安全认证和合规中心

2021 年 12 月

目录

Apple 安全保证介绍

作为践行安全承诺的一部分，Apple 会定期接洽第三方组织，以认证和证明 Apple 硬件、软件和服务的安全性。这些国际公认的组织伴随操作系统每个主要版本的发布为 Apple 提供认证。通过这种方式，此类组织提供了证明系统安全需求已得到满足的信任方式，即安全保证。对于未被相互认可协定 (MRA) 接受或者缺乏成熟安全认证标准的技术领域，Apple 会参与开发适当的安全标准。我们的使命是推动全球公认的安全认证全面涵盖所有 Apple 硬件、操作系统、App 和服务。

认证通常是满足法律、法规和行业规范要求的必要条件。Apple 的 ISO/IEC 27001 和 ISO/IEC 27018 认证涵盖 Apple 校园教务管理和 Apple 商务管理等服务。包括部署 Apple 设备的政府机构、企业和教育组织在内的所有客户都可借助硬件、操作系统、软件和服务认证来证明其达到合规要求。

硬件认证

安全软件需要以硬件内建的安全机制为基础，因此所有 Apple 设备（无论是运行 iOS、iPadOS、macOS、Apple tvOS 或 watchOS）的芯片中均设有安全功能。其中包括提供系统安全功能的定制 CPU 功能以及专为实现安全功能而设计的芯片。最关键的组件就是安全隔区协处理器，该协处理器全面使用于所有在售的 iOS、iPadOS、watchOS 和 Apple tvOS 设备、所有搭载 Apple 芯片的 Mac 电脑以及基于 Intel 且搭载 Apple T2 安全芯片的 Mac 电脑。安全隔区为静态数据加密、macOS 安全启动和生物识别的实现构建了基础。

Apple 为实现安全保证做出的努力始于对芯片中的基础安全组件进行认证，其中包括硬件信任根、安全启动执行、提供安全密钥库的安全隔区以及通过触控 ID 和面容 ID 进行的安全认证。Apple 设备的种种安全功能离不开只有 Apple 才能提供的芯片设计、硬件、软件和服务的紧密配合。这些组件的认证对于验证 Apple 提供的保证不可或缺。

有关硬件及关联固件组件的公开认证信息，请参阅：

- 适用于 Apple T2 安全芯片的安全认证
- 适用于安全隔区处理器的安全认证

软件和 App 认证

Apple 针对其操作系统和 App 持续获有独立的认证和证明，以确保它们符合适用于加密模块的美国联邦信息处理标准 (FIPS) 140-2/-3 以及适用于操作系统、App 和设备服务的通用标准。操作系统涵盖 iOS、iPadOS、macOS、sepOS、T2 固件、Apple tvOS 和 watchOS。针对 App 的独立认证最初包括 Safari 浏览器和“通讯录” App，后续会认证更多 App。

有关 Apple **操作系统**的公开认证信息，请参阅：

- 适用于 iOS 的安全认证
- 适用于 iPadOS 的安全认证
- 适用于 macOS 的安全认证
- 适用于 Apple tvOS 的安全认证
- 适用于 watchOS 的安全认证

有关 Apple **App** 的公开认证信息，请参阅：

- 适用于 Apple App 的安全认证

服务认证

Apple 维护的安全认证为从企业到教育领域的客户提供了支持。这些认证协助 Apple 客户在使用随 Apple 硬件和软件提供的 Apple 服务时履行其监管和合同义务。这些认证向客户提供了 Apple 系统中 Apple 信息安全、环境和隐私实践的独立证明。

有关 Apple **互联网服务**的公开认证信息，请参阅：

- 适用于 Apple 互联网服务的安全认证

有关 Apple 安全和隐私认证的问题，请联系 security-certifications@apple.com。

硬件安全认证

Apple 硬件安全认证概览

Apple 针对 sepOS 和 T2 固件持续获有美国联邦信息处理标准 (FIPS) 140-2/-3 符合性验证证书以及其他认证。Apple 酌情从广泛适用于多个平台的**认证构建块**着手。其中一个构建块便是 corecrypto 库的验证，该构建块被应用于 Apple 所开发操作系统中软件和硬件加密模块的部署。第二个构建块是内嵌于许多 Apple 设备中的安全隔区的认证。第三个是配备触控 ID 的 Apple 设备和配备面容 ID 的设备中的安全元件 (SE) 的认证。这些硬件认证构建块形成了更广泛平台安全认证的基础。

加密算法验证

验证很多加密算法和相关安全功能的实施正确性是进行 FIPS 140-3 验证的先决条件，也为其他认证提供了支持。该验证由美国国家标准与技术研究院 (NIST) 加密算法验证体系 (CAVP) 管理。针对 Apple 实施情况验证的证书可使用 CAVP 搜索功能进行查找。有关更多信息，请参阅加密算法验证体系 (CAVP) 网站。

加密模块验证：FIPS 140-2/3 (ISO/IEC 19790)

自 2012 年以来，在操作系统每个主要版本发布之后，加密模块验证体系 (CMVP) 都会对 Apple 加密模块重新进行验证，以确定其符合适用于加密模块的美国联邦信息处理标准 (FIPS 140-2)。在发布每个主要版本后，Apple 会将模块提交给 CMVP 以验证其是否符合标准。这些模块不仅被 Apple 操作系统和 App 使用，也为 Apple 的服务提供了加密功能，还可供第三方 App 使用。

Apple 每年均实现了适用于 macOS 且基于软件的模块“Corecrypto 模块 (Intel)”和“Corecrypto 内核模块 (Intel)”的 **1 级安全**。对于 Apple 芯片，“Corecrypto 模块 (ARM)”和“Corecrypto 内核模块 (ARM)”模块适用于 iOS、iPadOS、Apple tvOS、watchOS 以及 Mac 电脑内嵌 Apple T2 安全芯片中的固件。

在 2019 年，Apple 实现了标识为“Apple Corecrypto 模块：安全密钥库”的嵌入式硬件加密模块的第一个 FIPS 140-2 **2 级安全**，推动美国政府批准使用在安全隔区中生成和管理的密钥。随着后续操作系统每个主要版本的发布，Apple 会继续寻求针对硬件加密模块的验证。

FIPS 140-3 于 2019 年获得美国商务部的批准。此版本的标准中最显著的变化是指定了 ISO/IEC 标准，尤其是 ISO/IEC 19790:2015 及相关的测试标准 ISO/IEC 24759:2017。CMVP 已启动过渡计划，并表示从 2020 年开始，将开始使用 FIPS 140-3 作为基础来验证加密模块。Apple 将力争尽快使加密模块符合和过渡到 FIPS 140-3 标准。

对于当前正在测试和验证的加密模块，CMVP 会维护两份不同的列表，其中可能包含建议的验证信息。正在有资质的实验室进行测试的加密模块可能会在被测实现列表中列出。实验室完成 Apple 加密模块测试并建议交由 CMVP 进行验证后，该模块会显示在正在验证模块列表中。当前实验室测试已完成并等待 CMVP 进行测试验证。由于评估过程时长不定，因此在操作系统主要版本发布日后至 CMVP 颁发验证证书前，请同时参考以上两个过程列表来确定 Apple 加密模块的当前状态。

产品认证：通用标准 (ISO/IEC 15408)

通用标准 (ISO/IEC 15408) 是一种被许多组织用于 IT 产品安全评估基础的标准。

对于根据国际通用标准认可协定 (CCRA) 可能互相认可的认证，请参阅通用标准门户。CCRA 之外的国家/地区和私人验证方案也可能采用通用标准。在欧洲，相互认可同时受到 SOG-IS 协定以及 CCRA 的约束。

如通用标准社区所述，它的目标是制定一系列国际认可的安全标准，用于对信息技术产品的安全功能提供清晰可靠的评估。通过提供对产品符合安全标准能力的独立评估，通用标准认证可让客户增强对信息技术产品安全的信心，从而作出更加明智的决定。

通过 CCRA，成员国家/地区已同意以相同的信任等级认可信息技术产品的认证。认证前需要进行多项评估，包括：

- 保护描述文件 (PP)
- 安全目标 (ST)
- 安全功能要求 (SFR)
- 安全保证要求 (SAR)
- 评估保证等级 (EAL)

保护描述文件 (PP) 是指定某种设备类型安全要求（如移动性）的文稿，用于为同一类 IT 产品的评估提供可比性。CCRA 成员每年均不断增加，批准的 PP 列表也在不断扩充。此协定允许产品开发人员只需根据任一证书授权方案获得单次认证，该认证即会受到任一证书使用签署方的认可。

安全目标 (ST) 定义了认证 IT 产品时会评估**什么内容**。ST 会细化为更具体的**安全功能要求 (SFR)**，用于更细致地评估 ST。

通用标准 (CC) 还包括**安全保证要求**。**评估保证等级 (EAL)** 是一项被广泛认可的指标。EAL 集合了一系列常见的 SAR，可在 PP 和 ST 中指定以支持可比性。

许多较早的 PP 已归档，并逐步被专注于特定解决方案和环境而开发的针对性 PP 所取代。为了协力确保所有 CCRA 成员能够持续相互认可，国际技术社区 (iTC) 应运而生，其使命是开发和维护协作性保护描述文件 (cPP)，cPP 一开始就是在 CCRA 签署方案的基础上进行开发。针对用户群组和相互认可协定而非 CCRA 的 PP 继续由相应的利益相关方开发。

Apple 于 2015 年初就开始针对更新后的 CCRA 及其中所选 cPP 来寻求认证。自此之后，Apple 已经针对发布的每个 iOS 主要版本实现了通用标准认证，并扩大了覆盖范围以包括新 PP 所提供的安全保证。

Apple 在专注于移动安全技术评估的技术社区中积极发挥作用，其中包括负责开发和更新 cPP 的 iTC。Apple 将继续根据当前 PP 和 cPP 来评估和寻求认证。

Apple 一般通过美国国家信息保障合作联盟 (NIAP) 针对北美市场进行平台认证，该联盟维护了一个尚未认证但当前正在评估项目的列表。

除了列出的通用平台证书外，还有已签发的其他证书以说明某些市场的特定安全要求。

适用于安全隔区处理器的安全认证

安全隔区认证背景

硬件加密模块 **Apple SEP 安全密钥库加密模块**内嵌于以下产品的 Apple SoC 中：适用于 iPhone 和 iPad 的 Apple A 系列、适用于搭载 Apple 芯片的 Mac 电脑的 M 系列、适用于 Apple Watch 的 S 系列以及从 iMac Pro（2017 年推出）开始基于 Intel 的 Mac 电脑中的 T 系列安全芯片。

在 2018 年，Apple 对 2017 年发布的操作系统中软件加密模块的验证进行了同步，这些系统包括 iOS 11、macOS 10.13、Apple tvOS 11 和 watchOS 4。标识为 Apple SEP 安全密钥库加密模块 v1.0 的 SEP 硬件加密模块最初是根据 FIPS 140-2 1 级安全要求进行验证。

在 2019 年，Apple 根据 FIPS 140-2 2 级安全要求验证了硬件模块并将模块版本标识符更新至 v9.0，以与对应 corecrypto 用户模块和 corecrypto 内核模块验证的版本同步。在 2019 年，含这些模块的系统包括 iOS 12、macOS 10.14、Apple tvOS 12 和 watchOS 5。

在 2020 年和 2021 年，对于 A13、A14、S6 和 M1 这些 Apple 芯片，Apple 一直力争完成 FIPS 140-3 符合性验证，并实现 3 级物理安全要求额外保证。

对于所发布操作系统的每个主要版本，Apple 也会积极验证 corecrypto 用户模块和 corecrypto 内核模块。符合性验证的执行对象只能是最终发布版。

加密模块验证状态

加密模块验证体系 (CMVP) 根据加密模块的当前状态在三个单独的列表中维护了其验证状态：

- 为了在 CMVP 被测实现列表中列出，实验室必须和 Apple 签约以提供测试。
- 实验室完成测试并建议交由 CMVP 进行验证，并且支付了 CMVP 费用后，模块便会添加到正在验证模块列表。MIP 列表分四个阶段跟踪 CMVP 验证过程的进度：
  - **待审核：**等待分配 CMVP 资源。
  - **审核中：**CMVP 资源正在执行验证活动。
  - **协作：**实验室正携手 CMVP 解决发现的任何问题。
  - **最终完成：**与签发证书相关的活动和手续。
- 在经由 CMVP 验证后，模块便会获得符合性证书并添加到已验证的加密模块列表。其中：
  - 已验证模块会被标记为活跃。
  - 5 年后模块会被标记为历史。
  - 若出于某些原因模块证书被撤销，则会被标记为已撤销。

CMVP 在 2020 年采用了国际标准 ISO/IEC 19790 作为 FIPS 140-3 的基础。

FIPS 140-3 认证

目前状态

下表显示 2020 年和 2021 年内当前正在实验室中进行测试以确定是否符合 FIPS 140-3 的加密模块。

与 2020 年和 2021 年发布的操作系统关联的安全密钥库 (SKS) 已经完成实验室测试并被实验室建议交由 CMVP 进行验证。它们在正在验证模块列表中列出，一经验证即会移至已验证的加密模块列表。

iOS 15（2021 年）用户空间、内核空间和安全密钥库正在进行实验室测试。它们在被测实现列表中列出。

日期	证书/文档	模块信息
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**随 2021 年发布的 iOS、iPadOS、macOS、Apple tvOS 和 watchOS 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（A9-A14、T2、M1、S3-S6） **整体安全级别：**2
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 2021 年发布的 iOS、iPadOS、macOS、Apple tvOS 和 watchOS 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（A13、A14、S6、M1） **整体安全级别：**2 **物理安全级别：**3
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 2020 年发布的 iOS、iPadOS、macOS、Apple tvOS 和 watchOS 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（A9-A14、T2、M1、S3-S6） **整体安全级别：**2
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 2020 年发布的 iOS、iPadOS、macOS、Apple tvOS 和 watchOS 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（A13、A14、S6、M1） **整体安全级别：**2 **物理安全级别：**3

FIPS 140-2 认证

下表显示已在实验室中进行 FIPS 140-2 符合性测试的加密模块。

日期	证书/文档	模块信息
操作系统发布日期：2019 年 **验证日期：**2021/2/5	**证书：**3811 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v10.0 **操作系统：**macOS 10.15 Catalina 的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2018 年 **验证日期：**2019/9/10	**证书：**3523 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v9.0 **操作系统：**macOS 10.14 Mojave 的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2017 年 **验证日期：**2019/9/10	**证书：**3223 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v1.0 **操作系统：**macOS 10.13 High Sierra 的 sepOS **类型：**硬件 **安全级别：**2

通用标准 (CC) 认证

Apple 积极进行通用标准评估以使用适当的保护描述文件涵盖 Apple 技术的安全性功能。

通用标准 (CC) 认证状态

由 NIAP 执行的美国方案维护了评估中产品列表；该列表中包括的产品当前正在美国的经 NIAP 批准的通用标准测试实验室 (CCTL) 中进行评估，且产品已完成评估启动会议（或对等会议），CCEVS 管理团队在会议中正式接受产品进入评估阶段。

产品认证之后，NIAP 会将当前有效的认证在其产品合规列表中列出。2 年后，这些认证会受到检查以确定是否符合当前的保证维护政策。超过保证维护期后，NIAP 会将认证列表项移到其已归档产品列表。

通用标准门户列出了根据通用标准认可协定 (CCRA) 可互相认可的认证。CC 门户可能在 5 年内维护已认证产品列表中的产品；该门户会保留已归档认证的记录。

下表显示当前正在实验室中进行评估或已认证为符合通用标准的认证。

操作系统/认证日期	方案 ID/文档	标题/保护描述文件
操作系统：sepOS **认证日期：**—	**方案 ID：**尚未认证 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**Apple 安全隔区 [2020 年] **保护描述文件：**CPP_DSC_V1.0 **硬件：**安全隔区（A9-A14、M1、T2、S3-S6） **软件：**随 iOS 14、iPadOS 14、macOS 11 Big Sur、Apple tvOS 14、watchOS 7 分发的 sepOS

其他认证

下表显示不使用通用标准或 FIPS 140-3 的安全隔区认证。

日期	证书/文档	模块信息
操作系统发布日期：2020 年 **验证日期：**2019/12/7 到 2022/12/26	**证书：**CFNR201902910002（中华人民共和国：移动金融技术服务认证） 中文版 英文版	**标题：**移动终端可信执行环境 **操作系统：**iOS 13.5.1 **技术规范：**JR/T 0156-2017

适用于 Apple T2 安全芯片的安全认证

加密模块验证背景

对于所发布操作系统的每个主要版本，Apple 都会积极验证 Apple 内嵌的软件和硬件模块。符合性验证的执行对象只能是模块的最终发布版。

CMVP 在 2020 年采用了国际标准 ISO/IEC 19790 作为美国联邦信息处理标准 (FIPS) 140-3 的基础。

除了搭载 Intel CPU 外，自 2017 年以来推出的大多数 Mac 电脑还搭载了单独的 Apple T2 安全芯片，该芯片是基于 Apple 芯片的片上系统 (SoC)。这些搭载 T2 芯片的 Mac 电脑为各种设备端服务使用了所有五种加密模块。

- Corecrypto 用户模块（Intel，基于 Intel 的 Mac 电脑上的 macOS 使用）
- Corecrypto 内核模块（Intel，基于 Intel 的 Mac 电脑上的 macOS 使用）
- Corecrypto 用户模块（ARM，T2 芯片使用）
- Corecrypto 内核模块（ARM，T2 芯片使用）
- 安全密钥库加密模块（T2 芯片内嵌的安全隔区协处理器使用）

【注】T2 芯片上运行的基于 Apple 芯片的模块与在其他 Apple 芯片（如 Apple A 系列、S 系列和 M 系列）上运行的模块相同。

加密模块验证状态

加密模块验证体系 (CMVP) 根据加密模块的当前状态在三个单独的列表中维护了其验证状态：

- 为了在 CMVP 被测实现列表中列出，实验室必须和 Apple 签约以提供测试。
- 实验室完成测试并建议交由 CMVP 进行验证，并且支付了 CMVP 费用后，模块便会添加到正在验证模块 (MIP) 列表。MIP 列表分四个阶段跟踪 CMVP 验证过程的进度：
  - **待审核：**等待分配 CMVP 资源。
  - **审核中：**CMVP 资源正在执行验证活动。
  - **协作：**实验室正携手 CMVP 解决发现的任何问题。
  - **最终完成：**与签发证书相关的活动和手续。
- 在经由 CMVP 验证后，模块便会获得符合性证书并添加到已验证的加密模块列表。其中：
  - 已验证模块会被标记为活跃。
  - 5 年后模块会被标记为历史。
  - 若出于某些原因模块证书被撤销，则会被标记为已撤销。

FIPS 140-3 认证

目前状态

2020 年用户空间、内核空间和安全密钥库的模块已经完成实验室测试并被实验室建议交由 CMVP 进行验证。它们在正在验证模块列表中列出。

2021 年用户空间、内核空间和安全密钥库的模块正在进行实验室测试。它们在被测实现列表中列出。

日期	证书/文档	模块信息
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12.0 **操作系统：**macOS 12 Monterey 的 sepOS **环境：**Apple 芯片、用户、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12.0 **操作系统：**macOS 12 Monterey 的 sepOS **环境：**Apple 芯片、内核、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12.0 **操作系统：**macOS 12 Monterey 的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (T2) **安全级别：**2
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**macOS 11 Big Sur 的 sepOS **环境：**Apple 芯片、用户、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**macOS 11 Big Sur 的 sepOS **环境：**Apple 芯片、内核、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**Intel 上 macOS 11 Big Sur 的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 **安全级别：**2

FIPS 140-2 认证

下表显示已在实验室中进行 FIPS 140-2 符合性测试的加密模块。

日期	证书/文档	模块信息
操作系统发布日期：2019 年 **验证日期：**2021/3/23	**证书：**3856 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v10.0 **操作系统：**macOS 10.15 Catalina 的 sepOS **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**2021/3/23	**证书：**3855 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v10.0 **操作系统：**macOS 10.15 Catalina 的 sepOS **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**2021/2/5	**证书：**3811 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 安全密钥库加密模块 v10.0 **操作系统：**macOS 10.15 Catalina 的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2018 年 **验证日期：**2019/4/23	**证书：**3438 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v9.0 **操作系统：**macOS 10.14 Mojave 的 sepOS **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/4/11	**证书：**3433 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v9.0 **操作系统：**macOS 10.14 Mojave 的 sepOS **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/9/10	**证书：**3523 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v9.0 **操作系统：**macOS 10.14 Mojave 的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2017 年 **验证日期：**2018/3/9、2018/5/22、2018/7/6	**证书：**3148 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v8.0 **操作系统：**macOS 10.13 High Sierra 的 sepOS **类型：**软件 **安全级别：**1

日期	证书/文档	模块信息
操作系统发布日期：2017 年 **验证日期：**2018/3/9、2018/5/17、2018/7/3	**证书：**3147 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v8.0 **操作系统：**macOS 10.13 High Sierra 的 sepOS **类型：**软件 **安全级别：**1
操作系统发布日期：2017 年 **验证日期：**2018/7/10	**证书：**3223 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v1.0 **操作系统：**macOS 10.13 High Sierra 的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2016 年 **验证日期：**2017/2/1	**证书：**2828 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple iOS Corecrypto 内核模块 v7.0 **操作系统：**macOS 10.12 Sierra 的 sepOS **类型：**软件 **安全级别：**1
操作系统发布日期：2016 年 **验证日期：**2017/2/1	**证书：**2827 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple iOS Corecrypto 内核模块 v7.0 **操作系统：**macOS 10.12 Sierra 的 sepOS **类型：**软件 **安全级别：**1

操作系统安全认证

Apple 操作系统安全认证概览

Apple 针对 sepOS 和 T2 固件持续获有美国联邦信息处理标准 (FIPS) 140-2/-3 符合性验证证书以及其他认证。Apple 酌情从广泛适用于多个平台的**认证构建块**着手。其中一个构建块便是 corecrypto 验证，该构建块被应用于 Apple 所开发操作系统中软件和硬件加密模块的部署。第二个构建块是内嵌于许多 Apple 设备中的安全隔区的认证。第三个是配备触控 ID 的 Apple 设备和配备面容 ID 的设备中的安全元件 (SE) 的认证。这些硬件认证构建块形成了更广泛平台安全认证的基础。

加密算法验证

验证很多加密算法和相关安全功能的实施正确性是进行 FIPS 140-3 验证的先决条件，也为其他认证提供了支持。该验证由 NIST 加密算法验证体系 (CAVP) 管理。针对 Apple 实施情况验证的证书可使用 CAVP 搜索功能进行查找。

加密模块验证：FIPS 140-2/3 (ISO/IEC 19790)

自 2012 年以来，在操作系统每个主要版本发布之后，加密模块验证体系 (CMVP) 都会对 Apple 操作系统中的加密模块重新进行验证，以确定其符合美国联邦信息处理标准 (FIPS) 140-2。在发布每个主要版本后，Apple 会将所有模块提交给 CMVP 以进行完整的加密验证。这些经过验证的模块对 Apple 提供的服务进行加密操作，同时可供第三方 App 使用。

Apple 每年均实现了适用于 macOS 且基于软件的模块“Corecrypto 模块 (Intel)”和“Corecrypto 内核模块 (Intel)”的 **1 级安全**。对于 Apple 芯片，“Corecrypto 模块 (ARM)”和“Corecrypto 内核模块 (ARM)”模块适用于 iOS、iPadOS、Apple tvOS、watchOS 以及 Mac 电脑内嵌 Apple T2 安全芯片中的固件。

在 2019 年，Apple 实现了标识为“Apple Corecrypto 模块：安全密钥库”的嵌入式硬件加密模块的第一个 FIPS 140-2 **2 级安全**，推动美国政府批准使用在安全隔区中生成和管理的密钥。随着后续操作系统每个主要版本的发布，Apple 会继续寻求针对硬件加密模块的验证。

FIPS 140-3 于 2019 年获得美国商务部的批准。此版本的标准中最显著的变化是指定了 ISO/IEC 标准，尤其是 ISO/IEC 19790:2015 及相关的测试标准 ISO/IEC 24759:2017。CMVP 已启动过渡计划，并表示从 2020 年开始，将开始使用 FIPS 140-3 作为基础来验证加密模块。Apple 将力争尽快使加密模块符合和过渡到 FIPS 140-3 标准。

对于当前正在测试和验证的加密模块，CMVP 会维护两份不同的列表，其中可能包含建议的验证信息。正在有资质的实验室进行测试的加密模块可能会在被测实现列表中列出。实验室完成 Apple 加密模块测试并建议交由 CMVP 进行验证后，该模块会显示在正在验证模块列表中。当前实验室测试已完成并等待 CMVP 进行测试验证。由于评估过程时长不定，因此在操作系统主要版本发布日后至 CMVP 颁发验证证书前，请同时参考以上两个过程列表来确定 Apple 加密模块的当前状态。

产品认证：通用标准 (ISO/IEC 15408)

通用标准 (ISO/IEC 15408) 是一种被许多组织用于 IT 产品安全评估基础的标准。

对于根据国际通用标准认可协定 (CCRA) 可能互相认可的认证，请参阅通用标准门户。CCRA 之外的国家/地区和私人验证方案也可能采用通用标准。在欧洲，相互认可同时受到 SOG-IS 协定以及 CCRA 的约束。

如通用标准社区所述，它的目标是制定一系列国际认可的安全标准，用于对信息技术产品的安全功能提供清晰可靠的评估。通过提供对产品符合安全标准能力的独立评估，通用标准认证可让客户增强对信息技术产品安全的信心，从而作出更加明智的决定。

通过 CCRA，成员国家/地区已同意以相同的信任等级认可信息技术产品的认证。认证前需要进行多项评估，包括：

- 保护描述文件 (PP)
- 安全目标 (ST)
- 安全功能要求 (SFR)
- 安全保证要求 (SAR)
- 评估保证等级 (EAL)

保护描述文件 (PP) 是指定某种设备类型安全要求（如移动性）的文稿，用于为同一类 IT 产品的评估提供可比性。CCRA 成员每年均不断增加，批准的 PP 列表也在不断扩充。此协定允许产品开发人员只需根据任一证书授权方案获得单次认证，该认证即会受到任一证书使用签署方的认可。

安全目标 (ST) 定义了认证 IT 产品时会评估**什么内容**。ST 会细化为更具体的**安全功能要求 (SFR)**，用于更细致地评估 ST。

通用标准 (CC) 还包括**安全保证要求**。**评估保证等级 (EAL)** 是一项被广泛认可的指标。EAL 集合了一系列常见的 SAR，可在 PP 和 ST 中指定以支持可比性。

许多较早的 PP 已归档，并逐步被专注于特定解决方案和环境而开发的针对性 PP 所取代。为了协力确保所有 CCRA 成员能够持续相互认可，国际技术社区 (iTC) 应运而生，其使命是开发和维护**协作性保护描述文件 (cPP)**，cPP 一开始就是在 CCRA 签署方案的基础上进行开发。针对用户群组和相互认可协定而非 CCRA 的 PP 继续由相应的利益相关方开发。

Apple 于 2015 年初就开始针对更新后的 CCRA 及其中所选 cPP 来寻求认证。自此之后，Apple 已经针对发布的每个 iOS 主要版本实现了通用标准认证，并扩大了覆盖范围以包括新 PP 所提供的安全保证。

Apple 在专注于移动安全技术评估的技术社区中积极发挥作用，其中包括负责开发和更新 cPP 的 iTC。Apple 将继续根据当前 PP 和 cPP 来评估和寻求认证。

Apple 一般通过美国国家信息保障合作联盟 (NIAP) 针对北美市场进行平台认证，该联盟维护了一个尚未认证但当前正在评估项目的列表。

除了列出的通用平台证书外，还有已签发的其他证书以说明某些市场的特定安全要求。

适用于 iOS 的安全认证

iOS 认证背景

对于所发布操作系统的每个主要版本，Apple 都会积极验证 Apple 内嵌的软件和硬件模块。符合性验证的执行对象只能是最终发布版。

iOS 加密模块验证状态

加密模块验证体系 (CMVP) 根据加密模块的当前状态在三个单独的列表中维护了其验证状态：

- 为了在 CMVP 被测实现列表中列出，实验室必须和 Apple 签约以提供测试。
- 实验室完成测试并建议交由 CMVP 进行验证，并且支付了 CMVP 费用后，模块便会添加到正在验证模块 (MIP) 列表。MIP 列表分四个阶段跟踪 CMVP 验证过程的进度：
    - **待审核：**等待分配 CMVP 资源。
    - **审核中：**CMVP 资源正在执行验证活动。
    - **协作：**实验室正携手 CMVP 解决发现的任何问题。
    - **最终完成：**与签发证书相关的活动和手续。
- 在经由 CMVP 验证后，模块便会获得符合性证书并添加到已验证的加密模块列表。其中：
    - 已验证模块会被标记为活跃。
    - 5 年后模块会被标记为历史。
    - 若出于某些原因模块证书被撤销，则会被标记为已撤销。

CMVP 在 2020 年采用了国际标准 ISO/IEC 19790 作为 FIPS 140-3 的基础。

FIPS 140-3 认证

目前状态

iOS 14（2020 年）用户空间、内核空间和安全密钥库已经完成实验室测试并被实验室建议交由 CMVP 进行验证。它们在正在验证模块列表中列出。

iOS 15（2021 年）用户空间、内核空间和安全密钥库正在进行实验室测试。它们在被测实现列表中列出。

日期	证书/文档	模块信息
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**iOS 15 **环境：**Apple 芯片、用户、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**iOS 15 **环境：**Apple 芯片、内核、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**随 iOS 15 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (A9-A14) **整体安全级别：**2
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**随 iOS 15 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (A13、A14、A15) **整体安全级别：**2 **物理安全级别：**3
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**iOS 14 **环境：**Apple 芯片、用户、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**iOS 14 **环境：**Apple 芯片、内核、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 iOS 14 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (A9-A14) **整体安全级别：**2

日期	证书/文档	模块信息
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 iOS 14 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (A13-A14) **整体安全级别：**2 **物理安全级别：**3

FIPS 140-2 认证

下表显示为确定是否符合 FIPS 140-2, 当前正在实验室中进行测试以及已完成测试的加密模块。

日期	证书/文档	模块信息
操作系统发布日期：2019 年 **验证日期：**2021/3/23	**证书：**3856 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v10.0 **操作系统：**iOS 13 **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**2021/3/23	**证书：**3855 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v10.0 **操作系统：**iOS 13 **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**2021/2/5	**证书：**3811 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v10.0 **操作系统：**随 iOS 13 分发的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2018 年 **验证日期：**2019/4/23	**证书：**3438 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v9.0 **操作系统：**iOS 12 **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/4/11	**证书：**3433 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v9.0 **操作系统：**iOS 12 **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/9/10	**证书：**3523 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v9.0 **操作系统：**随 iOS 12 分发的 sepOS **类型：**硬件 **安全级别：**2

日期	证书/文档	模块信息
操作系统发布日期：2017 年 **验证日期：**2018/3/9、2018/5/22、2018/7/6	**证书：**3148 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v8.0 **操作系统：**iOS 11 **类型：**软件 **安全级别：**1
操作系统发布日期：2017 年 **验证日期：**2018/3/9、2018/5/17、2018/7/3	**证书：**3147 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v8.0 **操作系统：**iOS 11 **类型：**软件 **安全级别：**1
操作系统发布日期：2017 年 **验证日期：**2019/9/10	**证书：**3223 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v1.0 **操作系统：**随 iOS 11 分发的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2016 年 **验证日期：**2017/2/1	**证书：**2828 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple iOS Corecrypto 内核模块 v7.0 **操作系统：**iOS 10 **类型：**软件 **安全级别：**1
操作系统发布日期：2016 年 **验证日期：**2017/2/1	**证书：**2827 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple iOS Corecrypto 内核模块 v7.0 **操作系统：**iOS 10 **类型：**软件 **安全级别：**1

早期版本

CMVP 将早于 5 年前的认证列为历史状态。以下这些早期 iOS 版本验证了加密模块：

- iOS 9（Corecrypto 模块 v6.0）
- iOS 8（Corecrypto 模块 v5.0）
- iOS 7（Corecrypto 模块 v4.0）
- iOS 6（Corecrypto 模块 v3.0）

通用标准 (CC) 认证背景

对于所发布 iOS 操作系统的每个主要版本，Apple 会积极进行评估。评估的对象只能是操作系统最终公开发布的版本。在 iPadOS 13.1 之前，iPadOS 的名称为 iOS。

通用标准 (CC) 认证状态

由 NIAP 执行的美国方案维护了评估中产品列表；该列表中包括的产品当前正在美国的经 NIAP 批准的通用标准测试实验室 (CCTL) 中进行评估，且产品已完成评估启动会议（或对等会议），CCEVS 管理团队在会议中正式接受产品进入评估阶段。

产品认证之后，NIAP 会将当前有效的认证在其产品合规列表中列出。2 年后，这些认证会受到检查以确定是否符合当前的保证维护政策。超过保证维护期后，NIAP 会将认证列表项移到其已归档产品列表。

通用标准门户列出了根据通用标准认可协定 (CCRA) 可互相认可的认证。CC 门户可能在 5 年内维护已认证产品列表中的产品；该门户会保留已归档认证的记录。

下表显示当前正在实验室中进行评估或已认证为符合通用标准的认证。

目前状态

针对 iOS 15 的 NIAP 评估当前正在实验室接受测试。有关最新信息，请参阅评估中产品 (NIAP) 和产品合规列表。

操作系统/认证日期	方案 ID/文档	标题/保护描述文件
操作系统：iOS 15 **认证日期：**—	**方案 ID：**尚未认证 **文档：**—	**标题：**Apple iOS 15：iPhone **保护描述文件：**移动设备基础（PP-Module 模块待确认）
操作系统：iOS 14 **认证日期：**2021/9/1	**方案 ID：**11146 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**Apple iOS 14：iPhone **保护描述文件：**移动设备基础、VPN 客户端模块、无线局域网客户端 PP 模块、MDM 代理 EP
操作系统：iOS 13 **认证日期：**2020/11/6	**方案 ID：**11036 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**iPhone 上的 Apple iOS 13 **保护描述文件：**移动设备基础、VPN 客户端模块、无线局域网客户端 EP、MDM 代理 EP

已归档的适用于 iOS 的通用标准认证

以下这些早期 iOS 版本进行了通用标准验证，并且根据 NIAP 政策被 NIAP 归档：

操作系统/认证日期	方案 ID/文档	标题/保护描述文件
操作系统：iOS 12 **认证日期：**2019/3/14	**方案 ID：**10937 **文档：** 安全目标 指南	**标题：**运行 iOS 12 的 iPhone **保护描述文件：**移动设备基础、VPN 客户端模块、无线局域网客户端 EP、MDM 代理 EP
操作系统：iOS 11 **认证日期：**2018/7/17	**方案 ID：**10851 **文档：** 安全目标 指南	**标题：**Apple iOS 11 **保护描述文件：**移动设备基础、无线局域网客户端 EP、MDM 代理 EP
操作系统：iOS 10 **认证日期：**2017/7/27	**方案 ID：**10782 **文档：**安全目标、指南	**标题：**iPhone 和 iPad 设备上的 iOS 10.2 **保护描述文件：**移动设备基础、无线局域网客户端 EP、MDM 代理 EP
操作系统：iOS 10 **认证日期：**2017/7/27	**方案 ID：**10792 **文档：**安全目标、指南	**标题：**iPhone 和 iPad 上的 iOS 10.2 VPN 客户端 **保护描述文件：**VPN 客户端 PP
操作系统：iOS 9 **认证日期：**2016/10/14	**方案 ID：**10725 **文档：**安全目标、指南	**标题：**iOS 9.3.2 搭配 MDM 代理 **保护描述文件：**移动设备基础、MDM 代理 EP
操作系统：iOS 9 **认证日期：**2016/10/13	**方案 ID：**10714 **文档：**安全目标、指南	**标题：**iPhone 和 iPad 上的操作系统 VPN 客户端 **保护描述文件：**VPN 客户端 PP
操作系统：iOS 9 **认证日期：**2016/1/28	**方案 ID：**10695 **文档：**安全目标、指南	**标题：**iOS 9 **保护描述文件：**移动设备基础

适用于 iPadOS 的安全认证

iPadOS 认证背景

对于 Apple 操作系统的每个主要版本，Apple 都会积极使用相应的协作性保护描述文件并采用 FIPS 140-3 安全级别进行验证。符合性验证的执行对象只能是最终发布版。

【注】 2019 年，iPad 设备的操作系统更名为 iPadOS。在 iPadOS 13.1 之前，iPadOS 的名称为 iOS。

iPadOS 加密模块验证状态

加密模块验证体系 (CMVP) 根据加密模块的当前状态在三个单独的列表中维护了其验证状态：

- 为了在 CMVP 被测实现列表中列出，实验室必须和 Apple 签约以提供测试。
- 实验室完成测试并建议交由 CMVP 进行验证，并且支付了 CMVP 费用后，模块便会添加到正在验证模块 (MIP) 列表。MIP 列表分四个阶段跟踪 CMVP 验证过程的进度：
  - **待审核：**等待分配 CMVP 资源。
  - **审核中：**CMVP 资源正在执行验证活动。
  - **协作：**实验室正携手 CMVP 解决发现的任何问题。
  - **最终完成：**与签发证书相关的活动和手续。
- 在经由 CMVP 验证后，模块便会获得符合性证书并添加到已验证的加密模块列表。其中：
  - 已验证模块会被标记为活跃。
  - 5 年后模块会被标记为历史。
  - 若出于某些原因模块证书被撤销，则会被标记为已撤销。

CMVP 在 2020 年采用了国际标准 ISO/IEC 19790 作为 FIPS 140-3 的基础。

FIPS 140-3 认证

目前状态

iPadOS 14（2020 年）用户空间、内核空间和安全密钥库已经完成实验室测试并被实验室建议交由 CMVP 进行验证。它们在正在验证模块列表中列出。

iPadOS 15（2021 年）用户空间、内核空间和安全密钥库正在进行实验室测试。它们在被测实现列表中列出。

日期	证书/文档	模块信息
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**iPadOS 15 **环境：**Apple 芯片、用户、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**iPadOS 15 **环境：**Apple 芯片、内核、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**随 iPadOS 15 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（A9-A14、M1） **整体安全级别：**2
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**随 iPadOS 15 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（A9-A14、M1） **整体安全级别：**2 **物理安全级别：**3
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**iPadOS 14 **环境：**Apple 芯片、用户、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**iPadOS 14 **环境：**Apple 芯片、内核、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 iPadOS 14 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（A9-A14、M1） **整体安全级别：**2

日期	证书/文档	模块信息
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 iPadOS 14 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (A9-A14、M1) **整体安全级别：**2 **物理安全级别：**3

FIPS 140-2 认证

下表显示为确定是否符合 FIPS 140-2, 当前正在实验室中进行测试以及已完成测试的加密模块。

日期	证书/文档	模块信息
操作系统发布日期：2019 年 **验证日期：**2021/3/23	**证书：**3856 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v10.0 **操作系统：**iPadOS 13 **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**2021/3/23	**证书：**3855 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v10.0 **操作系统：**iPadOS 13 **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**2021/2/5	**证书：**3811 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 安全密钥库加密模块 v10.0 **操作系统：**随 iPadOS 13 分发的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2018 年 **验证日期：**2019/4/23	**证书：**3438 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v9.0 **操作系统：**iOS 12 **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/4/11	**证书：**3433 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v9.0 **操作系统：**iOS 12 **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/9/10	**证书：**3523 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v9.0 **操作系统：**随 iOS 12 分发的 sepOS **类型：**硬件 **安全级别：**2

日期	证书/文档	模块信息
操作系统发布日期：2017 年 **验证日期：**2018/3/9、2018/5/22、2018/7/6	**证书：**3148 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v8.0 **操作系统：**iOS 11 **类型：**软件 **安全级别：**1
操作系统发布日期：2017 年 **验证日期：**2018/3/9、2018/5/17、2018/7/3	**证书：**3147 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v8.0 **操作系统：**iOS 11 **类型：**软件 **安全级别：**1
操作系统发布日期：2017 年 **验证日期：**2019/9/10	**证书：**3223 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v1.0 **操作系统：**随 iOS 11 分发的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2016 年 **验证日期：**2017/2/1	**证书：**2828 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple iOS Corecrypto 内核模块 v7.0 **操作系统：**iOS 10 **类型：**软件 **安全级别：**1
操作系统发布日期：2016 年 **验证日期：**2017/2/1	**证书：**2827 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple iOS Corecrypto 内核模块 v7.0 **操作系统：**iOS 10 **类型：**软件 **安全级别：**1

早期版本

CMVP 将早于 5 年前的认证列为历史状态。以下这些早期 iOS 版本验证了加密模块：

- iOS 9（Corecrypto 模块 v6.0）
- iOS 8（Corecrypto 模块 v5.0）
- iOS 7（Corecrypto 模块 v4.0）
- iOS 6（Corecrypto 模块 v3.0）

通用标准 (CC) 认证背景

对于所发布 iPadOS 操作系统的每个主要版本，Apple 会积极进行评估。评估的对象只能是操作系统最终公开发布的版本。

通用标准 (CC) 认证状态

由 NIAP 执行的美国方案维护了评估中产品列表；该列表中包括的产品当前正在美国的经 NIAP 批准的通用标准测试实验室 (CCTL) 中进行评估，且产品已完成评估启动会议（或对等会议），CCEVS 管理团队在会议中正式接受产品进入评估阶段。

产品认证之后，NIAP 会将当前有效的认证在其产品合规列表中列出。2 年后，这些认证会受到检查以确定是否符合当前的保证维护政策。超过保证维护期后，NIAP 会将认证列表项移到其已归档产品列表。

通用标准门户列出了根据通用标准认可协定 (CCRA) 可互相认可的认证。CC 门户可能在 5 年内维护已认证产品列表中的产品；该门户会保留已归档认证的记录。

下表显示当前正在实验室中进行评估或已认证为符合通用标准的认证。

目前状态

针对 iPadOS 15 的 NIAP 评估当前正在实验室接受测试。有关最新信息，请参阅评估中产品 (NIAP) 和产品合规列表。

操作系统/认证日期	方案 ID/文档	标题/保护描述文件
操作系统：iPadOS 15 **认证日期：**2019/3/14	**方案 ID：**— **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**运行 iOS 12 的 iPad **保护描述文件：**移动设备基础、VPN 客户端模块、无线局域网客户端 EP、MDM 代理 EP
操作系统：iPadOS 14 **认证日期：**2021/9/1	**方案 ID：**11147 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**Apple iPadOS 14：iPad **保护描述文件：**移动设备基础、VPN 客户端模块、无线局域网客户端 EP、MDM 代理 EP
操作系统：iPadOS 13 **认证日期：**2020/11/6	**方案 ID：**11036 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**iPad 移动设备上的 iPadOS 13 **保护描述文件：**移动设备基础、VPN 客户端模块、无线局域网客户端 EP、MDM 代理 EP

早期版本

以下这些早期 iOS 版本进行了通用标准验证，并且根据 NIAP 政策被 NIAP 归档：

- iOS 12（方案 ID：10937）
- iOS 11（方案 ID：10851）
- iOS 10（方案 ID：107782、10792）
- iOS 9（方案 ID：10725、10714、10695）

适用于 macOS 的安全认证

macOS 认证背景

对于 Apple 操作系统的每个主要版本，Apple 都会积极使用相应的协作性保护描述文件并采用 FIPS 140-3 安全级别进行验证。符合性验证的执行对象只能是最终发布版。

macOS 加密模块验证状态

加密模块验证体系 (CMVP) 根据加密模块的当前状态在三个单独的列表中维护了其验证状态：

- 为了在 CMVP 被测实现列表中列出，实验室必须和 Apple 签约以提供测试。
- 实验室完成测试并建议交由 CMVP 进行验证，并且支付了 CMVP 费用后，模块便会添加到正在验证模块 (MIP) 列表。MIP 列表分四个阶段跟踪 CMVP 验证过程的进度：
  - **待审核：**等待分配 CMVP 资源。
  - **审核中：**CMVP 资源正在执行验证活动。
  - **协作：**实验室正携手 CMVP 解决发现的任何问题。
  - **最终完成：**与签发证书相关的活动和手续。
- 在经由 CMVP 验证后，模块便会获得符合性证书并添加到已验证的加密模块列表。其中：
  - 已验证模块会被标记为活跃。
  - 5 年后模块会被标记为历史。
  - 若出于某些原因模块证书被撤销，则会被标记为已撤销。

CMVP 在 2020 年采用了国际标准 ISO/IEC 19790 作为 FIPS 140-3 的基础。

针对 Apple Mac 电脑，下表显示适用于各 Mac 技术的加密模块。

加密模块	搭载 Apple 芯片的 Mac 电脑	搭载 Apple T2 安全芯片的 Mac 电脑	基于 Intel 且不搭载 Apple T2 安全芯片的 Mac 电脑
Apple 芯片用户空间	✓		
Apple 芯片内核	✓		
Intel 用户空间		✓	✓
Intel 内核		✓	✓
安全密钥库	✓	✓	

FIPS 140-3 认证

2020 年，Apple 推出了基于 Apple 芯片的 Mac 电脑。加密模块对基于 Apple 芯片或基于 Intel 的 Mac 电脑的适用性在下表的“模块信息”列中指出。

【注】许多基于 Intel 的 Mac 电脑中都包括 Apple T2 安全芯片。有关 T2 芯片认证的信息，请参阅适用于 Apple T2 安全芯片的安全认证。

macOS ssh 客户端

可将 OpenSSH 配置为针对特定的 FIPS 140-3 算法使用 FIPS 140-3 已验证模块。组织可运行一个已签名且经公证的安装器（可从 Apple 获取，密码为 **FIPS140Mode**）。安装器会在 Mac 上放置两个文件：

- **fips_ssh_config**：放置在 /private/etc/ssh/ssh_config.d/
- **fips_sshd_config**：放置在 /private/etc/ssh/sshd_config.d/

macOS 之后使用这些文件将可供 OpenSSH 使用的密码限制为仅由 NIST 验证的密码，并确保 OpenSSH 客户端使用平台提供且经验证的加密模块。管理员也可以创建自己的文件。有关更多信息，请参阅 macOS 12.0.1 或更高版本中的 `apple_ssh_and_fips` man 页面。

目前状态

macOS 11 Big Sur 用户空间、内核空间和安全密钥库已经完成实验室测试并被实验室建议交由 CMVP 进行验证。它们在正在验证模块列表中列出。

macOS 12 Monterey 用户空间、内核空间和安全密钥库正在进行实验室测试。它们在被测实现列表中列出。

日期	证书/文档	模块信息
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12.0 **操作系统：**Apple 芯片上的 macOS 12 Monterey **环境：**Apple 芯片、用户、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12.0 **操作系统：**Apple 芯片上的 macOS 12 Monterey **环境：**Apple 芯片、内核、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12.0 **操作系统：**Intel 上的 macOS 12 Monterey **环境：**Intel、用户、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12.0 **操作系统：**Intel 上的 macOS 12 Monterey **环境：**Intel、内核、软件 **类型：**软件 **安全级别：**1

日期	证书/文档	模块信息
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12.0 **操作系统：**随 Apple 芯片上 macOS 12 Monterey 分发的 sepOS、随基于 Intel 且搭载 T2 的 macOS 12 Monterey 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (M1 和 T2) **安全级别：**2
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12.0 **操作系统：**随 Apple 芯片上 macOS 12 Monterey 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (M1) **安全级别：**2 **物理安全级别：**3
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**Intel 上的 macOS 11 Big Sur **环境：**Intel、用户、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**Intel 上的 macOS 11 Big Sur **环境：**Intel、内核、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**Apple 芯片上的 macOS 11 Big Sur **环境：**Apple 芯片、用户、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**Apple 芯片上的 macOS 11 Big Sur **环境：**Apple 芯片、内核、软件 **类型：**软件 **安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 Apple 芯片上 macOS 11 Big Sur 分发的 sepOS、随 Intel 上 macOS 11 Big Sur 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (M1) **安全级别：**2

日期	证书/文档	模块信息
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 Apple 芯片上 macOS 11 Big Sur 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (M1) **安全级别：**2 **物理安全级别：**3

FIPS 140-2 认证

下表显示为确定是否符合 FIPS 140-2，当前正在实验室中进行测试以及已完成测试的加密模块。

macOS 10.15 Catalina 用户空间、内核空间和安全密钥库已经完成实验室测试并被实验室建议交由 CMVP 进行验证。它们在正在验证模块列表中列出。

【注】许多基于 Intel 的 Mac 电脑中都包括 Apple T2 安全芯片。有关 T2 芯片认证的信息，请参阅适用于 Apple T2 安全芯片的安全认证。

日期	证书/文档	模块信息
操作系统发布日期：2019 年 **验证日期：**2021/3/24	**证书：**3859 **文档：** 认证 安全策略 加密主管指南	**标题：**适用于 Intel 的 Apple Corecrypto 用户空间模块 (ccv10) **操作系统：**macOS 10.15 Catalina **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**2021/3/24	**证书：**3858 **文档：** 认证 安全策略 加密主管指南	**标题：**适用于 Intel 的 Apple Corecrypto 内核模块 (ccv10) **操作系统：**macOS 10.15 Catalina **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/4/12	**证书：**3402 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (Intel) v9.0 **操作系统：**macOS 10.14 Mojave **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/4/12	**证书：**3431 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (Intel) v9.0 **操作系统：**macOS 10.14 Mojave **类型：**软件 **安全级别：**1
操作系统发布日期：2017 年 **验证日期：**2018/3/22	**证书：**3155 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (Intel) v8.0 **操作系统：**macOS 10.13 High Sierra **类型：**软件 **安全级别：**1

日期	证书/文档	模块信息
操作系统发布日期：2017 年 **验证日期：**2018/3/22	**证书：**3156 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (Intel) v8.0 **操作系统：**macOS 10.13 High Sierra **类型：**软件 **安全级别：**1

早期版本

以下这些早期 OS X 和 macOS 版本验证了加密模块。早于 5 年前的版本由 CMVP 列出并且状态为历史状态：

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

通用标准 (CC) 认证背景

对于所发布 macOS 操作系统的每个主要版本，Apple 会积极进行评估。评估的对象只能是操作系统最终公开发布的版本。

通用标准 (CC) 认证状态

由 NIAP 执行的美国方案维护了评估中产品列表；该列表中包括的产品当前正在美国的经 NIAP 批准的通用标准测试实验室 (CCTL) 中进行评估，且产品已完成评估启动会议（或对等会议），CCEVS 管理团队在会议中正式接受产品进入评估阶段。

产品认证之后，NIAP 会将当前有效的认证在其产品合规列表中列出。2 年后，这些认证会受到检查以确定是否符合当前的保证维护政策。超过保证维护期后，NIAP 会将认证列表项移到其已归档产品列表。

通用标准门户列出了根据通用标准认可协定 (CCRA) 可互相认可的认证。CC 门户可能在 5 年内维护已认证产品列表中的产品；该门户会保留已归档认证的记录。

下表显示当前正在实验室中进行评估或已认证为符合通用标准的认证。

目前状态

目前正使用通用操作系统和全磁盘加密 (FDE) (AA 和 EE) 保护描述文件对 macOS 11 和 macOS 12 进行 NIAP 评估。

有关最新信息，请参阅评估中产品 (NIAP) 和产品合规列表。

操作系统/认证日期	方案 ID/文档	标题/保护描述文件
操作系统：macOS 12 Monterey **认证日期：**—	**方案 ID：**尚未认证 **文档：**—	**标题：**Apple 文件保险箱 2 搭配 macOS 12 Monterey **保护描述文件：**CPP_FDE_AA_V2.0E、CPP_FDE_EE_V2.0E (PP 待确认)
操作系统：macOS 12 Monterey **认证日期：**—	**方案 ID：**尚未认证 **文档：**—	**标题：**macOS 12 Monterey **保护描述文件：**PP_OS_V4.21 (PP 待确认)
操作系统：macOS 11 Big Sur **认证日期：**—	**方案 ID：**尚未认证 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**Apple 文件保险箱 2 搭配 macOS 11 Big Sur **保护描述文件：**CPP_FDE_AA_V2.0E、CPP_FDE_EE_V2.0E
操作系统：macOS 11 Big Sur **认证日期：**—	**方案 ID：**尚未认证 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**Apple macOS 11 Big Sur **保护描述文件：**PP_OS_V4.21
操作系统：macOS 10.15 Catalina **认证日期：**2021/4/29	**方案 ID：**11078 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**运行 macOS 10.15 Catalina 且搭载 T2 的电脑上的 Apple 文件保险箱 2 **保护描述文件：**CPP_FDE_AA_V2.0E、CPP_FDE_EE_V2.0E
操作系统：macOS 10.15 Catalina **认证日期：**2020/9/23	**方案 ID：**11077 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**macOS 10.15 Catalina **保护描述文件：**PP_OS_V4.21

适用于 Apple tvOS 的安全认证

Apple tvOS 认证背景

Apple 积极针对与 Apple tvOS 每个主要版本相关联的加密模块进行验证。符合性验证的执行对象只能是最终发布版。

Apple tvOS 加密模块验证状态

加密模块验证体系 (CMVP) 根据加密模块的当前状态在三个单独的列表中维护了其验证状态：

- 为了在 CMVP 被测实现列表中列出，实验室必须和 Apple 签约以提供测试。
- 实验室完成测试并建议交由 CMVP 进行验证，并且支付了 CMVP 费用后，模块便会添加到正在验证模块 (MIP) 列表。MIP 列表分四个阶段跟踪 CMVP 验证过程的进度：
  - **待审核：**等待分配 CMVP 资源。
  - **审核中：**CMVP 资源正在执行验证活动。
  - **协作：**实验室正携手 CMVP 解决发现的任何问题。
  - **最终完成：**与签发证书相关的活动和手续。
- 在经由 CMVP 验证后，模块便会获得符合性证书并添加到已验证的加密模块列表。其中：
  - 已验证模块会被标记为活跃。
  - 5 年后模块会被标记为历史。
  - 若出于某些原因模块证书被撤销，则会被标记为已撤销。

CMVP 在 2020 年采用了国际标准 ISO/IEC 19790 作为 FIPS 140-3 的基础。

FIPS 140-3 认证

目前状态

Apple tvOS 14（2020 年）用户空间、内核空间和安全密钥库已经完成实验室测试并被实验室建议交由 CMVP 进行验证。它们在正在验证模块列表中列出。

Apple tvOS 15（2021 年）用户空间、内核空间和安全密钥库正在进行实验室测试。它们在被测实现列表中列出。

日期	证书/文档	模块信息
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**Apple tvOS 15 **环境：**Apple 芯片、用户、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**Apple tvOS 15 **环境：**Apple 芯片、内核、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**随 Apple tvOS 15 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（A10、A12） **整体安全级别：**2
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**Apple tvOS 14 **环境：**Apple 芯片、用户、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**Apple tvOS 14 **环境：**Apple 芯片、内核、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 Apple tvOS 14 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（A10、A12） **整体安全级别：**2

FIPS 140-2 认证

下表显示为确定是否符合 FIPS 140-2, 当前正在实验室中进行测试以及已完成测试的加密模块。

Apple tvOS 13（2019 年）用户空间、内核空间和安全密钥库已经完成实验室测试并被实验室建议交由 CMVP 进行验证。它们在正在验证模块列表中列出。

日期	证书/文档	模块信息
操作系统发布日期：2019 年 **验证日期：**2021/3/23	**证书：**3856 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v10.0 **操作系统：**Apple tvOS 13 **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**2021/3/23	**证书：**3855 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v10.0 **操作系统：**Apple tvOS 13 **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**2021/2/5	**证书：**3811 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v10.0 **操作系统：**随 Apple tvOS 13 分发的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2018 年 **验证日期：**2019/4/23	**证书：**3438 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v9.0 **操作系统：**Apple tvOS 12 **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/4/11	**证书：**3433 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v9.0 **操作系统：**Apple tvOS 12 **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/9/10	**证书：**3523 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v9.0 **操作系统：**随 Apple tvOS 12 分发的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2017 年 **验证日期：**2018/3/9、2018/5/22、2018/7/6	**证书：**3148 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v8.0 **操作系统：**Apple tvOS 11 **类型：**软件 **安全级别：**1

日期	证书/文档	模块信息
操作系统发布日期：2017 年 **验证日期：**2018/3/9、2018/5/17、2018/7/3	**证书：**3147 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v8.0 **操作系统：**Apple tvOS 11 **类型：**软件 **安全级别：**1
操作系统发布日期：2017 年 **验证日期：**2019/9/10	**证书：**3223 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v1.0 **操作系统：**随 Apple tvOS 11 分发的 sepOS **类型：**硬件 **安全级别：**2

适用于 watchOS 的安全认证

watchOS 认证背景

Apple 积极针对与 watchOS 每个主要版本相关联的加密模块进行验证。符合性验证的执行对象只能是最终发布版。

watchOS 加密模块验证状态

加密模块验证体系 (CMVP) 根据加密模块的当前状态在三个单独的列表中维护了其验证状态：

- 为了在 CMVP 被测实现列表中列出，实验室必须和 Apple 签约以提供测试。
- 实验室完成测试并建议交由 CMVP 进行验证，并且支付了 CMVP 费用后，模块便会添加到正在验证模块 (MIP) 列表。MIP 列表分四个阶段跟踪 CMVP 验证过程的进度：
  - **待审核：**等待分配 CMVP 资源。
  - **审核中：**CMVP 资源正在执行验证活动。
  - **协作：**实验室正携手 CMVP 解决发现的任何问题。
  - **最终完成：**与签发证书相关的活动和手续。
- 在经由 CMVP 验证后，模块便会获得符合性证书并添加到已验证的加密模块列表。其中：
  - 已验证模块会被标记为活跃。
  - 5 年后模块会被标记为历史。
  - 若出于某些原因模块证书被撤销，则会被标记为已撤销。

CMVP 在 2020 年采用了国际标准 ISO/IEC 19790 作为 FIPS 140-3 的基础。

FIPS 140-3 认证

目前状态

watchOS 7（2020 年）用户空间、内核空间和安全密钥库已经完成实验室测试并被实验室建议交由 CMVP 进行验证。它们在正在验证模块列表中列出。

watchOS 8（2021 年）用户空间、内核空间和安全密钥库正在进行实验室测试。它们在被测实现列表中列出。

日期	证书/文档	模块信息
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**watchOS 8 **环境：**Apple 芯片、用户、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**watchOS 8 **环境：**Apple 芯片、内核、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**随 watchOS 8 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（S3、S4、S5、S6） **整体安全级别：**2
操作系统发布日期：2021 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v12 **操作系统：**随 watchOS 8 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（S6） **整体安全级别：**2 **物理安全级别：**3
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**watchOS 7 **环境：**Apple 芯片、用户、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**watchOS 7 **环境：**Apple 芯片、内核、软件 **类型：**软件 **整体安全级别：**1
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 watchOS 7 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件（S3、S4、S5、S6） **整体安全级别：**2

日期	证书/文档	模块信息
操作系统发布日期：2020 年 **验证日期：**—	**证书：**尚未认证 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 模块 v11.1 **操作系统：**随 watchOS 7 分发的 sepOS **环境：**Apple 芯片、安全密钥库、硬件 **类型：**硬件 (S6) **整体安全级别：**2 **物理安全级别：**3

FIPS 140-2 认证

下表显示为确定是否符合 FIPS 140-2, 当前正在实验室中进行测试以及已完成测试的加密模块。

日期	证书/文档	模块信息
操作系统发布日期：2019 年 **验证日期：**—	**证书：**3856 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v10.0 **操作系统：**watchOS 6 **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**—	**证书：**3855 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v10.0 **操作系统：**watchOS 6 **类型：**软件 **安全级别：**1
操作系统发布日期：2019 年 **验证日期：**2021/2/5	**证书：**3811 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v10.0 **操作系统：**随 watchOS 6 分发的 sepOS **类型：**硬件 **安全级别：**2
操作系统发布日期：2018 年 **验证日期：**2019/4/23	**证书：**3438 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v9.0 **操作系统：**watchOS 5 **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/4/11	**证书：**3433 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v9.0 **操作系统：**watchOS 5 **类型：**软件 **安全级别：**1
操作系统发布日期：2018 年 **验证日期：**2019/9/10	**证书：**3523 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v9.0 **操作系统：**随 watchOS 5 分发的 sepOS **类型：**硬件 **安全级别：**2

日期	证书/文档	模块信息
操作系统发布日期：2017 年 **验证日期：**2018/3/9、2018/5/22、2018/7/6	**证书：**3148 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 用户模块 (ARM) v8.0 **操作系统：**watchOS 4 **类型：**软件 **安全级别：**1
操作系统发布日期：2017 年 **验证日期：**2018/3/9、2018/5/17、2018/7/3	**证书：**3147 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple Corecrypto 内核模块 (ARM) v8.0 **操作系统：**watchOS 4 **类型：**软件 **安全级别：**1
操作系统发布日期：2017 年 **验证日期：**2019/9/10	**证书：**3223 **文档：** 认证 安全策略 加密主管指南	**标题：**Apple 安全密钥库加密模块 v1.0 **操作系统：**随 watchOS 4 分发的 sepOS **类型：**硬件 **安全级别：**2

软件安全认证

Apple 软件安全认证概览

Apple 针对 sepOS 和 T2 固件持续获有美国联邦信息处理标准 (FIPS) 140-2/-3 符合性验证证书以及其他认证。Apple 酌情从广泛适用于多个平台的**认证构建块**着手。其中一个构建块便是 corecrypto 验证，该构建块被应用于 Apple 所开发操作系统中软件和硬件加密模块的部署。第二个构建块是内嵌于许多 Apple 设备中的安全隔区的认证。第三个是配备触控 ID 的 Apple 设备和配备面容 ID 的设备中的安全元件 (SE) 的认证。这些硬件认证构建块形成了更广泛平台安全认证的基础。

产品认证：通用标准 (ISO/IEC 15408)

通用标准 (ISO/IEC 15408) 是一种被许多组织用于 IT 产品安全评估基础的标准。

对于根据国际通用标准认可协定 (CCRA) 可能互相认可的认证，请参阅通用标准门户。CCRA 之外的国家/地区和私人验证方案也可能采用通用标准。在欧洲，相互认可同时受到 SOG-IS 协定以及 CCRA 的约束。

如通用标准社区所述，它的目标是制定一系列国际认可的安全标准，用于对信息技术产品的安全功能提供清晰可靠的评估。通过提供对产品符合安全标准能力的独立评估，通用标准认证可让客户增强对信息技术产品安全的信心，从而作出更加明智的决定。

通过 CCRA，成员国家/地区已同意以相同的信任等级认可信息技术产品的认证。认证前需要进行多项评估，包括：

- 保护描述文件 (PP)
- 安全目标 (ST)
- 安全功能要求 (SFR)
- 安全保证要求 (SAR)
- 评估保证等级 (EAL)

保护描述文件 (PP) 是指定某种设备类型安全要求（如移动性）的文稿，用于为同一类 IT 产品的评估提供可比性。CCRA 成员每年均不断增加，批准的 PP 列表也在不断扩充。此协定允许产品开发人员只需根据任一证书授权方案获得单次认证，该认证即会受到任一证书使用签署方的认可。

安全目标 (ST) 定义了认证 IT 产品时会评估**什么内容**。ST 会细化为更具体的**安全功能要求 (SFR)**，用于更细致地评估 ST。

通用标准 (CC) 还包括**安全保证要求。评估保证等级 (EAL)** 是一项被广泛认可的指标。EAL 集合了一系列常见的 SAR，可在 PP 和 ST 中指定以支持可比性。

许多较早的 PP 已归档，并逐步被专注于特定解决方案和环境而开发的针对性 PP 所取代。为了协力确保所有 CCRA 成员能够持续相互认可，国际技术社区 (iTC) 应运而生，其使命是开发和维护协作性保护描述文件 (cPP)，cPP 一开始就是在 CCRA 签署方案的基础上进行开发。针对用户群组和相互认可协定而非 CCRA 的 PP 继续由相应的利益相关方开发。

Apple 于 2015 年初就开始针对更新后的 CCRA 及其中所选 cPP 来寻求认证。自此之后，Apple 已经针对发布的每个 iOS 主要版本实现了通用标准认证，并扩大了覆盖范围以包括新 PP 所提供的安全保证。

Apple 在专注于移动安全技术评估的技术社区中积极发挥作用，其中包括负责开发和更新 cPP 的 iTC。Apple 将继续根据当前 PP 和 cPP 来评估和寻求认证。

Apple 一般通过美国国家信息保障合作联盟 (NIAP) 针对北美市场进行平台认证，该联盟维护了一个尚未认证但当前正在评估项目的列表。

除了列出的通用平台证书外，还有已签发的其他证书以说明某些市场的特定安全要求。

适用于 Apple App 的安全认证

Apple App 认证背景

Apple 积极使用相应的通用标准保护描述文件 (PP) 对 Apple App 进行安全认证。这些评估建立于 Apple 所获得的硬件和操作系统认证之上。

Apple 在 2018 年针对 iOS 11 上运行的关键应用程序 Safari 浏览器和“通讯录” App 启动了应用程序安全评估。Apple 针对 iOS 12、iOS 13 和 iPadOS 13.1 上运行的 App 继续进行了此类评估。2021 年，此类评估正逐渐扩展到 macOS 11 上运行的 App。

加密模块认证状态

此处列出的 Apple App 使用适用操作系统的加密模块。有关更多信息，请参阅适用于 iOS 的安全认证、适用于 iPadOS 的安全认证和适用于 macOS 的安全认证。

通用标准 (CC) 认证状态

由 NIAP 执行的美国方案维护了评估中产品列表；该列表中包括的产品当前正在美国的经 NIAP 批准的通用标准测试实验室 (CCTL) 中进行评估，且产品已完成评估启动会议（或对等会议），CCEVS 管理团队在会议中正式接受产品进入评估阶段。

产品认证之后，NIAP 会将当前有效的认证在其产品合规列表中列出。2 年后，这些认证会受到检查以确定是否符合当前的保证维护政策。超过保证维护期后，NIAP 会将认证列表项移到其已归档产品列表。

通用标准门户列出了根据通用标准认可协定 (CCRA) 可互相认可的认证。CC 门户可能在 5 年内维护已认证产品列表中的产品；该门户会保留已归档认证的记录。

下表显示当前正在实验室中进行评估或已认证为符合通用标准的认证。

目前状态

- 发布为正在进行的 NIAP 评估列在评估中产品 (NIAP) 上。
- 已完成且经验证的评估列在 NIAP 产品合规列表上。

操作系统/认证日期	方案 ID/文档	标题/保护描述文件
操作系统：macOS 11 Big Sur **认证日期：**—	**方案 ID：**尚未认证 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**macOS 11 Big Sur：通讯录 **保护描述文件：**适用于应用程序软件的 PP、适用于网页浏览器的 EP
操作系统：macOS 11 Big Sur **认证日期：**—	**方案 ID：**尚未认证 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**macOS 11 Big Sur：Safari 浏览器 **保护描述文件：**适用于应用程序软件的 PP、适用于网页浏览器的 EP
操作系统：iOS 14、iPadOS 14 **认证日期：**2021/8/20	**方案 ID：**11191 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**Apple iOS 14 和 iPadOS 14：通讯录 **保护描述文件：**适用于应用程序软件的 PP、适用于网页浏览器的 EP
操作系统：iOS 14、iPadOS 14 **认证日期：**—	**方案 ID：**11192 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**Apple iOS 14 和 iPadOS 14：Safari 浏览器 **保护描述文件：**适用于应用程序软件的 PP、适用于网页浏览器的 EP
操作系统：iOS 13、iPadOS 13 **认证日期：**2020/6/5	**方案 ID：**11060 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**Apple iOS 13 和 iPadOS 13：Safari 浏览器 **保护描述文件：**适用于应用程序软件的 PP、适用于网页浏览器的 EP

操作系统/认证日期	方案 ID/文档	标题/保护描述文件
操作系统：iOS 13、iPadOS 13 **认证日期：**2020/6/5	**方案 ID：**11050 **文档：** 认证 安全目标 指南 验证报告 保证活动报告	**标题：**Apple iOS 13 和 iPadOS 13：通讯录 **保护描述文件：**适用于应用程序软件的 PP

适用于 Apple App 的已归档通用标准认证

操作系统/认证日期	方案 ID/文档	标题/保护描述文件
操作系统：iOS 12 **认证日期：**2019/6/12	**方案 ID：**10960 **文档：** 安全目标 指南	**标题：**iOS 12 Safari 浏览器 **保护描述文件：**适用于应用程序软件的 PP、适用于网页浏览器的 EP
操作系统：iOS 12 **认证日期：**2019/2/28	**方案 ID：**10961 **文档：** 安全目标 指南	**标题：**iOS 12 通讯录 **保护描述文件：**适用于应用程序软件的 PP
操作系统：iOS 11 **认证日期：**2018/11/9	**方案 ID：**10916 **文档：** 安全目标 指南	**标题：**iOS 11 Safari 浏览器 **保护描述文件：**适用于应用程序软件的 PP、适用于网页浏览器的 EP
操作系统：iOS 11 **认证日期：**2018/9/13	**方案 ID：**10915 **文档：** 安全目标 指南	**标题：**iOS 11 通讯录 **保护描述文件：**适用于应用程序软件的 PP

适用于 Apple 互联网服务的安全认证

Apple 持续获有符合 ISO/IEC 27001 和 ISO/IEC 27018 标准的认证，以协助 Apple 客户履行其监管和合同义务。这些认证针对特定范围内的系统向客户提供了 Apple 信息安全和隐私实践的独立证明。

ISO/IEC 27001 和 ISO/IEC 27018 是信息安全管理系统 (ISMS) 标准系列的一部分，由国际标准化组织 (ISO) 发布。作为 Apple ISMS 的一部分，附录 A 的所有控制要求都包括在 ISO/IEC 27001 和 ISO/IEC 27018 标准所定义的“适用性声明”中。Apple 每年都会接受有资质的认证登记机构的独立证明。

ISO/IEC 27001

ISO/IEC 27001 是一项信息安全管理系统标准，指定了建立、实施、维护和持续改进组织的信息安全管理系统的要求。ISO/IEC 27001 标准包括了 Apple ISO/IEC 认证所涵盖的以下安全领域：

- 信息安全策略
- 信息安全结构
- 资产管理
- 人力资源安全
- 物理和环境安全
- 通信与操作管理
- 访问控制
- 信息系统购置、开发和维护
- 信息安全事件管理
- 业务连续性管理
- 合规

ISO/IEC 27018

ISO/IEC 27018 是一项行为守则，目的在于保护公有云环境中的个人可识别信息 (PII)。ISO/IEC 27018 标准包括了 Apple ISO/IEC 认证所涵盖的以下安全领域：

- 同意与选择权
- 目的合法性和规范
- 收集限制
- 数据最小化
- 使用、保留和披露限制
- 准确性和质量
- 公开、透明和声明
- 个人参与和访问权限
- 责任
- 信息安全
- 隐私合规

ISO/IEC 27001 和 ISO/IEC 27018 所涵盖的 Apple 服务

Apple ISO/IEC 27001 和 ISO/IEC 27018 认证涵盖了以下服务：

- Apple 商务聊天
- Apple 商务管理
- Apple 推送通知服务 (APNs)
- Apple 校园教务管理
- Claris Connect
- FaceTime 通话
- FileMaker Cloud
- iCloud
- iMessage 信息
- iWork 服务
- 管理式 Apple ID
- 课业
- Siri

认证

有关 Apple ISO/IEC 27001 和 27018 认证的证据，请访问我们的认证登记机构页面。

若要查看 Apple 的认证，请前往英国标准协会 (BSI) 网站的证书和客户名录搜索，在“公司名称”搜索栏中输入“Apple”，点按“搜索”按钮，然后选择搜索结果以查看认证。

【注】对于所提供的有关非 Apple 生产的产品信息或者并非由 Apple 控制或测试的独立网站，我们既不推荐，也不认可。Apple 对于第三方网站或产品的选择、性能或使用不承担任何责任。Apple 对第三方网站的准确性或可靠性不做任何声明。请联系供应商以获得更多信息。

macOS 安全合规项目

macOS 安全合规项目 (mSCP) 是开源项目，旨在提供一种生成安全指南的程序化方式。这是一个由来自美国国家标准与技术研究院 (NIST)、美国国家航空航天局 (NASA)、美国国防信息系统局 (DISA) 和美国洛斯阿拉莫斯国家实验室 (LANL) 的联邦 IT 安全执行人员联合参与的项目。该项目使用一组经测试并验证的 macOS 控制项目，并将这些控制项目对应到由该项目支持的任何安全指南。另外，此项目可作为资源使用，通过利用经测试并验证的原子操作（配置设置）库以轻松创建技术性安全控制的自定安全基准。该项目会根据所使用的基准输出自定文档、脚本、配置描述文件和一个审核检查表。

mSCP 可生成结合管理和安全工具使用的输出内容，从而达到合规标准。此项目中的配置设置支持以下指南基准：

组织	支持的基准
美国国家标准与技术研究院 (NIST) 特殊出版物 (SP) 800-53，为联邦信息系统和组织推荐的安全控制，修订版 5	800-53 高，800-53 中，800-53 低
美国国家标准与技术研究院 (NIST) 特殊出版物 (SP) 800-171，保护非联邦系统和组织中的受控非机密信息，修订版 2	800-171
美国国防信息系统局 (DISA) macOS 11 STIG、Apple macOS 11 安全技术实施指南	STIG
美国国家安全系统委员会 (CNSSI) 1253，国家安全系统的安全分类和控制选择	1253

其他信息：

- 此处提供的基准可用于检查该项目中的所有规则。
- 若要了解该项目和用途的更多信息，请参阅 macOS Security Compliance Project wiki（macOS 安全合规项目 wiki）。
- 若要设置该项目以供使用，请参阅：Getting to Know the macOS Security Compliance Project, Part 1（了解 macOS 安全合规项目，第 1 部分）和 Getting to Know the macOS Security Compliance Project, Part 2（了解 macOS 安全合规项目，第 2 部分）。
- 如果您对支持该项目的开发有兴趣，请参阅参与者指南。

文档修订记录

日期	摘要
2021 年 10 月 27 日	更新的主题： • 适用于安全隔区处理器的安全认证 • 适用于 iOS 的安全认证 • 适用于 macOS 的安全认证
2021 年 8 月 17 日	更新的主题： • 适用于安全隔区处理器的安全认证 • 适用于 Apple T2 安全芯片的安全认证 • 适用于 iOS 的安全认证 • 适用于 iPadOS 的安全认证 • 适用于 macOS 的安全认证 • 适用于 Apple tvOS 的安全认证 • 适用于 watchOS 的安全认证 • 适用于 Apple App 的安全认证 • 安全认证 • macOS 安全合规项目
2021 年 4 月 26 日	添加的主题： • macOS 安全合规项目 更新的主题： • 适用于 Apple T2 安全芯片的安全认证：新的 FIPS 140-2 认证 3811 • 适用于安全隔区处理器的安全认证：新的 FIPS 140-2 认证 3811 和其他认证的新表格。 • 适用于 iOS 的安全认证：新的 FIPS 140-2 认证 3811 和 iOS 14 方案 ID 11146（评估中） • 适用于 iPadOS 的安全认证：新的 FIPS 140-2 认证 3811 和 iPadOS 14 方案 ID 11147（评估中） • 适用于 macOS 的安全认证：新的 FIPS 140-2 认证 3811。 • 适用于 Apple tvOS 的安全认证：新的 FIPS 140-2 认证 3811。 • 适用于 watchOS 的安全认证：新的 FIPS 140-2 认证 3811。 • 适用于 Apple App 的安全认证：更新“通用标准”状态，以及已归档“通用标准”认证的新表格。

术语表

安全隔区处理器 (SEP) 预制在片上系统 (SoC) 内的协处理器。

安全级别 (SL) ISO/IEC 19790 中定义的四个整体安全级别 (1–4)，用于描述一系列适用安全要求。4 级为最严格级别。

安全目标 (ST) 指定特定产品安全问题和安全要求的文档。

安全元件 (SE) 多款 Apple 设备中内嵌的用于支持 Apple Pay 等功能的芯片。

保护描述文件 (PP) 指定特定类产品安全问题和安全要求的文档。

被测实现列表 (IUT) 正在实验室中进行测试的加密模块。

国际技术社区 (iTC) 负责在通用标准认可协定 (CCRA) 的支持下开发保护描述文件或协作性保护描述文件的小组。

加密模块 提供加密功能并且符合声明的加密模块标准要求的硬件、软件和/或固件。

加密模块验证体系 (CMVP) 由美国和加拿大政府运营的组织，旨在验证是否符合 FIPS 140-3 标准。

加密算法验证体系 (CAVP) 由 NIST 运营的组织，为已批准（例如，经 FIPS 批准和 NIST 建议）的加密算法及其单个组件提供验证测试。

联邦信息处理标准 (FIPS) 当法规有要求或者有针对网络安全的强制联邦政府要求（或两者皆有）时，由美国国家标准与技术研究院刊发的出版物。

美国国家标准与技术研究院 (NIST) 美国商务部中负责推进测量科学、标准和技术的部门。

美国国家信息保障合作联盟 (NIAP) 负责执行美国“通用标准”标准实施和管理 NIAP 通用标准评估和验证方案 (CCEVS) 的美国政府组织。

片上系统 (SoC) 将多个组件整合进单个芯片的集成电路 (IC)。

全磁盘加密 (FDE) 加密储存宗卷上的所有数据。

适用性声明 (SOA) 描述在 ISMS 范围内实施的安全控制的文档，为支持 ISO/IEC 27001 认证而产生。

通用标准 (CC) 建立 IT 安全评估一般概念和准则并指定评估通用模型的标准，其中包括以标准化语言描述的安全要求目录。

通用标准认可协定 (CCRA) 为根据 ISO/IEC 15408 系列或“通用标准”标准颁发的证书得到国际认可而确立政策和要求的相互认可协定。

协作性保护描述文件 (cPP) 由专门负责创建 cPP 的专家组而形成的国际技术社区所开发的保护描述文件。

信息安全管理系统 (ISMS) 划定安全计划边界的一系列信息安全策略和规程，旨在通过系统性管理整个信息和/或系统寿命周期中的信息安全来保护该信息和系统范围。

信息系统安全高级官员小组 (SOG-IS) 管理若干欧洲国家之间相互认可协定的小组。

移动设备管理 (MDM) 一种可让用户远程管理已注册设备的服务。设备注册后，用户可通过网络使用 MDM 服务来在设备上配置设置以及执行其他任务，无需进行用户交互。

正在验证模块 (MIP) 由加密模块验证体系 (CMVP) 维护、当前正处于 CMVP 验证流程中的加密模块列表。

Apple 商务管理 一个针对 IT 管理员且基于网站的简单门户，为组织提供了一种快速简单的方法来部署 Apple 设备，无论设备是组织直接从 Apple 购买的，还是购买自 Apple 合作授权经销商或运营商处。在用户获得设备前，管理员无需实际操作或者准备设备，即可在移动设备管理 (MDM) 解决方案中自动注册设备。

Apple 推送通知服务 (APNs) 一项由 Apple 提供的全球服务，用于向 Apple 设备传送推送通知。

Apple 校园教务管理 一个针对 IT 管理员且基于网站的简单门户，为组织提供了一种快速简单的方法来部署 Apple 设备，无论设备是组织直接从 Apple 购买的，还是购买自 Apple 合作授权经销商或运营商处。在用户获得设备前，管理员无需实际操作或者准备设备，即可在移动设备管理 (MDM) 解决方案中自动注册设备。

corecrypto 提供低等级加密原语实施的加密库。请注意 corecrypto 不直接向开发者提供编程接口，而是通过向开发者提供 API 来使用。corecrypto 源代码已公开，从而允许对其安全特性和正确运行进行验证。

IPsec VPN Client 在保护描述文件中，为实体或虚拟主机平台和远程位置之间提供安全 Ipsec 连接的客户端。

sepOS 安全隔区固件，基于 Apple 定制版本的 L4 微内核。

T2 2017 年起推出的基于 Intel 的部分 Mac 电脑中包括的 Apple 安全芯片。

Apple Inc.

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

CN028-00499-B