

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 Certification Authority Operations Based on the Trust Services Principles and Criteria for Certification Authorities Version 2.0” that provides its Certification Authority (CA) services from Cupertino, California for the Subordinate CA(s) under external Root CAs referenced in **Appendix A** during the period from April 16, 2017 through April 15, 2018. Apple has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statements:
 - Apple IST CA 2 – G1 [Certification Practice Statement](#)
 - Apple IST CA 3 – G1 [Certification Practice Statement](#)
 - Apple IST CA 4 – G1 [Certification Practice Statement](#)
 - Apple IST CA 5 – G1 [Certification Practice Statement](#)
 - Apple IST CA 6 – G1 [Certification Practice Statement](#)
 - Apple IST CA 7 – G1 [Certification Practice Statement](#)
 - Apple IST CA 8 – G1 [Certification Practice Statement](#)
- maintained effective controls to provide reasonable assurance that:
 - Apple provides its services in accordance with its Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - 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

based on the American Institute of Certified Public Accountants (AICPA)'s [Trust Services Principles and Criteria for Certification Authorities 2.0](#).

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 AICPA. Those standards require that we plan and perform our 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, which includes: (1) obtaining an understanding of Apple's key and certificate life cycle management business practices, policies, processes and controls, and its suitability of the design and implementation of the controls intended to achieve the Criteria and examining evidence supporting management's assertion and performing such other procedures over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over the development, maintenance and operation of systems integrity as we considered necessary in the circumstances; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle 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. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, 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.

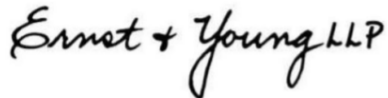
Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the 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.

The WebTrust seal of assurance for Certification Authority on Apple's website 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 [Trust Services Principles and Criteria for Certification Authorities 2.0](#) 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 Certification Authority Operations
Based on the Trust Services Principles and Criteria for Certification Authorities Version 2.0**

June 25, 2018

We, as management of Apple Inc. (Apple), are responsible for operating a Certification Authority (CA) at Cupertino, California for the Subordinate CAs under external Root CAs as listed in **Appendix A**.

Apple's CA services provide the following certification authority services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- 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 operations. Based on that assessment, in Apple Management's opinion, in providing its CA services for the Subordinate CAs under external Root CAs listed in **Appendix A** at Cupertino, California during the period from April 16, 2017 through April 15, 2018, Apple has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices as below:

Apple IST CA 2 – G1

[Certification Practice Statement](#)

Apple IST CA 3 – G1

[Certification Practice Statement](#)



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

Apple IST CA 5 – G1 [Certification Practice Statement](#)

Apple IST CA 6 – G1 [Certification Practice Statement](#)

Apple IST CA 7 – G1 [Certification Practice Statement](#)

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

- maintained effective controls to provide reasonable assurance that:
 - Apple's Certification Practice Statements are consistent with its Certificate Policy
 - Apple provides its services in accordance with its Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
 - the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
 - the subscriber information was properly authenticated (for the registration activities performed by Apple); and
 - subordinate CA certificate requests were accurate, authenticated and approved
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data was restricted to authorized individuals;
 - the continuity of key and certificate management operations was maintained; and
 - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the Subordinate CAs under external Root CAs listed in **Appendix A**, based on the [Trust Services Principles and Criteria for Certification Authorities Version 2.0](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management



- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System 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

Subscriber Key Lifecycle Management Controls

- CA provided Subscriber Key Generation Services
- CA provided Subscriber Key Storage and Recovery Services
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Apple Inc.

Appendix A

Subordinate 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:01:44:03:86:D6:2A:29	00:02:3A:74	AC:2B:92:2E:CF:D5:E0:17:11:77:2F:EA:8E:D3:72:DE:9D:1E:22:45:FC:E3:F5:7A:9C:DB:EC:77:29:6A:42:4B
Apple IST CA 3 – G1	52:4A:19:93:88:0F:4F:94:AD:4D:2C:58:A7:12:18:CB:6C:08:F2:83	52:84:2A:19:A5:C7:7B:A4:E7:E5:FF:F8:31:93:3D:6D	6D:E9:09:78:91:04:22:A8:9E:26:F2:DF:85:97:14:30:C3:F4:4C:D1:78:5D:AD:94:30:8F:7C:A4:B6:FB:E5:21
Apple IST CA 4 – G1	A2:73:E7:5C:3E:D3:3F:C D:76:88:70:35:68:83:41:A5:A8:E9:00:AF	35:61:F6:38:AB:C1:95:CB:BF:7C:FD:A7:03:DA:DE:C9	61:15:F0:6A:33:8A:64:9E:61:58:52:10:E7:6F:2E:CE:39:89:BC:A6:5A:62:B0:66:04:0C:D7:C5:F4:08:ED:D0
Apple IST CA 5 – G1	56:33:90:2F:9:F4:D2:30:D0:0D:62:25:13:78:1D:21:A7:51:12:0F	00:02:3A:75	3D:B7:6D:1D:D7:D3:A7:59:DC:CC:3F:8F:A7:F6:86:75:C0:80:CB:09:5E:48:81:06:3A:6B:85:0F:DD:68:B8:BC
Apple IST CA 6 – G1	F3:3E:A5:5C:2C:63:2A:1F:F8:B4:D5:FE:A4:15:66:D2:B9:E7:35	06:5D:CA:7D:0F:AA:22:98:C3:0A:B0:61:29:40:DE:7D	90:4F:B5:A4:37:75:4B:1B:32:B8:0E:BA:E7:41:6D:B6:3D:05:F5:6A:99:39:72:0B:7C:8E:3D:CC:54:F6:A3:D1
Apple IST CA 7 – G1	59:95:70:92:60:4C:D5:B7:8F:91:BD:7F:CC:CA:7E:2A:B4:1F:C1:B1	0F:82:2B:46:D4:3A:07:25:B4:F4:89:BF:E8:3D:62:DD	17:F9:66:09:AC:6A:D0:A2:D6:AB:0A:21:B2:D1:B5:B2:94:6B:D0:4D:BF:12:07:03:D1:DE:F6:FB:62:F4:B6:61
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:0A:EF:7A:AA:83:CF:6E:06:DE:B9:7C:A3:F9:09:DF:92:0A:C1:49:08:82:D4:88:ED