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 2023 to 31 July 2024 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, v2.7.

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, v2.7.

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 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 2023 to 31 July 2024, 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, v2.7.

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, v2.7, 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:

- On 4 March 2024, the representative of Google Root Program sent an email to CFCA via the registered email of CFCA for status about the error in issuance of certificates. However, CFCA failed to respond to the email in time and was requested to file an additional incident reporting and processing thread (Bug 1888881) for further explanations and remediations. CFCA acknowledged and made necessary changes to the list of registered contact email addresses to prevent the same deviation from happening again according to the feedback disclosed in the thread of discussions on 5 May 2024.

- CFCA received an email from the representative of Google Root Program about the basicConstraints extension error found in three SSL certificates issued by CFCA. An incident processing thread (Bug 1886135) on Mozilla's Bugzilla Platform created on 19 March 2024 for remediations of the mis-issued certificates. More mis-issued certificates were found after internal investigation. The remediation has been accomplished and the processing thread has been closed on 26 September 2024

- In the processing of the mis-issuance incident (Bug 1886135), a total of 2098 certificates had been found during the investigation and necessary procedures applied. Following the requirement in Section 4.9.1.1 of TLS baseline requirements, 840 affected certificates were revoked within 5 days. However, the remaining certificates had not been revoked successfully within the window of time required, so a new incident processing thread (Bug 1888882) was filed for processing the delayed revocation issue.

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.

Anthony Kam & Associates Ltd.
Certified Public Accountants
2105 Wing On Ctr, 111 Connaught Road, HK SAR, China
28 Oct 2024
KAM Hau Choi Anthony
Practising Certificate Number P02558

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 Global RSA ROOT G2 O = China Financial Certification Authority C = CN	Root Key	sha512RSA	4096 bits	fb54011310034c5884e2a70684f962055d1289b7	6E6EB29F5EBA910AFFD462FC921D724E526805EFE908AEC45BD409B624E14C09	CFCA Global RSA ROOT G2
CN = CFCA DV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	dcaae14b5c5a649f6b570fd0545d66a4e88e7973	CDC4606B6968C6D65FFB61B84FAD3906127C33EC7EACBB0B8B20B389767E6A0F	CFCA Global RSA ROOT G2

CN = CFCA OV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	31f12de8b7576955bb85734014b6214a21c2fbdd	EB6C466E647A5EB633A38290FD30131DD7B887B51E1340ABB502C7AB31688F04	CFCA Global RSA ROOT G2
CN = CFCA EV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	b1bcbe24db2d0a94810afa5001290dcafc2f443b	4D452B952FDCDE663C10400AED613C96BED8C4BF1A8F750D8A74D5C4183B1920	CFCA Global RSA ROOT G2
CN = CFCA Global ECC ROOT G2 O = China Financial Certification Authority C = CN	Root Key	sha384ECDSA	384 bits	cc4708eaa3d4f57626500f8786321dc992d610bd	23E4F8DA7D482CD105289433C2E10CE67C1E1092B4DC50101F6D0C346E965972	CFCA Global ECC ROOT G2
CN = CFCA DV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	c8cdaa65512277cf837ae5586899be2a0ac73069	ADBB46AF1FE1426F69BBCD0CDBD671650313A5C63993708CC4B465F14BD4E01B	CFCA Global ECC ROOT G2
CN = CFCA OV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	064e6c68b695d1454d4965838f60805657da05d6	6F6478FBFF45CC30AC0FE4EC3CC4EF3CAF0E959508B00342C229DD60C9A432A1	CFCA Global ECC ROOT G2
CN = CFCA EV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	b7202c74b5b5a5fceb183f3de7bd4ed225c5a044	80C868B316313761E34D6122AD687D462E7016FC54FDCBBA8D70F149752891C3	CFCA Global ECC ROOT G2

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	4.5	August 2023
CFCA Certificate Policy and Certification Practice Statement for Global Trusted System	4.4	November 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 SSL CA services.

The management of CFCA 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 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 SSL CA services. Based on that assessment, in CFCA management's opinion, in providing its SSL CA services at locations as enumerated in Appendix C, throughout the period 1 August 2023 to 31 July 2024, 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, v2.7.

On 4 March 2024, the representative of Google Root Program sent an email to CFCA via the registered email of CFCA for status about the error in issuance of certificates. However, CFCA failed to respond to the email in time and was requested to file an additional incident reporting and processing thread (Bug 1888881) for further explanations and remediations. CFCA acknowledged and made necessary changes to the list of registered contact email addresses to prevent the same deviation from happening again according to the feedback disclosed in the thread of discussions on 5 May 2024.

CFCA received an email from the representative of Google Root Program about the basicConstraints extension error found in three SSL certificates issued by CFCA. An incident processing thread (Bug 1886135) on Mozilla's Bugzilla Platform created on 19 March 2024 for remediations of the mis-issued certificates. More mis-issued certificates were found after internal investigation. The remediation has been accomplished and the processing thread has been closed on 26 September 2024.

In the processing of the mis-issuance incident (Bug 1886135), a total of 2098 certificates had been found during the investigation and necessary procedures applied. Following the requirement in Section 4.9.1.1 of TLS baseline requirements, 840 affected certificates were revoked within 5 days. However, the remaining certificates had not been revoked successfully within the window of time required, so a new incident processing thread (Bug 1888882) was filed for processing the delayed revocation issue.

Mr. _____

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

28 October 2024

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 Global RSA ROOT G2 O = China Financial Certification Authority C = CN	Root Key	sha512RSA	4096 bits	fb54011310034c5884e2a70684f962055d1289b7	6E6EB29F5EBA910AFFD462FC921D724E526805EFE908AEC45BD409B624E14C09	CFCA Global RSA ROOT G2
CN = CFCA DV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	dcaae14b5c5a649f6b570fd0545d66a4e88e7973	CDC4606B6968C6D65FFB61B84FAD3906127C33EC7EACBB0B8B20B389767E6A0F	CFCA Global RSA ROOT G2
CN = CFCA OV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	31f12de8b7576955bb85734014b6214a21c2fbdd	EB6C466E647A5EB633A38290FD30131DD7B887B51E1340ABB502C7AB31688F04	CFCA Global RSA ROOT G2

CN = CFCA EV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	b1bcbe24db2d0a94810afa5001290dcafc2f443b	4D452B952FDCDE663C10400AED613C96BED8C4BF1A8F750D8A74D5C4183B1920	CFCA Global RSA ROOT G2
CN = CFCA Global ECC ROOT G2 O = China Financial Certification Authority C = CN	Root Key	sha384ECDSA	384 bits	cc4708eaa3d4f57626500f8786321dc992d610bd	23E4F8DA7D482CD105289433C2E10CE67C1E1092B4DC50101F6D0C346E965972	CFCA Global ECC ROOT G2
CN = CFCA DV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	c8cdaa65512277cf837ae5586899be2a0ac73069	ADBB46AF1FE1426F69BBCD0CDBD671650313A5C63993708CC4B465F14BD4E01B	CFCA Global ECC ROOT G2
CN = CFCA OV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	064e6c68b695d1454d4965838f60805657da05d6	6F6478FBFF45CC30AC0FE4EC3CC4EF3CAF0E959508B00342C229DD60C9A432A1	CFCA Global ECC ROOT G2
CN = CFCA EV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	b7202c74b5b5a5fceb183f3de7bd4ed225c5a044	80C868B316313761E34D6122AD687D462E7016FC54FDCBBA8D70F149752891C3	CFCA Global ECC ROOT G2

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	4.5	August 2023
CFCA Certificate Policy and Certification Practice Statement for Global Trusted System	4.4	November 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 所列中金金融认证中心有限公司（简称“CFCA”）于 2023 年 8 月 1 日至 2024 年 7 月 31 日期间于附件表 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 列举的中金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, v2.7。

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, v2.7 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品质管理标准 （ISQM）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 2023 年 8 月 1 日至 2024 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, v2.7。

本报告并不包括任何在 WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, v2.7 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。

在不修改意见的情况下，我们在程序中注意到以下事项：

- 2024 年 3 月 4 日，Google Root Program 代表通过 CFCA 的注册邮箱向 CFCA 发送了一封电子邮件，询问证书颁发错误的情况。但 CFCA 未能及时回复该邮件，并被要求提交额外的事件报告和处理线程（Bug 1888881）以进行进一步解释和补救。根据 2024 年 5 月 5 日讨论线程中披露的反馈，CFCA 已确认并对注册联系电子邮件地址列表进行了必要的更改，以防止再次发生相同的偏差。

- CFCA 收到 Google Root Program 代表发来的电子邮件，称 CFCA 签发的三张 SSL 证书存在 basicConstraints 扩展错误。2024 年 3 月 19 日，Mozilla 的 Bugzilla 平台上创建了一个事件处理线程 (Bug 1886135)，用于整改证书颁发的错误。内部调查后发现更多错误颁发的证书。整改工作已完成，处理线程已于 2024 年 9 月 26 日关闭。

- 在处理错误颁发事件（Bug 1886135）时，调查期间共发现 2098 张证书，并应用了必要的程序。根据 TLS 基线要求第 4.9.1.1 节的要求，840 张受影响的证书在 5 天内被撤销。但是，其余证书未能在要求的时间内成功撤销，因此提交了新的事件处理线程（Bug 1888882）来处理延迟撤销问题。

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。

Anthony Kam & Associates Ltd.
Certified Public Accountants
2105 Wing On Ctr, 111 Connaught Road, HK SAR, China
28 Oct 2024
KAM Hau Choi Anthony
Practising Certificate Number P02558

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 Global RSA ROOT G2 O = China Financial Certification Authority C = CN	Root Key	sha512RSA	4096 bits	fb54011310034c5884e2a70684f962055d1289b7	6E6EB29F5EBA910AFFD462FC921D724E526805EFE908AEC45BD409B624E14C09	CFCA Global RSA ROOT G2
CN = CFCA DV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	dcaae14b5c5a649f6b570fd0545d66a4e88e7973	CDC4606B6968C6D65FFB61B84FAD3906127C33EC7EACBB0B8B20B389767E6A0F	CFCA Global RSA ROOT G2
CN = CFCA OV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	31f12de8b7576955bb85734014b6214a21c2fbdd	EB6C466E647A5EB633A38290FD30131DD7B887B51E1340ABB502C7AB31688F04	CFCA Global RSA ROOT G2

CN = CFCA EV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	b1bcbe24db2d0a94810afa5001290dcafc2f443b	4D452B952FDCDE663C10400AED613C96BED8C4BF1A8F750D8A74D5C4183B1920	CFCA Global RSA ROOT G2
CN = CFCA Global ECC ROOT G2 O = China Financial Certification Authority C = CN	Root Key	sha384ECDSA	384 bits	cc4708eaa3d4f57626500f8786321dc992d610bd	23E4F8DA7D482CD105289433C2E10CE67C1E1092B4DC50101F6D0C346E965972	CFCA Global ECC ROOT G2
CN = CFCA DV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	c8cdaa65512277cf837ae5586899be2a0ac73069	ADBB46AF1FE1426F69BBCD0CDBD671650313A5C63993708CC4B465F14BD4E01B	CFCA Global ECC ROOT G2
CN = CFCA OV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	064e6c68b695d1454d4965838f60805657da05d6	6F6478FBFF45CC30AC0FE4EC3CC4EF3CAF0E959508B00342C229DD60C9A432A1	CFCA Global ECC ROOT G2
CN = CFCA EV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	b7202c74b5b5a5fceb183f3de7bd4ed225c5a044	80C868B316313761E34D6122AD687D462E7016FC54FDCBBA8D70F149752891C3	CFCA Global ECC ROOT G2

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	4.5	August 2023
CFCA Certificate Policy and Certification Practice Statement for Global Trusted System	4.4	November 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 CA 所包括的根证书和中级证书），并提供 SSL 电子认证服务。

CFCA 的管理层负责针对 SSL CA 服务建立并维护有效的控制，包括：包括其网络和证书安全系统控制、其网站上的 SSL CA 业务实践披露、SSL 密钥生命周期管理控制和 SSL 证书生命周期管理控制。这些控制包含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 SSL 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 2023 年 8 月 1 日至 2024 年 7 月 31 日就 CFCA 在附件表 C 所列地点提供 SSL 电子认证服务期间，CFCA 已：

- 在附件表 B 列举的中金金融认证中心全球信任体系电子认证业务规则（CPS）和中金金融认证中心证书策略（CP）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, v2.7。

2024 年 3 月 4 日，Google Root Program 代表通过 CFCA 的注册邮箱向 CFCA 发送了一封电子邮件，询问证书颁发错误的情况。但 CFCA 未能及时回复该邮件，并被要求提交额外的事件报告和处理线程（Bug 1888881）以进行进一步解释和补救。根据 2024 年 5 月 5 日讨论线程中披露的反馈，CFCA 已确认并对注册联系电子邮件地址列表进行了必要的更改，以防止再次发生相同的偏差。

CFCA 收到 Google Root Program 代表发来的电子邮件，称 CFCA 签发的三张 SSL 证书存在 basicConstraints 扩展错误。2024 年 3 月 19 日，Mozilla 的 Bugzilla 平台上创建了一个事件处理线程 (Bug 1886135)，用于整改证书颁发的错误。内部调查后发现更多错误颁发的证书。整改工作已完成，处理线程已于 2024 年 9 月 26 日关闭。

在处理错误颁发事件（Bug 1886135）时，调查期间共发现 2098 张证书，并应用了必要的程序。根据 TLS 基线要求第 4.9.1.1 节的要求，840 张受影响的证书在 5 天内被撤销。但是，其余证书未能在要求的时间内成功撤销，因此提交了新的事件处理线程（Bug 1888882）来处理延迟撤销问题。

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

2024 年 10 月 28 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 Global RSA ROOT G2 O = China Financial Certification Authority C = CN	Root Key	sha512RSA	4096 bits	fb54011310034c5884e2a70684f962055d1289b7	6E6EB29F5EBA910AFFD462FC921D724E526805EFE908AEC45BD409B624E14C09	CFCA Global RSA ROOT G2
CN = CFCA DV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	dcaae14b5c5a649f6b570fd0545d66a4e88e7973	CDC4606B6968C6D65FFB61B84FAD3906127C33EC7EACBB0B8B20B389767E6A0F	CFCA Global RSA ROOT G2
CN = CFCA OV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	31f12de8b7576955bb85734014b6214a21c2fbdd	EB6C466E647A5EB633A38290FD30131DD7B887B51E1340ABB502C7AB31688F04	CFCA Global RSA ROOT G2

CN = CFCA EV RSA OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha256RSA	4096 bits	b1bcbe24db2d0a94810afa5001290dcafc2f443b	4D452B952FDCDE663C10400AED613C96BED8C4BF1A8F750D8A74D5C4183B1920	CFCA Global RSA ROOT G2
CN = CFCA Global ECC ROOT G2 O = China Financial Certification Authority C = CN	Root Key	sha384ECDSA	384 bits	cc4708eaa3d4f57626500f8786321dc992d610bd	23E4F8DA7D482CD105289433C2E10CE67C1E1092B4DC50101F6D0C346E965972	CFCA Global ECC ROOT G2
CN = CFCA DV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	c8cdaa65512277cf837ae5586899be2a0ac73069	ADBB46AF1FE1426F69BBCD0CDBD671650313A5C63993708CC4B465F14BD4E01B	CFCA Global ECC ROOT G2
CN = CFCA OV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	064e6c68b695d1454d4965838f60805657da05d6	6F6478FBFF45CC30AC0FE4EC3CC4EF3CAF0E959508B00342C229DD60C9A432A1	CFCA Global ECC ROOT G2
CN = CFCA EV ECC OCA G2 O = China Financial Certification Authority C = CN	Signing Key	sha384ECDSA	384 bits	b7202c74b5b5a5fceb183f3de7bd4ed225c5a044	80C868B316313761E34D6122AD687D462E7016FC54FDCBBA8D70F149752891C3	CFCA Global ECC ROOT G2

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	4.5	August 2023
CFCA Certificate Policy and Certification Practice Statement for Global Trusted System	4.4	November 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