

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 SSL Certification Authority Services Based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2”, that provides its Certification Authority (CA) services at Cupertino, California, throughout the period April 16, 2017 to April 15, 2018 for the Subordinate CAs under external Root CAs enumerated in **Appendix A**. Apple has:

- disclosed its SSL certificate lifecycle management business practices in its:

Apple IST CA 2 – G1 [Certification Practice Statement](#)

Apple IST CA 4 – G1 [Certification Practice Statement](#)

Apple IST CA 8 – G1 [Certification Practice Statement](#)

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Apple 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 subscriber information is properly authenticated (for the registration activities performed by Apple)
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2](#).

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.

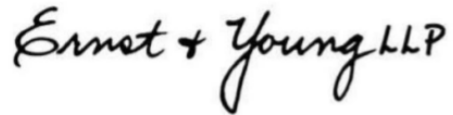
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, Apple may achieve reasonable, but not absolute assurance that all security events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

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 – SSL Baseline with Network Security v2.2](#) criteria, or the suitability of any of Apple's services for any customer's intended purpose.



Ernst & Young LLP
25 June 2018



**Management's Assertion Regarding the Effectiveness of Its Controls
Over the SSL Certification Authority Services**

Based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2

June 25, 2018

We, as management of Apple Inc. (Apple), are responsible for operating the SSL Certification Authority (CA) services at Cupertino, California for the Subordinate CAs under external Root CAs in scope for SSL Baseline Requirements and Network Security Requirements listed in **Appendix A**.

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 SSL CA services. Based on that assessment, in providing its SSL CA services at Cupertino, California, throughout the period April 16, 2017 to April 15, 2018, Apple has:

- disclosed its SSL certificate lifecycle management business practices in its:

Apple IST CA 2 – G1	Certification Practice Statement
---------------------	--

Apple IST CA 4 – G1	Certification Practice Statement
---------------------	--

Apple IST CA 8 – G1	Certification Practice Statement
---------------------	--

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Apple 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 was established and protected throughout their lifecycles; and
 - SSL subscriber information was properly authenticated (for the registration activities performed by Apple)
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data was restricted to authorized individuals;

Apple
One Apple Park Way
Cupertino, CA 95014
T 408 996-1010
F 408 996-0275
www.apple.com



- the continuity of key and certificate management operations was 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

for the Subordinate CAs under external Root CAs in scope for SSL Baseline Requirements and Network Security Requirements listed in **Appendix A**, based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2](#).

Apple Inc.

Appendix A

Subordinate CA Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple IST CA 2 – G1	D8:7A:94:44:7C:90:70:90: 16:9E:DD:17:9C:01:44:03:8 6:D6:2A:29	00:02:3A:74	AC:2B:92:2E:CF:D5:E0:17: 11:77:2F:EA:8E:D3:72:DE:9 D:1E:22:45:FC:E3:F5:7A:9 C:DB:EC:77:29:6A:42:4B
Apple IST CA 4 – G1	A2:73:E7:5C:3E:D3:3F:CD: 76:88:70:35:68:83:41:A5:A 8:E9:00:AF	35:61:F6:38:AB:C1:95:CB:B F:7C:FD:A7:03:DA:DE:C9	61:15:F0:6A:33:8A:64:9E: 61:58:52:10:E7:6F:2E:CE:3 9:89:BC:A6:5A:62:B0:66: 04:0C:D7:C5:F4:08:ED:D0
Apple IST CA 8 – G1	C3:C4:A4:58:05:63:D7:83: 06:BA:96:8D:DC:B2:8F:32: F6:BB:B7:41	13:52:2E:BF:C1:DD:5C:E1:1E :F2:76:40:75:1F:E7:DF	A4:FE:7C:7F:15:15:5F:3F:0 A:EF:7A:AA:83:CF:6E:06:D E:B9:7C:A3:F9:09:DF:92:0 A:C1:49:08:82:D4:88:ED