# Cryptographic Module Validation Program

## Certificate #3433

<table>
<thead>
<tr>
<th>Details</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Module Name</strong></td>
<td>Apple CoreCrypto Module v9.0 for ARM</td>
</tr>
<tr>
<td><strong>Standard</strong></td>
<td>FIPS 140-2</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Active</td>
</tr>
<tr>
<td><strong>Sunset Date</strong></td>
<td>4/10/2024</td>
</tr>
<tr>
<td><strong>Validation Dates</strong></td>
<td>4/11/2019</td>
</tr>
<tr>
<td><strong>Overall Level</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Caveat</strong></td>
<td>When operated in FIPS Mode. The module generates cryptographic keys whose strengths are modified by available entropy</td>
</tr>
<tr>
<td><strong>Security Level Exceptions</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Module Type</strong></td>
<td>Software</td>
</tr>
<tr>
<td><strong>Embodiment</strong></td>
<td>Multi-Chip Stand Alone</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>The Apple CoreCrypto Module v9.0 for ARM 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.</td>
</tr>
</tbody>
</table>

**Tested Configuration(s)**

- iOS 12 running on iPad Air 2 with Apple A8X CPU with PAA
- iOS 12 running on iPad Air 2 with Apple A8X CPU without PAA
- iOS 12 running on iPad Pro with Apple A10X Fusion CPU with PAA
- iOS 12 running on iPad Pro with Apple A10X Fusion CPU without PAA
- iOS 12 running on iPad Pro with Apple A12X Bionic CPU with PAA
- iOS 12 running on iPad Pro with Apple A12X Bionic CPU without PAA
- iOS 12 running on iPad Pro with Apple A9X CPU with PAA
- iOS 12 running on iPad Pro with Apple A9X CPU without PAA
- iOS 12 running on iPhone 5S with Apple A7 CPU with PAA
- iOS 12 running on iPhone 5S with Apple A7 CPU without PAA
- iOS 12 running on iPhone 6 (iPhone 6 and iPhone 6 Plus) with Apple A8 CPU with PAA
- iOS 12 running on iPhone 6 (iPhone 6 and iPhone 6 Plus) with Apple A8 CPU without PAA
- iOS 12 running on iPhone 6S (iPhone 6S and iPhone 6S Plus) with Apple A9 CPU with PAA
- iOS 12 running on iPhone 6S (iPhone 6S and iPhone 6S Plus) with Apple A9 CPU without PAA
- iOS 12 running on iPhone 7 (iPhone 7 and iPhone 7 Plus) with Apple A10 Fusion CPU with PAA
- iOS 12 running on iPhone 7 (iPhone 7 and iPhone 7 Plus) with Apple A10 Fusion CPU without PAA
- iOS 12 running on iPhone 8 (iPhone 8, iPhone 8 Plus and iPhone X) with Apple A11 Bionic CPU with PAA
- iOS 12 running on iPhone 8 (iPhone 8, iPhone 8 Plus and iPhone X) with Apple A11 Bionic CPU without PAA
- iOS 12 running on iPhone XS (iPhone XR, iPhone XS and iPhone XS Max) with Apple A12 Bionic CPU with PAA
- iOS 12 running on iPhone XS (iPhone XR, iPhone XS and iPhone XS Max) with Apple A12 Bionic CPU without PAA
- iOS 12 running on iPhone XS (iPhone XR, iPhone XS and iPhone XS Max) with Apple A12 Bionic CPU without PAA
- tvOS 12 running on Apple TV 4K with Apple A10X Fusion CPU with PAA
- tvOS 12 running on Apple TV 4K with Apple A10X Fusion CPU without PAA
- TxFW 16P374 running on Apple iMac Pro with Apple T2 with PAA
- TxFW 16P374 running on Apple iMac Pro with Apple T2 without PAA
- TxFW 16P374 running on Apple MacBook Pro with Apple T2 with PAA
- TxFW 16P374 running on Apple MacBook Pro with Apple T2 without PAA (single-user mode)
- watchOS 5 running on Apple Watch Series 1 with Apple S1P CPU with PAA
- watchOS 5 running on Apple Watch Series 1 with Apple S1P CPU without PAA
- watchOS 5 running on Apple Watch Series 3 with Apple S3 CPU with PAA
- watchOS 5 running on Apple Watch Series 3 with Apple S3 CPU without PAA
- watchOS 5 running on Apple Watch Series 4 with Apple S4 CPU with PAA
- watchOS 5 running on Apple Watch Series 4 with Apple S4 CPU without PAA

FIPS Algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Certs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>#5701, #5702, #5703, #5704, #5705, #5706, #5707, #5708, #5709, #5710, #5711, #5712, #5713, #5714, #5715, #5716, #5717, #5718, #5719, #5720, #5721, #5722, #5723, #5724, #5725, #5726, #5727, #5728, #5729, #5730, #5731, #5732, #5733, #5734, #5735, #5736, #5737, #5738, #5739, #5740, #5836, #5837, #5838, #5839, #5840, #5841, #5842, #5843, #5844, #5845, #5879, #5880, #5881, #5882, #5886, #c10, #c11, #c12, #c13, #c14, #c15, #c16, #c25, #c26, #c27, #c28, #c29, #c30, #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c105, #c106, #c107, #c145, #c146, #c148, #c239, #c240, #c241, #c242, #c243, #c245, #c246 and #c247</td>
</tr>
<tr>
<td>CVL</td>
<td>#2115, #2180, #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c107, #c148, #c239, #c242, #c243 and #c245</td>
</tr>
<tr>
<td>DRBG</td>
<td>#2312, #2313, #2314, #2315, #2316, #2317, #2318, #2319, #2320, #2321, #2322, #2323, #2324, #2325, #2326, #2327, #2328, #2329, #2330, #2331, #2332, #2333, #2334, #2335, #2429, #2430, #2431, #2432, #2433, #2434, #2443, #2444, #2445, #2449, #c13, #c16, #c29, #c30, #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c105, #c106, #c107, #c145, #c146, #c148, #c239, #c240, #c241, #c242, #c243, #c245, #c246 and #c247</td>
</tr>
<tr>
<td>DSA</td>
<td>#1481 and #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c107, #c148, #c239, #c242, #c243, #c245</td>
</tr>
<tr>
<td>ECDSA</td>
<td>#1567, #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c107, #c148, #c239, #c242, #c243, #c245</td>
</tr>
<tr>
<td>HMAC</td>
<td>#3798, #3799, #3800, #3801, #3802, #3803, #3804, #3805, #3856, #3857, #3861, #3863, #c13, #c16, #c29, #c30, #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c107, #c148, #c239, #c242, #c243 and #c245</td>
</tr>
<tr>
<td>KTS</td>
<td>AES Certs. #5701, #5702, #5703, #5704, #5705, #5706, #5707, #5716, #5836, #5841, #5879, #5886, #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c106, #c107, #c146, #c148, #c239, #c240, #c241, #c242, #c243, #c245 and #c245; key establishment methodology provides 128 bits of encryption strength</td>
</tr>
<tr>
<td>KTS</td>
<td>vendor affirmed</td>
</tr>
<tr>
<td>PBKDF</td>
<td>vendor affirmed</td>
</tr>
<tr>
<td>RSA</td>
<td>Certs. #3084, #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c107, #c148, #c239, #c242, #c243 and #c245</td>
</tr>
<tr>
<td>SHS</td>
<td>Certs. #4571, #4572, #4573, #4574, #4575, #4576, #4577, #4578, #4601, #4632, #4636, #4638, #c13, #c16, #c29, #c30, #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c107, #c148, #c239, #c242, #c243 and #c245</td>
</tr>
<tr>
<td>Triple-DES</td>
<td>Certs. #2866, #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c107, #c148, #c239, #c242, #c243 and #c245</td>
</tr>
</tbody>
</table>

Allowed Algorithms

Diffie-Hellman (CVL Certs. #2115, #c95, #c96, #c97, #c98, #c99, #c100, #c101, #c102, #c107, #c148, #c239, #c242, #c243, #c245, key agreement; key establishment methodology provides 112 or 128 bits of encryption)

Certificate Detail - Cryptographic Module Validation Program | CSRC

Software Versions

Vendor

Apple Inc.
One Apple Park Way
MS: 927-1CP5
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

Lab

ATSEC INFORMATION SECURITY CORP
NVLAP Code: 200658-0

Want updates about CSRC and our publications? Subscribe

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

Webmaster | Contact Us | Our Other Offices

PROJECTS
PUBLICATIONS
Draft Pubs
Final Pubs
FIPS
Special Publications (SPs)
NISTIRs
ITL Bulletins
White Papers
Journal Articles
Conference Papers
Books

TOPICS
Security & Privacy
Applications
Technologies
Sectors
Laws & Regulations
Activities & Products
NEWS & UPDATES
EVENTS
GLOSSARY

ABOUT CSRC
Computer Security Division
Applied Cybersecurity Division
Contact Us

Information Technology Laboratory (ITL)
Computer Security Division (CSD)
TEL: 301.975.8443
Applied Cybersecurity Division (ACD)

Contact CSRC Webmaster:
webmaster-csrc@nist.gov