

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 WebTrust Principles and Criteria for Certification Authorities Version 2.2.2” 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 Subordinate CA(s) referenced in **Appendix A** for the period of April 16, 2021 through April 15, 2022. Apple has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [Apple Public CA Certification Practice Statement Version 5.6](#)
- Maintained effective controls to provide reasonable assurance that:
 - Apple’s Certification Practice Statement is consistent with the relevant governing Certificate Policies; and
 - Apple provides its services in accordance with its Certification Practice Statement.
- Maintained effective controls to provide reasonable assurance that:
 - The integrity of keys and certificates it manages was established and protected throughout their lifecycles; and
 - The integrity of subscriber keys and certificates it manages was established and protected throughout their lifecycles; and
 - Subscriber information was properly authenticated; 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 is restricted to authorized individuals; and
 - 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 Chartered Professional Accountants of Canada (“CPA Canada”)’s [WebTrust Principles and Criteria for Certification Authorities Version 2.2.2](#).

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.

Apple does not escrow its CA keys, does not provide subscriber key generation services for TLS certificates, subscriber key management services for TLS certificates, subscriber key storage and recovery services for TLS certificates, integrated circuit card lifecycle management, certificate suspension, certificate renewal and certificate rekey services. Accordingly, our examination did not extend to controls that would address those criteria.

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.

Apple management has disclosed to us the attached matters (**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.

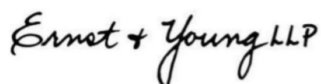
Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the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

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 [WebTrust Principles and Criteria for Certification Authorities Version 2.2.2](#) criteria, or the suitability of any of Apple's services for any customer's intended purpose.



Ernst & Young LLP
6 July 2022

Appendix A – Apple Subordinate CAs

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple IST CA 2 - G1 (Sub-CA under GeoTrust Global Root CA) Subject: CN= Apple IST CA 2 - G1 OU= Certification Authority O= Apple Inc. C= US	D87A94447C907090169EDD179C01440386D62A29	146036	AC2B922ECFD5E01711772FEA8ED372DE9D1E2245FCE3F57A9CDBEC77296A424B
Apple IST CA 8 - G1 (Sub-CA under GeoTrust Primary CA G2) Subject: CN= Apple IST CA 8 - G1 OU= Certification Authority O= Apple Inc. C= US	C3C4A4580563D78306BA968DDCB28F32F6BB741	13522EBFC1DD5CE11EF27640751FE7DF	A4FE7C7F15155F3F0AEF7AAA83CF6E06DEB97CA3F909DF920AC1490882D488ED
Apple IST CA 2 - G1 (Sub-CA under Baltimore CyberTrust Root) Subject: CN= Apple IST CA 2 - G1 OU= Certification Authority O= Apple Inc. C= US	D87A94447C907090169EDD179C01440386D62A29	0552C7EFFEEC292BA9F1387B07AF929F	C9B06CC083186220618E61A8772640F824DF69D561AD56BDC15AD56D0CE08608
Apple IST CA 8 - G1 (Sub-CA under Baltimore CyberTrust Root) Subject: CN= Apple IST CA 8 - G1 OU= Certification Authority	C3C4A4580563D78306BA968DDCB28F32F6BB741	0A48D57C65FB0E6CF704A3645F1418E4	5C29DBEA9B7CC8B02418F28C1C8736DFDF170665D098EF681D903BE76987D249

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
O= Apple Inc. C= US			
Apple Public Server RSA CA 2 - G1 (Sub-CA under Baltimore CyberTrust Root) Subject: CN= Apple Public Server RSA CA 2 - G1 O= Apple Inc. C= US	9061F3A3D706CEF517B6570ED98CA7954B163289	0B799AEF7B9DED2B418B8D3EAA3A8F7C	F518F0BB716521F0A26FDB40C304FF9B82FBDBE7ACBD46BF0EF23A180188EB5C
Apple Public Server ECC CA 2 - G1 (Sub-CA under Baltimore CyberTrust Root) Subject: CN= Apple Public Server ECC CA 2 - G1 O= Apple Inc. C= US	B5646FBC179FC95065D8F53F84E995097A7C5F66	05AECAD3A2D246D587EC9391711D1114	DA8546816D891C1241E9387DE436D1B9F7EA70DBA1EB3D25F58271CE816A7ABC
Apple Public Client RSA CA 2 - G1 (Sub-CA under Baltimore CyberTrust Root) Subject: CN= Apple Public Client RSA CA 2 - G1 O= Apple Inc. C= US	019C7649C5EE1A77A48A53A0CC03AA27BE2C48C7	0D4E55BBBADFA78C14398D94ABED2FBC	32B4B3768CA5A4D80E9DF8D557B7424F80AF5560B1148D05548DC3D76A7ED619
Apple Public Server RSA CA 1 - G1 (Sub-CA under Digicert Global Root G2) Subject: CN= Apple Public EV Server RSA CA1 - G1 O= Apple Inc. S= California C=US	A37C9BEA4C0FC1B014CFA4791900D43C6F4DA095	0FD2A106FC12F606DBE5127FBE166812	392583543B93B10E0506DE75D69399FCBBC1469C8DE396066C756088B92241DA

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public Client RSA CA 1 - G1 (Sub-CA under DigiCert Global Root G2) Subject: CN= Apple Public Client RSA CA 1 - G1 O= Apple Inc. C= US	E8DD7EF8EAE8CA01FB7C85B69166CA024042F671	0B8A5B9DD501A88775399B9A048811A3	BE13A5D2F5C78F440119D484C710427325EB10CEA9623EF6200CB11B04F650E1
Apple Public EV Server RSA CA 1 - G1 (Sub-CA under DigiCert Global Root G2) Subject: CN= Apple Public EV Server RSA CA1 - G1 O= Apple Inc. C=US	D3BDC13CA0CF35B934C5D4DBDA100E4CDE6AFE58	04F22ECC21FCB4382AC28B8F2D641FC0	340CA5BA402D140B65A2C976E7AE8128A1505C29D190E0E034F59CCAE7A92BC2
Apple Public Server ECC CA 1 - G1 (Sub-CA under DigiCert Global Root G3) Subject: CN= Apple Public Server ECC CA 1 - G1 O= Apple Inc. C= US	6C9782459ECC6F1647F6B813F3735322FA791126	06B4543FF33BB19827C187A0213EC11A	2AF988F26F6EF0DAB9055697F0941FB4E5C42247CA982826895EF29985D30CD6
Apple IST CA 8 - G1 (Sub-CA under DigiCert Global Root G3) Subject: CN= Apple IST CA 8 - G1 O= Apple Inc. C= US	C3C4A4580563D78306BA968DDCB28F32F6BB741	05AE84C4406C98F01BDD0F0E6020FE9A	8711EE539E74213F5F412EB4A18A98C3B58DA620B4D43E75B0542AFC39FC6033
Apple IST CA 8 - G1 (Sub-CA under DigiCert Global Root G3) Subject:	C3C4A4580563D78306BA968DDCB28F32F6BB741	0C67620777A5ABC4BA535D8DADCF9AD7	9218BAB94E7D5D1F81D62D0FC23E31C8BBCBEE3545D1D7E9D3FD29B30BC188C8

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
CN= Apple IST CA 8 - G1 OU= Certification Authority O= Apple Inc. C= US			
Apple Public EV Server ECC CA1 G1 (Sub-CA under Digicert Global Root G3) Subject: CN= Apple Public EV Server ECC CA1 - G1 O= Apple Inc. C=US	E085487D13A6D310199F5CCB6B782492F8AE1BAE	0CABAAD1CEC4E97CC2665881D02138F7	2585928D2C5BFD952E025BD12E27C6776224CF752EC362D3031CD D49351844D4
Apple Public EV Server RSA CA 2 - G1 (Sub-CA under Digicert High Assurance EV Root) Subject: CN= Apple Public EV Server RSA CA2 - 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) Subject: CN= Apple Public EV Server RSA CA3 - G1 O= Apple Inc. C=US	77FC2F34695313CEC9AC5F9A3DA388D7866349BA	069AC439BB31C11AB2914025C3AE15D7	E881D3B83C3BC694D7D99F92DE83B2BFF5C6EE2D9871A446DEA107D6397565FC
Apple Public Server RSA CA 12 - G1 (Sub-CA under AAA Certificate Services Root) Subject: CN= Apple Public Server RSA CA 12 - G1	1E5C1791055702FC775CE37043EC6BFDDDD2D869	0AE48F23013064419259E1C29AE98D18	0B405CFE9A6BEB098FB969121C5F6710F3F7FA9EA101A6418F7AF201D3D3938

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
O= Apple Inc. S= California C=US			
Apple Public Client RSA CA 12 - G1 (Sub-CA under AAA Certificate Services Root) Subject: CN= Apple Public Client RSA CA 12 - G1 O= Apple Inc. S= California C=US	CA06F092123D7B005 AE92847A8251BF0D0 8042CC	00CB79513FDF5A41B7 EBA3B5012C665762	EB62BFFA6CBC802E4D AE6F8C53908020BE7F 07774A55E67BBD63E CC37679DEC8
Apple Public Server ECC CA 12 - G1 (Sub-CA under AAA Certificate Services Root) Subject: CN= Apple Public Server ECC CA 12 - G1 O= Apple Inc. S= California C=US	5FE32E8A9497DED35C E1B7D4BC988E3129C9 903A	726618753AD6C922C 56C9DE1F38478B0	70DB9DED944DD35D4 74EA15FF2AA4E25F39 3A893ECDA54359D30 5BC319649817
Apple Public Server RSA CA 11 - G1 (Sub-CA under USERTrust RSA Certification Authority) Subject: CN= Apple Public Server RSA CA 11 - G1 O= Apple Inc. S= California C=US	5002B8132C1583D14 1C3118A8B423B0123 43A956	5DFABB9577CFAB671F C7DDFED1CF205B	6C66578DC96AD13EB 7B688BDC09DB472D5 FBF03B3BD213096650 52A886D7E9B4
Apple Public Client RSA CA 11 - G1 (Sub-CA under USERTrust RSA Certification Authority) Subject:	5FF6968F8EB5881D73 DC207B7831DC5FB6B 73D18	4E418394B240A7CCA 8E76AAE9D849793	301E8CBB8C665CAB2 56EB196F73F4D296C9 CAD25F32744904279E 1B318233E3B

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
CN= Apple Public Client RSA CA 11 - G1 O= Apple Inc. S= California C=US			
Apple Public Server ECC CA 11 - G1 (Sub-CA under COMODO ECC Certification Authority) Subject: CN= Apple Public Server ECC CA 11 - G1 O= Apple Inc. S= California C=US	85B594D87182CECE56 80B3AF3598AB764B6 DAC29	0098C17276AA83690 8DCDC5B4EF8BD4174	C451BEFBA87014ECD5 7851D1E682403E3CA 60963773AE7FAA00FF D6FFAC8B2A3

Appendix B - Matters of Disclosure

	Observation	Relevant WebTrust Criteria	Publicly Disclosed Link
1	<p>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.</p> <p>This incident was closed during the current examination period.</p>	N/A	Bug 1724528 - Bugzilla Link
2	<p>On September 9, 2021, Apple CA compliance identified that demo certificates on the Apple Public CA Repository (https://www.apple.com/certificateauthority/public/) 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. New demo certificates were issued and the Apple Public CA Repository was updated accordingly.</p> <p>This incident was closed during the current examination period.</p>	N/A	Bug 1730291 - Bugzilla Link
3	<p>On January 14, 2022 Apple's operations team changed the OCSP publisher configuration for S/MIME certificates and the affected TLS certificate profile to only publish when a certificate is revoked. The resulting behavior of that change is that the OCSP responder began responding as 'unknown' for issued non-revoked non-expired certificates instead of 'good'.</p> <p>Revoked certificates were not impacted by this issue and would display the "revoked" status for relying parties.</p>	<p>Criterion number 6.6. The CA maintains controls to provide reasonable assurance that certificates are revoked, based on authorized and validated certificate revocation requests within the time frame in accordance with the CA's disclosed business practices.</p> <p>Criterion number 6.8 The CA maintains controls to provide reasonable assurance that timely, complete and accurate certificate status information (including Certificate Revocation Lists and other certificate status mechanisms)</p>	Bug 1771398 - Bugzilla Link

	Observation	Relevant WebTrust Criteria	Publicly Disclosed Link
		is made available to relevant entities (Subscribers and Relying Parties or their agents) in accordance with the CA's disclosed business practices.	



Management's Assertion Regarding the Effectiveness of Its Controls
Over the Certification Authority Operations
Based on the WebTrust Principles and Criteria for Certification Authorities Version 2.2.2

6 July 2022

We, as management of Apple Inc. (Apple), operate the Certification Authority (CA) services for 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, and 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 business, key life cycle management, certificate life cycle management, and CA environmental control practices as specified in its:
 - [Apple Public CA Certification Practice Statement Version 5.6](#)

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



- Maintained effective controls to provide reasonable assurance that:
 - Apple's Certification Practice Statement is consistent with the relevant governing Certificate Policies; and
 - Apple provides its services in accordance with its Certification Practice Statement.
- Maintained effective controls to provide reasonable assurance that:
 - The integrity of keys and certificates it manages was established and protected throughout their life cycles; and
 - The integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles; and
 - The Subscriber information was properly authenticated; 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; and
 - 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 [WebTrust Principles and Criteria for Certification Authorities Version 2.2.2](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

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



- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and 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 Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management



Apple Inc.

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



Appendix A – Apple Subordinate CAs

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple IST CA 2 – G1 (Sub-CA under GeoTrust Global Root CA) Subject: CN= Apple IST CA 2 – G1 OU= Certification Authority O= Apple Inc. C= US	D87A94447C907090169 EDD179C01440386D62 A29	146036	AC2B922ECFD5E0171177 2FEA8ED372DE9D1E224 5FCE3F57A9CDBEC77296 A424B
Apple IST CA 8 - G1 (Sub-CA under GeoTrust Primary CA G2) Subject: CN= Apple IST CA 8 – G1 OU= Certification Authority O= Apple Inc. C= US	C3C4A4580563D78306B A968DDCB28F32F6BBB 741	13522EBFC1DD5CE11EF27 640751FE7DF	A4FE7C7F15155F3F0AEF 7AAA83CF6E06DEB97CA 3F909DF920AC1490882 D488ED
Apple IST CA 2 – G1 (Sub-CA under Baltimore CyberTrust Root) Subject: CN= Apple IST CA 2 – G1 OU= Certification Authority O= Apple Inc. C= US	D87A94447C907090169 EDD179C01440386D62 A29	0552C7EFFEEC292BA9F13 87B07AF929F	C9B06CC083186220618E 61A8772640F824DF69D5 61AD56BDC15AD56D0C E08608
Apple IST CA 8 – G1 (Sub-CA under Baltimore CyberTrust Root)	C3C4A4580563D78306B A968DDCB28F32F6BBB 741	0A48D57C65FB0E6CF704 A3645F1418E4	5C29DBEA9B7CC8B0241 8F28C1C8736DFDF17066

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



Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Subject: CN= Apple IST CA 8 – G1 OU= Certification Authority O= Apple Inc. C= US			5D098EF681D903BE7698 7D249
Apple Public Server RSA CA 2 – G1 (Sub-CA under Baltimore CyberTrust Root) Subject: CN= Apple Public Server RSA CA 2 – G1 O= Apple Inc. C= US	9061F3A3D706CEF517B 6570ED98CA7954B1632 89	0B799AEF7B9DED2B418B 8D3EAA3A8F7C	F518F0BB716521F0A26F DB40C304FF9B82FDBE7 ACBD46BF0EF23A180188 EB5C
Apple Public Server ECC CA 2 – G1 (Sub-CA under Baltimore CyberTrust Root) Subject: CN= Apple Public Server ECC CA 2 – G1 O= Apple Inc. C= US	B5646FBC179FC95065D 8F53F84E995097A7C5F 66	05AECAD3A2D246D587E C9391711D1114	DA8546816D891C1241E 9387DE436D1B9F7EA70 DBA1EB3D25F58271CE8 16A7ABC
Apple Public Client RSA CA 2 – G1 (Sub-CA under Baltimore CyberTrust Root) Subject:	019C7649C5EE1A77A48 A53A0CC03AA27BE2C4 8C7	0D4E55BBBADFA78C1439 8D94ABED2FBC	32B4B3768CA5A4D80E9 DF8D557B7424F80AF556 0B1148D05548DC3D76A 7ED619

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



Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
CN= Apple Public Client RSA CA 2 – G1 O= Apple Inc. C= US			
Apple Public Server RSA CA 1 - G1 (Sub-CA under Digicert Global Root G2) Subject: CN= Apple Public EV Server RSA CA1 - G1 O= Apple Inc. S= California C=US	A37C9BEA4C0FC1B014 CFA4791900D43C6F4D A095	0FD2A106FC12F606DBE5 127FBE166812	392583543B93B10E0506 DE75D69399FCBBC1469 C8DE396066C756088B92 241DA
Apple Public Client RSA CA 1 – G1 (Sub-CA under DigiCert Global Root G2) Subject: CN= Apple Public Client RSA CA 1 – G1 O= Apple Inc. C= US	E8DD7EF8EAE8CA01FB7 C85B69166CA024042F6 71	0B8A5B9DD501A8877539 9B9A048811A3	BE13A5D2F5C78F440119 D484C710427325EB10CE A9623EF6200CB11B04F6 50E1
Apple Public EV Server RSA CA 1 - G1 (Sub-CA under Digicert Global Root G2) Subject: CN= Apple Public EV Server RSA CA1 - G1 O= Apple Inc. C=US	D3BDC13CA0CF35B934 C5D4DBDA100E4CDE6A FE58	04F22ECC21FCB4382AC28 B8F2D641FC0	340CA5BA402D140B65A 2C976E7AE8128A1505C2 9D190E0E034F59CCAE7A 92BC2

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



Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public Server ECC CA 1 – G1 (Sub-CA under DigiCert Global Root G3) Subject: CN= Apple Public Server ECC CA 1 – G1 O= Apple Inc. C= US	6C9782459ECC6F1647F 6B813F3735322FA7911 26	06B4543FF33BB19827C18 7A0213EC11A	2AF988F26F6EF0DAB905 5697F0941FB4E5C42247 CA982826895EF29985D3 0CD6
Apple IST CA 8 – G1 (Sub-CA under DigiCert Global Root G3) Subject: CN= Apple IST CA 8 – G1 O= Apple Inc. C= US	C3C4A4580563D78306B A968DDCB28F32F6BBB 741	05AE84C4406C98F01BDD 0F0E6020FE9A	8711EE539E74213F5F412 EB4A18A98C3B58DA620 B4D43E75B0542AFC39FC 6033
Apple IST CA 8 – G1 (Sub-CA under DigiCert Global Root G3) Subject: CN= Apple IST CA 8 – G1 OU= Certification Authority O= Apple Inc. C= US	C3C4A4580563D78306B A968DDCB28F32F6BBB 741	0C67620777A5ABC4BA53 5D8DADCF9AD7	9218BAB94E7D5D1F81D 62D0FC23E31C8BBCBEE3 545D1D7E9D3FD29B30B C188C8
Apple Public EV Server ECC CA1 G1 (Sub-CA under Digicert Global Root G3) Subject:	E085487D13A6D310199 F5CCB6B782492F8AE1B AE	0CABAAD1CEC4E97CC266 5881D02138F7	2585928D2C5BFD952E02 5BD12E27C6776224CF75 2EC362D3031CDD49351 844D4

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



Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
CN= Apple Public EV Server ECC CA1 - G1 O= Apple Inc. C=US			
Apple Public EV Server RSA CA 2 - G1 (Sub-CA under Digicert High Assurance EV Root) Subject: CN= Apple Public EV Server RSA CA2 - G1 O= Apple Inc. C=US	5055AB43A1AFA9482B5 AC1A2878904E47A0EC ADA	07177911005D2267F6889 2F68F8B5058	D6EF3E09EBE0D9370E51 F5C09A532B3AC70D3CE 822253F9FC84C28E9BFA 550D5
Apple Public EV Server RSA CA 3 - G1 (Sub-CA under Digicert High Assurance EV Root) Subject: CN= Apple Public EV Server RSA CA3 - G1 O= Apple Inc. C=US	77FC2F34695313CEC9A C5F9A3DA388D786634 9BA	069AC439BB31C11AB291 4025C3AE15D7	E881D3B83C3BC694D7D 99F92DE83B2BFF5C6EE2 D9871A446DEA107D639 7565FC
Apple Public Server RSA CA 12 – G1 (Sub-CA under AAA Certificate Services Root) Subject: CN= Apple Public Server RSA CA 12 - G1 O= Apple Inc. S= California	1E5C1791055702FC775 CE37043EC6BFDDDD2D 869	0AE48F23013064419259E 1C29AE98D18	0B405CFE9A6BEB098FFB 969121C5F6710F3F7FA9 EA101A6418F7AF201D3 D3938

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



Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
C=US			
Apple Public Client RSA CA 12 – G1 (Sub-CA under AAA Certificate Services Root) Subject: CN= Apple Public Client RSA CA 12 - G1 O= Apple Inc. S= California C=US	CA06F092123D7B005AE 92847A8251BF0D08042 CC	00CB79513FDF5A41B7EB A3B5012C665762	EB62BFFA6CBC802E4DA E6F8C53908020BE7F077 74A55E67BBD63ECC376 79DEC8
Apple Public Server ECC CA 12 – G1 (Sub-CA under AAA Certificate Services Root) Subject: CN= Apple Public Server ECC CA 12 - G1 O= Apple Inc. S= California C=US	5FE32E8A9497DED35CE 1B7D4BC988E3129C990 3A	726618753AD6C922C56C 9DE1F38478B0	70DB9DED944DD35D47 4EA15FF2AA4E25F393A8 93ECDA54359D305BC31 9649817
Apple Public Server RSA CA 11 – G1 (Sub-CA under USERTrust RSA Certification Authority) Subject: CN= Apple Public Server RSA CA 11 - G1 O= Apple Inc. S= California C=US	5002B8132C1583D141C 3118A8B423B012343A9 56	5DFABB9577CFAB671FC7 DDFED1CF205B	6C66578DC96AD13EB7B 688BDC09DB472D5FBF0 3B3BD21309665052A886 D7E9B4

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



Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public Client RSA CA 11 – G1 (Sub-CA under USERTrust RSA Certification Authority) Subject: CN= Apple Public Client RSA CA 11 - G1 O= Apple Inc. S= California C=US	5FF6968F8EB5881D73D C207B7831DC5FB6B73 D18	4E418394B240A7CCA8E7 6AAE9D849793	301E8CBB8C665CAB256E B196F73F4D296C9CAD2 5F32744904279E1B3182 33E3B
Apple Public Server ECC CA 11 – G1 (Sub-CA under COMODO ECC Certification Authority) Subject: CN= Apple Public Server ECC CA 11 - G1 O= Apple Inc. S= California C=US	85B594D87182CECE568 0B3AF3598AB764B6DA C29	0098C17276AA836908DC DC5B4EF8BD4174	C451BEFBA87014ECD578 51D1E682403E3CA60963 773AE7FAA00FFD6FFAC8 B2A3

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