

Report of Independent Accountants

To the Management of Apple:

Scope

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 Services Based on the WebTrust Principles and Criteria for Certification Authorities Version 2.2.2” that for its Certification Authority (CA) operations at Cupertino, California, and supporting facilities at Prineville, Oregon; Maiden, North Carolina; and Reno, Nevada, USA for the Subordinate CA(s) referenced in [Appendix A](#), during the period from April 1, 2024 through March 31, 2025, 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 6.3.1](#), dated March 7, 2025
- maintained effective controls to provide reasonable assurance that:
 - Apple’s Certification Practice Statement is consistent with the relevant governing Certificate Policies
 - 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 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); and
 - subordinate CA certificate requests are 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;
 - 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 [WebTrust Principles and Criteria for Certification Authorities Version 2.2.2](#).

Management’s Responsibilities

Apple’s management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the [WebTrust Principles and Criteria for Certification Authorities Version 2.2.2](#).

Apple does not provide subscriber key management services for certificates, integrated circuit card lifecycle management, certificate suspension, certificate renewal, certificate rekey. Accordingly, our examination did not extend to controls that would address those criteria.

Our Responsibilities

Our responsibility is to express an opinion on Apple 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 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. 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’s management has disclosed to us matters referenced in [Appendix B](#) that the Company has posted publicly in the online forums of the CA/Browser Forum, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum. We have considered the nature of these matters in our risk assessment and 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. Our examination did not extend to controls at individual subscriber and relying party locations, and we have not evaluated the effectiveness of such controls.

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.

This report does not include any representation as to the quality of Apple’s CA services beyond those covered by the [WebTrust Services 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.

Inherent Limitations

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. Further, the projection to the future of any evaluations of effectiveness of specific controls is subject to the risk that controls may become ineffective.



Opinion

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

Use of the WebTrust Seal

Apple's use of the WebTrust for Certification Authorities 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.

Ernst & Young LLP

Ernst & Young LLP
20 June 2025

Appendix A - Subordinate CAs

Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organization (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public Client RSA CA 12 - G1	Sub-CA	AAA Certificate Services	Apple Public Client RSA CA 12 - G1	Apple Inc.	US	CA06F092123D7B005AE92847A8251BF0D08042CC	00CB79513FDF5A41B7EBA3B5012C665762	EB62BFFA6CBC802E4DAE6F8C53908020BE7F07774A55E67BBD63ECC37679DEC8
Apple Public Server ECC CA 12 - G1	Sub-CA	AAA Certificate Services	Apple Public Server ECC CA 12 - G1	Apple Inc.	US	5FE32E8A9497DED35CE1B7D4BC988E3129C9903A	726618753AD6C922C56C9DE1F38478B0	70DB9DED944DD35D474EA15FF2AA4E25F393A893ECD A54359D305BC319649817
Apple Public Server RSA CA 12 - G1	Sub-CA	AAA Certificate Services	Apple Public Server RSA CA 12 - G1	Apple Inc.	US	1E5C1791055702FC775CE37043EC6BFDDDD2D869	0AE48F23013064419259E1C29AE98D18	0B405CFE9A6BEB098FFB969121C5F6710F3F7FA9EA101A6418F7AF201D3D3938
Apple IST CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple IST CA 2 - G1	Apple Inc.	US	D87A94447C907090169EDD179C01440386D62A29	0552C7EFFEEC292BA9F1387B07AF929F	C9B06CC083186220618E61A8772640F824DF69D561AD56BDC15AD56D0CE08608
Apple IST CA 8 - G1	Sub-CA	Baltimore CyberTrust Root	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D78306BA968DDCB28F32F6BBB741	0A48D57C65FB0E6CF704A3645F1418E4	5C29DBEA9B7CC8B02418F28C1C8736DFDF170665D098EF681D903BE76987D249
Apple Public Client RSA CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple Public Client RSA CA 2 - G1	Apple Inc.	US	019C7649C5EE1A77A48A53A0CC03AA27BE2C48C7	0D4E55BBBADFA78C14398D94ABED2FBC	32B4B3768CA5A4D80E9DF8D557B7424F80AF5560B1148D05548DC3D76A7ED619

Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organization (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public Server ECC CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple Public Server ECC CA 2 - G1	Apple Inc.	US	B5646FBC179FC95065D8F53F84E995097A7C5F66	05AECAD3A2D246D587EC9391711D1114	DA8546816D891C1241E9387DE436D1B9F7EA70DBA1EB3D25F58271CE816A7ABC
Apple Public Server RSA CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple Public Server RSA CA 2 - G1	Apple Inc.	US	9061F3A3D706CEF517B6570ED98CA7954B163289	0B799AEF7B9DED2B418B8D3EAA3A8F7C	F518F0BB716521F0A26FDB40C304FF9B82FDBDE7ACBD46BF0EF23A180188EB5C
Apple Public Server ECC CA 11 - G1	Sub-CA	COMODO ECC Certification Authority	Apple Public Server ECC CA 11 - G1	Apple Inc.	US	85B594D87182CECE5680B3AF3598AB764B6DAC29	0098C17276AA836908DCDC5B4EF8BD4174	C451BEFBA87014ECD57851D1E682403E3CA60963773AE7FAA00FFD6FFAC8B2A3
Apple Public Client RSA CA 1 - G1	Sub-CA	DigiCert Global Root G2	Apple Public Client RSA CA 1 - G1	Apple Inc.	US	E8DD7EF8EAE8CA01FB7C85B69166CA024042F671	0B8A5B9DD501A88775399B9A048811A3	BE13A5D2F5C78F440119D484C710427325EB10CEA9623EF6200CB11B04F650E1
Apple Public EV Server RSA CA 1 - G1	Sub-CA	DigiCert Global Root G2	Apple Public EV Server RSA CA 1 - G1	Apple Inc.	US	D3BDC13CA0CF35B934C5D4DBDA100E4CDE6AFE58	04F22ECC21FCB4382AC28B8F2D641FC0	340CA5BA402D140B65A2C976E7AE8128A1505C29D190E0E034F59CCAE7A92BC2
Apple Public Server RSA CA 1 - G1	Sub-CA	DigiCert Global Root G2	Apple Public Server RSA CA 1 - G1	Apple Inc.	US	A37C9BEA4C0FC1B014CFA4791900D43C6F4DA095	0FD2A106FC12F606DBE5127FBE166812	392583543B93B10E0506DE75D69399FCBBC1469C8DE396066C756088B92241DA

Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organization (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple IST CA 8 - G1	Sub-CA	DigiCert Global Root G3	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D78306BA968DDCB28F32F6BBB741	05AE84C4406C98F01BDD0F0E6020FE9A	8711EE539E74213F5F412EB4A18A98C3B58DA620B4D43E75B0542AFC39FC6033
Apple IST CA 8 - G1	Sub-CA	DigiCert Global Root G3	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D78306BA968DDCB28F32F6BBB741	0C67620777A5ABC4BA535D8DADCF9AD7	9218BAB94E7D5D1F81D62D0FC23E31C8BBCBEE3545D1D7E9D3FD29B30BC188C8
Apple Public EV Server ECC CA 1 - G1	Sub-CA	DigiCert Global Root G3	Apple Public EV Server ECC CA 1 - G1	Apple Inc.	US	E085487D13A6D310199F5CCB6B782492F8AE1BAE	0CABAAD1CEC4E97CC2665881D02138F7	2585928D2C5BFD952E025BD12E27C6776224CF752EC362D3031CDD49351844D4
Apple Public Server ECC CA 1 - G1	Sub-CA	DigiCert Global Root G3	Apple Public Server ECC CA 1 - G1	Apple Inc.	US	6C9782459ECC6F1647F6B813F3735322FA791126	06B4543FF33BB19827C187A0213EC11A	2AF988F26F6EF0DAB9055697F0941FB4E5C42247CA982826895EF29985D30CD6
Apple Public EV Server RSA CA 2 - G1	Sub-CA	DigiCert High Assurance EV Root CA	Apple Public EV Server RSA CA 2 - G1	Apple Inc.	US	5055AB43A1AFA9482B5AC1A2878904E47A0ECADA	07177911005D2267F68892F68F8B5058	D6EF3E09EBE0D9370E51F5C09A532B3AC70D3CE822253F9FC84C28E9BFA550D5
Apple Public EV Server RSA CA 3 - G1	Sub-CA	DigiCert High Assurance EV Root CA	Apple Public EV Server RSA CA 3 - G1	Apple Inc.	US	77FC2F34695313CEC9AC5F9A3DA388D7866349BA	069AC439BB31C11AB2914025C3AE15D7	E881D3B83C3BC694D7D99F92DE83B2BFF5C6EE2D9871A446DEA107D6397565FC

Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organization (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public Client RSA CA 3 - G1	Sub-CA	DigiCert Trusted Root G4	Apple Public Client RSA CA 3 - G1	Apple Inc.	US	436911FF96E16349DD3DEA9D8D57A36D3E3A7BC2	0A6B5216B1CBEB0E95E4D299B28405F3	F74553757F2C6397D154296A86230C17B25DA8C7C426CD198A5107AD49047C30
Apple IST CA 8 - G1	Sub-CA	GeoTrust Primary Certification Authority - G2	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D78306BA968DDCB28F32F6BBB741	13522EBFC1DD5CE11EF27640751FE7DF	A4FE7C7F15155F3FOAEF7AAA83CF6E06DEB97CA3F909DF920AC1490882D488ED
Apple Public Client ECC CA 11 - G1	Sub-CA	USERTrust ECC Certification Authority	Apple Public Client ECC CA 11 - G1	Apple Inc.	US	85E92976E8218D07F432CEC38B88913A815E1F15	77EAE0D50978C421CC2E1B29F1319D54	7EA4FDF4721367AFEDBFD391101BE74A48D30D5ACDF873862A122B3A57B2B8C2
Apple Public Client ECC CA 20 - G1	Sub-CA	USERTrust ECC Certification Authority	Apple Public Client ECC CA 20 - G1	Apple Inc.	US	D490423177558B9BBE862891931CD56268B9C213	6480A3B22099DEC45E973C911A9730EA	18EC4A52CBFA5A02D6A10E2899318185E394B0294D5DEC7FF59BBF3012598B4C
Apple Public Client ECC CA 50 - G1	Sub-CA	USERTrust ECC Certification Authority	Apple Public Client ECC CA 50 - G1	Apple Inc.	US	E68997A9D1D1063329649F511D100CE73E6ECC6A	00B6BA1D802E9C2740FCA40653FA66FA57	5F8AD1286DD9D1DAF23272E4E13CC995CCE5BE27BBF79029152BE09EF39ED296
Apple Public Client RSA CA 11 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Client RSA CA 11 - G1	Apple Inc.	US	5FF6968F8EB5881D73DC207B7831DC5FB6B73D18	4E418394B240A7CCA8E76AAE9D849793	301E8CBB8C665CAB256EB196F73F4D296C9CAD25F32744904279E1B318233E3B

Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organization (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public Client RSA CA 13 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Client RSA CA 13 - G1	Apple Inc.	US	018B3637A4BEDF191C32B85159037F538179181F	0110B4ED5816D08CA50796305D1E8552	2C72DCBF8CB804CD0267043021238FE5A47C25912F4672E9001B1B0C28097C2B
Apple Public Client RSA CA 14 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Client RSA CA 14 - G1	Apple Inc.	US	D8CBD9E54C0E875961A8ABA66310F69C45E3ECE5	00A888ACF65B85F1AF5F31BD988BDA4421	C1A99C82AD9BC8A2D7B7D599EA2C572BA8CBE0614B6A01C9064F396AC6B124DF
Apple Public Client RSA CA 20 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Client RSA CA 20 - G1	Apple Inc.	US	2D224CF17B179F4EDA7932B6865DAC11C28ADC5B	008F9355F1736E4EC4227E99669517063A	A0F130F70059F6DE9FFC01F8004C8E07D438475C57134601B9EB65A36DD426C9
Apple Public Client RSA CA 50 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Client RSA CA 50 - G1	Apple Inc.	US	D20642091CEAD8DC4422AF8A928447BACF6602AB	757FBAFFE64A1D80BAC783DFA8CAE213	9EC26DA7082782DE9ED89221DE7B02F7417557C261BA5BCB87CE68C0801E7341
Apple Public Server RSA CA 11 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Server RSA CA 11 - G1	Apple Inc.	US	5002B8132C1583D141C3118A8B423B012343A956	5DFABB9577CFAB671FC7DDFED1CF205B	6C66578DC96AD13EB7B688BDC09DB472D5FBF03B3BD21309665052A886D7E9B4

Appendix B - Matters of Disclosure

No.	Observation	Public Disclosure Link
1	On March 17, 2025, Apple CA compliance identified a condition whereby multiple certificates could be issued to a given public key, which was inconsistent with the permitted activities within Apple's certification practice statement (CPS) document. Revocation of affected certificates was tracked as a part of Bug 1955365 . The matter was resolved on April 3, 2025.	Bug 1955365 - Bugzilla Link



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

20 June 2025

We, as management of Apple Inc. (Apple), are responsible for operating a Certification Authority (CA) at Cupertino, California, and supporting facilities at Prineville, Oregon; Maiden, North Carolina; and Reno, Nevada, USA locations for the Subordinate CA(s) listed in Appendix A.

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

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

Management of Apple 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.

There are inherent limitations in any controls, 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.

Management of Apple has assessed the disclosures 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(s) listed in Appendix A at Cupertino, California; Prineville, Oregon; Maiden, North Carolina; and Reno, Nevada, USA locations during the period from April 1, 2024 through March 31, 2025, Apple has:

- Disclosed its Business, key life cycle management, certificate life cycle management, and CA environmental control practices as below:
 - [Apple Public CA Certification Practice Statement Version 6.3.1](#), March 7, 2025
- Maintained effective controls to provide reasonable assurance that:
 - Apple's Certification Practice Statement is consistent with the relevant governing Certificate Policies
 - Apple provides its services in accordance with its Certification Practice Statement

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:
 - 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

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

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- 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

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



- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

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.
20 June 2025

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



Appendix A - Subordinate CAs

Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organization (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public Client RSA CA 12 - G1	Sub-CA	AAA Certificate Services	Apple Public Client RSA CA 12 - G1	Apple Inc.	US	CA06F092123D7B005AE92847A8251BF0D08042CC	00CB79513FDF5A41B7EBA3B5012C665762	EB62BFFA6CBC802E4DAE6F8C53908020BE7F07774A55E67BBD63ECC37679DEC8
Apple Public Server ECC CA 12 - G1	Sub-CA	AAA Certificate Services	Apple Public Server ECC CA 12 - G1	Apple Inc.	US	5FE32E8A9497DED35CE1B7D4BC988E3129C9903A	726618753AD6C922C56C9DE1F38478B0	70DB9DED944DD35D474EA15FF2AA4E25F393A893ECDA54359D305BC319649817
Apple Public Server RSA CA 12 - G1	Sub-CA	AAA Certificate Services	Apple Public Server RSA CA 12 - G1	Apple Inc.	US	1E5C1791055702FC775CE37043EC6BFDDDD2D869	0AE48F23013064419259E1C29AE98D18	0B405CFE9A6BEB098FFB969121C5F6710F3F7FA9EA101A6418F7AF201D3D3938
Apple IST CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple IST CA 2 - G1	Apple Inc.	US	D87A94447C907090169EDD179C01440386D62A29	0552C7EFFECC292BA9F1387B07AF929F	C9B06CC083186220618E61A8772640F824DF69D561AD56BDC15AD56D0CE08608
Apple IST CA 8 - G1	Sub-CA	Baltimore CyberTrust Root	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D78306BA968DDCB28F32F6BBB741	0A48D57C65FB0E6CF704A3645F1418E4	5C29DBEA9B7CC8B02418F28C1C8736DFDF170665D098EF681D903BE76987D249
Apple Public Client RSA CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple Public Client RSA CA 2 - G1	Apple Inc.	US	019C7649C5EE1A77A48A53A0CC03AA27BE2C48C7	0D4E55BBBADFA78C14398D94ABED2FBC	32B4B3768CA5A4D80E9DF8D557B7424F80AF5560B1148D05548DC3D76A7ED619

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



Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organization (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public Server ECC CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple Public Server ECC CA 2 - G1	Apple Inc.	US	B5646FBC179FC95065D8F53F84E995097A7C5F66	05AECAD3A2D246D587EC9391711D1114	DA8546816D891C1241E9387DE436D1B9F7EA70DBA1EB3D25F58271CE816A7ABC
Apple Public Server RSA CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple Public Server RSA CA 2 - G1	Apple Inc.	US	9061F3A3D706CEF517B6570ED98CA7954B163289	0B799AEF7B9DED2B418B8D3EAA3A8F7C	F518F0BB716521F0A26FDB40C304FF9B82FBDBE7ACBD46BF0EF23A180188EB5C
Apple Public Server ECC CA 11 - G1	Sub-CA	COMODO ECC Certification Authority	Apple Public Server ECC CA 11 - G1	Apple Inc.	US	85B594D87182CECE5680B3AF3598AB764B6DAC29	0098C17276AA836908DCDC5B4EF8BD4174	C451BEFBA87014ECD57851D1E682403E3CA60963773AE7FAA00FFD6FFAC8B2A3
Apple Public Client RSA CA 1 - G1	Sub-CA	DigiCert Global Root G2	Apple Public Client RSA CA 1 - G1	Apple Inc.	US	E8DD7EF8EAE8CA01FB7C85B69166CA024042F671	0B8A5B9DD501A88775399B9A048811A3	BE13A5D2F5C78F440119D484C710427325EB10CEA9623EF6200CB11B04F650E1
Apple Public EV Server RSA CA 1 - G1	Sub-CA	DigiCert Global Root G2	Apple Public EV Server RSA CA 1 - G1	Apple Inc.	US	D3BDC13CA0CF35B934C5D4DBDA100E4CDE6AFE58	04F22ECC21FCB4382AC28B8F2D641FC0	340CA5BA402D140B65A2C976E7AE8128A1505C29D190E0E034F59CCAE7A92BC2
Apple Public Server RSA CA 1 - G1	Sub-CA	DigiCert Global Root G2	Apple Public Server RSA CA 1 - G1	Apple Inc.	US	A37C9BEA4C0FC1B014CFA4791900D43C6F4DA095	0FD2A106FC12F606DBE5127FBE166812	392583543B93B10E0506DE75D69399FCBBC1469C8DE396066C756088B92241DA
Apple IST CA 8 - G1	Sub-CA	DigiCert Global Root G3	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D78306BA968DDCB28F32F6BBB741	05AE84C4406C98F01BDD0F0E6020FE9A	8711EE539E74213F5F412EB4A18A98C3B58DA620B4D43E75B0542AFC39FC6033

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



Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organization (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple IST CA 8 - G1	Sub-CA	DigiCert Global Root G3	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D78306BA968DDCB28F32F6BBB741	0C67620777A5ABC4BA535D8DADCF9AD7	9218BAB94E7D5D1F81D62D0FC23E31C8BBCBEE3545D1D7E9D3FD29B30BC188C8
Apple Public EV Server ECC CA 1 - G1	Sub-CA	DigiCert Global Root G3	Apple Public EV Server ECC CA 1 - G1	Apple Inc.	US	E085487D13A6D310199F5CCB6B782492F8AE1BAE	0CABAAD1CEC4E97CC2665881D02138F7	2585928D2C5BFD952E025BD12E27C6776224CF752EC362D3031CDD49351844D4
Apple Public Server ECC CA 1 - G1	Sub-CA	DigiCert Global Root G3	Apple Public Server ECC CA 1 - G1	Apple Inc.	US	6C9782459ECC6F1647F6B813F3735322FA791126	06B4543FF33BB19827C187A0213EC11A	2AF988F26F6EF0DAB9055697F0941FB4E5C42247CA982826895EF29985D30CD6
Apple Public EV Server RSA CA 2 - G1	Sub-CA	DigiCert High Assurance EV Root CA	Apple Public EV Server RSA CA 2 - G1	Apple Inc.	US	5055AB43A1AFA9482B5AC1A2878904E47A0ECADA	07177911005D2267F68892F68F8B5058	D6EF3E09EBE0D9370E51F5C09A532B3AC70D3CE822253F9FC84C28E9BFA550D5
Apple Public EV Server RSA CA 3 - G1	Sub-CA	DigiCert High Assurance EV Root CA	Apple Public EV Server RSA CA 3 - G1	Apple Inc.	US	77FC2F34695313CEC9AC5F9A3DA388D7866349BA	069AC439BB31C11AB2914025C3AE15D7	E881D3B83C3BC694D7D99F92DE83B2BF5C6EE2D9871A446DEA107D6397565FC
Apple Public Client RSA CA 3 - G1	Sub-CA	DigiCert Trusted Root G4	Apple Public Client RSA CA 3 - G1	Apple Inc.	US	436911FF96E16349DD3DEA9D8D57A36D3E3A7BC2	0A6B5216B1CBEB0E95E4D299B28405F3	F74553757F2C6397D154296A86230C17B25DA8C7C426CD198A5107AD49047C30

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



Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organization (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple IST CA 8 - G1	Sub-CA	GeoTrust Primary Certification Authority - G2	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D78306BA968DDCB28F32F6BBB741	13522EBFC1DD5CE11EF27640751FE7DF	A4FE7C7F15155F3F0AEF7AAA83CF6E06DEB97CA3F909DF920AC1490882D488ED
Apple Public Client ECC CA 11 - G1	Sub-CA	USERTrust ECC Certification Authority	Apple Public Client ECC CA 11 - G1	Apple Inc.	US	85E92976E8218D07F432CEC38B88913A815E1F15	77EAE0D50978C421CC2E1B29F1319D54	7EA4FDF4721367AFEDBFD391101BE74A48D30D5ACDF873862A122B3A57B2B8C2
Apple Public Client ECC CA 20 - G1	Sub-CA	USERTrust ECC Certification Authority	Apple Public Client ECC CA 20 - G1	Apple Inc.	US	D490423177558B9B8E862891931CD56268B9C213	6480A3B22099DEC45E973C911A9730EA	18EC4A52CBFA5A02D6A10E2899318185E394B0294D5DEC7FF59BBF3012598B4C
Apple Public Client ECC CA 50 - G1	Sub-CA	USERTrust ECC Certification Authority	Apple Public Client ECC CA 50 - G1	Apple Inc.	US	E68997A9D1D1063329649F511D100CE73E6ECC6A	00B6BA1D802E9C2740FCA40653FA66FA57	5F8AD1286DD9D1DAF23272E4E13CC995CCE5BE27BBF79029152BE09EF39ED296
Apple Public Client RSA CA 11 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Client RSA CA 11 - G1	Apple Inc.	US	5FF6968F8EB5881D73DC207B7831DC5FB6B73D18	4E418394B240A7CCA8E76AAE9D849793	301E8CBB8C665CAB256EB196F73F4D296C9CAD25F32744904279E1B318233E3B

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



Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organization (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple Public Client RSA CA 13 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Client RSA CA 13 - G1	Apple Inc.	US	018B3637A4BEDF191C32B85159037F538179181F	0110B4ED5816D08CA50796305D1E8552	2C72DCBF8CB804CD0267043021238FE5A47C25912F4672E9001B1B0C28097C2B
Apple Public Client RSA CA 14 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Client RSA CA 14 - G1	Apple Inc.	US	D8CBD9E54C0E875961A8ABA66310F69C45E3ECE5	00A888ACF65B85F1AF5F31BD988BDA4421	C1A99C82AD9BC8A2D7B7D599EA2C572BA8CBE0614B6A01C9064F396AC6B124DF
Apple Public Client RSA CA 20 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Client RSA CA 20 - G1	Apple Inc.	US	2D224CF17B179F4EDA7932B6865DAC11C28ADC5B	008F9355F1736E4EC4227E99669517063A	A0F130F70059F6DE9FFC01F8004C8E07D438475C57134601B9EB65A36DD426C9
Apple Public Client RSA CA 50 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Client RSA CA 50 - G1	Apple Inc.	US	D20642091CEAD8DC4422AF8A928447BACF6602AB	757FBABFE64A1D80BAC783DFA8CAE213	9EC26DA7082782DE9ED89221DE7B02F7417557C261BA5BCB87CE68C0801E7341
Apple Public Server RSA CA 11 - G1	Sub-CA	USERTrust RSA Certification Authority	Apple Public Server RSA CA 11 - G1	Apple Inc.	US	5002B8132C1583D141C3118A8B423B012343A956	5DFABB9577CFAB671FC7DDFED1CF205B	6C66578DC96AD13EB7B688BDC09DB472D5FBF03B3BD21309665052A886D7E9B4

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