# Cryptographic Module Validation Program

## Certificate #3431

### Details

| | |
|---|---|
| Module Name | Apple CoreCrypto Kernel Module v9.0 for Intel |
| Standard | FIPS 140-2 |
| Status | Active |
| Sunset Date | 4/3/2024 |
| Validation Dates | 4/4/2019<br>4/12/2019 |
| Overall Level | 1 |
| Caveat | When operated in FIPS mode. |
| Security Level Exceptions | • Physical Security: N/A |
| Module Type | Software |
| Embodiment | Multi-Chip Stand Alone |
| Description | The Apple CoreCrypto Kernel Module v9.0 for Intel is a software cryptographic module running on a multi-chip standalone hardware device and provides services intended to protect data in transit and at rest. |
| Tested Configuration(s) | • macOS Mojave 10.14 running on iMac Pro with Intel Xeon CPU with PAA<br>• macOS Mojave 10.14 running on iMac Pro with Intel Xeon CPU without PAA<br>• macOS Mojave 10.14 running on Mac mini with Intel i5 CPU with PAA<br>• macOS Mojave 10.14 running on Mac mini with Intel i5 CPU without PAA<br>• macOS Mojave 10.14 running on MacBook Pro with Intel i7 CPU with PAA<br>• macOS Mojave 10.14 running on MacBook Pro with Intel i7 CPU without PAA<br>• macOS Mojave 10.14 running on MacBook Pro with Intel i9 CPU with PAA<br>• macOS Mojave 10.14 running on MacBook Pro with Intel i9 CPU without PAA<br>• macOS Mojave 10.14 running on MacBook with Intel Core M CPU with PAA<br>• macOS Mojave 10.14 running on MacBook with Intel Core M CPU without PAA (single-user mode) |

FIPS Algorithms

| | |
|---|---|
| AES | Certs. #5815, #5816, #5817, #5818, #5819, #5820, #5821, #5822, #5823, #5824, #5825, #5826, #5827, #5828, #5830, #5831, #5832, #5833, #5834, #5835, #C171, #C172, #C173, #C174 and #C175 |
| DRBG | Certs. #2403, #2404, #2405, #2406, #2408, #2409, #2410, #2411, #2412, #2413, #2414, #2415, #2416, #2417, #2418, #2419, #2420, #2421, #2422, #2423, #2424, #2425, #2426, #2427, #2428, #C171, #C172, #C173, #C174, #C175, #C176, #C177, #C236, #C237 and #C238 |
| ECDSA | Certs. #C176, #C177, #C236, #C237 and #C238 |
| HMAC | Certs. #3841, #3842, #3843, #3844, #3845, #3846, #3847, #3848, #3849, #3850, #3851, #3852, #3853, #3854, #3855, #C176, #C177, #C236, #C237 and #C238 |
| KTS | AES Certs. #5824, #5826, #5827, #5828, #5835, #C171, #C172, #C173, #C174 and #C175; key establishment methodology provides between 128 and 256 bits of encryption strength |
| PBKDF | vendor affirmed |
| RSA | Certs. #C176, #C177, #C236, #C237 and #C238 |
| SHS | Certs. #4616, #4617, #4618, #4619, #4620, #4621, #4622, #4623, #4624, #4625, #4626, #4627, #4628, #4629, #4630, #C176, #C177, #C236, #C237 and #C238 |
| Triple-DES | Certs. #C176, #C177, #C236, #C237 and #C238 |

| | |
|---|---|
| Allowed Algorithms | MD5; NDRNG; RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength) |
| Software Versions | 9.0 |
| Product URL | http://support.apple.com/en-us/HT201159 |

### Vendor

Apple Inc.
One Apple Park Way
MS: 927-1CPS
Cupertino, CA 95014
USA

Shawn Geddis
geddis@apple.com
Phone: 669-227-3579
Fax: 866-315-1954

Stephanie Motre Martin
smotre@apple.com
Phone: 408-750-6235
Fax: 866-315-1954

### Related Files

Security Policy
Consolidated Certificate

### Lab

ATSEC INFORMATION SECURITY CORP
NVLAP Code: 200658-0