露、CA 业务规则管理、CA 环境控制、CA 密钥生命周期管理、以及证书生命周期管理。这些控制包括监控机制及为纠正已识别的缺陷所采取的改进措施。

任何控制都有其固有限制，包括人为失误，以及规避或逾越控制的可能性。因此，即使有效的控制也仅能对 CFCA 运营的电子认证服务提供合理保证。此外，由于控制环境的变化，控制的有效性可能随时间而发生变化。

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 2022 年 8 月 1 日至 2023 年 7 月 31 日就 CFCA 在附件表 C 所列地点所提供的电子认证服务期间，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（CPS）和中国金融认证中心证书策略（CP）中披露了电子认证业务、密钥生命周期管理、证书生命周期管理，以及 CA 环境控制管理

- 通过有效控制机制，以提供以下合理保证：
    - CFCA 的 CPS 与 CP 相符；以及
    - CFCA 遵循 CP 和 CPS 提供电子认证服务；

- 通过有效控制机制，以提供以下合理保证：
    - 有效维护所管理的密钥与证书在生命周期中的完整性；
    - 建立并保护所管理的订户密钥和订户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；

以符合 WebTrust Principles and Criteria for Certification Authorities v2.2.2，包括以下内容：

- **CA 业务规则披露**
    - 电子认证业务规则（CPS）
    - 证书策略（CP）

- **CA 业务规则管理**
    - 证书策略管理
    - 电子认证业务规则管理
    - CP 和 CPS 的一致性

- **CA 环境控制**
    - 安全管理
    - 资产分类与管理
    - 人员安全
    - 物理及环境安全
    - 运营管理
    - 系统访问管理
    - 系统开发与维护管理
    - 业务持续性管理
    - 监控与合规管理
    - 审计日志管理

- **CA 密钥生命周期管理**
    - CA 密钥生成
    - CA 密钥存储、备份和恢复
    - CA 公钥分发
    - CA 密钥使用
    - CA 密钥归档和销毁
    - CA 密钥泄露
    - CA 密码设备生命周期管理

- **证书生命周期管理**
    - 订户注册
    - 证书更新
    - 证书密钥更新
    - 证书发布
    - 证书分发
    - 证书吊销
    - 证书验证

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。因此，我们的认定报告未延伸至相关标准的有关控制。

2023 年 6 月 13 日，一名通报者在 Mozilla 的 Bugzilla 平台上披露了一起事件（Bug 1838371）。在事件中，通报者发现颁发的证书的组织名称与域名所有者的名称不匹配。

2022 年 5 月 27 日，一名通报者在 Mozilla 的 Bugzilla 平台上披露了一起事件（Bug 1771482）。在事件中，通报者发现了 CFCA 颁发的预证书，将邮政编码和街道地址字段互换了。该事件已于 2022 年 8 月 15 日在本审计週期内得到确认、处理和关闭，一如上述 Mozilla Bugzilla 平台上的帖子中所述。

CFCA 发现了 OCSP 问题，并于 2022 年 7 月 4 日在 Mozilla 的 Bugzilla 平台上处理事件（(Bug 1771482）时将其报告为事件（Bug 1778035）。在事件中，CFCA 发现 OCSP 缓存数据在应用系统更新后未同步，这将导致不正确的 OCSP 证书状态响应。该事件已于 2023 年 4 月 19 日在本审计期内得到确认、处理和关闭，一如上述 Mozilla Bugzilla 平台上的帖子中所述。

源自事件（Bug 1752685）的事件（Bug 1784820）已于 2022 年 8 月 14 日在 Mozilla 的 Bugzilla 平台上通报。在这一事件中，ICA 证书颁发的延迟通报得到了处置。该事件已于 2023 年 6 月 30 日在本审计期内得到确认、处理和关闭，一如上述 Mozilla 的 Bugzilla 平台上的帖子所披露的那样。

源自事件（Bug 1752685）的事件（Bug 1793053）已于 2022 年 9 月 30 日在 Mozilla 的 Bugzilla 平台上通报。在这一事件中，ICA 证书的 EKU 栏目未被配置。该事件已于 2023 年 6 月 30 日在本审计期内得到确认、处理和关闭，一如上述 Mozilla 的 Bugzilla 平台上的帖子所披露的那样。

源自事件（Bug 1752685）的事件（Bug 1793059）已于 2022 年 9 月 30 日在 Mozilla 的 Bugzilla 平台上通报。在这一事件中，ICA 证书吊销的延迟通报得到了处置。该事件已于 2023 年 6 月 30 日在本审计期内得到确认、处理和关闭，一如上述 Mozilla 的 Bugzilla 平台上的帖子所披露的那样。

董事长

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

2023 年 10 月 27 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	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 DV OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	55200db47d29fe2c6dcf9dd31cbf015aa7dc81bd	DA738A474EE7473C9699ECBA8EB5F483ADA967988185A05975C4BA0C01B39559	CFCA EV ROOT
CN = CFCA Identity CA O = China Financial Certification Authority C = CN	Root Key	sha256RSA	4096 bits	c0ac76a2d35dfff6cd16005b38a77f557d85596c	FFB85C26308A961351249EA641F659D49F639E91DAED9C92D046CCDCECC93D2F	CFCA Identity CA
CN = CFCA Identity OCA O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	2048 bits	9c44f4bf378f460b5991e5b6d81c0e77bc9af272	0566635F27C08FB062922648B4EDCB370801A2F586D6A7840D4140312FD5A24	CFCA Identity CA

附件表 B

适用范围内的电子认证业务规则（CPS）和证书策略（CP）版本:

Name	Version	Date
CFCA Certificate Policy and Certification Practice Statement for Global Trusted System	4.4	November 2022
Certification Practice Statement of CFCA Global-Trust System CFCA	4.3	July 2022

附件表 C

范围中的地点:

位置	功能
北京 (北), 中国	数据中心
北京 (南), 中国	数据中心
北京 (中), 中国	行政支持
成都, 中国	註册与客户服务