

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 1.6.8”, that provides its Certification Authority (CA) services at Cupertino, California, throughout the period April 29, 2020 to July 28, 2020 for the Subordinate CAs under external Root CAs enumerated in **Appendix A**.

Apple has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in its:
 - Apple Public EV Server RSA CA2 - G1 (Sub-CA under DigiCert High Assurance EV Root CA) [Apple Public CA CPS v5.0](#)
 - Apple Public EV Server RSA CA 1 - G1 (Sub-CA under DigiCert Global Root G2) [Apple Public CA CPS v5.0](#)
 - Apple Public EV Server ECC CA 1- G1 (Sub-CA under DigiCert Global Root G3) [Apple Public CA CPS v5.0](#)
- maintained effective controls to provide reasonable assurance that:
 - 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 \(CA\) - Extended Validation SSL - Version 1.6.8](#).

Apple 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.

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.

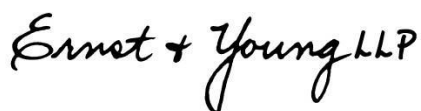
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, Apple may achieve reasonable, but not absolute assurance that all security events 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 \(CA\) - Extended Validation SSL - Version 1.6.8](#) criteria, or the suitability of any of Apple's services for any customer's intended purpose.



Ernst & Young LLP
17 August 2020

Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public EV Server RSA CA 2 - G1 (Sub-CA under DigiCert High Assurance EV Root CA) CN= Apple Public EV Server RSA CA 2 - G1 O= Apple Inc. C= US	5055AB43A1AFA9482 B5AC1A2878904E47A 0ECADA	07177911005D2267F6 8892F68F8B5058	D6EF3E09EBE0D9370E 51F5C09A532B3AC70 D3CE822253F9FC84C2 8E9BFA550D5
Apple Public EV Server RSA CA 1 - G1 (Sub-CA under DigiCert Global Root G2) CN= Apple Public EV Server RSA CA 1 - G1 O= Apple Inc. C= US	D3BDC13CA0CF35B93 4C5D4DBDA100E4CDE 6AFE58	04F22ECC21FCB4382A C28B8F2D641FC0	340CA5BA402D140B6 5A2C976E7AE8128A1 505C29D190E0E034F5 9CCAE7A92BC2
Apple Public EV Server ECC CA 1 - G1 (Sub-CA under DigiCert Global Root G3) CN= Apple Public EV Server ECC CA 1 - G1 O= Apple Inc. C= US	E085487D13A6D3101 99F5CCB6B782492F8A E1BAE	0CABAAD1CEC4E97CC 2665881D02138F7	2585928D2C5BFD952E 025BD12E27C6776224 CF752EC362D3031CD D49351844D4



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 1.6.8

August 17, 2020

Apple Inc. (Apple) operates the Certification Authority ("CA") services for the Subordinate CA(s) under external Root CAs as listed in Appendix A. and provides Extended Validation SSL ("EV SSL") Certification Authority ("CA") services.

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 its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in management's opinion, in providing its EV SSL CA services in Cupertino, California, throughout the period April 29, 2020 to July 28, 2020, Apple has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:

Apple Public EV Server RSA CA 2 – G1
(Sub-CA under DigiCert High Assurance
EV Root CA)

[Apple Public CA CPS v5.0](#)

Apple Public EV Server RSA CA 1 – G1
(Sub-CA under DigiCert Global Root G2)

[Apple Public CA CPS v5.0](#)

Apple Public EV Server ECC CA 1- G1
(Sub-CA under DigiCert Global Root G3)

[Apple Public CA CPS v5.0](#)

- Maintained effective controls to provide reasonable assurance that:
 - 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 \(CA\) – Extended Validation SSL – Version 1.6.8.](#)

Apple Inc.



Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public EV Server RSA CA 2 - G1 (Sub-CA under DigiCert High Assurance EV Root CA) CN= Apple Public EV Server RSA CA 2 - G1 O= Apple Inc. C= US	5055AB43A1AFA9482B 5AC1A2878904E47A0E CADA	07177911005D2267F68 892F68F8B5058	D6EF3E09EBE0D9370E 51F5C09A532B3AC70 D3CE822253F9FC84C 28E9BFA550D5
Apple Public EV Server RSA CA 1 - G1 (Sub-CA under DigiCert Global Root G2) CN= Apple Public EV Server RSA CA 1 - G1 O= Apple Inc. C= US	D3BDC13CA0CF35B93 4C5D4DBDA100E4CDE 6AFE58	04F22ECC21FCB4382A C28B8F2D641FC0	340CA5BA402D140B6 5A2C976E7AE8128A15 05C29D190E0E034F59 CCAE7A92BC2
Apple Public EV Server ECC CA 1 - G1 (Sub-CA under DigiCert Global Root G3) CN= Apple Public EV Server ECC CA 1 - G1 O= Apple Inc. C= US	E085487D13A6D31019 9F5CCB6B782492F8A E1BAE	0CABAAD1CEC4E97CC 2665881D02138F7	2585928D2C5BFD952 E025BD12E27C677622 4CF752EC362D3031C DD49351844D4