



CERTAINLY LLC

WEBTRUST FOR CERTIFICATION AUTHORITIES REPORT

JULY 1, 2023, TO JUNE 30, 2024

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1	INDEPENDENT ACCOUNTANT REPORT	1
SECTION 2	MANAGEMENT’S ASSERTION	7
APPENDIX A	CERTAINLY’S ROOT AND ISSUING CAS.....	10

SECTION I

INDEPENDENT ACCOUNTANT'S REPORT

REPORT OF THE INDEPENDENT ACCOUNTANT

To the Management of Certainly LLC ("Certainly"):

Scope

We have examined [Certainly management's assertion](#) that for its Certification Authority (CA) operations at its San Francisco, California, USA, Santa Clara, California, USA, and Reston, Virginia, USA, locations, for its root and subordinate CA certificates as listed in Appendix A, Certainly has:

- disclosed its business, key and certificate lifecycle management, and CA environmental control practices in its:
 - [Certificate Policy and Certification Practice Statement \(v1.5, v1.6, and v1.7\)](#).
- maintained effective controls to provide reasonable assurance that:
 - Certainly 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; and
 - subscriber information is properly authenticated (for the registration activities performed by Certainly).
- 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.

throughout the period July 1, 2023, to June 30, 2024, based on the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Certainly does not escrow its CA keys and does not provide subscriber key generation services, subscriber key management services, certificate rekeys, subscriber key storage and recovery services, integrated circuit card lifecycle management, certificate suspension, or subordinate CA and cross certificate lifecycle management services. Accordingly, our examination did not extend to controls that would address those criteria.

Certification Authority's Responsibilities

Certainly'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](#).

Practitioner's Responsibilities

Our responsibility is to express an opinion on Certainly management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and 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. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct Established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

The relative effectiveness and significance of specific controls at Certainly 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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, Certainly management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of Certainly's services other than its CA operations at its San Francisco, California, USA, Santa Clara, California, USA, and Reston, Virginia, USA, locations, nor the suitability of any of Certainly's services for any customer's intended purpose.

[Intentionally Blank]

Other Matters

Without modifying our opinion, we noted the following other matters during our examination:

Matter Topic		Matter Description
1	Serving Invalid or Incomplete CRLs	The service responsible for updating Certainly's R1 intermediate issuer CRL shards began to store them incorrectly on May 24th, 2024. E1 issuer CRLs continued to be updated, but were sometimes overwritten by the R1 CRLs. OCSP continued to function normally, and Certainly did not serve expired CRLs. However, E1 and R1 CRLs became intermixed, and Certainly sometimes served the wrong CRL (R1 when it should have been E1) and also served CRLs that, while valid, did not contain recent revocations. This state continued until the issue was discovered on May 29th, 2024. The CRLs were corrected approximately two hours after discovery, with the affected CRL shards manually updated. A change using our automation systems with the corrected configuration was rolled out shortly after.

During our assessment, Schellman performed testing of certificate issuance, on a sample basis, and noted that there were no certificate deficiencies identified in any of the samples tested. As a result, our opinion is not modified with respect to these matters.

While Certainly disclosed its reported issues in Bugzilla during the period July 1, 2023, to June 30, 2024, we have noted only those disclosures relevant to the CAs enumerated in Appendix A and applicable to the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Use of the WebTrust Seal

Certainly'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.

Schellman & Company, LLC

Schellman & Company, LLC
Tampa, Florida, United States
August 29, 2024

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

Certainly, LLC ("Certainly") operates the Certification Authority ("CA") services for its root and subordinate CA certificates as listed in Appendix A and provides the following CA services:

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

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

Certainly management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in Certainly management's opinion, in providing its CA services at its San Francisco, California, USA, Santa Clara, California, USA, and Reston, Virginia, USA, locations, Certainly has:

- disclosed its business, key and certificate lifecycle management, and CA environmental control practices in its:
 - [Certificate Policy and Certification Practice Statement \(v1.5, v1.6, and v1.7\).](#)
- maintained effective controls to provide reasonable assurance that:
 - Certainly 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; and
 - subscriber information is properly authenticated (for the registration activities performed by Certainly).
- 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.

throughout the period July 1, 2023, to June 30, 2024, based on 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 and Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems 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

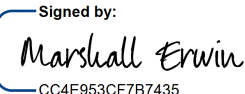
Certificate Lifecycle Management Controls

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

Certainly does not escrow its CA keys and does not provide subscriber key generation services, subscriber key management services, certificate renewals, certificate rekeys, subscriber key storage and recovery services, integrated circuit card lifecycle management, certificate suspension, or subordinate CA and cross certificate lifecycle management services. Accordingly, our assertion does not extend to controls that would address those criteria.

Certainly has disclosed the following matters publicly on Mozilla’s Bugzilla platform. These matters were included below due to being open during the period July 1, 2023, to June 30, 2024.

Bug ID	Summary	Opened	Closed	Resolution
1900129	Serving Invalid or Incomplete CRLs	05/31/2024	06/28/2024	Closed

Signed by:

CC4E953CF7B7435...
Marshall Erwin
Chief Information Security Officer
Fastly, Inc. (parent company of Certainly LLC)
August 29, 2024

APPENDIX A

CERTAINLY'S ROOT AND ISSUING CAs

CERTAINLY'S ROOT AND ISSUING CAs

Root CA	SubCA	SHA256 Fingerprint
Subject: C=US, O=Certainly, CN=Certainly Root R1		77B82CD8644C4305F7ACC5CB156B45675004033D51C60C6202A8E0C33467D3A0
	Subject: C=US, O=Certainly, CN=Certainly Intermediate R1	575C09B07A001CA0EF6B3B1C5730BFAFEBBC7AD9F56A009F1966C32F08E659713
Subject: C=US, O=Certainly, CN=Certainly Root E1		B4585F22E4AC756A4E8612A1361C5D9D031A93FD84FEBB778FA3068B0FC42DC2
	Subject: C=US, O=Certainly, CN=Certainly Intermediate E1	98DD2A75F65748F2667BC4B079177813647C17EDCC6DEE92F1F06668BE0F1A3D

The following certificates were signed by Starfield Technologies, Inc. for Certainly.

Root CA	SubCA	SHA256 Fingerprint
Subject: C=US. O=Starfield Technologies, Inc., CN=Starfield Root Certificate Authority - G2	Subject: C=US, O=Certainly, CN=Certainly Intermediate R1	FEC41E32CA75C295A6240FA639D3ABE3BFB5CB131D6690E2331A176BED2E5BD2
	Subject: C=US, O=Certainly, CN=Certainly Intermediate E1	3379233C434610C8EAA9361ACBDD24C7D655409C6D680A8C2585FFDA27011EE7
	Subject: C=US, O=Certainly, CN=Certainly Intermediate R1	1D233EDB537734EDDC55D9BDDD81A9AA4468B33040654D0342CD676C6B70EF33
	Subject: C=US, O=Certainly, CN=Certainly Intermediate E1	0B18D4C20C67A99E72DFBFCA5A2E256B8BBC9E082B0270378CC1A1F0CC461AB4