

Report of Independent Accountants

To the Management of Apple:

We have examined the accompanying [assertion](#) made by the management of Apple Inc. (Apple), titled “Management’s Assertion Regarding the Effectiveness of Its Controls Over the SSL Certification Authority Services Based on the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security - Version 2.6” 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 SSL certificate lifecycle management business practices in its:

- [Apple Public CA Certification Practice Statement Version 5.6](#)

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
- 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 life cycle management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security - Version 2.6](#).

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 American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management’s assertion, whether due to fraud or error.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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.

Apple's use of the WebTrust for Certification Authorities - SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report, and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of Apple's CA services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security - Version 2.6](#) criteria, or the suitability of any of Apple's services for any customer's intended purpose.

Ernst & Young LLP

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	D87A94447C9070901 69EDD179C01440386 D62A29	146036	AC2B922ECFD5E01711 772FEA8ED372DE9D1E 2245FCE3F57A9CDBEC 77296A424B
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	C3C4A4580563D7830 6BA968DDCB28F32F6B BB741	13522EBFC1DD5CE11E F27640751FE7DF	A4FE7C7F15155F3F0A EF7AAA83CF6E06DEB9 7CA3F909DF920AC14 90882D488ED
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	D87A94447C9070901 69EDD179C01440386 D62A29	0552C7EFFEEC292BA9 F1387B07AF929F	C9B06CC0831862206 18E61A8772640F824D F69D561AD56BDC15A D56D0CE08608
Apple IST CA 8 - G1 (Sub-CA under Baltimore CyberTrust Root) Subject: CN= Apple IST CA 8 - G1 OU= Certification Authority O= Apple Inc.	C3C4A4580563D7830 6BA968DDCB28F32F6B BB741	0A48D57C65FB0E6CF7 04A3645F1418E4	5C29DBEA9B7CC8B02 418F28C1C8736DFDF1 70665D098EF681D903 BE76987D249

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
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	F518F0BB716521F0A26FDB40C304FF9B82FBD7ACBD46BF0EF23A180188EB5C
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 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
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

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	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: CN= Apple IST CA 8 - G1 OU= Certification Authority O= Apple Inc. C= US	C3C4A4580563D78306BA968DDCB28F32F6BB741	0C67620777A5ABC4BA535D8DADCF9AD7	9218BAB94E7D5D1F81D62D0FC23E31C8BBCBEE3545D1D7E9D3FD29B30BC188C8
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	2585928D2C5BFD952E025BD12E27C677622ACF752EC362D3031CD49351844D4
Apple Public EV Server RSA CA 2 - G1 (Sub-CA under DigiCert High Assurance EV Root)	5055AB43A1AFA9482B5AC1A2878904E47A0ECADA	07177911005D2267F68892F68F8B5058	D6EF3E09EBE0D9370E51F5C09A532B3AC70D3CE822253F9FC84C28E9BFA550D5

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Subject: CN= Apple Public EV Server RSA CA2 - G1 O= Apple Inc. C=US			
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	77FC2F34695313CEC9 AC5F9A3DA388D7866 349BA	069AC439BB31C11AB 2914025C3AE15D7	E881D3B83C3BC694D 7D99F92DE83B2BFF5C 6EE2D9871A446DEA1 07D6397565FC
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 C=US	1E5C1791055702FC77 5CE37043EC6BFDDDD 2D869	0AE48F230130644192 59E1C29AE98D18	0B405CFE9A6BEB098F FB969121C5F6710F3F 7FA9EA101A6418F7AF 201D3D3938
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:	5002B8132C1583D14 1C3118A8B423B0123 43A956	5DFABB9577CFAB671F C7DDFED1CF205B	6C66578DC96AD13EB 7B688BDC09DB472D5 FBF03B3BD213096650 52A886D7E9B4

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
CN= Apple Public Server 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	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. This incident was closed during the current examination period.	N/A	Bug 1724528 - Bugzilla Link
2	On September 9, 2021, Apple CA compliance identified certificates on Apple CA's test web page (https://www.apple.com/certificateauthority/public/) that 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. The new certificates were issued and the test web page was updated accordingly. This incident was closed during the current examination period.	N/A	Bug 1730291 - Bugzilla Link
3	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'. Revoked certificates were not impacted by this issue and would display the "revoked" status for relying parties.	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. Criterion number 6.8 The CA maintains controls to provide reasonable assurance that timely, complete and accurate certificate status information (including Certificate	Bug 1771398 - Bugzilla Link

	Observation	Relevant WebTrust Criteria	Publicly Disclosed Link
		Revocation Lists and other certificate status mechanisms) 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 SSL Certification Authority Services
Based on the WebTrust Principles and Criteria for Certification Authorities –
SSL Baseline with Network Security – Version 2.6

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 SSL CA services.

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 SSL certificate lifecycle management business practices in its:

- [Apple Public CA Certification Practice Statement Version 5.6](#)

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.
- 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 are properly authorized and performed to maintain CA systems integrity.
- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

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



for the Subordinate CAs under external Root CAs in scope for SSL Baseline Requirements and Network Security Requirements listed in Appendix A based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.6](#).

Apple Inc.



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	AC2B922ECFD5E017117 72FEA8ED372DE9D1E2 245FCE3F57A9CDBEC7 7296A424B
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	C3C4A4580563D78306 BA968DDCB28F32F6BB B741	13522EBFC1DD5CE11EF 27640751FE7DF	A4FE7C7F15155F3F0AE F7AAA83CF6E06DEB97 CA3F909DF920AC1490 882D488ED
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	0552C7EFFEEC292BA9F 1387B07AF929F	C9B06CC083186220618 E61A8772640F824DF69 D561AD56BDC15AD56 D0CE08608
Apple IST CA 8 – G1 (Sub-CA under Baltimore CyberTrust Root)	C3C4A4580563D78306 BA968DDCB28F32F6BB B741	0A48D57C65FB0E6CF70 4A3645F1418E4	5C29DBEA9B7CC8B024 18F28C1C8736DFDF170 665D098EF681D903BE7 6987D249



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			
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	F518F0BB716521F0A26FDB40C304FF9B82FBDDBE7ACBD46BF0EF23A180188EB5C
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 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
Apple Public EV Server RSA CA 1 - G1 (Sub-CA under Digicert Global Root G2)	D3BDC13CA0CF35B934C5D4DBDA100E4CDE6AFE58	04F22ECC21FCB4382AC28B8F2D641FC0	340CA5BA402D140B65A2C976E7AE8128A1505C29D190E0E034F59CCAE7A92BC2



Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Subject: CN= Apple Public EV Server RSA CA1 - G1 O= Apple Inc. C=US			
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	06B4543FF33BB19827C 187A0213EC11A	2AF988F26F6EF0DAB90 55697F0941FB4E5C422 47CA982826895EF2998 5D30CD6
Apple IST CA 8 – G1 (Sub-CA under DigiCert Global Root G3) Subject: CN= Apple IST CA 8 – G1 O= Apple Inc. C= US	C3C4A4580563D78306 BA968DDCB28F32F6BB B741	05AE84C4406C98F01B DD0F0E6020FE9A	8711EE539E74213F5F41 2EB4A18A98C3B58DA6 20B4D43E75B0542AFC3 9FC6033
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	C3C4A4580563D78306 BA968DDCB28F32F6BB B741	0C67620777A5ABC4BA 535D8DADCF9AD7	9218BAB94E7D5D1F81 D62D0FC23E31C8BBCB EE3545D1D7E9D3FD29 B30BC188C8
Apple Public EV Server ECC CA1 G1 (Sub-CA under DigiCert Global Root G3) Subject:	E085487D13A6D31019 9F5CCB6B782492F8AE1 BAE	0CABAAD1CEC4E97CC2 665881D02138F7	2585928D2C5BFD952E0 25BD12E27C6776224CF 752EC362D3031CDD49 351844D4



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	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 O= Apple Inc. S= California C=US	1E5C1791055702FC775CE37043EC6BFDDDD2D869	0AE48F23013064419259E1C29AE98D18	0B405CFE9A6BEB098FFB969121C5F6710F3F7FA9EA101A6418F7AF201D3D3938
Apple Public Server ECC CA 12 – G1 (Sub-CA under AAA Certificate Services Root) Subject:	5FE32E8A9497DED35CE1B7D4BC988E3129C9903A	726618753AD6C922C56C9DE1F38478B0	70DB9DED944DD35D474EA15FF2AA4E25F393A893ECDA54359D305BC319649817



Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
CN= Apple Public Server ECC CA 12 - G1 O= Apple Inc. S= California C=US			
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	5002B8132C1583D141C3118A8B423B012343A956	5DFABB9577CFAB671FC7DDFED1CF205B	6C66578DC96AD13EB7B688BDC09DB472D5FBF03B3BD21309665052A886D7E9B4
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	85B594D87182CECE5680B3AF3598AB764B6DAC29	0098C17276AA836908DCDC5B4EF8BD4174	C451BEFBA87014ECD57851D1E682403E3CA60963773AE7FAA00FFD6FAC8B2A3