



保安認證和合規中心

2021 年 12 月

目錄

Apple 保安保障簡介	4
.....
硬件認證	4
軟件和 App 認證	5
服務認證	5
硬件保安認證	6
.....
Apple 硬件保安認證概覽	6
安全隔離區處理器的保安認證	8
Apple T2 保安晶片的保安認證	11
作業系統保安認證	15
.....
Apple 作業系統保安認證概覽	15
iOS 的保安認證	17
iPadOS 的保安認證	23
macOS 的保安認證	29
tvOS 的保安認證	35
watchOS 的保安認證	39
軟件保安認證	43
.....
Apple 軟件保安認證概覽	43
Apple App 的保安認證	44
Apple 互聯網服務的保安認證	47
.....
ISO/IEC 27001	47
ISO/IEC 27018	48
ISO/IEC 27001 和 ISO/IEC 27018 所涵蓋的 Apple 服務	48
認證	49

macOS 保安合規計劃	50
文件版本記錄	51
詞彙表	52

Apple 保安保障簡介

Apple 定期與第三方組織接觸，以認證和證明 Apple 的硬件、軟件和服務的保安，作為我們致力於保安的實踐。這些國際認可的組織為 Apple 提供了配合每個主要作業系統版本的認證。透過這種方式，它們提供了滿足系統保安需求的可信度（即保安保證）。對於尚未為「相互認可協議」（MRA）接受的技術領域或缺乏成熟的保安認證標準的技術領域，Apple 致力於開發適當的保安標準。我們的使命是讓 Apple 硬件、作業系統、App 和服務均獲得全球認可的全方位保安認證。

符合法律、規範和產業標準的要求，通常都需要認證。如 Apple School Manager 和 Apple Business Manager 之類的服務獲 Apple 的 ISO/IEC 27001 和 ISO/IEC 27018 認證。所有客戶，包括部署 Apple 裝置的政府機關以及企業和教育機構，都可以使用硬件、作業系統、軟件和服務認證來證明合規性。

硬件認證

因為安全軟件需以硬件的內置保安為基礎，因此 Apple 裝置（無論是使用 iOS、iPadOS、macOS、tvOS 或 watchOS）的晶片便植入了保安功能。這些包含支援系統安全功能的 CPU 技術，以及專用於安全功能的晶片。最關鍵的元件是「安全隔離區」協同處理器，該協同處理器出現在所有現今的 iOS、iPadOS、watchOS 和 tvOS 裝置，以及所有配備 Apple 晶片的 Mac 電腦和配備 Apple T2 保安晶片的以 Intel 為基礎的 Mac 電腦上。「安全隔離區」提供了加密靜態資料、macOS 安全開機和生物特徵辨識功能的基礎。

Apple 對保安保障的投入始於對晶片基礎安全元件的認證，從硬件信任根到安全開機執行，再到提供安全密鑰儲存庫的「安全隔離區」，以及使用 Touch ID 和 Face ID 的安全驗證。透過結合僅由 Apple 提供的晶片設計、硬件、軟件和服務，Apple 裝置的安全功能方能得以實現。這些元件的認證是驗證 Apple 所提供之保證很重要的一部份。

如需與硬件和相關韌體元件有關的公開認證資料，請參閱：

- [Apple T2 保安晶片的保安認證](#)
- [安全隔離區處理器的保安認證](#)

軟件和 App 認證

Apple 會針對作業系統和 App 分別維護認證和證明以遵循加密編譯模組的美國「聯邦資訊處理標準」(FIPS) 140-2/-3，以及作業系統、App 和裝置服務的「共同準則」。涵蓋的作業系統包括 iOS、iPadOS、macOS、sepOS、T2 韌體、tvOS 和 watchOS。至於 App 方面，獨立認證一開始包括 Safari 瀏覽器和「通訊錄」App，未來會認證更多 App。

如需與 Apple 作業系統有關的公開認證資訊，請參閱：

- [iOS 的保安認證](#)
- [iPadOS 的保安認證](#)
- [macOS 的保安認證](#)
- [tvOS 的保安認證](#)
- [watchOS 的保安認證](#)

如需與 Apple App 有關的公開認證資料，請參閱：

- [Apple App 的保安認證](#)

服務認證

Apple 維護保安認證，從企業到教育層面支持我們的客戶。這些認證使 Apple 客戶在將 Apple 服務與 Apple 硬件和軟件一起使用時，能夠履行其監管和合約義務。這些認證針對 Apple 系統的 Apple 資訊保安、環境和私隱權實務，為客戶提供了獨立證明。

如需與 Apple 互聯網服務有關的公開認證資料，請參閱：

- [Apple 互聯網服務的保安認證](#)

如有 Apple 保安和私隱認證的相關問題，請聯絡 security-certifications@apple.com。

硬件保安認證

Apple 硬件保安認證概覽

Apple 為 sepOS 和 T2 韌體維護美國「聯邦資訊處理標準」(FIPS) 140-2/-3 的「符合標準驗證憑證」以及其他認證。Apple 從**認證建置組塊**開始著手，此建置組塊可在適用情況下跨多個平台廣泛應用。其中一個建置組塊就是 Corecrypto 資料庫的驗證，其用於 Apple 所開發作業系統內的軟硬件加密編譯模組部署。第二個建置組塊是「安全隔離區」(內嵌在許多 Apple 裝置內)的認證。第三個則是配備 Touch ID 的 Apple 裝置和配備 Face ID 的裝置所包含 Secure Element (SE) 的認證。這些硬件認證建置組塊為更廣泛的平台保安認證形成了基礎。

加密編譯演算法驗證

驗證許多加密編譯演算法和相關保安功能的執行正確性，是 FIPS 140-3 驗證和支援其他認證的先決條件。驗證由美國「國家標準技術研究院」(NIST)「加密編譯演算法驗證計劃」(CAVP) 管理。你可使用 [CAVP 搜尋](#) 工具來找到 Apple 落實有關計劃的驗證憑證。如需更多資料，請參閱：[「加密編譯演算法驗證計劃」\(CAVP\) 網站](#)。

加密編譯模組驗證：FIPS 140-2/3 (ISO/IEC 19790)

自 2012 年起，每個主要作業系統版本發佈後，「加密編譯模組驗證計劃」(CMVP) 都會反覆驗證 Apple 的加密編譯模組是否符合加密編譯模組的美國「聯邦資訊處理標準」(FIPS 140-2)。每次發行主要版本後，Apple 都會向 CMVP 提交模組，以驗證是否符合標準。這些模組不僅可以由 Apple 作業系統和 App 使用，還可以為 Apple 提供的服務提供加密編譯功能，並且可供第三方 App 使用。

Apple 每年都針對以軟件為基礎的模組 (macOS 的「Intel 適用的 Corecrypto 模組」和「Intel 適用的 Corecrypto 核心模組」) 達到**保安層級 1**。至於 Apple 晶片，「ARM 適用的 Corecrypto 模組」和「ARM 適用的 Corecrypto 核心模組」此兩個模組適用於 iOS、iPadOS、tvOS、watchOS 以及 Mac 電腦所配備 Apple T2 保安晶片內嵌的韌體。

2019 年，Apple 已針對嵌入式硬件加密編譯模組 (稱為「Apple CoreCrypto 模組：安全密鑰儲存庫」) 實現第一個 FIPS 140-2 **保安層級 2**，進而讓美國政府核准使用「安全隔離區」中產生和管理的密鑰。Apple 會繼續致力為後續每個主要作業系統版本達成硬件加密編譯模組的驗證。

FIPS 140-3 已於 2019 年獲得美國商務部核准。此版本標準中最重要的變更為 ISO/IEC 標準規格，特別是 ISO/IEC 19790:2015 及相關的測試標準 ISO/IEC 24759:2017。CMVP 已啟動轉移計劃，並表示自 2020 年起，將開始使用 FIPS 140-3 為基礎來驗證加密編譯模組。一旦可實行，Apple 加密編譯模組將以符合並轉移至 FIPS 140-3 標準為目標。

針對目前正在進行測試和驗證流程的加密編譯模組，CMVP 維護兩份獨立列表，其中可能包含有關建議驗證的資料。針對正透過官方授權實驗室進行測試的加密編譯模組，[實作待測列表 \(Implementation Under Test List\)](#) 可能會列出模組。在實驗室完成測試後，便可以建議 CMVP 進行驗證，Apple 加密編譯模組就會顯示在[檢測中的模組列表 \(Modules in Process List\)](#) 中。目前，實驗室測試已經完成，並正在等待 CMVP 對測試進行驗證。因為評估程序所需的時間各異，請查看這兩個程序列表，以確定在主要作業系統版本發佈之日與 CMVP 發出驗證憑證之間，Apple 加密編譯模組的目前狀態。

產品認證：共同準則 (ISO/IEC 15408)

「共同準則」(ISO/IEC 15408) 是許多組織採用的標準，以其為基礎進行 IT 產品的保安評估。

如需了解有哪些認證可根據國際「共同準則承認協定」(CCRA) 相互認可，請參閱：[共同準則入口網站](#)。國家和私人驗證架構也可在不受 CCRA 限制的情況下使用「共同準則」標準。在歐洲，相互認可受 [SOG-IS 協議](#) 和 CCRA 管轄。

根據「共同準則」社群所述，其目標是制訂一套國際認可的保安標準，以明確可靠地評估資訊科技產品的保安功能。「共同準則認證」會對產品能否符合保安標準進行獨立評估，以讓客戶提升對資訊科技產品保安的信心，進而作出更有依據的決定。

透過 CCRA，[會員國家](#) 已同意抱持相同的信心度，認可該資訊技術產品認證。認證之前需要進行的評估相當廣泛，包括：

- 保護剖繪 (PP)
- 保安目標 (ST)
- 保安功能要求 (SFR)
- 保安保障要求 (SAR)
- 評估保證等級 (EAL)

「保護剖繪」(PP) 是用於指定一類別之裝置類型 (例如「流動性」) 的保安需求的文件，並用於提供同一類別 IT 產品評估之間的比較性。CCRA 會員數量以及已核准 PP 的累積列表每年均持續成長。這項協定讓產品開發者無論採用任何一種認證授權架構，都只需取得單一認證，並會獲得任何 CCRA 簽署者的認可。

「保安目標」(ST) 定義了認證 IT 產品時將評估的內容。ST 被演繹成更具體的「**保安功能要求**」(SFR)，用於更詳細地評估 ST。

「共同準則」(CC) 還包括「**保安保障要求**」。一種常見的認可指標是「**評估保證等級**」(EAL)。EAL 將頻繁出現的 SAR 集群組合在一起，可以在 PP 和 ST 中加以指定以提高比較性。

許多舊版 PP 已封存，且已由專為特定解決方案和環境所制訂的針對式 PP 取代。為協力確保所有 CCRA 會員之間能持續相互認可，已建立了「國際技術社群」(ITC)，以推動和維護從一開始就在 CCRA 簽署架構的參與下所開發的「合作保護剖繪」(cPP)。相關的持份者將繼續開發以 CCRA 以外之用戶群組和相互認可協議為對象的 PP。

從 2015 年初開始，Apple 便開始根據更新的 CCRA (包含特定 cPP) 致力取得認證。自當時起，Apple 的每個主要 iOS 版本均獲得「共同準則」認證，並擴展涵蓋範圍以納入新版 PP 提供的保安保障。

Apple 在專門進行流動保安技術評估的技術社群中扮演著積極角色。這些包含負責開發和更新 cPP 的 ITC。Apple 持續依據目前的 PP 和 cPP 進行評估和爭取認證。

針對北美市場，Apple 平台認證一般透過美國「國家資訊保證合作組織」(NIAP) 進行，此組織維護一份列表，以列出 [目前已在評估中但尚未通過認證的專案](#)。

除了列出的一[般平台憑證](#)以外，亦有核發其他認證，以證明部份市場的特定安全要求。

安全隔離區處理器的保安認證

安全隔離區認證背景

硬件加密編譯模組 (Apple SEP 安全密鑰儲存庫加密編譯模組) 內嵌在以下產品的 Apple SOC 中: 適用於 iPhone 和 iPad 的 Apple A 系列、適用於配備 Apple 晶片的 Mac 電腦的 M 系列、適用於 Apple Watch 的 S 系列, 以及從 2017 年推出的 iMac Pro 開始, 在以 Intel 為基礎的 Mac 電腦所採用的 T 系列安全晶片。

在 2018 年, Apple 將軟件加密編譯模組的驗證與 2017 年發布的作業系統 (iOS 11、macOS 10.13、tvOS 11 和 watchOS 4) 加以同步化。SEP 硬件加密編譯模組 (被識別為「Apple SEP 安全密鑰儲存庫加密編譯模組 v1.0」) 最初是根據 FIPS 140-2 保安層級 1 的要求完成驗證。

在 2019 年, Apple 根據 FIPS 140-2 保安層級 2 的要求驗證了硬件模組, 並將模組版本識別碼更新為 v9.0, 以便與對應的「CoreCrypto 用戶」和「CoreCrypto 核心」模組驗證的版本保持同步。在 2019 年, 這包含 iOS 12、macOS 10.14、tvOS 12 和 watchOS 5。

在 2020 和 2021 年, Apple 致力取得驗證以與 FIPS 140-3 達成一致, 並額外保證 Apple 晶片物理保安需求的保安層級 3: A13、A14、S6 和 M1 晶片。

Apple 也針對作業系統每個主要版本積極參與「CoreCrypto 用戶」和「CoreCrypto 核心」模組的驗證。一致性驗證只能針對最終發行版本執行。

加密編譯模組驗證狀態

「加密編譯模組驗證計劃」(CMVP) 根據其目前狀態在三個單獨列表下維護加密編譯模組的驗證狀態:

- 為了被列入 CMVP [實作待測列表 \(Implementation Under Test List\)](#) 中, 實驗室必須與 Apple 簽約以提供測試。
- 在實驗室完成測試後, 便可以建議 CMVP 進行驗證並且支付 CMVP 費用, 然後將該模組加到 [檢測中的模組列表 \(Modules in Process List\)](#) 中。「MIP 列表」會分開四個階段來追蹤 CMVP 驗證工作的進度:
 - **待審核:** 等待指派 CMVP 資源。
 - **審核中:** CMVP 資源正在執行其驗證程序。
 - **協調:** 實驗室和 CMVP 正在解決發現的所有問題。
 - **最終處理:** 與簽發認證有關的程序和手續。
- 在通過 CMVP 驗證後, 將向模組授予一致性認證, 並將其加到 [已驗證的加密編譯模組列表](#) 中。這包括:
 - 標示為 **作用中** 的已驗證模組。
 - 5 年過後, 模組會標示為 **歷史**。
 - 如果模組憑證因某些原因遭撤銷時, 則會標示為 **已撤銷**。

在 2020 年, CMVP 採用了國際標準 ISO/IEC 19790 作為 FIPS 140-3 的基礎。

FIPS 140-3 認證

目前狀態

下表顯示實驗室目前正在測試是否符合 FIPS 140-3 的 2020 和 2021 加密編譯模組。

與 2020 和 2021 年作業系統發佈相關聯的「安全密鑰儲存庫」(SKS) 已完成實驗室測試，並已由實驗室推薦給 CMVP 進行驗證。它們列於[檢測中的模組列表 \(Modules in Process List\)](#)，驗證完成後會移至[已驗證的加密編譯模組列表](#)。

iOS 15 (2021 年) 用戶空間、核心空間和安全密鑰儲存庫正在接受實驗室測試。它們列於[實作待測列表 \(Implementation Under Test List\)](#) 中。

日期	認證/文件	模組資料
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: 與 2021 年發佈的 iOS、iPadOS、macOS、tvOS 和 watchOS 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (A9-A14、T2、M1、S3-S6) 整體保安層級: 2
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: 與 2021 年發佈的 iOS、iPadOS、macOS、tvOS 和 watchOS 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (A13、A14、S6、M1) 整體保安層級: 2 物理保安層級: 3
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: 與 2020 年發佈的 iOS、iPadOS、macOS、tvOS 和 watchOS 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (A9-A14、T2、M1、S3-S6) 整體保安層級: 2
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: 與 2020 年發佈的 iOS、iPadOS、macOS、tvOS 和 watchOS 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (A13、A14、S6、M1) 整體保安層級: 2 物理保安層級: 3

FIPS 140-2 認證

下表顯示已經過實驗室測試是否符合 FIPS 140-2 的加密編譯模組。

日期	認證/文件	模組資料
作業系統發佈日期: 2019 完成驗證日期: 2021 年 2 月 5 日	認證: 3811 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple 安全密鑰儲存庫加密編譯模組 v10.0 作業系統: macOS 10.15 Catalina 的 sepOS 類型: 硬件 保安層級: 2
作業系統發佈日期: 2018 完成驗證日期: 2019 年 9 月 10 日	認證: 3523 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple 安全密鑰儲存庫加密編譯模組 v9.0 作業系統: macOS 10.14 Mojave 的 sepOS 類型: 硬件 保安層級: 2
作業系統發佈日期: 2017 完成驗證日期: 2019 年 9 月 10 日	認證: 3223 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple 安全密鑰儲存庫加密編譯模組 v1.0 作業系統: macOS 10.13 High Sierra 的 sepOS 類型: 硬件 保安層級: 2

「共同準則」(CC) 認證

Apple 積極參與「共同準則」評估, 其中適當的保護剖繪涵蓋 Apple 技術的保安功能。

「共同準則」(CC) 認證狀態

由 NIAP 運作的美國計劃維護著一份「[評估中的產品](#)」列表, 該列表包括目前正在美國透過 NIAP 認可的共同準則測試實驗室 (CCTL) 進行評估並且已經完成「評估啟動會議」(或同級) 的產品, 而 CCEVS 管理層在該會議中已正式接受產品進行評估。

在產品認證後, NIAP 會在「[產品相容](#)」列表中列出目前有效的認證。2 年後, 將對這些認證進行審查以確保其符合目前的保障維護政策。在保障維護日期到期後, NIAP 會將認證列表項目移至其「[已封存產品](#)」列表。

「[共同準則入口網站](#)」列出了可以在「共同準則承認協定」(CCRA) 下互相認可的認證。CC 入口網站可以將產品保留在認證產品列表中 5 年, 記錄則會由 CC 入口網站保留以供[存檔認證](#)。

下表顯示了目前正在由實驗室評估的認證，或已被認證符合「共同準則」的認證。

作業系統/認證日期	計劃 ID/文件	標題/保護剖繪
作業系統: sepOS 認證日期: —	計劃 ID: 尚未通過認證 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: Apple 安全隔離區 [2020] 保護剖繪: CPP_DSC_V1.0 硬件: 安全隔離區 (A9-A14、M1、T2、S3-S6) 軟件: 與 iOS 14、iPadOS 14、macOS 11 Big Sur、tvOS 14、watchOS 7 一起發佈的 sepOS

其他認證

以下表格顯示不使用「共同準則」或 FIPS 140-3 的「安全隔離區」認證。

日期	認證/文件	模組資料
作業系統發佈日期: 2020 完成驗證日期: 2019 年 12 月 7 日到 2022 年 12 月 26 日	認證: CFNR201902910002 (中華人民共和國: 移動金融技術服務認證) 中文版 英文版	標題: 流動終端可信執行環境 作業系統: iOS 13.5.1 規範: JR/T 0156-2017

Apple T2 保安晶片的保安認證

加密編譯模組驗證背景

Apple 針對作業系統每個主要版本積極參與 Apple 內嵌軟件和硬件模組的驗證。一致性驗證只能針對最終模組發行版本執行。

2020 年，CMVP 採用了國際標準 ISO/IEC 19790 作為美國「聯邦資訊處理標準」(FIPS) 140-3 的基礎。

自 2017 年以來，除了 Intel CPU 外，大多數 Mac 電腦也配備獨立的 Apple T2 保安晶片，該晶片是以 Apple 晶片為基礎的單晶片系統 (SoC)。這些配備 T2 晶片的 Mac 電腦會使用所有五個加密編譯模組來提供各個裝置上的服務。

- Intel 適用的 Corecrypto 用戶模組 (由以 Intel 為基礎的 Mac 電腦的 macOS 使用)
- Intel 適用的 Corecrypto 核心模組 (由以 Intel 為基礎的 Mac 電腦的 macOS 使用)
- ARM 適用的 Corecrypto 用戶模組 (由 T2 晶片使用)
- ARM 適用的 Corecrypto 核心模組 (由 T2 晶片使用)
- 安全密鑰儲存庫加密編譯模組 (由 T2 晶片中的內嵌「安全隔離區」協同處理器使用)

附註: 在 T2 晶片上執行的 Apple 晶片架構模組與在其他 Apple 晶片 (例如 Apple A 系列、S 系列和 M 系列) 上執行的模組相同。

加密編譯模組驗證狀態

「加密編譯模組驗證計劃」(CMVP) 根據其目前狀態在三個單獨列表下維護加密編譯模組的驗證狀態：

- 為了被列入 CMVP [實作待測列表 \(Implementation Under Test List\)](#) 中，實驗室必須與 Apple 簽約以提供測試。
- 在實驗室完成測試後，便可以建議 CMVP 進行驗證並且支付 CMVP 費用，然後將該模組加到[檢測中的模組 \(MIP\) 列表](#)中。「MIP 列表」會分開四個階段來追蹤 CMVP 驗證工作的進度：
 - 待審核**：等待指派 CMVP 資源。
 - 審核中**：CMVP 資源正在執行其驗證程序。
 - 協調**：實驗室和 CMVP 正在解決發現的所有問題。
 - 最終處理**：與簽發認證有關的程序和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性認證，並將其加到[已驗證的加密編譯模組列表](#)中。這包括：
 - 標示為**作用中**的已驗證模組。
 - 5 年過後，模組會標示為**歷史**。
 - 如果模組憑證因某些原因遭撤銷時，則會標示為**已撤銷**。

FIPS 140-3 認證

目前狀態

用戶空間、核心空間和安全密鑰儲存庫的 2020 年模組已完成實驗室測試，並已由實驗室推薦給 CMVP 進行驗證。它們列於[檢測中的模組列表 \(Modules in Process List\)](#)。

用戶空間、核心空間和安全密鑰儲存庫的 2021 年模組正在接受實驗室測試。它們列於[實作待測列表 \(Implementation Under Test List\)](#) 中。

日期	認證/文件	模組資料
作業系統發佈日期：2021 完成驗證日期：—	認證：尚未通過認證 文件： 認證 保安規則 Crypto Officer 指引	標題：Apple Corecrypto 模組 v12.0 作業系統：macOS 12 Monterey 的 sepOS 環境：Apple 晶片、用戶、軟件 類型：軟件 保安層級：1
作業系統發佈日期：2021 完成驗證日期：—	認證：尚未通過認證 文件： 認證 保安規則 Crypto Officer 指引	標題：Apple Corecrypto 模組 v12.0 作業系統：macOS 12 Monterey 的 sepOS 環境：Apple 晶片、核心、軟件 類型：軟件 保安層級：1
作業系統發佈日期：2021 完成驗證日期：—	認證：尚未通過認證 文件： 認證 保安規則 Crypto Officer 指引	標題：Apple Corecrypto 模組 v12.0 作業系統：macOS 12 Monterey 的 sepOS 環境：Apple 晶片、安全密鑰儲存庫、硬件 類型：硬件 (T2) 保安層級：2

日期	認證/文件	模組資料
作業系統發佈日期:2020 完成驗證日期:—	認證:尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 模組 v11.1 作業系統:macOS 11 Big Sur 的 sepOS 環境:Apple 晶片、用戶、軟件 類型:軟件 保安層級:1
作業系統發佈日期:2020 完成驗證日期:—	認證:尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 模組 v11.1 作業系統:macOS 11 Big Sur 的 sepOS 環境:Apple 晶片、核心、軟件 類型:軟件 保安層級:1
作業系統發佈日期:2020 完成驗證日期:—	認證:尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 模組 v11.1 作業系統:Intel 上的 macOS 11 Big Sur 的 sepOS 環境:Apple 晶片、安全密鑰儲存庫、硬件 類型:硬件 保安層級:2

FIPS 140-2 認證

下表顯示已經過實驗室測試是否符合 FIPS 140-2 的加密編譯模組。

日期	認證/文件	模組資料
作業系統發佈日期:2019 完成驗證日期:2021年3月23日	認證: 3856 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶 模組 v10.0 作業系統:macOS 10.15 Catalina 的 sepOS 類型:軟件 保安層級:1
作業系統發佈日期:2019 完成驗證日期:2021年3月23日	認證: 3855 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心 模組 v10.0 作業系統:macOS 10.15 Catalina 的 sepOS 類型:軟件 保安層級:1
作業系統發佈日期:2019 完成驗證日期:2021年2月5日	認證: 3811 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 安全密鑰儲存庫加 密編譯模組 v10.0 作業系統:macOS 10.15 Catalina 的 sepOS 類型:硬件 保安層級:2
作業系統發佈日期:2018 完成驗證日期:2019年4月23日	認證: 3438 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶 模組 v9.0 作業系統:macOS 10.14 Mojave 的 sepOS 類型:軟件 保安層級:1

日期	認證/文件	模組資料
作業系統發佈日期:2018 完成驗證日期:2019年4月11日	認證: 3433 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心模組 v9.0 作業系統:macOS 10.14 Mojave 的 sepOS 類型:軟件 保安層級:1
作業系統發佈日期:2018 完成驗證日期:2019年9月10日	認證: 3523 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple 安全密鑰儲存庫加密編譯模組 v9.0 作業系統:macOS 10.14 Mojave 的 sepOS 類型:硬件 保安層級:2
作業系統發佈日期:2017 完成驗證日期:2018年3月9日、 2018年5月22日、2018年7月6日	認證: 3148 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶模組 v8.0 作業系統:macOS 10.13 High Sierra 的 sepOS 類型:軟件 保安層級:1
作業系統發佈日期:2017 完成驗證日期:2018年3月9日、 2018年5月17日、2018年7月3日	認證: 3147 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心模組 v8.0 作業系統:macOS 10.13 High Sierra 的 sepOS 類型:軟件 保安層級:1
作業系統發佈日期:2017 完成驗證日期:2018年7月10日	認證: 3223 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple 安全密鑰儲存庫加密編譯模組 v1.0 作業系統:macOS 10.13 High Sierra 的 sepOS 類型:硬件 保安層級:2
作業系統發佈日期:2016 完成驗證日期:2017年2月1日	認證: 2828 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple iOS CoreCrypto 核心模組 v7.0 作業系統:macOS 10.12 Sierra 的 sepOS 類型:軟件 保安層級:1
作業系統發佈日期:2016 完成驗證日期:2017年2月1日	認證: 2827 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple iOS CoreCrypto 核心模組 v7.0 作業系統:macOS 10.12 Sierra 的 sepOS 類型:軟件 保安層級:1

作業系統保安認證

Apple 作業系統保安認證概覽

Apple 為 sepOS 和 T2 韌體維護美國「聯邦資訊處理標準」(FIPS) 140-2/-3 的「符合標準驗證憑證」以及其他認證。Apple 從**認證建置組塊**開始著手，此建置組塊可在適用情況下跨多個平台廣泛應用。其中一個建置組塊就是 Corecrypto 的驗證，其用於 Apple 所開發作業系統內的軟硬件加密編譯模組部署。第二個建置組塊是「安全隔離區」(內嵌在許多 Apple 裝置內)的認證。第三個則是配備 Touch ID 的 Apple 裝置和配備 Face ID 的裝置所包含 Secure Element (SE) 的認證。這些硬件認證建置組塊為更廣泛的平台保安認證形成了基礎。

加密編譯演算法驗證

驗證許多加密編譯演算法和相關保安功能的執行正確性，是 FIPS 140-3 驗證和支援其他認證的先決條件。驗證由 NIST [加密編譯演算法驗證程式 \(CAVP\)](#) 管理。你可使用 [CAVP 搜尋](#) 工具來找到 Apple 落實有關計劃的驗證憑證。

加密編譯模組驗證：FIPS 140-2/3 (ISO/IEC 19790)

自 2012 年起，每個主要作業系統版本發佈後，「加密編譯模組驗證計劃」(CMVP) 都會反覆驗證 Apple 作業系統中的加密編譯模組是否符合美國「聯邦資訊處理標準」(FIPS) 140-2。每次發行主要版本後，Apple 都會向 CMVP 提交所有模組以進行完整的加密編譯驗證。這些經過驗證的模組為 Apple 供應的服務提供了加密編譯作業，且可供第三方 App 取用。

Apple 每年都針對以軟件為基礎的模組 (macOS 的「Intel 適用的 Corecrypto 模組」和「Intel 適用的 Corecrypto 核心模組」達到**保安層級 1**。至於 Apple 晶片，「ARM 適用的 Corecrypto 模組」和「ARM 適用的 Corecrypto 核心模組」此兩個模組適用於 iOS、iPadOS、tvOS、watchOS 以及 Mac 電腦所配備 Apple T2 保安晶片內嵌的韌體。

2019 年，Apple 已針對嵌入式硬件加密編譯模組 (稱為「Apple CoreCrypto 模組：安全密鑰儲存庫」) 實現第一個 FIPS 140-2 **保安層級 2**，進而讓美國政府核准使用「安全隔離區」中產生和管理的密鑰。Apple 會繼續致力為後續每個主要作業系統版本達成硬件加密編譯模組的驗證。

FIPS 140-3 已於 2019 年獲得美國商務部核准。此版本標準中最重要的變更為 ISO/IEC 標準規格，特別是 ISO/IEC 19790:2015 及相關的測試標準 ISO/IEC 24759:2017。CMVP 已啟動轉移計劃，並表示自 2020 年起，將開始使用 FIPS 140-3 為基礎來驗證加密編譯模組。一旦可實行，Apple 加密編譯模組將以符合並轉移至 FIPS 140-3 標準為目標。

針對目前正在進行測試和驗證流程的加密編譯模組，CMVP 維護兩份獨立列表，其中可能包含有關建議驗證的資料。針對正透過官方授權實驗室進行測試的加密編譯模組，[實作待測列表 \(Implementation Under Test List\)](#) 可能會列出模組。在實驗室完成測試後，便可以建議 CMVP 進行驗證，Apple 加密編譯模組就會顯示在[檢測中的模組列表 \(Modules in Process List\)](#) 中。目前，實驗室測試已經完成，並正在等待 CMVP 對測試進行驗證。因為評估程序所需的時間各異，請查看這兩個程序列表，以確定在主要作業系統版本發佈之日與 CMVP 發出驗證憑證之間，Apple 加密編譯模組的目前狀態。

產品認證：共同準則 (ISO/IEC 15408)

「共同準則」(ISO/IEC 15408) 是許多組織採用的標準，以其為基礎進行 IT 產品的保安評估。

如需了解有哪些認證可根據國際「共同準則承認協定」(CCRA) 相互認可，請參閱：[共同準則入口網站](#)。國家和私人驗證架構也可在不受 CCRA 限制的情況下使用「共同準則」標準。在歐洲，相互認可受 [SOG-IS 協議](#) 和 CCRA 管轄。

根據「共同準則」社群所述，其目標是制訂一套國際認可的保安標準，以明確可靠地評估資訊科技產品的保安功能。「共同準則認證」會對產品能否符合保安標準進行獨立評估，以讓客戶提升對資訊科技產品保安的信心，進而作出更有依據的決定。

透過 CCRA，[會員國家](#) 已同意抱持相同的信心度，認可該資訊技術產品認證。認證之前需要進行的評估相當廣泛，包括：

- 保護剖繪 (PP)
- 保安目標 (ST)
- 保安功能要求 (SFR)
- 保安保障要求 (SAR)
- 評估保證等級 (EAL)

「保護剖繪」(PP) 是用於指定一類別之裝置類型 (例如「流動性」) 的保安需求的文件，並用於提供同一類別 IT 產品評估之間的可比較性。CCRA 會員數量以及已核准 PP 的累積列表每年均持續成長。這項協定讓產品開發者無論採用任何一種認證授權架構，都只需取得單一認證，並會獲得任何 CCRA 簽署者的認可。

「保安目標」(ST) 定義了認證 IT 產品時將評估的內容。ST 被演繹成更具體的「**保安功能要求**」(SFR)，用於更詳細地評估 ST。

「共同準則」(CC) 還包括「**保安保障要求**」。一種常見的認可指標是「**評估保證等級**」(EAL)。EAL 將頻繁出現的 SAR 集群組合在一起，可以在 PP 和 ST 中加以指定以提高可比較性。

許多舊版 PP 已封存，且已由專為特定解決方案和環境所制訂的針對式 PP 取代。為協力確保所有 CCRA 會員之間能持續相互認可，已建立了「國際技術社群」(ITC)，以推動和維護從一開始就在 CCRA 簽署架構的參與下所開發的「**合作保護剖繪**」(cPP)。相關的持份者將繼續開發以 CCRA 以外之用戶群組和相互認可協議為對象的 PP。

從 2015 年初開始，Apple 便開始根據更新的 CCRA (包含特定 cPP) 致力取得認證。自當時起，Apple 的每個主要 iOS 版本均獲得「共同準則」認證，並擴展涵蓋範圍以納入新版 PP 提供的保安保障。

Apple 在專門進行流動保安技術評估的技術社群中扮演著積極角色。這些包含負責開發和更新 cPP 的 ITC。Apple 持續依據目前的 PP 和 cPP 進行評估和爭取認證。

針對北美市場，Apple 平台認證一般透過美國「國家資訊保證合作組織」(NIAP) 進行，此組織維護一份列表，以列出 [目前已在評估中但尚未通過認證的專案](#)。

除了列出的一般平台憑證以外，亦有核發其他認證，以證明部份市場的特定安全要求。

iOS 的保安認證



iOS 認證背景

Apple 針對作業系統每個主要版本積極參與 Apple 內嵌軟件和硬件模組的驗證。一致性驗證只能針對最終發行版本執行。

iOS 加密編譯模組驗證狀態

「加密編譯模組驗證計劃」(CMVP) 根據其目前狀態在三個單獨列表下維護加密編譯模組的驗證狀態：

- 為了被列入 CMVP [實作待測列表 \(Implementation Under Test List\)](#) 中，實驗室必須與 Apple 簽約以提供測試。
- 在實驗室完成測試後，便可以建議 CMVP 進行驗證並且支付 CMVP 費用，然後將該模組加到[檢測中的模組 \(MIP\) 列表](#)中。「MIP 列表」會分開四個階段來追蹤 CMVP 驗證工作的進度：
 - **待審核**：等待指派 CMVP 資源。
 - **審核中**：CMVP 資源正在執行其驗證程序。
 - **協調**：實驗室和 CMVP 正在解決發現的所有問題。
 - **最終處理**：與簽發認證有關的程序和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性認證，並將其加到[已驗證的加密編譯模組列表](#)中。這包括：
 - 標示為**作用中**的已驗證模組。
 - 5 年過後，模組會標示為**歷史**。
 - 如果模組憑證因某些原因遭撤銷時，則會標示為**已撤銷**。

在 2020 年，CMVP 採用了國際標準 ISO/IEC 19790 作為 FIPS 140-3 的基礎。

FIPS 140-3 認證

目前狀態

iOS 14 (2020) 用戶空間、核心空間和安全密鑰儲存庫已完成實驗室測試，並已由實驗室推薦給 CMVP 進行驗證。它們列於[檢測中的模組列表 \(Modules in Process List\)](#)。

iOS 15 (2021 年) 用戶空間、核心空間和安全密鑰儲存庫正在接受實驗室測試。它們列於[實作待測列表 \(Implementation Under Test List\)](#) 中。

日期	認證/文件	模組資料
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: iOS 15 環境: Apple 晶片、用戶、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: iOS 15 環境: Apple 晶片、核心、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: 與 iOS 15 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (A9-A14) 整體保安層級: 2
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: 與 iOS 15 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (A13、A14、A15) 整體保安層級: 2 物理保安層級: 3
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: iOS 14 環境: Apple 晶片、用戶、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: iOS 14 環境: Apple 晶片、核心、軟件 類型: 軟件 整體保安層級: 1

日期	認證/文件	模組資料
作業系統發佈日期:2020 完成驗證日期:—	認證:尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 模組 v11.1 作業系統:與 iOS 14 一起發佈的 sepOS 環境:Apple 晶片、安全密鑰儲存庫、硬件 類型:硬件 (A9-A14) 整體保安層級:2
作業系統發佈日期:2020 完成驗證日期:—	認證:尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 模組 v11.1 作業系統:與 iOS 14 一起發佈的 sepOS 環境:Apple 晶片、安全密鑰儲存庫、硬件 類型:硬件 (A13-A14) 整體保安層級:2 物理保安層級:3

FIPS 140-2 認證

下表顯示實驗室目前正在測試以及已通過測試符合 FIPS 140-2 的加密編譯模組。

日期	認證/文件	模組資料
作業系統發佈日期:2019 完成驗證日期:2021年3月23日	認證:3856 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶模組 v10.0 作業系統:iOS 13 類型:軟件 保安層級:1
作業系統發佈日期:2019 完成驗證日期:2021年3月23日	認證:3855 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心模組 v10.0 作業系統:iOS 13 類型:軟件 保安層級:1
作業系統發佈日期:2019 完成驗證日期:2021年2月5日	認證:3811 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple 安全密鑰儲存庫加密編譯模組 v10.0 作業系統:與 iOS 13 一起發佈的 sepOS 類型:硬件 保安層級:2
作業系統發佈日期:2018 完成驗證日期:2019年4月23日	認證:3438 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心模組 v9.0 作業系統:iOS 12 類型:軟件 保安層級:1
作業系統發佈日期:2018 完成驗證日期:2019年4月11日	認證:3433 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶模組 v9.0 作業系統:iOS 12 類型:軟件 保安層級:1

日期	認證/文件	模組資料
作業系統發佈日期:2018 完成驗證日期:2019年9月10日	認證: 3523 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple 安全密鑰儲存庫加密編譯模組 v9.0 作業系統:與 iOS 12 一起發佈的 sepOS 類型:硬件 保安層級:2
作業系統發佈日期:2017 完成驗證日期:2018年3月9日、2018年5月22日、2018年7月6日	認證: 3148 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶模組 v8.0 作業系統:iOS 11 類型:軟件 保安層級:1
作業系統發佈日期:2017 完成驗證日期:2018年3月9日、2018年5月17日、2018年7月3日	認證: 3147 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心模組 v8.0 作業系統:iOS 11 類型:軟件 保安層級:1
作業系統發佈日期:2017 完成驗證日期:2019年9月10日	認證: 3223 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple 安全密鑰儲存庫加密編譯模組 v1.0 作業系統:與 iOS 11 一起發佈的 sepOS 類型:硬件 保安層級:2
作業系統發佈日期:2016 完成驗證日期:2017年2月1日	認證: 2828 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple iOS CoreCrypto 核心模組 v7.0 作業系統:iOS 10 類型:軟件 保安層級:1
作業系統發佈日期:2016 完成驗證日期:2017年2月1日	認證: 2827 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple iOS CoreCrypto 核心模組 v7.0 作業系統:iOS 10 類型:軟件 保安層級:1

先前版本

超過 5 年的認證會由 CMVP 列出，並具有[歷史記錄狀態](#)。以下先前的 iOS 版本擁有加密編譯模組驗證：

- iOS 9 (CoreCrypto 模組 v6.0)
- iOS 8 (CoreCrypto 模組 v5.0)
- iOS 7 (CoreCrypto 模組 v4.0)
- iOS 6 (CoreCrypto 模組 v3.0)

「共同準則」(CC) 認證背景

Apple 針對作業系統每個主要版本積極參與 iOS 的評估。評估只能針對最終公開發行的作業系統版本進行。在 iPadOS 13.1 以前, iPadOS 的名稱為 iOS。

「共同準則」(CC) 認證狀態

由 NIAP 運作的美國計劃維護著一份「[評估中的產品](#)」列表, 該列表包括目前正在美國透過 NIAP 認可的共同準則測試實驗室 (CCTL) 進行評估並且已經完成「評估啟動會議」(或同級) 的產品, 而 CCEVS 管理層在該會議中已正式接受產品進行評估。

在產品認證後, NIAP 會在「[產品相容](#)」列表中列出目前有效的認證。2 年後, 將對這些認證進行審查以確保其符合目前的保障維護政策。在保障維護日期到期後, NIAP 會將認證列表項目移至其「[已封存產品](#)」列表。

「[共同準則入口網站](#)」列出了可以在「共同準則承認協定」(CCRA) 下互相認可的認證。CC 入口網站可以將產品保留在認證產品列表中 5 年, 記錄則會由 CC 入口網站保留以供[存檔認證](#)。

下表顯示了目前正在由實驗室評估的認證, 或已被認證符合「共同準則」的認證。

目前狀態

針對 iOS 15 的 NIAP 評估, 正在進行實驗室測試。如需最新資料, 請參閱:[評估中的產品 \(NIAP\)](#) 和「[產品相容列表](#)」。

作業系統/認證日期	計劃 ID/文件	標題/保護剖繪
作業系統: iOS 15 認證日期: —	計劃 ID: 尚未通過認證 文件: —	標題: Apple iOS 15: iPhone 保護剖繪: 流動裝置基礎 (PP 模組待確認)
作業系統: iOS 14 認證日期: 2021 年 9 月 1 日	計劃 ID: 11146 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: Apple iOS 14: iPhone 保護剖繪: 流動裝置基礎、VPN 用戶端模組、WLAN 用戶端 PP 模組、MDM 代理程式 EP
作業系統: iOS 13 認證日期: 2020 年 11 月 6 日	計劃 ID: 11036 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: iPhone 上的 Apple iOS 13 保護剖繪: 流動裝置基礎、VPN 用戶端模組、WLAN 用戶端 EP、MDM 代理程式 EP

已封存的 iOS 共同準則認證

以下先前的 iOS 版本具有「共同準則」驗證。它們是根據 NIAP 規則由 [NIAP 封存](#)：

作業系統/認證日期	計劃 ID/文件	標題/保護剖繪
作業系統:iOS 12 認證日期:2019 年 3 月 14 日	計劃 ID: 10937 文件: 保安目標 指引	標題:安裝 iOS 12 的 iPhone 保護剖繪:流動裝置基礎、VPN 用戶端模組、無線 LAN 用戶端 EP、MDM 代理程式 EP
作業系統:iOS 11 認證日期:2018 年 7 月 17 日	計劃 ID: 10851 文件: 保安目標 指引	標題:Apple iOS 11 保護剖繪:流動裝置基礎、無線 LAN 用戶端 EP、MDM 代理程式 EP
作業系統:iOS 10 認證日期:2017 年 7 月 27 日	計劃 ID: 10782 文件:保安目標、指引	標題:iPhone 和 iPad 裝置上的 iOS 10.2 保護剖繪:流動裝置基礎、無線 LAN 用戶端 EP、MDM 代理程式 EP
作業系統:iOS 10 認證日期:2017 年 7 月 27 日	計劃 ID: 10792 文件:保安目標、指引	標題:iPhone 和 iPad 上的 iOS 10.2 VPN 用戶端 保護剖繪:VPN 用戶端 PP
作業系統:iOS 9 認證日期:2016 年 10 月 14 日	計劃 ID: 10725 文件:保安目標、指引	標題:iOS 9.3.2 配搭 MDM 代理程式 保護剖繪:流動裝置基礎、MDM 代理程式 EP
作業系統:iOS 9 認證日期:2016 年 10 月 13 日	計劃 ID: 10714 文件:保安目標、指引	標題:iPhone 和 iPad 上的 OS VPN 用戶端 保護剖繪:VPN 用戶端 PP
作業系統:iOS 9 認證日期:2016 年 1 月 28 日	計劃 ID: 10695 文件:保安目標、指引	標題:iOS 9 保護剖繪:流動裝置基礎

iPadOS 的保安認證



iPadOS 認證背景

Apple 會使用適合的合作保護剖繪和 FIPS 140-3 保安層級，針對其作業系統的每個主要版本積極參與驗證。一致性驗證只能針對最終發行版本執行。

附註：在 2019 年，iPad 裝置的作業系統重新命名為 iPadOS。在 iPadOS 13.1 以前，iPadOS 的名稱為 iOS。

iPadOS 加密編譯模組驗證狀態

「加密編譯模組驗證計劃」(CMVP) 根據其目前狀態在三個單獨列表下維護加密編譯模組的驗證狀態：

- 為了被列入 CMVP [實作待測列表 \(Implementation Under Test List\)](#) 中，實驗室必須與 Apple 簽約以提供測試。
- 在實驗室完成測試後，便可以建議 CMVP 進行驗證並且支付 CMVP 費用，然後將該模組加到[檢測中的模組 \(MIP\) 列表](#)中。MIP 列表會分開四個階段來追蹤 CMVP 驗證工作的進度：
 - **待審核**：等待指派 CMVP 資源。
 - **審核中**：CMVP 資源正在執行其驗證程序。
 - **協調**：實驗室和 CMVP 正在解決發現的所有問題。
 - **最終處理**：與簽發認證有關的程序和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性認證，並將其加到[已驗證的加密編譯模組列表](#)中。這包括：
 - 標示為[作用中的已驗證模組](#)。
 - 5 年過後，模組會標示為[歷史](#)。
 - 如果模組憑證因某些原因遭撤銷時，則會標示為[已撤銷](#)。

在 2020 年，CMVP 採用了國際標準 ISO/IEC 19790 作為 FIPS 140-3 的基礎。

FIPS 140-3 認證

目前狀態

iPadOS 14 (2020) 用戶空間、核心空間和安全密鑰儲存庫已完成實驗室測試，並已由實驗室推薦給 CMVP 進行驗證。它們列於[檢測中的模組列表 \(Modules in Process List\)](#)。

iPadOS 15 (2021 年) 用戶空間、核心空間和安全密鑰儲存庫正在接受實驗室測試。它們列於[實作待測列表 \(Implementation Under Test List\)](#) 中。

日期	認證/文件	模組資料
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: iPadOS 15 環境: Apple 晶片、用戶、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: iPadOS 15 環境: Apple 晶片、核心、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: 與 iPadOS 15 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (A9-A14、M1) 整體保安層級: 2
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: 與 iPadOS 15 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (A9-A14、M1) 整體保安層級: 2 物理保安層級: 3
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: iPadOS 14 環境: Apple 晶片、用戶、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: iPadOS 14 環境: Apple 晶片、核心、軟件 類型: 軟件 整體保安層級: 1

日期	認證/文件	模組資料
作業系統發佈日期:2020 完成驗證日期:—	認證:尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 模組 v11.1 作業系統:與 iPadOS 14 一起發佈的 sepOS 環境:Apple 晶片、安全密鑰儲存庫、硬件 類型:硬件 (A9-A14、M1) 整體保安層級:2
作業系統發佈日期:2020 完成驗證日期:—	認證:尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 模組 v11.1 作業系統:與 iPadOS 14 一起發佈的 sepOS 環境:Apple 晶片、安全密鑰儲存庫、硬件 類型:硬件 (A9-A14、M1) 整體保安層級:2 物理保安層級:3

FIPS 140-2 認證

下表顯示實驗室目前正在測試以及已通過測試符合 FIPS 140-2 的加密編譯模組。

日期	認證/文件	模組資料
作業系統發佈日期:2019 完成驗證日期:2021年3月23日	認證:3856 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶模組 v10.0 作業系統:iPadOS 13 類型:軟件 保安層級:1
作業系統發佈日期:2019 完成驗證日期:2021年3月23日	認證:3855 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心模組 v10.0 作業系統:iPadOS 13 類型:軟件 保安層級:1
作業系統發佈日期:2019 完成驗證日期:2021年2月5日	認證:3811 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 安全密鑰儲存庫加密編譯模組 v10.0 作業系統:與 iPadOS 13 一起發佈的 sepOS 類型:硬件 保安層級:2
作業系統發佈日期:2018 完成驗證日期:2019年4月23日	認證:3438 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心模組 v9.0 作業系統:iOS 12 類型:軟件 保安層級:1
作業系統發佈日期:2018 完成驗證日期:2019年4月11日	認證:3433 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶模組 v9.0 作業系統:iOS 12 類型:軟件 保安層級:1

日期	認證/文件	模組資料
作業系統發佈日期: 2018 完成驗證日期: 2019 年 9 月 10 日	認證: 3523 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple 安全密鑰儲存庫加密編譯模組 v9.0 作業系統: 與 iOS 12 一起發佈的 sepOS 類型: 硬件 保安層級: 2
作業系統發佈日期: 2017 完成驗證日期: 2018 年 3 月 9 日、2018 年 5 月 22 日、2018 年 7 月 6 日	認證: 3148 文件: 認證 保安規則 Crypto Officer 指引	標題: ARM 適用的 Apple Corecrypto 用戶模組 v8.0 作業系統: iOS 11 類型: 軟件 保安層級: 1
作業系統發佈日期: 2017 完成驗證日期: 2018 年 3 月 9 日、2018 年 5 月 17 日、2018 年 7 月 3 日	認證: 3147 文件: 認證 保安規則 Crypto Officer 指引	標題: ARM 適用的 Apple Corecrypto 核心模組 v8.0 作業系統: iOS 11 類型: 軟件 保安層級: 1
作業系統發佈日期: 2017 完成驗證日期: 2019 年 9 月 10 日	認證: 3223 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple 安全密鑰儲存庫加密編譯模組 v1.0 作業系統: 與 iOS 11 一起發佈的 sepOS 類型: 硬件 保安層級: 2
作業系統發佈日期: 2016 完成驗證日期: 2017 年 2 月 1 日	認證: 2828 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple iOS CoreCrypto 核心模組 v7.0 作業系統: iOS 10 類型: 軟件 保安層級: 1
作業系統發佈日期: 2016 完成驗證日期: 2017 年 2 月 1 日	認證: 2827 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple iOS CoreCrypto 核心模組 v7.0 作業系統: iOS 10 類型: 軟件 保安層級: 1

先前版本

超過 5 年的認證會由 CMVP 列出，並具有[歷史記錄狀態](#)。以下先前的 iOS 版本擁有加密編譯模組驗證：

- iOS 9 (CoreCrypto 模組 v6.0)
- iOS 8 (CoreCrypto 模組 v5.0)
- iOS 7 (CoreCrypto 模組 v4.0)
- iOS 6 (CoreCrypto 模組 v3.0)

「共同準則」(CC) 認證背景

Apple 針對作業系統每個主要版本積極參與 iPadOS 的評估。評估只能針對最終公開發行的作業系統版本進行。

「共同準則」(CC) 認證狀態

由 NIAP 運作的美國計劃維護著一份「[評估中的產品](#)」列表，該列表包括目前正在美國透過 NIAP 認可的共同準則測試實驗室 (CCTL) 進行評估並且已經完成「評估啟動會議」(或同級) 的產品，而 CCEVS 管理層在該會議中已正式接受產品進行評估。

在產品認證後，NIAP 會在「[產品相容](#)」列表中列出目前有效的認證。2 年後，將對這些認證進行審查以確保其符合目前的保障維護政策。在保障維護日期到期後，NIAP 會將認證列表項目移至其「[已封存產品](#)」列表。

「[共同準則入口網站](#)」列出了可以在「共同準則承認協定」(CCRA) 下互相認可的認證。CC 入口網站可以將產品保留在認證產品列表中 5 年，記錄則會由 CC 入口網站保留以供[存檔認證](#)。

下表顯示了目前正在由實驗室評估的認證，或已被認證符合「共同準則」的認證。

目前狀態

針對 iPadOS 15 的 NIAP 評估，正在進行實驗室測試。如需最新資料，請參閱：[評估中的產品 \(NIAP\)](#) 和「[產品相容列表](#)」。

作業系統/認證日期	計劃 ID/文件	標題/保護剖繪
作業系統: iPadOS 15 認證日期: 2019 年 3 月 14 日	計劃 ID: — 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: 安裝 iOS 12 的 iPad 保護剖繪: 流動裝置基礎、VPN 用戶端模組、無線 LAN 用戶端 EP、MDM 代理程式 EP
作業系統: iPadOS 14 認證日期: 2021 年 9 月 1 日	計劃 ID: 11147 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: Apple iPadOS 14: iPad 保護剖繪: 流動裝置基礎、VPN 用戶端模組、無線 LAN 用戶端 EP、MDM 代理程式 EP
作業系統: iPadOS 13 認證日期: 2020 年 11 月 6 日	計劃 ID: 11036 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: iPad 流動裝置上的 iPadOS 13 保護剖繪: 流動裝置基礎、VPN 用戶端模組、無線 LAN 用戶端 EP、MDM 代理程式 EP

先前版本

以下先前的 iOS 版本具有「共同準則」驗證。它們是根據 NIAP 規則由 [NIAP 封存](#)：

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

macOS 的保安認證



macOS 認證背景

Apple 會使用適合的合作保護剖繪和 FIPS 140-3 保安層級，針對其作業系統的每個主要版本積極參與驗證。一致性驗證只能針對最終發行版本執行。

macOS 加密編譯模組驗證狀態

「加密編譯模組驗證計劃」(CMVP) 根據其目前狀態在三個單獨列表下維護加密編譯模組的驗證狀態：

- 為了被列入 CMVP [實作待測列表 \(Implementation Under Test List\)](#) 中，實驗室必須與 Apple 簽約以提供測試。
- 在實驗室完成測試後，便可以建議 CMVP 進行驗證並且支付 CMVP 費用，然後將該模組加到[檢測中的模組 \(MIP\) 列表](#)中。「MIP 列表」會分開四個階段來追蹤 CMVP 驗證工作的進度：
 - 待審核**：等待指派 CMVP 資源。
 - 審核中**：CMVP 資源正在執行其驗證程序。
 - 協調**：實驗室和 CMVP 正在解決發現的所有問題。
 - 最終處理**：與簽發認證有關的程序和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性認證，並將其加到[已驗證的加密編譯模組列表](#)中。這包括：
 - 標示為**作用中**的已驗證模組。
 - 5 年過後，模組會標示為**歷史**。
 - 如果模組憑證因某些原因遭撤銷時，則會標示為**已撤銷**。

在 2020 年，CMVP 採用了國際標準 ISO/IEC 19790 作為 FIPS 140-3 的基礎。

針對 Apple Mac 電腦，以下表格顯示適用於各 Mac 技術的加密編譯模組。

加密編譯模組	配備 Apple 晶片的 Mac 電腦	配備 Apple T2 保安晶片的 Mac 電腦	以 Intel 為基礎而未配備 Apple T2 保安晶片的 Mac 電腦
Apple 晶片用戶空間	✓		
Apple 晶片核心	✓		
Intel 用戶空間		✓	✓
Intel 核心		✓	✓
安全密鑰儲存庫	✓	✓	

FIPS 140-3 認證

2020 年, Apple 發表了以 Apple 晶片為基礎的 Mac 電腦。下表的「模組資訊」欄指出了加密編譯模組對 Apple 晶片或以 Intel 為基礎的 Mac 電腦的適用性。

附註: 許多以 Intel 為基礎的 Mac 電腦都包含 Apple T2 保安晶片。如需 T2 晶片認證的相關資料, 請參閱:
[Apple T2 保安晶片的保安認證](#)。

macOS ssh 用戶端

針對特定 FIPS 140-3 演算法, OpenSSH 可以設定為使用 FIPS 140-3 已驗證模組。機構可以執行 [Apple](#) 所提供經簽署與公證的安裝程式 (密碼為 **FIPS140Mode**)。安裝程式在會 Mac 上放置兩個檔案:

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

macOS 接著會使用這些檔案, 將 OpenSSH 適用的加密方式限制為僅由 NIST 驗證的加密方式, 並確保 OpenSSH 用戶端使用由平台提供且經過驗證的加密編譯模組。管理員也可以製作自己的檔案。如需更多資料, 請參閱 macOS 12.0.1 或較新版本中的 [apple_ssh_and_fips](#) man 頁面。

目前狀態

macOS 11 Big Sur 用戶空間、核心空間和安全密鑰儲存庫已完成實驗室測試, 並已由實驗室推薦給 CMVP 進行驗證。它們列於[檢測中的模組列表 \(Modules in Process List\)](#)。

macOS 12 Monterey 用戶空間、核心空間和安全密鑰儲存庫正在接受實驗室測試。它們列於[實作待測列表 \(Implementation Under Test List\)](#)中。

日期	認證/文件	模組資料
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12.0 作業系統: Apple 晶片上的 macOS 12 Monterey 環境: Apple 晶片、用戶、軟件 類型: 軟件 保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12.0 作業系統: Apple 晶片上的 macOS 12 Monterey 環境: Apple 晶片、核心、軟件 類型: 軟件 保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12.0 作業系統: Intel 上的 macOS 12 Monterey 環境: Intel、用戶、軟件 類型: 軟件 保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12.0 作業系統: Intel 上的 macOS 12 Monterey 環境: Intel、核心、軟件 類型: 軟件 保安層級: 1

日期	認證/文件	模組資料
作業系統發佈日期:2021 完成驗證日期:—	<p>認證:尚未通過認證</p> <p>文件: 認證 保安規則 Crypto Officer 指引</p>	<p>標題:Apple Corecrypto 模組 v12.0</p> <p>作業系統:與 Apple 晶片上的 macOS 12 Monterey 一起發佈的 sepOS、與配備 T2 之 Intel 上的 macOS 12 Monterey 一起發佈的 sepOS</p> <p>環境:Apple 晶片、安全密鑰儲存庫、硬件</p> <p>類型:硬件 (M1 和 T2)</p> <p>保安層級:2</p>
作業系統發佈日期:2021 完成驗證日期:—	<p>認證:尚未通過認證</p> <p>文件: 認證 保安規則 Crypto Officer 指引</p>	<p>標題:Apple Corecrypto 模組 v12.0</p> <p>作業系統:與 Apple 晶片上的 macOS 12 Monterey 一起發佈的 sepOS</p> <p>環境:Apple 晶片、安全密鑰儲存庫、硬件</p> <p>類型:硬件 (M1)</p> <p>保安層級:2</p> <p>物理保安層級:3</p>
作業系統發佈日期:2020 完成驗證日期:—	<p>認證:尚未通過認證</p> <p>文件: 認證 保安規則 Crypto Officer 指引</p>	<p>標題:Apple Corecrypto 模組 v11.1</p> <p>作業系統:Intel 上的 macOS 11 Big Sur</p> <p>環境:Intel、用戶、軟件</p> <p>類型:軟件</p> <p>保安層級:1</p>
作業系統發佈日期:2020 完成驗證日期:—	<p>認證:尚未通過認證</p> <p>文件: 認證 保安規則 Crypto Officer 指引</p>	<p>標題:Apple Corecrypto 模組 v11.1</p> <p>作業系統:Intel 上的 macOS 11 Big Sur</p> <p>環境:Intel、核心、軟件</p> <p>類型:軟件</p> <p>保安層級:1</p>
作業系統發佈日期:2020 完成驗證日期:—	<p>認證:尚未通過認證</p> <p>文件: 認證 保安規則 Crypto Officer 指引</p>	<p>標題:Apple Corecrypto 模組 v11.1</p> <p>作業系統:Apple 晶片上的 macOS 11 Big Sur</p> <p>環境:Apple 晶片、用戶、軟件</p> <p>類型:軟件</p> <p>保安層級:1</p>
作業系統發佈日期:2020 完成驗證日期:—	<p>認證:尚未通過認證</p> <p>文件: 認證 保安規則 Crypto Officer 指引</p>	<p>標題:Apple Corecrypto 模組 v11.1</p> <p>作業系統:Apple 晶片上的 macOS 11 Big Sur</p> <p>環境:Apple 晶片、核心、軟件</p> <p>類型:軟件</p> <p>保安層級:1</p>
作業系統發佈日期:2020 完成驗證日期:—	<p>認證:尚未通過認證</p> <p>文件: 認證 保安規則 Crypto Officer 指引</p>	<p>標題:Apple Corecrypto 模組 v11.1</p> <p>作業系統:與 Apple 晶片上的 macOS 11 Big Sur 一起發佈的 sepOS、與 Intel 上的 macOS 11 Big Sur 一起發佈的 sepOS</p> <p>環境:Apple 晶片、安全密鑰儲存庫、硬件</p> <p>類型:硬件 (M1)</p> <p>保安層級:2</p>

日期	認證/文件	模組資料
作業系統發佈日期:2020 完成驗證日期:—	認證:尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 模組 v11.1 作業系統:與 Apple 晶片上的 macOS 11 Big Sur 一起發佈的 sepOS 環境:Apple 晶片、安全密鑰儲存庫、硬件 類型:硬件 (M1) 保安層級:2 物理保安層級:3

FIPS 140-2 認證

下表顯示實驗室目前正在測試以及已通過測試符合 FIPS 140-2 的加密編譯模組。

macOS 10.15 Catalina 用戶空間、核心空間和安全密鑰儲存庫已完成實驗室測試，並已由實驗室推薦給 CMVP 進行驗證。它們列於[檢測中的模組列表 \(Modules in Process List\)](#)。

附註:許多以 Intel 為基礎的 Mac 電腦都包含 Apple T2 保安晶片。如需 T2 晶片認證的相關資料，請參閱:[Apple T2 保安晶片的保安認證](#)。

日期	認證/文件	模組資料
作業系統發佈日期:2019 完成驗證日期:2021 年 3 月 24 日	認證: 3859 文件: 認證 保安規則 Crypto Officer 指引	標題:Intel (ccv10) 適用的 Apple Corecrypto 用戶模組 作業系統:macOS 10.15 Catalina 類型:軟件 保安層級:1
作業系統發佈日期:2019 完成驗證日期:2021 年 3 月 24 日	認證: 3858 文件: 認證 保安規則 Crypto Officer 指引	標題:Intel (ccv10) 適用的 Apple Corecrypto 核心模組 作業系統:macOS 10.15 Catalina 類型:軟件 保安層級:1
作業系統發佈日期:2018 完成驗證日期:2019 年 4 月 12 日	認證: 3402 文件: 認證 保安規則 Crypto Officer 指引	標題:Intel 適用的 Apple Corecrypto 用戶模組 v9.0 作業系統:macOS 10.14 Mojave 類型:軟件 保安層級:1
作業系統發佈日期:2018 完成驗證日期:2019 年 4 月 12 日	認證: 3431 文件: 認證 保安規則 Crypto Officer 指引	標題:Intel 適用的 Apple Corecrypto 核心模組 v9.0 作業系統:macOS 10.14 Mojave 類型:軟件 保安層級:1
作業系統發佈日期:2017 完成驗證日期:2018 年 3 月 22 日	認證: 3155 文件: 認證 保安規則 Crypto Officer 指引	標題:Intel 適用的 Apple Corecrypto 用戶模組 v8.0 作業系統:macOS 10.13 High Sierra 類型:軟件 保安層級:1

日期	認證/文件	模組資料
作業系統發佈日期: 2017	認證: 3156	標題: Intel 適用的 Apple Corecrypto 核心模組 v8.0
完成驗證日期: 2018 年 3 月 22 日	文件: 認證 保安規則 Crypto Officer 指引	作業系統: macOS 10.13 High Sierra 類型: 軟件 保安層級: 1

先前版本

以下先前的 OS X 和 macOS 版本擁有加密編譯模組驗證。超過 5 年的版本會由 CMVP 以[歷史記錄狀態](#)列出:

- 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

「共同準則」(CC) 認證背景

Apple 針對作業系統每個主要版本積極參與 macOS 的評估。評估只能針對最終公開發行的作業系統版本進行。

「共同準則」(CC) 認證狀態

由 NIAP 運作的美國計劃維護著一份「[評估中的產品](#)」列表, 該列表包括目前正在美國透過 NIAP 認可的共同準則測試實驗室 (CCTL) 進行評估並且已經完成「評估啟動會議」(或同級) 的產品, 而 CCEVS 管理層在該會議中已正式接受產品進行評估。

在產品認證後, NIAP 會在「[產品相容](#)」列表中列出目前有效的認證。2 年後, 將對這些認證進行審查以確保其符合目前的保障維護政策。在保障維護日期到期後, NIAP 會將認證列表項目移至其「[已封存產品列表](#)」。

「[共同準則入口網站](#)」列出了可以在「共同準則承認協定」(CCRA) 下互相認可的認證。CC 入口網站可以將產品保留在認證產品列表中 5 年, 記錄則會由 CC 入口網站保留以供[存檔認證](#)。

下表顯示了目前正在由實驗室評估的認證, 或已被認證符合「共同準則」的認證。

目前狀態

針對 macOS 11 和 macOS 12, 使用「一般用途作業系統」和「完整磁碟加密」(FDE) (AA 和 EE) 保護剖繪的 NIAP 評估正在進行中。

如需最新資料，請參閱：[評估中的產品 \(NIAP\)](#) 和 [「產品相容列表」](#)。

作業系統/認證日期	計劃 ID/文件	標題/保護剖繪
作業系統: macOS 12 Monterey 認證日期:—	計劃 ID: 尚未通過認證 文件:—	標題: macOS 12 Monterey 的 Apple 檔案保險箱 2 保護剖繪: CPP_FDE_AA_V2.0E、CPP_FDE_EE_V2.0E (PP 待確認)
作業系統: macOS 12 Monterey 認證日期:—	計劃 ID: 尚未通過認證 文件:—	標題: macOS 12 Monterey 保護剖繪: PP_OS_V4.21 (PP 待確認)
作業系統: macOS 11 Big Sur 認證日期:—	計劃 ID: 尚未通過認證 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: macOS 11 Big Sur 的 Apple 檔案保險箱 2 保護剖繪: CPP_FDE_AA_V2.0E、CPP_FDE_EE_V2.0E
作業系統: macOS 11 Big Sur 認證日期:—	計劃 ID: 尚未通過認證 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: Apple macOS 11 Big Sur 保護剖繪: PP_OS_V4.21
作業系統: macOS 10.15 Catalina 認證日期: 2021 年 4 月 29 日	計劃 ID: 11078 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: 執行 macOS 10.15 Catalina 之 T2 電腦上的 Apple 檔案保險箱 2 保護剖繪: CPP_FDE_AA_V2.0E、CPP_FDE_EE_V2.0E
作業系統: macOS 10.15 Catalina 認證日期: 2020 年 9 月 23 日	計劃 ID: 11077 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: macOS 10.15 Catalina 保護剖繪: PP_OS_V4.21

tvOS 的保安認證



tvOS 認證背景

Apple 針對與 tvOS 每個主要版本相關的加密編譯模組積極參與驗證。一致性驗證只能針對最終發行版本執行。

tvOS 加密編譯模組驗證狀態

「加密編譯模組驗證計劃」(CMVP) 根據其目前狀態在三個單獨列表下維護加密編譯模組的驗證狀態：

- 為了被列入 CMVP [實作待測列表 \(Implementation Under Test List\)](#) 中，實驗室必須與 Apple 簽約以提供測試。
- 在實驗室完成測試後，便可以建議 CMVP 進行驗證並且支付 CMVP 費用，然後將該模組加到[檢測中的模組 \(MIP\) 列表](#)中。「MIP 列表」會分開四個階段來追蹤 CMVP 驗證工作的進度：
 - **待審核**：等待指派 CMVP 資源。
 - **審核中**：CMVP 資源正在執行其驗證程序。
 - **協調**：實驗室和 CMVP 正在解決發現的所有問題。
 - **最終處理**：與簽發認證有關的程序和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性認證，並將其加到[已驗證的加密編譯模組列表](#)中。這包括：
 - 標示為**作用中**的已驗證模組。
 - 5 年過後，模組會標示為**歷史**。
 - 如果模組憑證因某些原因遭撤銷時，則會標示為**已撤銷**。

在 2020 年，CMVP 採用了國際標準 ISO/IEC 19790 作為 FIPS 140-3 的基礎。

FIPS 140-3 認證

目前狀態

tvOS 14 (2020) 用戶空間、核心空間和安全密鑰儲存庫已完成實驗室測試，並已由實驗室推薦給 CMVP 進行驗證。它們列於[檢測中的模組列表 \(Modules in Process List\)](#)。

tvOS 15 (2021 年) 用戶空間、核心空間和安全密鑰儲存庫正在接受實驗室測試。它們列於[實作待測列表 \(Implementation Under Test List\)](#) 中。

日期	認證/文件	模組資料
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: tvOS 15 環境: Apple 晶片、用戶、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: tvOS 15 環境: Apple 晶片、核心、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: 與 tvOS 15 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (A10、A12) 整體保安層級: 2
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: tvOS 14 環境: Apple 晶片、用戶、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: tvOS 14 環境: Apple 晶片、核心、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: 與 tvOS 14 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (A10、A12) 整體保安層級: 2

FIPS 140-2 認證

下表顯示實驗室目前正在測試以及已通過測試符合 FIPS 140-2 的加密編譯模組。

tvOS 13 (2019) 用戶空間、核心空間和安全密鑰儲存庫已完成實驗室測試，並已由實驗室推薦給 CMVP 進行驗證。它們列於[檢測中的模組列表 \(Modules in Process List\)](#)。

日期	認證/文件	模組資料
作業系統發佈日期: 2019 完成驗證日期: 2021 年 3 月 23 日	認證: 3856 文件: 認證 保安規則 Crypto Officer 指引	標題: ARM 適用的 Apple Corecrypto 用戶模組 v10.0 作業系統: tvOS 13 類型: 軟件 保安層級: 1
作業系統發佈日期: 2019 完成驗證日期: 2021 年 3 月 23 日	認證: 3855 文件: 認證 保安規則 Crypto Officer 指引	標題: ARM 適用的 Apple Corecrypto 核心模組 v10.0 作業系統: tvOS 13 類型: 軟件 保安層級: 1
作業系統發佈日期: 2019 完成驗證日期: 2021 年 2 月 5 日	認證: 3811 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple 安全密鑰儲存庫加密編譯模組 v10.0 作業系統: 與 tvOS 13 一起發佈的 sepOS 類型: 硬件 保安層級: 2
作業系統發佈日期: 2018 完成驗證日期: 2019 年 4 月 23 日	認證: 3438 文件: 認證 保安規則 Crypto Officer 指引	標題: ARM 適用的 Apple Corecrypto 核心模組 v9.0 作業系統: tvOS 12 類型: 軟件 保安層級: 1
作業系統發佈日期: 2018 完成驗證日期: 2019 年 4 月 11 日	認證: 3433 文件: 認證 保安規則 Crypto Officer 指引	標題: ARM 適用的 Apple Corecrypto 用戶模組 v9.0 作業系統: tvOS 12 類型: 軟件 保安層級: 1
作業系統發佈日期: 2018 完成驗證日期: 2019 年 9 月 10 日	認證: 3523 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple 安全密鑰儲存庫加密編譯模組 v9.0 作業系統: 與 tvOS 12 一起發佈的 sepOS 類型: 硬件 保安層級: 2
作業系統發佈日期: 2017 完成驗證日期: 2018 年 3 月 9 日、 2018 年 5 月 22 日、2018 年 7 月 6 日	認證: 3148 文件: 認證 保安規則 Crypto Officer 指引	標題: ARM 適用的 Apple Corecrypto 用戶模組 v8.0 作業系統: tvOS 11 類型: 軟件 保安層級: 1

日期	認證/文件	模組資料
作業系統發佈日期: 2017 完成驗證日期: 2018 年 3 月 9 日、2018 年 5 月 17 日、2018 年 7 月 3 日	認證: 3147 文件: 認證 保安規則 Crypto Officer 指引	標題: ARM 適用的 Apple Corecrypto 核心模組 v8.0 作業系統: tvOS 11 類型: 軟件 保安層級: 1
作業系統發佈日期: 2017 完成驗證日期: 2019 年 9 月 10 日	認證: 3223 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple 安全密鑰儲存庫加密編譯模組 v1.0 作業系統: 與 tvOS 11 一起發佈的 sepOS 類型: 硬件 保安層級: 2

watchOS 的保安認證



watchOS 認證背景

Apple 針對與 watchOS 每個主要版本相關的加密編譯模組積極參與驗證。一致性驗證只能針對最終發行版本執行。

watchOS 加密編譯模組驗證狀態

「加密編譯模組驗證計劃」(CMVP) 根據其目前狀態在三個單獨列表下維護加密編譯模組的驗證狀態：

- 為了被列入 CMVP [實作待測列表 \(Implementation Under Test List\)](#) 中，實驗室必須與 Apple 簽約以提供測試。
- 在實驗室完成測試後，便可以建議 CMVP 進行驗證並且支付 CMVP 費用，然後將該模組加到[檢測中的模組 \(MIP\) 列表](#)中。「MIP 列表」會分開四個階段來追蹤 CMVP 驗證工作的進度：
 - **待審核**：等待指派 CMVP 資源。
 - **審核中**：CMVP 資源正在執行其驗證程序。
 - **協調**：實驗室和 CMVP 正在解決發現的所有問題。
 - **最終處理**：與簽發認證有關的程序和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性認證，並將其加到[已驗證的加密編譯模組列表](#)中。這包括：
 - 標示為[作用中](#)的已驗證模組。
 - 5 年過後，模組會標示為[歷史](#)。
 - 如果模組憑證因某些原因遭撤銷時，則會標示為[已撤銷](#)。

在 2020 年，CMVP 採用了國際標準 ISO/IEC 19790 作為 FIPS 140-3 的基礎。

FIPS 140-3 認證

目前狀態

watchOS 7 (2020) 用戶空間、核心空間和安全密鑰儲存庫已完成實驗室測試，並已由實驗室推薦給 CMVP 進行驗證。它們列於[檢測中的模組列表 \(Modules in Process List\)](#)。

watchOS 8 (2021 年) 用戶空間、核心空間和安全密鑰儲存庫正在接受實驗室測試。它們列於[實作待測列表 \(Implementation Under Test List\)](#) 中。

日期	認證/文件	模組資料
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: watchOS 8 環境: Apple 晶片、用戶、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: watchOS 8 環境: Apple 晶片、核心、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: 與 watchOS 8 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (S3、S4、S5、S6) 整體保安層級: 2
作業系統發佈日期: 2021 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v12 作業系統: 與 watchOS 8 一起發佈的 sepOS 環境: Apple 晶片、安全密鑰儲存庫、硬件 類型: 硬件 (S6) 整體保安層級: 2 物理保安層級: 3
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: watchOS 7 環境: Apple 晶片、用戶、軟件 類型: 軟件 整體保安層級: 1
作業系統發佈日期: 2020 完成驗證日期: —	認證: 尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題: Apple Corecrypto 模組 v11.1 作業系統: watchOS 7 環境: Apple 晶片、核心、軟件 類型: 軟件 整體保安層級: 1

日期	認證/文件	模組資料
作業系統發佈日期:2020 完成驗證日期:—	認證:尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 模組 v11.1 作業系統:與 watchOS 7 一起發佈的 sepOS 環境:Apple 晶片、安全密鑰儲存庫、硬件 類型:硬件 (S3、S4、S5、S6) 整體保安層級:2
作業系統發佈日期:2020 完成驗證日期:—	認證:尚未通過認證 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple Corecrypto 模組 v11.1 作業系統:與 watchOS 7 一起發佈的 sepOS 環境:Apple 晶片、安全密鑰儲存庫、硬件 類型:硬件 (S6) 整體保安層級:2 物理保安層級:3

FIPS 140-2 認證

下表顯示實驗室目前正在測試以及已通過測試符合 FIPS 140-2 的加密編譯模組。

日期	認證/文件	模組資料
作業系統發佈日期:2019 完成驗證日期:—	認證:3856 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶模組 v10.0 作業系統:watchOS 6 類型:軟件 保安層級:1
作業系統發佈日期:2019 完成驗證日期:—	認證:3855 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心模組 v10.0 作業系統:watchOS 6 類型:軟件 保安層級:1
作業系統發佈日期:2019 完成驗證日期:2021 年 2 月 5 日	認證:3811 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple 安全密鑰儲存庫加密編譯模組 v10.0 作業系統:與 watchOS 6 一起發佈的 sepOS 類型:硬件 保安層級:2
作業系統發佈日期:2018 完成驗證日期:2019 年 4 月 23 日	認證:3438 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心模組 v9.0 作業系統:watchOS 5 類型:軟件 保安層級:1
作業系統發佈日期:2018 完成驗證日期:2019 年 4 月 11 日	認證:3433 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶模組 v9.0 作業系統:watchOS 5 類型:軟件 保安層級:1

日期	認證/文件	模組資料
作業系統發佈日期:2018 完成驗證日期:2019年9月10日	認證: 3523 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple 安全密鑰儲存庫加密編譯模組 v9.0 作業系統:與 watchOS 5 一起發佈的 sepOS 類型:硬件 保安層級:2
作業系統發佈日期:2017 完成驗證日期:2018年3月9日、 2018年5月22日、2018年7月6日	認證: 3148 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 用戶模組 v8.0 作業系統:watchOS 4 類型:軟件 保安層級:1
作業系統發佈日期:2017 完成驗證日期:2018年3月9日、 2018年5月17日、2018年7月3日	認證: 3147 文件: 認證 保安規則 Crypto Officer 指引	標題:ARM 適用的 Apple Corecrypto 核心模組 v8.0 作業系統:watchOS 4 類型:軟件 保安層級:1
作業系統發佈日期:2017 完成驗證日期:2019年9月10日	認證: 3223 文件: 認證 保安規則 Crypto Officer 指引	標題:Apple 安全密鑰儲存庫加密編譯模組 v1.0 作業系統:與 watchOS 4 一起發佈的 sepOS 類型:硬件 保安層級:2

軟件保安認證

Apple 軟件保安認證概覽

Apple 為 sepOS 和 T2 韌體維護美國「聯邦資訊處理標準」(FIPS) 140-2/-3 的「符合標準驗證憑證」以及其他認證。Apple 從**認證建置組塊**開始著手，此建置組塊可在適用情況下跨多個平台廣泛應用。其中一個建置組塊就是 Corecrypto 的驗證，其用於 Apple 所開發作業系統內的軟硬件加密編譯模組部署。第二個建置組塊是「安全隔離區」(內嵌在許多 Apple 裝置內)的認證。第三個則是配備 Touch ID 的 Apple 裝置和配備 Face ID 的裝置所包含 Secure Element (SE) 的認證。這些硬件認證建置組塊為更廣泛的平台保安認證形成了基礎。

產品認證：共同準則 (ISO/IEC 15408)

「共同準則」(ISO/IEC 15408) 是許多組織採用的標準，以其為基礎進行 IT 產品的保安評估。

如需了解有哪些認證可根據國際「共同準則承認協定」(CCRA) 相互認可，請參閱：[共同準則入口網站](#)。國家和私人驗證架構也可在不受 CCRA 限制的情況下使用「共同準則」標準。在歐洲，相互認可受 [SOG-IS 協議](#) 和 CCRA 管轄。

根據「共同準則」社群所述，其目標是制訂一套國際認可的保安標準，以明確可靠地評估資訊科技產品的保安功能。「共同準則認證」會對產品能否符合保安標準進行獨立評估，以讓客戶提升對資訊科技產品保安的信心，進而作出更有依據的決定。

透過 CCRA，[會員國家](#) 已同意抱持相同的信心度，認可該資訊技術產品認證。認證之前需要進行的評估相當廣泛，包括：

- 保護剖繪 (PP)
- 保安目標 (ST)
- 保安功能要求 (SFR)
- 保安保障要求 (SAR)
- 評估保證等級 (EAL)

「保護剖繪」(PP) 是用於指定一類別之裝置類型 (例如「流動性」) 的保安需求的文件，並用於提供同一類別 IT 產品評估之間的可比較性。CCRA 會員數量以及已核准 PP 的累積列表每年均持續成長。這項協定讓產品開發者無論採用任何一種認證授權架構，都只需取得單一認證，並會獲得任何 CCRA 簽署者的認可。

「保安目標」(ST) 定義了認證 IT 產品時將評估的內容。ST 被演繹成更具體的「**保安功能要求**」(SFR)，用於更詳細地評估 ST。

「共同準則」(CC) 還包括「**保安保障要求**」。一種常見的認可指標是「**評估保證等級**」(EAL)。EAL 將頻繁出現的 SAR 集群組合在一起，可以在 PP 和 ST 中加以指定以提高可比較性。

許多舊版 PP 已封存，且已由專為特定解決方案和環境所制訂的針對式 PP 取代。為協力確保所有 CCRA 會員之間能持續相互認可，已建立了「國際技術社群」(iTC)，以推動和維護從一開始就在 CCRA 簽署架構的參與下所開發的「合作保護剖繪」(cPP)。相關的持份者將繼續開發以 CCRA 以外之用戶群組和相互認可協議為對象的 PP。

從 2015 年初開始，Apple 便開始根據更新的 CCRA (包含特定 cPP) 致力取得認證。自當時起，Apple 的每個主要 iOS 版本均獲得「共同準則」認證，並擴展涵蓋範圍以納入新版 PP 提供的保安保障。

Apple 在專門進行流動保安技術評估的技術社群中扮演著積極角色。這些包含負責開發和更新 cPP 的 iTC。Apple 持續依據目前的 PP 和 cPP 進行評估和爭取認證。

針對北美市場，Apple 平台認證一般透過美國「國家資訊保證合作組織」(NIAP) 進行，此組織維護一份列表，以列出[目前已在評估中但尚未通過認證的專案](#)。

除了列出的一般平台憑證以外，亦有核發其他認證，以證明部份市場的特定安全要求。

Apple App 的保安認證

Apple App 認證背景

Apple 會使用適合的共同準則保護剖繪 (PP) 來積極參與 Apple App 的保安認證。這些評估基於 Apple 已取得的硬件和作業系統認證。

在 2018 年，Apple 針對使用 Safari 瀏覽器和「通訊錄」App 在 iOS 11 上執行的重要應用程式，啟動了應用程式保安評估。Apple 繼續對在 iOS 12、iOS 13 和 iPadOS 13.1 上執行的 App 進行評估。在 2021 年將涵蓋範圍擴展至在 macOS 11 上執行的 App。

加密編譯模組認證狀態

此處列出的 Apple App 使用適用於作業系統的加密編譯模組。如需更多資料，請參閱：[iOS 的保安認證](#)、[iPadOS 的保安認證](#)與[macOS 的保安認證](#)。

「共同準則」(CC) 認證狀態

由 NIAP 運作的美國計劃維護著一份「[評估中的產品](#)」列表，該列表包括目前正在美國透過 NIAP 認可的共同準則測試實驗室 (CCTL) 進行評估並且已經完成「評估啟動會議」(或同級) 的產品，而 CCEVS 管理層在該會議中已正式接受產品進行評估。

在產品認證後，NIAP 會在「[產品相容](#)」列表中列出目前有效的認證。2 年後，將對這些認證進行審查以確保其符合目前的保障維護政策。在保障維護日期到期後，NIAP 會將認證列表項目移至其「[已封存產品](#)」列表。

[「共同準則入口網站」](#)列出了可以在「共同準則承認協定」(CCRA) 下互相認可的認證。CC 入口網站可以將產品保留在認證產品列表中 5 年，記錄則會由 CC 入口網站保留以供[存檔認證](#)。

下表顯示了目前正在由實驗室評估的認證，或已被認證符合「共同準則」的認證。

目前狀態

- 對已發佈之正在進行的 NIAP 評估會列示於評估中的產品 (NIAP) 中。
- 已完成並經過驗證的評估會於 NIAP「[產品相容列表](#)」中列出。

作業系統/認證日期	計劃 ID/文件	標題/保護剖繪
作業系統: macOS 11 Big Sur 認證日期: —	計劃 ID: 尚未通過認證 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: macOS 11 Big Sur: 通訊錄 保護剖繪: 應用程式軟件的 PP、 網頁瀏覽器的 EP
作業系統: macOS 11 Big Sur 認證日期: —	計劃 ID: 尚未通過認證 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: macOS 11 Big Sur: Safari 保護剖繪: 應用程式軟件的 PP、 網頁瀏覽器的 EP
作業系統: iOS 14、iPadOS 14 認證日期: 2021 年 8 月 20 日	計劃 ID: 11191 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: Apple iOS 14 和 iPadOS 14: 通訊錄 保護剖繪: 應用程式軟件的 PP、 網頁瀏覽器的 EP
作業系統: iOS 14、iPadOS 14 認證日期: —	計劃 ID: 11192 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: Apple iOS 14 和 iPadOS 14: Safari 保護剖繪: 應用程式軟件的 PP、 網頁瀏覽器的 EP
作業系統: iOS 13、iPadOS 13 認證日期: 2020 年 6 月 5 日	計劃 ID: 11060 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題: Apple iOS 13 和 iPadOS 13: Safari 保護剖繪: 應用程式軟件的 PP、 網頁瀏覽器的 EP

作業系統/認證日期	計劃 ID/文件	標題/保護剖繪
作業系統:iOS 13、iPadOS 13 認證日期:2020年6月5日	計劃 ID: 11050 文件: 認證 保安目標 指引 驗證報告 保證作業報告	標題:Apple iOS 13 和 iPadOS 13: 通訊錄 保護剖繪: 應用程式軟件的 PP

Apple App 已封存的「共同準則」認證

作業系統/認證日期	計劃 ID/文件	標題/保護剖繪
作業系統:iOS 12 認證日期:2019年6月12日	計劃 ID:10960 文件: 保安目標 指引	標題:iOS 12:Safari 保護剖繪: 應用程式軟件的 PP、 網頁瀏覽器的 EP
作業系統:iOS 12 認證日期:2019年2月28日	計劃 ID:10961 文件: 保安目標 指引	標題:iOS 12:通訊錄 保護剖繪: 應用程式軟件的 PP
作業系統:iOS 11 認證日期:2018年11月9日	計劃 ID:10916 文件: 保安目標 指引	標題:iOS 11:Safari 保護剖繪: 應用程式軟件的 PP、 網頁瀏覽器的 EP
作業系統:iOS 11 認證日期:2018年9月13日	計劃 ID:10915 文件: 保安目標 指引	標題:iOS 11:通訊錄 保護剖繪: 應用程式軟件的 PP

Apple 互聯網服務的保安認證

Apple 為符合 ISO/IEC 27001 和 ISO/IEC 27018 標準而維持多項認證資格，以使 Apple 客戶可行使其法規與合約義務。這些證書為我們的客戶提供了針對範圍內系統的 Apple 資訊安全和私隱實務的獨立證明。

ISO/IEC 27001 和 ISO/IEC 27018 是國際標準化組織 (ISO) 所發佈之「資訊保安管理系統」(ISMS) 標準系列的一部份。作為 Apple ISMS 的一部份，所有附件 A 控制要求已包含在 ISO/IEC 27001 和 ISO/IEC 27018 標準中所定義的「適用性聲明」中。Apple 每年都會由認可的註冊商進行獨立的認證。

ISO/IEC 27001

ISO/IEC 27001 是「資訊保安管理系統」標準，規定了建立、執行、維護和持續改善機構的「資訊保安管理系統」的相關要求。ISO/IEC 27001 標準包括 Apple 的 ISO/IEC 認證所涵蓋的以下保安領域：

- 資訊保安規則
- 資訊保安的組織
- 資產管理
- 人力資源保安
- 物理和環境保安
- 通訊和營運管理
- 存取權限控制
- 資訊系統的取得、開發和維護
- 資訊保安事件管理
- 業務連續性管理
- 合規

ISO/IEC 27018

ISO/IEC 27018 是在公開雲端環境中保護個人身份資料 (PII) 的行為準則。ISO/IEC 27018 標準包括 Apple 的 ISO/IEC 認證所涵蓋的以下保安領域：

- 同意和選擇
- 目的合法性和規範
- 資料收集限制
- 資料最小化
- 使用、保留和披露限制
- 準確性和品質
- 公開性、透明度和通告
- 個別參與和存取
- 問責
- 資訊保安
- 私隱合規

ISO/IEC 27001 和 ISO/IEC 27018 所涵蓋的 Apple 服務

Apple 的 ISO/IEC 27001 和 ISO/IEC 27018 認證涵蓋下列服務：

- Apple 商務聊天
- Apple Business Manager
- Apple 推送通知服務 (APNs)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iWork 服務
- 管理式 Apple ID
- 功課 App
- Siri

認證

我們的註冊商可提供 Apple ISO/IEC 27001 和 27018 認證的證明。

如要檢視 Apple 的認證，請前往「英國標準學會」(BSI) 網站上的[認證與客戶名錄搜尋](#)，在 Company (公司) 搜尋欄位中輸入 Apple，按一下 Search (搜尋) 按鈕，然後選擇搜尋結果來檢視認證。

附註：有關非 Apple 製造之產品或非 Apple 控制或測試之獨立網站所提供的資料非經推薦或保證。對於第三方網站或產品的選擇、效能或使用，Apple 概不承擔任何責任。Apple 不對第三方網站的準確性或可靠性做任何陳述。請[聯絡廠商](#)以取得額外資料。

macOS 保安合規計劃

[macOS 保安合規計劃 \(mSCP\)](#) 是一項開放原始碼作業，目的是提供程式設計方式以產生保安指引。這是一項由美國的「國家標準技術研究院」(NIST)、「國家航空暨太空總署」(NASA)、「國防通訊局」(DISA) 和「洛斯阿拉莫斯國家實驗室」(LANL) 的聯邦作業 IT 保安人員聯合參與的計劃。此計劃使用一組經過測試及驗證的 macOS 控制項目，並將這些控制項目對應至此計劃支援的任何保安指南。此外，此計劃可以用作資源，利用經過測試及驗證的原子化動作 (配置設定) 資料庫，輕鬆建立技術保安控制的自訂保安基準。此計劃會根據所使用的基準輸出自訂文件、指令碼、設定描述檔，以及審核檢查表。

mSCP 可以產生要與管理和保安工具結合使用的輸出內容，以達成合規性。此計劃中的配置設定支援以下指引準則：

機構	支援的準則
美國「國家標準技術研究院」(NIST) 特別出版物 (SP) 800-53，建議聯邦資訊系統與機構使用的保安控制，修訂版 5	800-53 高、800-53 中、800-53 低
美國「國家標準技術研究院」(NIST) 特別出版物 (SP) 800-171，保護非聯邦系統與機構中的受管非機密資料，修訂版 2	800-171
美國「國防通訊局」(DISA) macOS 11 STIG，Apple macOS 11 保安技術實施指南	STIG
美國「國家安全系統委員會」(CNSSI) 1253，國家安全系統的保安分類和控制選擇	1253

其他資料：

- [此處](#)提供的準則可用於檢視此計劃中的所有規則。
- 如要進一步了解此計劃與使用方式，請參閱：[macOS 保安合規計劃 wiki](#)。
- 如要設定此計劃以使用，請參閱：[了解 macOS 保安合規專案第一部份](#)和[了解 macOS 保安合規專案第二部份](#)。
- 如你有興趣支援此計劃的開發，請參閱：[參與者指引](#)。

文件版本記錄

日期	摘要
2021 年 10 月 27 日	<p>已更新的主題：</p> <ul style="list-style-type: none">• 安全隔離區處理器的保安認證• iOS 的保安認證• macOS 的保安認證
2021 年 8 月 17 日	<p>已更新的主題：</p> <ul style="list-style-type: none">• 安全隔離區處理器的保安認證• Apple T2 保安晶片的保安認證• iOS 的保安認證• iPadOS 的保安認證• macOS 的保安認證• tvOS 的保安認證• watchOS 的保安認證• Apple App 的保安認證• 保安認證• macOS 保安合規計劃
2021 年 4 月 26 日	<p>已加入的主題：</p> <ul style="list-style-type: none">• macOS 保安合規計劃 <p>已更新的主題：</p> <ul style="list-style-type: none">• Apple T2 保安晶片的保安認證：新 FIPS 140-2 認證，3811• 安全隔離區處理器的保安認證：新 FIPS 140-2 認證，3811 和其他認證的新表格。• iOS 的保安認證：新 FIPS 140-2 認證，3811、iOS 14 計劃 ID 11146 (評估中)• iPadOS 的保安認證：新 FIPS 140-2 認證，3811、iPadOS 14 計劃 ID 11147 (評估中)• macOS 的保安認證：新 FIPS 140-2 認證，3811。• tvOS 的保安認證：新 FIPS 140-2 認證，3811。• watchOS 的保安認證：新 FIPS 140-2 認證，3811。• Apple App 的保安認證：更新「共同準則」狀態，以及封存「共同準則」認證的新表格。

詞彙表

加密編譯演算法驗證計劃 (CAVP) 由 NIST 運作的組織，提供對已核准 (例如 FIPS 核准和 NIST 推薦) 加密編譯演算法及其各個元件的驗證測試。

加密編譯模組 提供加密編譯功能並滿足規定之加密編譯模組標準要求的硬件、軟件和/或韌體。

加密編譯模組驗證計劃 (CMVP) 由美國和加拿大政府運作的組織，負責驗證是否符合 FIPS 140-3 標準。

共同準則 (CC) 建立 IT 保安評估的一般概念和原則，並具體說明一般評估模型的標準，當中包括以標準化語言寫成的保安要求目錄。

共同準則承認協定 (CCRA) 相互承認的協定，根據 ISO/IEC 15408 系列或「共同準則」標準建立國際認可憑證的政策和要求。

合作保護剖繪 (cPP) 由「國際技術社群」(負責建立 cPP 的專家群組) 所開發的「保護剖繪」。

安全隔離區處理器 (SEP) 單晶片系統 (SoC) 內裝配的協同處理器。

完整磁碟加密 (FDE) 加密儲存卷宗上的所有資料。

保安目標 (ST) 具體說明特定產品的保安問題和保安要求的文件。

保安層級 (SL) ISO/IEC 19790 中定義的四個整體保安層級 (1-4)，用於描述四套適用的保安要求。層級 4 為當中最嚴格的。

保護剖繪 (PP) 具體說明特定產品類別的保安問題和保安要求的文件。

流動裝置管理 (MDM) 讓用戶遙距管理已註冊裝置的服務。在裝置註冊後，用戶可透過網絡使用 MDM 服務來配置設定及執行其他操作，過程中無需與用戶互動。

國家資訊保證合作組織 (NIAP) 美國政府的組織，負責在美國落實「共同準則」並管理 NIAP「共同準則評估和驗證計劃」(CCEVS)。

國家標準技術研究院 (NIST) 隸屬於美國商務部，負責推動測量科學、標準和技術。

國際技術社群 (ITC) 在「共同準則承認協定」(CCRA) 的支持下，負責制定「保護剖繪」或合作「保護剖繪」的小組。

單晶片系統 (SoC) 一種集成電路 (IC)，可將多重元件整合到單片晶片上。

資訊保安管理系統 (ISMS) 一套資訊保安規則和程序，用於管理保安程式的界線，這些程序的目的是在資料和/或系統的整個生命週期中，可系統性地管理資訊保安，藉此保護資訊和系統的範疇。

資深官員小組資訊系統保安 (SOG-IS) 管理數個歐洲國家之間的相互承認協議的小組。

實作待測 (IUT) 實驗室正在測試的加密編譯模組。

適用性聲明 (SOA) 描述保安控制的文件，這些控制措施會在 ISMS 範疇內執行以支援 ISMS/IEC 27001 認證。

檢測中的模組 (MIP) 由「加密編譯模組驗證計劃」(CMVP) 所維護，載有正在 CMVP 驗證程序中的加密編譯模組之列表。

聯邦資訊處理標準 (FIPS) 由美國「國家標準技術研究院」在法規要求下、或在聯邦政府對網絡保安提出強制要求下，又或在兩者同時發生時所制定的發表內容。

Apple 推送通知服務 (APNs) 由 Apple 提供的全球性服務，可傳送推送通知到 Apple 裝置。

Apple Business Manager 一個易於使用的入口網站，能提供快速、簡化的方式讓 IT 管理者為機構部署直接購自 Apple 或與 Apple 合作之授權經銷商或電訊商的 Apple 裝置。他們可以在流動裝置管理 (MDM) 解決方案中自動註冊裝置，無須在用戶取得前實際觸碰或準備裝置。

Apple School Manager 一個易於使用的入口網站，能提供快速、簡化的方式讓 IT 管理者為機構部署直接購自 Apple 或與 Apple 合作之授權經銷商或電訊商的 Apple 裝置。他們可以在流動裝置管理 (MDM) 解決方案中自動註冊裝置，無須在用戶取得前實際觸碰或準備裝置。

Corecrypto 提供低層級加密編譯原始語言導入的程式庫。請注意，Corecrypto 不會直接為開發者提供程式設計介面，而是透過提供給開發者的 API 來使用。Corecrypto 原始碼可公開取得，以驗證其保安特點和正確運作。

IPsec VPN 用戶端 在「保護剖繪」中，提供實體或虛擬主機平台與遙距位置之間之安全 IPsec 連線的用戶端。

Secure Element (SE) 內嵌於許多 Apple 裝置中的晶片，支援 Apple Pay 等功能。

sepOS 「安全隔離區」韌體，採用 Apple 特製的 L4 microkernel 版本。

T2 2017 年後，部份以 Intel 為基礎的 Mac 電腦中所配備的 Apple 保安晶片。

Apple Inc.

© 2021 Apple Inc. 保留一切權利。

如在未經 Apple 事先書面許可的情況下將「鍵盤」上的 Apple 標誌 (Option + Shift + K) 用於商業用途, 可能會違反美國聯邦和州法律, 並構成侵犯商標權和 unfair competition 行為。

Apple、蘋果、Apple 標誌、Apple Pay、Apple TV、Apple Watch、Face ID、FaceTime、FileVault、iMac、iMac Pro、iMessage、iPad、iPad Air、iPadOS、iPad Pro、iPhone、iPod、iPod touch、iTunes、iWork、Mac、MacBook、MacBook Pro、macOS、OS X、Safari、Siri、Touch ID、tvOS 和 watchOS 是 Apple Inc. 在美國及其他國家和地區註冊的商標。

iCloud 是 Apple Inc. 在美國及其他國家和地區註冊的服務標誌。

iOS 是 Cisco 在美國及其他國家和地區的商標或註冊商標, 且經過授權使用。

此處提及的其他產品和公司名稱可能為其各自公司的商標。產品規格如有變更, 恕不另行通知。

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

HK028-00499-B