Building a better
working world

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 918 5987
ey.com

Report of Independent Accountants

To the Management of Apple:

We have examined the accompanying assertion made by the management of Apple Inc. (Apple), titled "Management's Assertion Regarding the Effectiveness of Its Controls Over the EV SSL Certification Authority Services Based on the WebTrust Principles and Criteria for Certification Authorities (CA) - Extended Validation (EV) SSL - Version 1.7.8" that provides its Certification Authority (CA) services, at Cupertino, California, and supporting facilities, at Prineville, Oregon; Maiden, North Carolina; Reno, Nevada; and Sunnyvale, California, USA locations for the Root CA(s) and Subordinate CA(s) referenced in **Appendix A** for the period of April 16, 2021 through April 15, 2022. Apple has:

- Disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
  - Apple Public CA Certification Practice Statement Version 5.6
- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.
  - The integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated

based on WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.7.8.

Apple's management is responsible for its assertion and for specifying the aforementioned Criteria. Our responsibility is to express an opinion on 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 (AICPA). 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.

Apple's management has disclosed to us the attached matters (see **Appendix B**) that have been posted publicly in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum. We have considered the nature of these comments in determining the nature, timing, and extent of our procedures.

The relative effectiveness and significance of specific controls at Apple 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.

Our examination was not conducted for the purpose of evaluating Apple's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of Apple and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, Apple may achieve reasonable, but not absolute assurance that all security events are prevented and, for those controls may provide reasonable, but not absolute assurance that its commitments and system requirements are achieved. 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.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations.

In our opinion, Apple's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria.

Apple's use of the WebTrust for Certification Authorities – Extended Validation 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.

This report does not include any representation as to the quality of Apple's CA services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.7.8 criteria, or the suitability of any of Apple's services for any customer's intended purpose.

Ernst + Young LLP

Ernst & Young LLP
6 July 2022

Appendix A – Apple Root and Subordinate CAs

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint

Apple Public EV Server RSA CA 1 - G1 (Sub-CA under DigiCert Global Root G2)
Subject:
CN= Apple Public EV Server RSA CA 1 - G1
O= Apple Inc.
C= US
	D3BDC13CA0CF35B934C5D4DBDA100E4CDE6AFE58	04F22ECC21FCB4382AC28B8F2D641FC0	340CA5BA402D140B65A2C976E7AE8128A1505C29D190E0E034F59CCAE7A92BC2

Apple Public EV Server ECC CA 1 - G1 (Sub-CA under DigiCert Global Root G3)
Subject:
CN= Apple Public EV Server ECC CA 1 - G1
O= Apple Inc.
C= US
	E085487D13A6D310199F5CCB6B782492F8AE1BAE	0CABAAD1CEC4E97CC2665881D02138F7	2585928D2C5BFD952E025BD12E27C6776224CF752EC362D3031CDD49351844D4

Apple Public EV Server RSA CA 2 - G1 (Sub-CA under DigiCert High Assurance EV Root CA)
Subject:
CN= Apple Public EV Server RSA CA 2 - G1
O= Apple Inc.
C= US
	5055AB43A1AFA9482B5AC1A2878904E47A0ECADA	07177911005D2267F68892F68F8B5058	D6EF3E09EBE0D9370E51F5C09A532B3AC70D3CE822253F9FC84C28E9BFA550D5

Apple Public EV Server RSA CA 3 - G1 (Sub-CA under DigiCert High Assurance EV Root CA)
Subject:
CN= Apple Public EV Server RSA CA 3 - G1
O= Apple Inc.
C= US
	77FC2F34695313CEC9AC5F9A3DA388D7866349BA	069AC439BB31C11AB2914025C3AE15D7	E881D3B83C3BC694D7D99F92DE83B2BFF5C6EE2D9871A446DEA107D6397565FC

Appendix B – Matters of Disclosure

	Observation	Relevant WebTrust Criteria	Publicly Disclosed Link
1	On August 3, 2021, Apple received a notification from root vendor DigiCert that 3 EV sub-CAs were not listed on the recently issued audit statement. The EV sub-CAs were appropriately included in the testing procedures of the external auditor. As such, following the review, an amended audit statement was issued that included the omitted EV sub-CAs. This incident was closed during the current examination period.	N/A	Bug 1724528 - Bugzilla Link
2	On September 9, 2021, Apple CA compliance identified certificates on Apple CA's test web page (https://www.apple.com/certificateauthority/public/) that had expired. It was determined that expiration notifications were sent but not received, and additional monitoring precautions were added to mitigate recurrence of this bug. The new certificates were issued, and the test web page was updated accordingly. This incident was closed during the current examination period.	N/A	Bug 1730291 - Bugzilla Link

Management's Assertion Regarding the Effectiveness of Its Controls
Over the EV SSL Certification Authority Services
Based on the WebTrust Principles and Criteria for Certification Authorities (CA) –
Extended Validation (EV) SSL - Version 1.7.8

6 July 2022

We, as management of Apple Inc. (Apple), operate the Certification Authority (CA) services for Apple's root and subordinate CA certificates listed in **Appendix A** and provide the following CA services:

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

Apple Management 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, 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.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to Apple's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Apple management has assessed the disclosure of its certificate practices and its controls over its CA services. Based on that assessment, in Apple management's opinion, in providing its CA services for the subordinate CA certificates listed in **Appendix A** at its Cupertino, California; Prineville, Oregon; Maiden, North Carolina; Reno, Nevada; and Sunnyvale, California, USA locations, throughout the period April 16, 2021 to April 15, 2022, Apple has:

- Disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
  - Apple Public CA Certification Practice Statement Version 5.6

- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals; and

- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity; and
- The integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
- EV SSL subscriber information is properly authenticated.

based on WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.7.8.

Apple Inc.

Appendix A – Apple Root and Subordinate CAs

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint

Apple Public EV Server RSA CA 1 - G1
(Sub-CA under DigiCert Global Root G2)
 	
Subject:
CN= Apple Public EV Server RSA CA 1 - G1
O= Apple Inc.
C= US
	D3BDC13CA0CF35B934C5D4DBDA100E4CDE6AFE58	04F22ECC21FCB4382AC28B8F2D641FC0	340CA5BA402D140B65A2C976E7AE8128A1505C29D190E0E034F59CCAE7A92BC2

Apple Public EV Server ECC CA 1 - G1
(Sub-CA under DigiCert Global Root G3)
 	
Subject:
CN= Apple Public EV Server ECC CA 1 - G1
O= Apple Inc.
C= US
	E085487D13A6D310199F5CCB6B782492F8AE1BAE	0CABAAD1CEC4E97CC2665881D02138F7	2585928D2C5BFD952E025BD12E27C6776224CF752EC362D3031CDD49351844D4

Apple Public EV Server RSA CA 2 - G1
(Sub-CA under DigiCert High Assurance EV Root CA)
 	
Subject:
CN= Apple Public EV Server RSA CA 2 - G1
O= Apple Inc.
C= US
	5055AB43A1AFA9482B5AC1A2878904E47A0ECADA	07177911005D2267F68892F68F8B5058	D6EF3E09EBE0D9370E51F5C09A532B3AC70D3CE822253F9FC84C28E9BFA550D5

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint

Apple Public EV Server RSA CA 3 - G1(Sub-CA under DigiCert High Assurance EV Root CA)
Subject:
CN= Apple Public EV Server RSA CA 3 - G1
O= Apple Inc.
C= US
	77FC2F34695313CEC9AC5F9A3DA388D7866349BA	069AC439BB31C11AB2914025C3AE15D7	E881D3B83C3BC694D7D99F92DE83B2BFF5C6EE2D9871A446DEA107D6397565FC