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 SSL Certification Authority Services Based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline Version 2.8" that for its Certification Authority (CA) operations at Cupertino, California, and supporting facilities at Prineville, Oregon; Maiden, North Carolina; and Reno, Nevada, USA locations throughout the period April 1, 2024 to March 31, 2025 for CAs as enumerated in Appendix A, Apple has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Apple Public CA Certification Practice Statement Version 6.3.1, dated March 7, 2025 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 SSL Baseline Requirements as set forth by the CA/Browser Forum

based on the *WebTrust Principles and Criteria for Certification Authorities – SSL Baseline Version 2.8*.

Management's Responsibilities

Apple 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 – SSL Baseline Version 2.8.

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 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 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 Principles and Criteria for Certification Authorities – SSL Baseline Version 2.8* criteria, or the suitability of any of Apple's services for any customer's intended purposes.

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 of any evaluations of effectiveness to future periods 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 – SSL Baseline 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)	Organiza-tion (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
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	GeoTrust Primary Certification Authority - G2	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D78306BA968DDCB28F32F6BBB741	13522EBFC1DD5CE11EF27640751FE7DF	A4FE7C7F15155F3F0AEF7AAA83CF6E06DEB97CA3F909DF920AC1490882D488ED
Apple IST CA 8 - G1	Sub-CA	Baltimore CyberTrust Root	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D78306BA968DDCB28F32F6BBB741	0A48D57C65FB0E6CF704A3645F1418E4	5C29DBEA9B7CC8B02418F28C1C8736DFDF170665D098EF681D903BE76987D249
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

Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organiza-tion (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
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 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
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 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 Server ECC CA 12 - G1	Sub-CA	AAA Certificate Services	Apple Public Server ECC CA 12 - G1	Apple Inc.	US	5FE32E8A9497DED35CE1B7D4BC988E3129C9903A	726618753AD6C922C56C9DE1F38478B0	70DB9DED944DD35D474EA15FF2AA4E25F393A893ECDA54359D305BC319649817

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 1 - G1	Sub-CA	DigiCert Global Root G2	Apple Public Server RSA CA 1 - G1	Apple Inc.	US	A37C9BEA4C0FC1B014CFA4791900D43C6F4DA095	0FD2A106FC12F606DBE5127FBE166812	392583543B93B10E0506DE75D69399FCBBC1469C8DE396066C756088B92241DA
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 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 Public Server RSA CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple Public Server RSA CA 2 - G1	Apple Inc.	US	9061F3A3D706CEF517B6570ED98CA7954B163289	0B799AEF7B9DED2B418B8D3EAA3A8F7C	F518F0BB716521F0A26FDB40C304FF9B82FBDBE7ACBD46BF0EF23A180188EB5C

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 SSL Certification Authority Services
Based on the WebTrust Principles and Criteria for Certification Authorities –
SSL Baseline Version 2.8

20 June 2025

We, as management of Apple Inc. (Apple), are responsible for operating the SSL Certification Authority (CA) operations at Cupertino, California, and supporting facilities at Prineville, Oregon; Maiden, North Carolina; and Reno, Nevada; USA locations for the Subordinate CA(s) in scope for SSL Baseline 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. Further, 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 SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services at Subordinate CA(s) listed in at Cupertino, California; Prineville, Oregon; Maiden, North Carolina; and Reno, Nevada; USA locations throughout the period April 1, 2024 to March 31, 2025, Apple has:

- Disclosed its SSL certificate lifecycle management business practices in its:
  - [Apple Public CA Certification Practice Statement Version 6.3.1](), dated March 7, 2025
  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;
  - 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 SSL Baseline Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline Version 2.8]().

Apple Inc.
20 June 2025

Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organiza-tion (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Apple IST CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple IST CA 2 - G1	Apple Inc.	US	D87A94447C907090 169EDD179C014403 86D62A29	0552C7EFFEEC292BA 9F1387B07AF929F	C9B06CC083186220 618E61A8772640F82 4DF69D561AD56BD C15AD56D0CE08608
Apple IST CA 8 - G1	Sub-CA	GeoTrust Primary Certificatio n Authority - G2	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D783 06BA968DDCB28F32 F6BBB741	13522EBFC1DD5CE1 1EF27640751FE7DF	A4FE7C7F15155F3F0 AEF7AAA83CF6E06D EB97CA3F909DF920 AC1490882D488ED
Apple IST CA 8 - G1	Sub-CA	Baltimore CyberTrust Root	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D783 06BA968DDCB28F32 F6BBB741	0A48D57C65FB0E6C F704A3645F1418E4	5C29DBEA9B7CC8B0 2418F28C1C8736DF DF170665D098EF68 1D903BE76987D249
Apple IST CA 8 - G1	Sub-CA	DigiCert Global Root G3	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D783 06BA968DDCB28F32 F6BBB741	05AE84C4406C98F0 1BDD0F0E6020FE9A	8711EE539E74213F5 F412EB4A18A98C3B 58DA620B4D43E75B 0542AFC39FC6033
Apple IST CA 8 - G1	Sub-CA	DigiCert Global Root G3	Apple IST CA 8 - G1	Apple Inc.	US	C3C4A4580563D783 06BA968DDCB28F32 F6BBB741	0C67620777A5ABC4 BA535D8DADCF9AD 7	9218BAB94E7D5D1F 81D62D0FC23E31C8 BBCBEE3545D1D7E9 D3FD29B30BC188C8
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	E085487D13A6D310 199F5CCB6B782492 F8AE1BAE	0CABAAD1CEC4E97 CC2665881D02138F 7	2585928D2C5BFD95 2E025BD12E27C677 6224CF752EC362D3 031CDD49351844D4

Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organiza-tion (O)	Country (C)	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
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 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
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 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 Server ECC CA 12 - G1	Sub-CA	AAA Certificate Services	Apple Public Server ECC CA 12 - G1	Apple Inc.	US	5FE32E8A9497DED35CE1B7D4BC988E3129C9903A	726618753AD6C922C56C9DE1F38478B0	70DB9DED944DD35D474EA15FF2AA4E25F393A893ECDA54359D305BC319649817

Certification Authority (CA)	CA Type	Issued By	Common Name (CN)	Organiza-tion (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	B5646FBC179FC950 65D8F53F84E995097 A7C5F66	05AECAD3A2D246D 587EC9391711D111 4	DA8546816D891C12 41E9387DE436D1B9 F7EA70DBA1EB3D25 F58271CE816A7ABC
Apple Public Server RSA CA 1 - G1	Sub-CA	DigiCert Global Root G2	Apple Public Server RSA CA 1 - G1	Apple Inc.	US	A37C9BEA4C0FC1B0 14CFA4791900D43C 6F4DA095	0FD2A106FC12F606 DBE5127FBE166812	392583543B93B10E0 506DE75D69399FCB BC1469C8DE396066 C756088B92241DA
Apple Public Server RSA CA 11 - G1	Sub-CA	USERTrust RSA Certificatio n Authority	Apple Public Server RSA CA 11 - G1	Apple Inc.	US	5002B8132C1583D1 41C3118A8B423B01 2343A956	5DFABB9577CFAB67 1FC7DDFED1CF205B	6C66578DC96AD13E B7B688BDC09DB472 D5FBF03B3BD21309 665052A886D7E9B4
Apple Public Server RSA CA 12 - G1	Sub-CA	AAA Certificate Services	Apple Public Server RSA CA 12 - G1	Apple Inc.	US	1E5C1791055702FC7 75CE37043EC6BFDD DD2D869	0AE48F23013064419 259E1C29AE98D18	0B405CFE9A6BEB09 8FFB969121C5F6710 F3F7FA9EA101A641 8F7AF201D3D3938
Apple Public Server RSA CA 2 - G1	Sub-CA	Baltimore CyberTrust Root	Apple Public Server RSA CA 2 - G1	Apple Inc.	US	9061F3A3D706CEF5 17B6570ED98CA795 4B163289	0B799AEF7B9DED2B 418B8D3EAA3A8F7C	F518F0BB716521F0A 26FDB40C304FF9B8 2FBDBE7ACBD46BF0 EF23A180188EB5C