Security Certifications and Compliance Center

February 2021

Contents

Introduction to Apple security assurance

As part of our commitment to security, Apple regularly engages with third-party organizations to certify and attest to the security of Apple's hardware, software, and services. These internationally recognized organizations provide Apple with certifications that align with each major operating system release. In this way, they provide a measure of confidence—that is, security assurance—that the security needs of a system are being satisfied. For technical areas that aren't accepted under mutual recognition arrangements (MRAs) or that lack mature security certification standards, Apple is engaged with developing appropriate security standards. Our mission is to drive globally accepted, comprehensive coverage of security certification across all Apple hardware, operating systems, apps, and services.

Certifications are often necessary to meet the requirements of legislation, regulation, and industry norms. Services like Apple School Manager and Apple Business Manager are covered under Apple's ISO/IEC 27001 and ISO/IEC 27018 certifications. All customers, including government agencies and enterprise and education organizations deploying Apple devices, can use the hardware, operating system, software, and services certifications to support demonstrating compliance.

Hardware certifications

Because secure software requires a foundation of security built into hardware, all Apple devices—whether running iOS, iPadOS, macOS, tvOS, or watchOS—have security capabilities designed into silicon. These include custom CPU capabilities that power system security features and silicon dedicated to security functions. The most critical component is the Secure Enclave coprocessor, which appears on all modern iOS, iPadOS, watchOS, tvOS devices, on all Mac computers with Apple silicon, and Intel-based Mac computers with the Apple T2 Security Chip. The Secure Enclave provides the foundation for encrypting data at rest, secure boot in macOS, and biometrics.

Apple's commitment to security assurance starts with the certification of the foundational security components in silicon, from the hardware root of trust, to the secure boot enforcement, to the Secure Enclave providing secure key store, to the secure authentication with Touch ID and Face ID. The security features of Apple devices are made possible by the combination of silicon design, hardware, software, and services available only from Apple. Certification of these components is an important part of verifying the assurance that Apple provides.

For information on public certifications related to hardware and associated firmware components, see:

- Security certifications for the Apple T2 Security Chip
- Security certifications for the Secure Enclave Processor

Software and app certifications

Apple maintains independent certifications and attestations over its operating system and apps in conformance with the U.S. Federal Information Processing Standards (FIPS) 140-2/-3 for cryptographic modules and Common Criteria for operating systems, apps, and device services. The coverage of operating systems includes iOS, iPadOS, macOS, sepOS, T2 firmware, tvOS, and watchOS. For apps, independent certification will initially include the Safari browser and Contacts apps, with more apps to be certified in the future.

For information on public certifications related to Apple *operating systems*, see:

- Security certifications for iOS
- Security certifications for iPadOS
- Security certifications for macOS
- Security certifications for tvOS
- Security certifications for watchOS

For information on public certifications related to Apple *apps*, see:

- Security certifications for Apple apps

Service certifications

Apple maintains security certifications to support our customers, from enterprise to education. These certifications enable Apple customers to address their regulatory and contractual obligations when using Apple services with Apple hardware and software. These certifications provide our customers with an independent attestation over Apple information security, environmental and privacy practices for Apple systems.

For information on public certifications related to Apple *internet services*, see:

- Security certifications for Apple internet services

For questions about Apple Security and Privacy Certifications, contact security-certifications@apple.com.

Hardware security certifications

Apple hardware security certifications overview

Apple maintains U.S. Federal Information Processing Standard (FIPS) 140-2/-3 Conformance Validation Certificates for sepOS and T2 firmware as well as other certifications. Apple starts with *certification building blocks* that apply broadly across multiple platforms where appropriate. One building block is the validation of corecrypto, which is used for software and hardware cryptographic module deployments within Apple developed operating systems. A second building block is the certification of the Secure Enclave, which is embedded in many Apple devices. A third is the certification of the Secure Element (SE), found in Apple devices with Touch ID and devices with Face ID. These hardware certification building blocks form a foundation for broader platform security certifications.

Cryptographic algorithm validations

Validation of the implementation correctness of many cryptographic algorithms and related security functions is a prerequisite for FIPS 140-3 validation and supportive of other certifications. Validation is managed by the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program (CAVP). Certificates of validation for Apple implementations can be found using the CAVP search facility. For more information, see the Cryptographic Algorithm Validation Program (CAVP) website.

Cryptographic module validations FIPS 140-2/3 (ISO/IEC 19790)

Apple's cryptographic modules have been repeatedly validated by the Cryptographic Module Validation Program (CMVP) as being conformant with U.S. Federal Information Processing Standard for cryptographic modules (FIPS 140-2) following each major release of the operating systems since 2012. After each major release, Apple submits the modules to the CMVP for validation of conformance with the standard. As well as being used by Apple operating systems and apps, these modules provide cryptographic functionality for Apple-provided services and are available for third-party apps to use.

Apple achieves **Security Level 1** each year for the software-based modules "Corecrypto Module for Intel" and "Corecrypto Kernel Module for Intel" for macOS. For Apple silicon, the modules "Corecrypto Module for ARM" and "Corecrypto Kernel Module for ARM" are applicable to iOS, iPadOS, tvOS, watchOS and to the firmware in the embedded Apple T2 Security Chip in Mac computers.

In 2019, Apple achieved the first FIPS 140-2 **Security Level 2** for the embedded hardware cryptographic module identified as "Apple Corecrypto Module: Secure Key Store," enabling US government approved use of the keys generated and managed in the Secure Enclave. Apple continues to pursue validations for the hardware cryptographic module with each successive major operating system release.

FIPS 140-3 was approved by the U.S. Department of Commerce in 2019. The most notable change in this version of the standard is the specification of ISO/IEC standards—in particular, ISO/IEC 19790:2015 and the associated testing standard ISO/IEC 24759:2017. The CMVP has initiated a transition program and has indicated that starting in 2020, cryptographic modules will begin to be validated using FIPS 140-3 as a basis. Apple cryptographic modules will aim to meet and transition to the FIPS 140-3 standard as soon as practicable.

For cryptographic modules currently in the testing and validation processes, the CMVP maintains two separate lists that may contain information about proposed validations. For cryptographic modules under testing with an accredited laboratory, the Implementation Under Test List may list the module. After the laboratory has completed testing and recommends validation by the CMVP, the Apple cryptographic modules appear in the Modules in Process List. Currently, the laboratory testing is complete and is waiting for validation of the testing by the CMVP. Because the length of the evaluation process can vary, look at the above two process lists to determine the current status of Apple cryptographic modules between the date of a major operating system release and the issuance of the validation certificate by the CMVP.

Product certifications (Common Criteria ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) is a standard that's used by many organizations as a basis for performing security evaluations of IT products.

For certifications that may be mutually recognized under the international Common Criteria Recognition Arrangement (CCRA), see the Common Criteria Portal. The Common Criteria standard may also be used outside the CCRA by national and private validation schemes. In Europe, mutual recognition is governed under the SOG-IS agreement as well as the CCRA.

The goal, as stated by the Common Criteria community, is for an internationally approved set of security standards to provide a clear and reliable evaluation of the security capabilities of Information Technology products. By providing an independent assessment of a product's ability to meet security standards, Common Criteria Certification gives customers more confidence in the security of Information Technology products and leads to more informed decisions.

Through the CCRA, member countries have agreed to recognize the certification of Information Technology products with the same level of confidence. Evaluations required before certification are extensive and include:

- Protection Profiles (PPs)
- Security Targets (STs)
- Security Functional Requirements (SFRs)
- Security Assurance Requirements (SARs)
- Evaluation Assurance Levels (EALs)

Protection Profiles (PPs) are documents that specify security requirements for a class of device types (such as Mobility) and are used to provide comparability between the evaluations of IT products within the same class. Membership of the CCRA, along with an increasing list of approved PPs, continues to grow on a yearly basis. This arrangement permits a product developer to pursue a single certification under any one of the certificate authorizing schemes and have it recognized by any of the certificate consuming signatories.

Security Targets (STs) define *what* will be evaluated when an IT product is being certified. The STs are translated to more specific *Security Functional Requirements (SFRs)*, used for evaluating the STs in more detail.

The Common Criteria (CC) also includes *Security Assurance Requirements*. One commonly identified metric is the *Evaluation Assurance Level (EAL)*. EALs group together frequently occurring sets of SARs and may be specified in PPs and STs to support comparability.

Many older PPs have been archived and are being replaced with targeted PPs, which are being developed and focus on specific solutions and environments. In a concerted effort to ensure continued mutual recognition across all CCRA members, international Technical Communities (iTCs) have been established to develop and maintain collaborative Protection Profiles (cPPs), which are developed from the start with involvement from CCRA signatory schemes. PPs targeted for user groups and mutual recognition arrangements other than the CCRA continue to be developed by appropriate stakeholders.

Apple began pursuing certifications under the updated CCRA with selected cPPs starting in early 2015. Since then, Apple has achieved Common Criteria certifications for each major iOS release and has expanded coverage to include the security assurance provided by new PPs.

Apple takes an active role within the technical communities focused on evaluating mobile security technologies. These include the iTCs responsible for developing and updating cPPs. Apple continues to evaluate and pursue certifications against current PPs and cPPs.

Apple platform certifications for the North America market are generally performed with the National Information Assurance Partnership (NIAP), which maintains a list of projects currently in evaluation but not yet certified.

In addition to the general platform certificates listed, other certificates have been issued in order to demonstrate specific security requirements for some markets.

Security certifications for the Apple T2 Security Chip

Cryptographic module validation background

Apple actively engages in the validation of Apple embedded software and hardware modules for each major release of an operating system. Validation of conformance can only be performed against a final module release version; the validation is formally submitted upon the public release of the operating system.

In 2020 the CMVP adopted the international standard ISO/IEC 19790 as the basis for U.S. Federal Information Processing Standard (FIPS) 140-3.

In addition to having an Intel CPU, most Mac computers since 2017 also have a separate Apple T2 Security Chip, which is an Apple silicon-based system on chip (SoC). These Mac computers use all five cryptographic modules for various on-device services.

- Corecrypto user module for Intel (used by macOS)
- Corecrypto kernel module for Intel (used by macOS)
- Corecrypto user module for ARM (used by the T2 chip)
- Corecrypto kernel module for ARM (used by the T2 chip)
- Secure Key Store Cryptographic Module (used by the embedded Secure Enclave coprocessor in the T2 chip)

Note: The Apple silicon-based modules running on the T2 chip are the same as those running on other Apple silicon, such as the Apple A series, S series, and M series.

Cryptographic module validation status

The Cryptographic Module Validation Program (CMVP) maintains the validation status of cryptographic modules under four separate lists depending on their current status:

- To be listed on the CMVP Implementation Under Test List, the laboratory must be contracted with Apple to provide testing.
- After the testing has been completed by the laboratory, the lab has recommended validation by the CMVP, and the CMVP fees have been paid, the module is then added to the Modules in Process (MIP) List. The MIP List tracks the progress of the CMVP validation efforts in four phases:
  - *Review Pending:* Waiting for CMVP resource to be assigned.
  - *In Review:* CMVP resources are performing their validation activities.
  - *Coordination:* The lab and the CMVP are resolving any issues found.
  - *Finalization:* The activities and formalities related to issuing the certificate.
- After validation by the CMVP, the modules are awarded a certificate of conformance and added to the validated cryptographic modules list.
- After 5 years or if the module certificate is revoked for some reason, the modules are moved to the "historical" list.

In 2020, the CMVP adopted the international standard ISO/IEC 19790 as the basis for FIPS 140-3.

FIPS 140-3 certifications

The table below shows the 2020 cryptographic modules that are currently being tested by the laboratory for conformance with FIPS 140-3.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, User, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Kernel, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Secure key store, Hardware, Overall Security Level 2 *Type:* Hardware *Security level:* 2

See a complete list of cryptographic modules at the NIST Computer Security Resource Center. You can see a list of modules currently being tested at the same website.

FIPS 140-2 certifications

The table below shows the cryptographic modules that are currently being tested and have been tested by the laboratory for conformance with FIPS 140-2.

Apple T2 Security Chip (2019) user space, kernel space, and secure key store have completed laboratory testing and have been recommended by the laboratory to the CMVP for validation. They are listed on the Modules in Process List.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 13, iPadOS 13, macOS 10.15 Catalina, tvOS 13, watchOS 6 *Name:* Apple Corecrypto Kernel Module v10.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 13, iPadOS 13, macOS 10.15 Catalina, tvOS 13, watchOS 6 *Name:* Apple Corecrypto User Module v10.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 13, iPadOS 13, macOS 10.15 Catalina, tvOS 13, watchOS 6 *Name:* Apple Corecrypto Secure key store Cryptographic Module v10.0 *Type:* Hardware *Security level:* 2
OS release date: 2018 *Validation dates:* 2019-04-23	*Certificates:* 3438 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 12, macOS 10.14 Mojave, tvOS 12, watchOS 5 *Name:* Apple Corecrypto User Module v9.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-04-11	*Certificates:* 3433 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 12, macOS 10.14 Mojave, tvOS 12, watchOS 5 *Name:* Apple Corecrypto Kernel Module v9.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-09-10	*Certificates:* 3523 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 12, macOS 10.14 Mojave, tvOS 12, watchOS 5 *Name:* Apple Secure key store Cryptographic Module v9.0 *Type:* Hardware *Security level:* 2

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2017 *Validation dates:* 2018-03-09, 2018-05-22, 2018-07-06	*Certificates:* 3148 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 11, macOS 10.13 High Sierra, tvOS 11, watchOS 4 *Name:* Apple Corecrypto User Module v8.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2017 *Validation dates:* 2018-03-09, 2018-05-17, 2018-07-03	*Certificates:* 3147 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 11, macOS 10.13 High Sierra, tvOS 11, watchOS 4 *Name:* Apple Corecrypto Kernel Module v8.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2017 *Validation dates:* 2018-07-10	*Certificates:* 3223 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 11, macOS 10.13 High Sierra, tvOS 11, watchOS 4 *Name:* Apple Secure key store Cryptographic Module v1.0 *Type:* Hardware *Security level:* 1

Security certifications for the Secure Enclave Processor

The Secure Enclave Processor (SEP) is a coprocessor that's fabricated within the system on chip (SoC). It uses encrypted memory and includes a hardware random number generator. The Secure Enclave provides all cryptographic operations for Data Protection key management and maintains the integrity of Data Protection even if the kernel has been compromised. Communication between the Secure Enclave and the application processor is isolated to an interrupt-driven mailbox and to shared memory data buffers.

The Secure Enclave Processor includes a dedicated Secure Enclave Boot ROM. Like the application processor Boot ROM, the Secure Enclave Boot ROM is immutable code that establishes the hardware root of trust for the Secure Enclave.

The Secure Enclave Processor runs sepOS, which is based on an Apple-customized version of the L4 microkernel. This sepOS is signed by Apple, verified by the Secure Enclave Boot ROM, and updated through a personalized software update process.

Here are some built-in services that use the hardware-protected secure key store:

- Unlock of device or account (password and biometric)
- Hardware encryption, Data Protection, FileVault (data-at-rest)
- Secure Boot (firmware and operating system trust and integrity)
- Hardware control of camera (FaceTime)

Cryptographic module validation background

The Hardware Cryptographic Module—*Apple SEP Secure Key Store Cryptographic Module*—comes embedded in the Apple SOC that's in the following products: The Apple A series for iPhone and iPad, the M series for Mac computers with Apple silicon, the S series for the Apple Watch, and the T series security chip found in Mac computers starting with iMac Pro introduced in 2017.

Apple will pursue U.S. Federal Information Processing Standard (FIPS) 140-2/-3 Security Level 3 for the SEP Secure Key Store Cryptographic Module used by future operating system releases and devices.

In 2019, Apple validated the hardware module against the FIPS 140-2 Security Level 2 requirements and updated the module version identifier to v9.0 to sync with the versions of the corresponding corecrypto User and corecrypto Kernel module validations. In 2019, this included iOS 12, macOS 10.14, tvOS 12, and watchOS 5.

In 2018, Apple synced with the validation of the software cryptographic modules with the operating systems released in 2017: iOS 11, macOS 10.13, tvOS 11, and watchOS 4. The SEP hardware cryptographic module identified as the Apple SEP Secure Key Store Cryptographic Module v1.0 was initially validated against FIPS 140-2 Security Level 1 requirements.

Apple also actively engages in the validation of the corecrypto User and corecrypto Kernel modules for each major release of an operating system. Validation of conformance can only be performed against a final module release version; the validation is formally submitted upon the public release of the operating system.

Cryptographic module validation status

The Cryptographic Module Validation Program (CMVP) maintains the validation status of cryptographic modules under four separate lists depending on their current status:

- To be listed on the CMVP Implementation Under Test List, the laboratory must be contracted with Apple to provide testing.
- After the testing has been completed by the laboratory, the lab has recommended validation by the CMVP, and the CMVP fees have been paid, the module is then added to the Modules in Process List. The MIP List tracks the progress of the CMVP validation efforts in four phases:
  - *Review Pending:* Waiting for CMVP resource to be assigned.
  - *In Review:* CMVP resources are performing their validation activities.
  - *Coordination:* The lab and the CMVP are resolving any issues found.
  - *Finalization:* The activities and formalities related to issuing the certificate.
- After validation by the CMVP, the modules are awarded a certificate of conformance and added to the validated cryptographic modules list.
- After 5 years or if the module certificate is revoked for some reason, the modules are moved to the "historical" list.

In 2020, the CMVP adopted the international standard ISO/IEC 19790 as the basis for FIPS 140-3.

FIPS 140-3 certifications

The table below shows the 2020 cryptographic modules that are currently being tested by the laboratory for conformance with FIPS 140-3.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Secure key store, Hardware, Overall Security Level 2 *Type:* Hardware *Security level:* 2

See a complete list of cryptographic modules at the NIST Computer Security Resource Center. You can see a list of modules currently being tested at the same website.

FIPS 140-2 certifications

The table below shows the cryptographic modules that are currently being tested and have been tested by the laboratory for conformance with FIPS 140-2.

2019 operating system releases' Secure Key Store cryptographic module has completed laboratory testing and has been recommended by the laboratory to the CMVP for validation. They are listed on the Modules in Process List. After the CMVP validation has been successfully completed, the CMVP will list them on the validated cryptographic modules list.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 13, macOS 10.15 Catalina, tvOS 13, watchOS 6 *Name:* Apple Secure Key Store Cryptographic Module v10.0 *Type:* Hardware *Security level:* 2
OS release date: 2018 *Validation dates:* 2019-09-10	*Certificates:* 3523 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 12, macOS 10.14 Mojave, tvOS 12, watchOS 5 *Name:* Apple Secure Key Store Cryptographic Module v9.0 *Type:* Hardware *Security level:* 2
OS release date: 2017 *Validation dates:* 2018-07-10	*Certificates:* 3223 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 11, macOS 10.13 High Sierra, tvOS 11, watch OS 4 *Name:* Apple Secure Key Store Cryptographic Module v1.0 *Type:* Hardware *Security level:* 1

Operating system security certifications

Apple operating system security certifications overview

Apple maintains U.S. Federal Information Processing Standard (FIPS) 140-2/-3 Conformance Validation Certificates for sepOS and T2 firmware as well as other certifications. Apple starts with *certification building blocks* that apply broadly across multiple platforms where appropriate. One building block is the validation of corecrypto, which is used for software and hardware cryptographic module deployments within Apple developed operating systems. A second building block is the certification of the Secure Enclave, which is embedded in many Apple devices. A third is the certification of the Secure Element (SE), found in Apple devices with Touch ID and devices with Face ID. These hardware certification building blocks form a foundation for broader platform security certifications.

Cryptographic algorithm validations

Validation of the implementation correctness of many cryptographic algorithms and related security functions is a prerequisite for FIPS 140-3 validation and supportive of other certifications. Validation is managed by the NIST Cryptographic Algorithm Validation Program (CAVP). Certificates of validation for Apple implementations can be found using the CAVP search facility.

Cryptographic module validations FIPS 140-2/3 (ISO/IEC 19790)

The cryptographic modules in Apple operating systems have been repeatedly validated by the Cryptographic Module Validation Program (CMVP) as being conformant with U.S. Federal Information Processing Standards (FIPS) 140-2 following each major release of the operating systems since 2012. After each major release, Apple submits all modules to the CMVP for full cryptographic validation. These validated modules provide cryptographic operations for Apple provided services and are available for third-party apps to use.

Apple achieves **Security Level 1** each year for the software-based modules “Corecrypto Module for Intel” and “Corecrypto Kernel Module for Intel” for macOS. For Apple silicon, the modules “Corecrypto Module for ARM” and “Corecrypto Kernel Module for ARM” are applicable to iOS, iPadOS, tvOS, watchOS and to the firmware in the embedded Apple T2 Security Chip in Mac computers.

In 2019, Apple achieved the first FIPS 140-2 **Security Level 2** for the embedded hardware cryptographic module identified as "Apple Corecrypto Module: Secure Key Store," enabling US government approved use of the keys generated and managed in the Secure Enclave. Apple continues to pursue validations for the hardware cryptographic module with each successive major operating system release.

FIPS 140-3 was approved by the U.S. Department of Commerce in 2019. The most notable change in this version of the standard is the specification of ISO/IEC standards—in particular, ISO/IEC 19790:2015 and the associated testing standard ISO/IEC 24759:2017. The CMVP has initiated a transition program and has indicated that starting in 2020, cryptographic modules will begin to be validated using FIPS 140-3 as a basis. Apple cryptographic modules will aim to meet and transition to the FIPS 140-3 standard as soon as practicable.

For cryptographic modules currently in the testing and validation processes, the CMVP maintains two separate lists that may contain information about proposed validations. For cryptographic modules under testing with an accredited laboratory, the Implementation Under Test List may list the module. After the laboratory has completed testing and recommends validation by the CMVP, the Apple cryptographic modules appear in the Modules in Process List. Currently, the laboratory testing is complete and is waiting for validation of the testing by the CMVP. Because the length of the evaluation process can vary, look at the above two process lists to determine the current status of Apple cryptographic modules between the date of a major operating system release and the issuance of the validation certificate by the CMVP.

Product certifications (Common Criteria ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) is a standard that's used by many organizations as a basis for performing security evaluations of IT products.

For certifications that may be mutually recognized under the international Common Criteria Recognition Arrangement (CCRA), see the Common Criteria Portal. The Common Criteria standard may also be used outside the CCRA by national and private validation schemes. In Europe, mutual recognition is governed under the SOG-IS agreement as well as the CCRA.

The goal, as stated by the Common Criteria community, is for an internationally approved set of security standards to provide a clear and reliable evaluation of the security capabilities of Information Technology products. By providing an independent assessment of a product's ability to meet security standards, Common Criteria Certification gives customers more confidence in the security of Information Technology products and leads to more informed decisions.

Through the CCRA, member countries have agreed to recognize the certification of Information Technology products with the same level of confidence. Evaluations required before certification are extensive and include:

- Protection Profiles (PPs)
- Security Targets (STs)
- Security Functional Requirements (SFRs)
- Security Assurance Requirements (SARs)
- Evaluation Assurance Levels (EALs)

Protection Profiles (PPs) are documents that specify security requirements for a class of device types (such as Mobility) and are used to provide comparability between the evaluations of IT products within the same class. Membership of the CCRA, along with an increasing list of approved PPs, continues to grow on a yearly basis. This arrangement permits a product developer to pursue a single certification under any one of the certificate authorizing schemes and have it recognized by any of the certificate consuming signatories.

Security Targets (STs) define *what* will be evaluated when an IT product is being certified. The STs are translated to more specific *Security Functional Requirements (SFRs)*, used for evaluating the STs in more detail.

The Common Criteria (CC) also includes *Security Assurance Requirements*. One commonly identified metric is the *Evaluation Assurance Level (EAL)*. EALs group together frequently occurring sets of SARs and may be specified in PPs and STs to support comparability.

Many older PPs have been archived and are being replaced with targeted PPs, which are being developed and focus on specific solutions and environments. In a concerted effort to ensure continued mutual recognition across all CCRA members, international Technical Communities (iTCs) have been established to develop and maintain *collaborative Protection Profiles (cPPs)*, which are developed from the start with involvement from CCRA signatory schemes. PPs targeted for user groups and mutual recognition arrangements other than the CCRA continue to be developed by appropriate stakeholders.

Apple began pursuing certifications under the updated CCRA with selected cPPs starting in early 2015. Since then, Apple has achieved Common Criteria certifications for each major iOS release and has expanded coverage to include the security assurance provided by new PPs.

Apple takes an active role within the technical communities focused on evaluating mobile security technologies. These include the iTCs responsible for developing and updating cPPs. Apple continues to evaluate and pursue certifications against current PPs and cPPs.

Apple platform certifications for the North America market are generally performed with the National Information Assurance Partnership (NIAP), which maintains a list of projects currently in evaluation but not yet certified.

In addition to the general platform certificates listed, other certificates have been issued in order to demonstrate specific security requirements for some markets.

Security certifications for iOS

iOS cryptographic module validation background

Apple actively engages in the validation of Apple embedded software and hardware modules for each major release of an operating system. Validation of conformance can only be performed against a final module release version; the validation is formally submitted upon the public release of the operating system.

iOS cryptographic module validation status

The Cryptographic Module Validation Program (CMVP) maintains the validation status of cryptographic modules under four separate lists depending on their current status:

- To be listed on the CMVP Implementation Under Test List, the laboratory must be contracted with Apple to provide testing.
- After the testing has been completed by the laboratory, the lab has recommended validation by the CMVP, and the CMVP fees have been paid, the module is then added to the Modules in Process List. The MIP List tracks the progress of the CMVP validation efforts in four phases:
  - *Review Pending:* Waiting for CMVP resource to be assigned.
  - *In Review:* CMVP resources are performing their validation activities.
  - *Coordination:* The lab and the CMVP are resolving any issues found.
  - *Finalization:* The activities and formalities related to issuing the certificate.
- After validation by the CMVP, the modules are awarded a certificate of conformance and added to the validated cryptographic modules list.
- After 5 years or if the module certificate is revoked for some reason, the modules are moved to the "historical" list.

In 2020, the CMVP adopted the international standard ISO/IEC 19790 as the basis for FIPS 140-3.

FIPS 140-3 certifications

The table below shows the 2020 cryptographic modules for iOS that are currently being tested by the laboratory for conformance with FIPS 140-3.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* iOS 14 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, User, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* iOS 14 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Kernel, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Secure key store, Hardware, Overall Security Level 2 *Type:* Hardware *Security level:* 2

See a complete list of cryptographic modules at the NIST Computer Security Resource Center. You can see a list of modules currently being tested at the same website.

FIPS 140-2 certifications

The table below shows the cryptographic modules that are currently being tested and have been tested by the laboratory for conformance with FIPS 140-2.

iOS 13 (2019) user space, kernel space, and secure key store have completed laboratory testing and have been recommended by the laboratory to the CMVP for validation. They are listed on the Modules in Process List.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* iOS 13 *Name:* Apple Corecrypto User Module v10.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* iOS 13 *Name:* Apple Corecrypto Kernel Module v10.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 13, macOS 10.15 Catalina, tvOS 13, watchOS 6 *Name:* Apple Secure Key Store Cryptographic Module v10.0 *Type:* Hardware *Security level:* 2
OS release date: 2018 *Validation dates:* 2019-04-23	*Certificates:* 3438 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 12 *Name:* Apple Corecrypto Kernel Module v9.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-04-11	*Certificates:* 3433 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 12 *Name:* Apple Corecrypto User Module v9.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-9-10	*Certificates:* 3523 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 12, macOS 10.14 Mojave, tvOS 12, watchOS 5 *Name:* Apple Secure Key Store Cryptographic Module v9.0 *Type:* Hardware *Security level:* 2
OS release date: 2017 *Validation dates:* 2018-03-09, 2018-05-22, 2018-07-06	*Certificates:* 3148 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 11 *Name:* Apple Corecrypto User Module v8.0 for ARM *Type:* Software *Security level:* 1

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2017 *Validation dates:* 2018-03-09, 2018-05-17, 2018-07-03	*Certificates:* 3147 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 11 *Name:* Apple Corecrypto Kernel Module v8.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2017 *Validation dates:* 2019-09-10	*Certificates:* 3223 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 11, macOS 10.13 High Sierra, tvOS 11, watchOS 4 *Name:* Apple Secure Key Store Cryptographic Module v1.0 *Type:* Hardware *Security level:* 2
OS release date: 2016 *Validation dates:* 2017-02-01	*Certificates:* 2828 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 10 *Name:* Apple iOS Corecrypto Kernel Module v7.0 *Type:* Software *Security level:* 1
OS release date: 2016 *Validation dates:* 2017-02-01	*Certificates:* 2827 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 10 *Name:* Apple iOS Corecrypto Kernel Module v7.0 *Type:* Software *Security level:* 1

Previous versions

These previous iOS versions had cryptographic module validations. Those greater than 5 years old are listed by the CMVP with historical status:

- iOS 9 (corecrypto modules v6.0)
- iOS 8 (corecrypto modules v5.0)
- iOS 7 (corecrypto modules v4.0)
- iOS 6 (corecrypto modules v3.0)

Common Criteria (CC) certification background

Apple actively engages in the evaluation of iOS for each major release of the operating system. Evaluation can only be performed against a final publicly released version of the operating system. Prior to iPadOS 13.1, iPadOS was named iOS.

Common Criteria (CC) certification status

The U.S. scheme, operated by NIAP, maintains a list of Products in Evaluation; this list includes products that are currently undergoing evaluation in the United States with a NIAP-approved Common Criteria Testing Laboratory (CCTL) and that have completed an Evaluation Kickoff Meeting (or equivalent) in which CCEVS management officially accepts the product into evaluation.

After products are certified, NIAP puts currently valid certifications on its Product Compliant list. After 2 years, these certifications are reviewed for conformance with the current assurance maintenance policy. After the assurance maintenance date has expired, NIAP moves the certification listing to its Archived Products list.

The Common Criteria Portal lists certifications that can be mutually recognized under the Common Criteria Recognition Arrangement (CCRA). The CC Portal may maintain products on the certified product list for 5 years; records are kept by the CC Portal for archived certifications.

The table below shows the certifications that are currently being evaluated by a laboratory, or that have been certified as conforming with Common Criteria.

Laboratory testing for evaluations with NIAP for iOS 14 (iPhone and iPad mobile device/ VPN/Wireless/MDM Agent) are under way. For more information, see Products in evaluation (NIAP).

Operating system / Certification date	Scheme ID / Documents	Title / Protection Profiles
Operating system: iOS 13 *Certification date:* 2020-11-06	*Scheme ID:* 11036 *Documents:* Certificate, Security Target, Guidance, Validation Report, Assurance Activity Report	*Title:* Apple iOS 13 on iPhone *Protection Profiles:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP
Operating system: iOS 12 *Certification date:* 2019-03-14	*Scheme ID:* 10937 *Documents:* Certificate, Security Target, Guidance, Validation Report, Assurance Activity Report	*Title:* iPhone with iOS 12 *Protection Profiles:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP

Previous versions

These previous iOS versions had Common Criteria validations. They are archived by NIAP according to the NIAP policy:

- iOS 11 (Scheme ID: 10851)
- iOS 10 (Scheme ID: 107782, 10792)
- iOS 9 (Scheme ID: 10725, 10714, 10695)

Security certifications for iPadOS

iPadOS cryptographic module validation background

Apple actively engages in the validation of Apple embedded software and hardware modules for each major release of an operating system. Validation of conformance can only be performed against a final module release version; the validation is formally submitted upon the public release of the operating system.

Note: In 2019, the operating system for iPad devices was rebranded as iPadOS.

iPadOS cryptographic module validation status

The Cryptographic Module Validation Program (CMVP) maintains the validation status of cryptographic modules under four separate lists depending on their current status:

- To be listed on the CMVP Implementation Under Test List, the laboratory must be contracted with Apple to provide testing.
- After the testing has been completed by the laboratory, the lab has recommended validation by the CMVP, and the CMVP fees have been paid, the module is then added to the Modules in Process List. The MIP List tracks the progress of the CMVP validation efforts in four phases:
  - *Review Pending:* Waiting for CMVP resource to be assigned.
  - *In Review:* CMVP resources are performing their validation activities.
  - *Coordination:* The lab and the CMVP are resolving any issues found.
  - *Finalization:* The activities and formalities related to issuing the certificate.
- After validation by the CMVP, the modules are awarded a certificate of conformance and added to the validated cryptographic modules list.
- After 5 years or if the module certificate is revoked for some reason, the modules are moved to the "historical" list.

In 2020, the CMVP adopted the international standard ISO/IEC 19790 as the basis for FIPS 140-3.

FIPS 140-3 certifications

The table below shows the 2020 cryptographic modules for iPadOS that are currently being tested by the laboratory for conformance with FIPS 140-3.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* iPadOS 14 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, User, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* iPadOS 14 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Kernel, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 14, iPad OS 14, macOS 11 Big Sur, tvOS 14, watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Secure key store, Hardware, Overall Security Level 2 *Type:* Hardware *Security level:* 2

See a complete list of cryptographic modules at the NIST Computer Security Resource Center. You can see a list of modules currently being tested at the same website.

FIPS 140-2 certifications

The table below shows the cryptographic modules that are currently being tested and have been tested by the laboratory for conformance with FIPS 140-2.

iPadOS 13 (2019) user space, kernel space, and secure key store have completed laboratory testing and have been recommended by the laboratory to the CMVP for validation. They are listed on the Modules in Process List.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* iPadOS 13 *Name:* Apple Corecrypto User Module v10.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* iPadOS 13 *Name:* Apple Corecrypto Kernel Module v10.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 13, iPadOS 13, macOS 10.15 Catalina, tvOS 13, watchOS 6 *Name:* Apple Secure Key Store Cryptographic Module v10.0 *Type:* Hardware *Security level:* 2
OS release date: 2018 *Validation dates:* 2019-04-23	*Certificates:* 3438 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 12 *Name:* Apple Corecrypto Kernel Module v9.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-04-11	*Certificates:* 3433 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 12 *Name:* Apple Corecrypto User Module v9.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-9-10	*Certificates:* 3523 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 12, macOS 10.14 Mojave, tvOS 12, watchOS 5 *Name:* Apple Secure Key Store Cryptographic Module v9.0 *Type:* Hardware *Security level:* 2
OS release date: 2017 *Validation dates:* 2018-03-09, 2018-05-22, 2018-07-06	*Certificates:* 3148 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 11 *Name:* Apple Corecrypto User Module v8.0 for ARM *Type:* Software *Security level:* 1

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2017 *Validation dates:* 2018-03-09, 2018-05-17, 2018-07-03	*Certificates:* 3147 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 11 *Name:* Apple Corecrypto Kernel Module v8.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2017 *Validation dates:* 2019-09-10	*Certificates:* 3223 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* iOS 11, macOS 10.13 High Sierra, tvOS 11, watchOS 4 *Name:* Apple Secure Key Store Cryptographic Module v1.0 *Type:* Hardware *Security level:* 2
OS release date: 2016 *Validation dates:* 2017-02-01	*Certificates:* 2828 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 10 *Name:* Apple iOS Corecrypto Kernel Module v7.0 *Type:* Software *Security level:* 1
OS release date: 2016 *Validation dates:* 2017-02-01	*Certificates:* 2827 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* iOS 10 *Name:* Apple iOS Corecrypto Kernel Module v7.0 *Type:* Software *Security level:* 1

Previous versions

These previous iOS versions had cryptographic module validations. Those greater than 5 years old are listed by the CMVP with historical status:

- iOS 9 (corecrypto modules v6.0)
- iOS 8 (corecrypto modules v5.0)
- iOS 7 (corecrypto modules v4.0)
- iOS 6 (corecrypto modules v3.0)

Common Criteria (CC) certification background

Apple actively engages in the evaluation of iOS for each major release of the operating system. Evaluation can only be performed against a final publicly released version of the operating system. Prior to iPadOS 13.1, iPadOS was named iOS.

Common Criteria (CC) certification status

The U.S. scheme, operated by NIAP, maintains a list of Products in Evaluation; this list includes products that are currently undergoing evaluation in the United States with a NIAP-approved Common Criteria Testing Laboratory (CCTL) and that have completed an Evaluation Kickoff Meeting (or equivalent) in which CCEVS management officially accepts the product into evaluation.

After products are certified, NIAP puts currently valid certifications on its Product Compliant list. After 2 years, these certifications are reviewed for conformance with the current assurance maintenance policy. After the assurance maintenance date has expired, NIAP moves the certification listing to its Archived Products list.

The Common Criteria Portal lists certifications that can be mutually recognized under the Common Criteria Recognition Arrangement (CCRA). The CC Portal may maintain products on the certified product list for 5 years; records are kept by the CC Portal for archived certifications.

The table below shows the certifications that are currently being evaluated by a laboratory, or that have been certified as conforming with Common Criteria.

Laboratory testing for evaluations with NIAP for iPadOS 14 (iPad mobile device/VPN/Wireless/MDM Agent) is under way. For more information, see Products in evaluation (NIAP).

Operating system / Certification date	Scheme ID / Documents	Title / Protection Profiles
Operating system: iPadOS 13 *Certification date:* 2020-11-06	*Scheme ID:* 11036 *Documents:* Certificate, Security Target, Guidance, Validation Report, Assurance Activity Report	*Title:* iPadOS 13 on iPad Mobile Devices *Protection Profiles:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP
Operating system: iOS 12 *Certification date:* 2019-03-14	*Scheme ID:* 10937 *Documents:* Certificate, Security Target, Guidance, Validation Report, Assurance Activity Report	*Title:* iPad with iOS 12 *Protection Profiles:* Mobile Device Fundamentals, VPN Client module, Wireless LAN client EP, MDM Agent EP

Previous versions

These previous iOS versions had Common Criteria validations. They are archived by NIAP according to the NIAP policy:

- iOS 11 (Scheme ID: 10851)
- iOS 10 (Scheme ID: 107782, 10792)
- iOS 9 (Scheme ID: 10725, 10714, 10695)

Security certifications for macOS

macOS cryptographic module validation background

Apple actively engages in the validation of Apple embedded software and hardware modules for each major release of an operating system. Validation of conformance can only be performed against a final module release version; the validation is formally submitted upon the public release of the operating system.

macOS cryptographic module validation status

The Cryptographic Module Validation Program (CMVP) maintains the validation status of cryptographic modules under four separate lists depending on their current status:

- To be listed on the CMVP Implementation Under Test List, the laboratory must be contracted with Apple to provide testing.
- After the testing has been completed by the laboratory, the lab has recommended validation by the CMVP, and the CMVP fees have been paid, the module is then added to the Modules in Process List. The MIP List tracks the progress of the CMVP validation efforts in four phases:
  - *Review Pending:* Waiting for CMVP resource to be assigned.
  - *In Review:* CMVP resources are performing their validation activities.
  - *Coordination:* The lab and the CMVP are resolving any issues found.
  - *Finalization:* The activities and formalities related to issuing the certificate.
- After validation by the CMVP, the modules are awarded a certificate of conformance and added to the validated cryptographic modules list.
- After 5 years or if the module certificate is revoked for some reason, the modules are moved to the "historical" list.

In 2020, the CMVP adopted the international standard ISO/IEC 19790 as the basis for FIPS 140-3.

FIPS 140-3 certifications

In 2020, Apple released Mac computers that are based on Apple silicon. The applicability of cryptographic modules to either Apple silicon or Intel-based Mac computers are indicated in column 3 in the table below.

Note: Apple T2 Security chips are included in many Intel-based Mac computers. For information about T2 chip certifications see Security certifications for the Apple T2 Security Chip.

The table below shows the 2020 cryptographic modules for macOS that are currently being tested by the laboratory for conformance with FIPS 140-3.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* macOS 11 Big Sur on Apple silicon *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, User, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* macOS 11 Big Sur on Apple silicon *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Kernel, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* macOS 11 Big Sur on Intel *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, User, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* macOS 11 Big Sur on Intel *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Kernel, Software *Type:* Software *Security level:* 1

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 14, iPad OS 14, macOS 11 Big Sur on Apple silicon, macOS 11 Big Sur on Intel, tvOS 14, watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Secure key store, Hardware *Type:* Hardware *Security level:* 2

See a complete list of cryptographic modules at the NIST Computer Security Resource Center. You can see a list of modules currently being tested at the same website.

FIPS 140-2 certifications

The table below shows the cryptographic modules that are currently being tested and have been tested by the laboratory for conformance with FIPS 140-2.

macOS 10.15 Catalina user space, kernel space, and secure key store have completed laboratory testing and have been recommended by the laboratory to the CMVP for validation. They are listed on the Modules in Process List.

Note: Apple T2 Security chips are included in many Intel-based Mac computers. For information about T2 chip certifications see Security certifications for the Apple T2 Security Chip.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* macOS 10.15 Catalina *Name:* Apple Corecrypto User Module v10.0 for Intel *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* macOS 10.15 Catalina *Name:* Apple Corecrypto Kernel Module v10.0 for Intel *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-04-12	*Certificates:* 3431 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* macOS 10.14 Mojave *Name:* Apple Corecrypto Kernel Module v9.0 for Intel *Type:* Software *Security level:* 1

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2018 *Validation dates:* 2019-04-12	*Certificates:* 3402 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* macOS 10.14 Mojave *Name:* Apple Corecrypto User Module v9.0 for Intel *Type:* Software *Security level:* 1
OS release date: 2017 *Validation dates:* 2018-03-22	*Certificates:* 3516 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* macOS 10.13 High Sierra *Name:* Apple Corecrypto Kernel Module v8.0 for Intel *Type:* Software *Security level:* 1
OS release date: 2017 *Validation dates:* 2018-03-22	*Certificates:* 3155 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* macOS 10.13 High Sierra *Name:* Apple Corecrypto User Module v8.0 for Intel *Type:* Software *Security level:* 1

Previous versions

These previous OS X and macOS versions had cryptographic module validations. Those greater than 5 years old are listed by the CMVP with historical status:

- macOS Sierra 10.12
- OS X El Capitan 10.11
- OS X Yosemite 10.10
- OS X Mavericks 10.9
- OS X Mountain Lion 10.8
- OS X Lion 10.7
- OS X Snow Leopard 10.6

Common Criteria (CC) certification background

Apple actively engages in the evaluation of macOS for each major release of the operating system. Evaluation can only be performed against a final publicly released version of the operating system.

Common Criteria (CC) certification status

The U.S. scheme, operated by NIAP, maintains a list of Products in Evaluation; this list includes products that are currently undergoing evaluation in the United States with a NIAP-approved Common Criteria Testing Laboratory (CCTL) and that have completed an Evaluation Kickoff Meeting (or equivalent) in which CCEVS management officially accepts the product into evaluation.

After products are certified, NIAP puts currently valid certifications on its Product Compliant list. After 2 years, these certifications are reviewed for conformance with the current assurance maintenance policy. After the assurance maintenance date has expired, NIAP moves the certification listing to its Archived Products list.

The Common Criteria Portal lists certifications that can be mutually recognized under the Common Criteria Recognition Arrangement (CCRA). The CC Portal may maintain products on the certified product list for 5 years; records are kept by the CC Portal for archived certifications.

The table below shows the certifications that are currently being evaluated by a laboratory, or that have been certified as conforming with Common Criteria.

Evaluations with NIAP for macOS evaluations using the General Purpose Operating System and Full Disk Encryption (FDE) (AA and EE) Protection Profiles are under way. For more information, see Products in evaluation (NIAP).

Operating system / Certification date	Scheme ID / Documents	Title / Protection Profiles
Operating system: macOS Catalina 10.15 *Certification date:* 2020-09-23	*Scheme ID:* 11077 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Title:* macOS 10.15 *Protection Profiles:* PP_OS_V4.21

Security certifications for tvOS

tvOS cryptographic module validation background

All Apple FIPS 140-2/-3 Conformance Validation Certificates are on the CMVP website. Apple actively engages in the validation of Apple embedded software and hardware modules for each major release of an operating system. Validation of conformance can only be performed against a final module release version; the validation is formally submitted upon the public release of the operating system.

tvOS cryptographic module validation status

The Cryptographic Module Validation Program (CMVP) maintains the validation status of cryptographic modules under four separate lists depending on their current status:

- To be listed on the CMVP Implementation Under Test List, the laboratory must be contracted with Apple to provide testing.
- After the testing has been completed by the laboratory, the lab has recommended validation by the CMVP, and the CMVP fees have been paid, the module is then added to the Modules in Process List. The MIP List tracks the progress of the CMVP validation efforts in four phases:
  - *Review Pending:* Waiting for CMVP resource to be assigned.
  - *In Review:* CMVP resources are performing their validation activities.
  - *Coordination:* The lab and the CMVP are resolving any issues found.
  - *Finalization:* The activities and formalities related to issuing the certificate.
- After validation by the CMVP, the modules are awarded a certificate of conformance and added to the validated cryptographic modules list.
- After 5 years or if the module certificate is revoked for some reason, the modules are moved to the "historical" list.

In 2020, the CMVP adopted the international standard ISO/IEC 19790 as the basis for FIPS 140-3.

FIPS 140-3 certifications

The table below shows the 2020 cryptographic modules for tvOS that are currently being tested by the laboratory for conformance with FIPS 140-3.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* tvOS 14 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, User, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* tvOS 14 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Kernel, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 14, iPad OS 14, macOS 11 Big Sur, tvOS 14, watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Secure key store, Hardware, Overall Security Level 2 *Type:* Hardware *Security level:* 2

See a complete list of cryptographic modules at the NIST Computer Security Resource Center. You can see a list of modules currently being tested at the same website.

FIPS 140-2 certifications

The table below shows the cryptographic modules that are currently being tested and have been tested by the laboratory for conformance with FIPS 140-2.

tvOS 13 (2019) user space, kernel space, and secure key store have completed laboratory testing and have been recommended by the laboratory to the CMVP for validation. They are listed on the Modules in Process List.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* tvOS 13 *Name:* Apple Corecrypto User Module v10.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* tvOS 13 *Name:* Apple Corecrypto Kernel Module v10.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating systems:* iOS 13, iPadOS 13, macOS 10.15 Catalina, tvOS 13, watchOS 6 *Name:* Apple Secure Key Store Cryptographic Module v10.0 *Type:* Hardware *Security level:* 2
OS release date: 2018 *Validation dates:* 2019-04-23	*Certificates:* 3438 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* tvOS 12 *Name:* Apple Corecrypto Kernel Module v9.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-04-11	*Certificates:* 3433 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* tvOS 12 *Name:* Apple Corecrypto User Module v9.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-9-10	*Certificates:* 3523 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* tvOS 12, macOS 10.14 Mojave, tvOS 12, watchOS 5 *Name:* Apple Secure Key Store Cryptographic Module v9.0 *Type:* Hardware *Security level:* 2
OS release date: 2017 *Validation dates:* 2018-03-09, 2018-05-22, 2018-07-06	*Certificates:* 3148 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* tvOS 11 *Name:* Apple Corecrypto User Module v8.0 for ARM *Type:* Software *Security level:* 1

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2017 *Validation dates:* 2018-03-09, 2018-05-17, 2018-07-03	*Certificates:* 3147 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* tvOS 11 *Name:* Apple Corecrypto Kernel Module v8.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2017 *Validation dates:* 2019-09-10	*Certificates:* 3223 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* tvOS 11 *Name:* Apple Secure Key Store Cryptographic Module v1.0 *Type:* Hardware *Security level:* 1

Security certifications for watchOS

watchOS cryptographic module validation background

All Apple FIPS 140-2/-3 Conformance Validation Certificates are on the CMVP website. Apple actively engages in the validation of Apple embedded software and hardware modules for each major release of an operating system. Validation of conformance can only be performed against a final module release version; the validation is formally submitted upon the public release of the operating system.

watchOS cryptographic module validation status

The Cryptographic Module Validation Program (CMVP) maintains the validation status of cryptographic modules under four separate lists depending on their current status:

- To be listed on the CMVP Implementation Under Test List, the laboratory must be contracted with Apple to provide testing.
- After the testing has been completed by the laboratory, the lab has recommended validation by the CMVP, and the CMVP fees have been paid, the module is then added to the Modules in Process List. The MIP List tracks the progress of the CMVP validation efforts in four phases:
  - *Review Pending:* Waiting for CMVP resource to be assigned.
  - *In Review:* CMVP resources are performing their validation activities.
  - *Coordination:* The lab and the CMVP are resolving any issues found.
  - *Finalization:* The activities and formalities related to issuing the certificate.
- After validation by the CMVP, the modules are awarded a certificate of conformance and added to the validated cryptographic modules list.
- After 5 years or if the module certificate is revoked for some reason, the modules are moved to the "historical" list.

In 2020, the CMVP adopted the international standard ISO/IEC 19790 as the basis for FIPS 140-3.

FIPS 140-3 certifications

The table below shows the 2020 cryptographic modules for watchOS 7 that are currently being tested by the laboratory for conformance with FIPS 140-3.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, User, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Kernel, Software *Type:* Software *Security level:* 1
OS release date: 2020 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* watchOS 7 *Name:* Apple Corecrypto Module v11.1 *Environment:* Apple silicon, Secure key store, Hardware, Overall Security Level 2 *Type:* Hardware *Security level:* 2

See a complete list of cryptographic modules at the NIST Computer Security Resource Center. You can see a list of modules currently being tested at the same website.

FIPS 140-2 certifications

The table below shows the cryptographic modules that are currently being tested and have been tested by the laboratory for conformance with FIPS 140-2.

watchOS 6 (2019) user space, kernel space, and secure key store have completed laboratory testing and have been recommended by the laboratory to the CMVP for validation. They are listed on the Modules in Process List.

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* watchOS 6 *Name:* Apple Corecrypto User Module v10.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* watchOS 6 *Name:* Apple Corecrypto Kernel Module v10.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2019 *Validation dates:* —	*Certificates:* — *Documents:* —	*Operating system:* watchOS 6 *Name:* Apple Secure Key Store Cryptographic Module v10.0 *Type:* Hardware *Security level:* 2
OS release date: 2018 *Validation dates:* 2019-04-23	*Certificates:* 3438 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* watchOS 5 *Name:* Apple Corecrypto Kernel Module v9.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-04-11	*Certificates:* 3433 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* watchOS 5 *Name:* Apple Corecrypto User Module v9.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2018 *Validation dates:* 2019-9-10	*Certificates:* 3523 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* watchOS 5 *Name:* Apple Secure Key Store Cryptographic Module v9.0 *Type:* Hardware *Security level:* 2
OS release date: 2017 *Validation dates:* 2018-03-09, 2018-05-22, 2018-07-06	*Certificates:* 3148 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* watchOS 4 *Name:* Apple Corecrypto User Module v8.0 for ARM *Type:* Software *Security level:* 1

Dates	Certificates / Documents	Operating systems / Module info
OS release date: 2017 *Validation dates:* 2018-03-09, 2018-05-17, 2018-07-03	*Certificates:* 3147 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating system:* watchOS 4 *Name:* Apple Corecrypto Kernel Module v8.0 for ARM *Type:* Software *Security level:* 1
OS release date: 2017 *Validation dates:* 2019-09-10	*Certificates:* 3223 *Documents:* Certificate, Security Policy, Crypto Officer Guidance	*Operating systems:* watchOS 4 *Name:* Apple Secure Key Store Cryptographic Module v1.0 *Type:* Hardware *Security level:* 1

Software security certifications

Apple software security certifications overview

Apple maintains U.S. Federal Information Processing Standard (FIPS) 140-2/-3 Conformance Validation Certificates for sepOS and T2 firmware as well as other certifications. Apple starts with *certification building blocks* that apply broadly across multiple platforms where appropriate. One building block is the validation of corecrypto, which is used for software and hardware cryptographic module deployments within Apple developed operating systems. A second building block is the certification of the Secure Enclave, which is embedded in many Apple devices. A third is the certification of the Secure Element (SE), found in Apple devices with Touch ID and devices with Face ID. These hardware certification building blocks form a foundation for broader platform security certifications.

Product certifications (Common Criteria ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) is a standard that's used by many organizations as a basis for performing security evaluations of IT products.

For certifications that may be mutually recognized under the international Common Criteria Recognition Arrangement (CCRA), see the Common Criteria Portal. The Common Criteria standard may also be used outside the CCRA by national and private validation schemes. In Europe, mutual recognition is governed under the SOG-IS agreement as well as the CCRA.

The goal, as stated by the Common Criteria community, is for an internationally approved set of security standards to provide a clear and reliable evaluation of the security capabilities of Information Technology products. By providing an independent assessment of a product's ability to meet security standards, Common Criteria Certification gives customers more confidence in the security of Information Technology products and leads to more informed decisions.

Through the CCRA, member countries have agreed to recognize the certification of Information Technology products with the same level of confidence. Evaluations required before certification are extensive and include:

- Protection Profiles (PPs)
- Security Targets (STs)
- Security Functional Requirements (SFRs)
- Security Assurance Requirements (SARs)
- Evaluation Assurance Levels (EALs)

Protection Profiles (PPs) are documents that specify security requirements for a class of device types (such as Mobility) and are used to provide comparability between the evaluations of IT products within the same class. Membership of the CCRA, along with an increasing list of approved PPs, continues to grow on a yearly basis. This arrangement permits a product developer to pursue a single certification under any one of the certificate authorizing schemes and have it recognized by any of the certificate consuming signatories.

Security Targets (STs) define *what* will be evaluated when an IT product is being certified. The STs are translated to more specific *Security Functional Requirements (SFRs)*, used for evaluating the STs in more detail.

The Common Criteria (CC) also includes *Security Assurance Requirements*. One commonly identified metric is the *Evaluation Assurance Level (EAL)*. EALs group together frequently occurring sets of SARs and may be specified in PPs and STs to support comparability.

Many older PPs have been archived and are being replaced with targeted PPs, which are being developed and focus on specific solutions and environments. In a concerted effort to ensure continued mutual recognition across all CCRA members, international Technical Communities (iTCs) have been established to develop and maintain collaborative Protection Profiles (cPPs), which are developed from the start with involvement from CCRA signatory schemes. PPs targeted for user groups and mutual recognition arrangements other than the CCRA continue to be developed by appropriate stakeholders.

Apple began pursuing certifications under the updated CCRA with selected cPPs starting in early 2015. Since then, Apple has achieved Common Criteria certifications for each major iOS release and has expanded coverage to include the security assurance provided by new PPs.

Apple takes an active role within the technical communities focused on evaluating mobile security technologies. These include the iTCs responsible for developing and updating cPPs. Apple continues to evaluate and pursue certifications against current PPs and cPPs.

Apple platform certifications for the North America market are generally performed with the National Information Assurance Partnership (NIAP), which maintains a list of projects currently in evaluation but not yet certified.

In addition to the general platform certificates listed, other certificates have been issued in order to demonstrate specific security requirements for some markets.

Security certifications for Apple apps

Common Criteria (CC) certification background

Apple actively engages in security certifications of Apple apps using appropriate Protection Profiles (PPs). These evaluations build on the hardware and operating system certifications that Apple has gained. In 2018, Apple initiated application security evaluations for key applications running on iOS 11 with the Safari browser and Contacts apps. Apple continued these evaluations on apps running in iOS 12 in 2019 and iOS 13 and iPadOS 13.1 in 2020.

Apple will pursue further security evaluations of key apps on future operating system releases.

Cryptographic module certification status

Apple apps listed in the tables below use the cryptographic modules for the applicable operating system. For more information, see Security certifications for iOS and Security certifications for iPadOS.

Common Criteria (CC) certification status

The U.S. scheme, operated by NIAP, maintains a list of Products in Evaluation; this list includes products that are currently undergoing evaluation in the United States with a NIAP-approved Common Criteria Testing Laboratory (CCTL) and that have completed an Evaluation Kickoff Meeting (or equivalent) in which CCEVS management officially accepts the product into evaluation.

After products are certified, NIAP puts currently valid certifications on its Product Compliant list. After 2 years, these certifications are reviewed for conformance with the current assurance maintenance policy. After the assurance maintenance date has expired, NIAP moves the certification listing to its Archived Products list.

The Common Criteria Portal lists certifications that can be mutually recognized under the Common Criteria Recognition Arrangement (CCRA). The CC Portal may maintain products on the certified product list for 5 years; records are kept by the CC Portal for archived certifications.

The table below shows the certifications that are currently being evaluated by a laboratory, or that have been certified as conforming with Common Criteria.

Evaluations with NIAP that are published as being under way are listed at Products in evaluation (NIAP).

Operating system / Certification date	Scheme ID / Documents	Title / Protection Profiles
Operating system: iOS 13, iPadOS 13 *Certification date:* 2020-06-05	*Scheme ID:* 11060 *Documents:* Certificate, Security Target, Guidance, Validation Report, Assurance Activity Report	*Title:* Apple iOS 13 and iPadOS 13: Safari *Protection Profiles:* PP for Application SW, EP for Web Browsers
Operating system: iOS 13, iPadOS 13 *Certification date:* 2020-06-05	*Scheme ID:* 11050 *Documents:* Certificate, Security Target, Guidance, Validation Report, Assurance Activity Report	*Title:* Apple iOS 13 and iPadOS 13: Contacts *Protection Profiles:* PP for Application SW
Operating system: iOS 12 *Certification date:* 2019-06-12	*Scheme ID:* 10960 *Documents:* Certificate, Security Target, Guidance, Validation Report, Assurance Activity Report	*Title:* iOS 12 Safari *Protection Profiles:* PP for Application SW, EP for Web Browsers
Operating system: iOS 12 *Certification date:* 2019-02-28	*Scheme ID:* 10961 *Documents:* Certificate, Security Target, Guidance, Validation Report, Assurance Activity Report	*Title:* iOS 12 Contacts *Protection Profiles:* PP for Application SW

Archived Common Criteria certifications for Apple apps

Operating system / Certification date	Scheme ID / Documents	Title / Protection Profiles
Operating system: iOS 11 *Certification date:* 2018-11-09	*Scheme ID:* 10916 *Documents:* Security Target, Guidance	*Title:* iOS 11 Safari *Protection Profiles:* PP for Application SW, EP for Web Browsers
Operating system: iOS 11 *Certification date:* 2018-09-13	*Scheme ID:* 10915 *Documents:* Security Target, Guidance	*Title:* iOS 11 Contacts *Protection Profiles:* PP for Application SW

Security certifications for Apple internet services

Apple maintains certifications in compliance with the ISO/IEC 27001 and ISO/IEC 27018 standards to enable Apple customers to address their regulatory and contractual obligations. These certifications provide our customers with an independent attestation over Apple's Information Security and Privacy practices for in-scope systems.

ISO/IEC 27001 and ISO/IEC 27018 are part of a family of Information Security Management System (ISMS) standards published by the International Organization for Standardization (ISO). As part of Apple's ISMS, all Annex A control requirements have been included in the Statement of Applicability as defined within the ISO/IEC 27001and ISO/IEC 27018 standards. Apple undergoes an independent attestation by an accredited registrar on an annual basis.

ISO/IEC 27001

ISO/IEC 27001 is an Information Security Management System standard specifying requirements for establishing, implementing, maintaining, and continuously improving an organization's Information Security Management System.

The ISO/IEC 27001 standard includes the following security domains covered by Apple's ISO/IEC certifications:

- Information security policies
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

ISO/IEC 27018

ISO/IEC 27018 is a code of practice for the protection of personally identifiable information (PII) in public cloud environments. The ISO/IEC 27018 standard includes the following security domains covered by Apple's ISO/IEC certifications:

- Consent and choice
- Purpose legitimacy and specification
- Collection limitation
- Data minimization
- Use, retention, and disclosure limitation
- Accuracy and quality
- Openness, transparency, and notice
- Individual participation and access
- Accountability
- Information security
- Privacy compliance

Apple services covered by ISO/IEC 27001 and ISO/IEC 27018

Apple's ISO/IEC 27001 and ISO/IEC 27018 certifications cover the following services:

- Apple Business Chat
- Apple Business Manager
- Apple Push Notification service (APNs)
- Apple School Manager
- FaceTime
- iCloud
- iMessage
- iTunes U
- Managed Apple IDs
- Schoolwork
- Siri

Certifications

Evidence of Apple's ISO/IEC 27001 and 27018 certifications are available at our registrar:

- Apple's ISO/IEC 27001 Certificate
- Apple's ISO/IEC 27018 Certificate

Note: Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. Contact the vendor for additional information.

Glossary

Apple Business Manager A simple, web-based portal for IT administrators that provides a fast, streamlined way for organizations to deploy Apple devices that they have purchased directly from Apple or from a participating Apple Authorized Reseller or carrier. They can automatically enroll devices in their mobile device management (MDM) solution without having to physically touch or prepare the devices before users get them.

Apple Push Notification service (APNs) A worldwide service provided by Apple that delivers push notifications to Apple devices.

Apple School Manager A simple, web-based portal for IT administrators that provides a fast, streamlined way for organizations to deploy Apple devices that they have purchased directly from Apple or from a participating Apple Authorized Reseller or carrier. They can automatically enroll devices in their mobile device management (MDM) solution without having to physically touch or prepare the devices before users get them.

collaborative Protection Profile (cPP) A Protection Profile developed by an international Technical Community, a group of experts charged with the creation of cPPs.

Common Criteria (CC) A standard that establishes the general concepts and principles of IT security evaluation and specifies a general model of evaluation. It includes catalogues of security requirements in a standardized language.

Common Criteria Recognition Arrangement (CCRA) A mutual recognition arrangement that establishes the policies and requirements for international recognition of certificates issued in accordance with the ISO/IEC 15408 or Common Criteria standard.

corecrypto A library that provides implementations of low-level cryptographic primitives. Note that corecrypto does not directly provide programming interfaces for developers and is used through APIs provided to developers. The corecrypto source code is publicly available to allow for verification of its security characteristics and correct functioning.

cryptographic module The hardware, software, and/or firmware that provide cryptographic functions and meet the requirements of a stated cryptographic module standard.

Cryptographic Algorithm Validation Program (CAVP) An organization operated by NIST to provide validation testing of Approved (for example, FIPS-approved and NIST-recommended) cryptographic algorithms and their individual components.

Cryptographic Module Validation Program (CMVP) An organization operated by the U.S. and Canadian governments to validate conformance with the FIPS 140-3 standard.

Federal Information Processing Standard (FIPS) Publications developed by the National Institute of Standards and Technology, either when required by statute, or when there are compelling federal government requirements for cybersecurity, or both.

Full Disk Encryption (FDE) Encryption of all data on a storage volume.

Information Security Management System (ISMS) A set of information security policies and procedures governing the boundaries of a security program designed to protect a scope of information and systems by systematically managing information security throughout the information and or system's life cycle.

Implementation under Test (IUT) A cryptographic module being tested by a laboratory.

international Technical Community (iTC) A group responsible for developing Protection Profiles or collaborative Protection Profiles under the auspices of the Common Criteria Recognition Arrangement (CCRA).

IPsec VPN Client In a Protection Profile, a client that provides a secure IPsec connection between a physical or virtual host platform and a remote location.

mobile device management (MDM) A service that lets the user remotely manage enrolled devices. After a device is enrolled, the user can use the MDM service over the network to configure settings and perform other tasks on the device without user interaction.

Modules in Process (MIP) A list maintained by the Cryptographic Module Validation Program (CMVP) of cryptographic modules currently in the CMVP validation process.

National Information Assurance Partnership (NIAP) An organization of the U.S. government responsible for operating the U.S. implementation of the Common Criteria standard and managing the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS).

National Institute of Standards and Technology (NIST) A part of the U.S. Department of Commerce responsible for advancing measurement science, standards, and technology.

Protection Profile (PP) A document specifying the security problem and the security requirements for a particular class of products.

Secure Element (SE) A silicon chip embedded in many Apple devices that supports functions such as Apple Pay.

Secure Enclave Processor (SEP) A coprocessor fabricated within a system on chip (SoC).

Security Level (SL) The four overall security levels (1–4) that are defined within ISO/IEC 19790 to describe sets of applicable security requirements. Level 4 is the most stringent.

Security Target (ST) A document that specifies the security problem and security requirements for a particular product.

sepOS The Secure Enclave firmware, based on an Apple-customized version of the L4 microkernel.

Senior Officials Group Information Systems Security (SOG-IS) A group that manages a mutual recognition agreement between several European nations.

Statement of Applicability (SOA) A document that describes the security controls implemented in the scope of an ISMS, produced in support of an ISO/IEC 27001 certification.

system on chip (SoC) An integrated circuit (IC) that incorporates multiple components into a single chip.

T2 An Apple security chip included in some Intel-based Mac computers since 2017.

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

028-00369