安全性認證與合規中心

2021 年 12 月

目錄

Apple 安全性保障簡介

Apple 定期與第三方組織密切合作，以認證和證明 Apple 的硬體、軟體和服務的安全性，作為我們致力於安全性的實踐。這些國際認可的組織為 Apple 提供了適用於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安全性需求的可信度（即安全性保證）。對於相互認可協議（MRA）不接受的技術領域或缺乏成熟的安全性認證標準的技術領域，Apple 致力於開發適當的安全性標準。我們的使命是讓 Apple 硬體、作業系統、App 和服務均獲得全球認可的全方位安全性認證。

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 之類的服務受 Apple 的 ISO/IEC 27001 和 ISO/IEC 27018 認證保護。所有客戶，包括部署 Apple 裝置的政府機關以及企業和教育組織，都可以使用硬體、作業系統、軟體和服務認證來證明合規性。

硬體認證

因為安全軟體需以硬體的內建安全性為基礎，因此 Apple 裝置（執行 iOS、iPadOS、macOS、tvOS 或 watchOS）的晶片便植入了安全性功能。這些社群包含支援系統安全功能的 CPU 能力，以及專用於安全功能的矽晶片。最關鍵的元件是「安全隔離區」副處理器，該副處理器出現在所有現今 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 安全晶片的 intel 架構 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 對安全性保障的投入始於對矽晶片基礎安全元件的認證，從信任硬體根到安全開機執行，再到提供 Secure Key Store 的「安全隔離區」，以及具有 Touch ID 和 Face ID 的安全驗證。藉由結合僅可從 Apple 取得的晶片設計、硬體、軟體和服務，可實現 Apple 裝置的安全功能。這些元件的認證是驗證 Apple 所提供之保證很重要的一部分。

如需與硬體和相關韌體元件有關的公開認證資訊，請參閱：

- Apple T2 安全晶片的安全性認證
- 安全隔離區處理器的安全性認證

軟體和 App 認證

Apple 會針對作業系統和應用程式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、應用程式和裝置服務的共同準則。作業系統的涵蓋範圍包括 iOS、iPadOS、macOS、sepOS、T2 韌體、tvOS 和 watchOS。若為 App，獨立認證一開始包括 Safari 瀏覽器和「聯絡人」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 的安全性認證
- iPadOS 的安全性認證
- macOS 的安全性認證
- tvOS 的安全性認證
- watchOS 的安全性認證

如需與 Apple **App** 有關的公開認證資訊，請參閱：

- Apple App 的安全性認證

服務認證

Apple 維護安全性認證，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 軟硬體搭配使用時，能夠履行其監管和合約義務。這些認證針對 Apple 系統的 Apple 資訊安全性、環境和隱私權作法，為客戶提供了獨立證明。

如需與 Apple **Internet 服務**有關的公開認證資訊，請參閱：

- Apple Internet 服務的安全性認證

若有 Apple 安全性和隱私權認證的問題，請聯絡 security-certifications@apple.com。

硬體安全性認證

Apple 硬體安全性認證概覽

Apple 為 sepOS 和 T2 韌體維護聯邦資訊處理標準 (FIPS) 140-2/-3 符合性驗證憑證以及其他認證。Apple 從**認證基本要件**開始著手，這些基本要件可在適用情況下跨多個平台廣泛應用。其中一個基本要件就是 Corecrypto 資料庫的驗證，其用於 Apple 所開發作業系統內的軟硬體加密編譯密模組開發。第二個基本要件是安全隔離區 (內嵌在許多 Apple 裝置內) 的認證。第三個則是 Secure Element 的認證，應用於配備 Touch ID 的 Apple 裝置和配備 Face ID 的裝置。這些硬體認證基本要件為更廣泛的平台安全性認證形成了基礎。

加密演算法驗證

驗證許多加密演算法和相關安全性功能的導入正確性，是 FIPS 140-3 驗證和支援其他認證的先決條件。驗證由國家標準技術研究院 (NIST) 加密編譯演算法驗證計畫 (CAVP) 管理。您可使用 CAVP 搜尋工具來找到 Apple 導入的驗證憑證。如需更多資訊，請參閱加密編譯演算法驗證計畫 (CAVP) 網站。

加密編譯密模組驗證：FIPS 140-2/3 (ISO/IEC 19790)

自 2012 年起，每個主要作業系統發佈後，「加密編譯模組驗證計畫」(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 每年都針對以軟體為基礎的模組 (macOS 的 Corecrypto 模組 (Intel) 和 Corecrypto Kernel 模組 (Intel)) 達到**安全性層級 1**。若是 Apple 晶片，模組「Corecrypto 模組 (ARM)」和「Corecrypto Kernel 模組 (ARM)」適用於 iOS、iPadOS、tvOS、watchOS 以及 Mac 電腦所配備 Apple T2 安全晶片內嵌的韌體。

2019 年，Apple 已針對嵌入式硬體加密編譯模組 (稱為「Apple Corecrypto 模組：安全鑰匙儲存」) 實現第一個 FIPS 140-2 **安全性層級 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體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訊。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。因為該評估程序的長度可能有所變動，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，用來當作 IT 產品安全性評估的基礎。

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，相互承認受 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安全性標準，以明確可靠地評估資訊科技產品的安全性功能。「共同準則認證」會對產品能否符合安全性標準進行獨立評估，以讓客戶提升對資訊科技產品安全性的信心，進而根據充足的資訊作出決策。

透過 CCRA，各會員國家已同意抱持相同的信心度，承認該資訊技術產品認證。認證之前需要進行的評估相當廣，包括：

- 保護剖繪（PP）
- 安全性目標（ST）
- 安全性功能要求（SFR）
- 安全性保障要求（SAR）
- 評估保證等級（EAL）

「保護剖繪」（PP）是一種明定各項安全性需求的文件，適用於特定的裝置型態分類（例如「行動性」），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，皆只須取得單一認證，並得到任何 CCRA 簽署者的認可。

安全性目標（ST）定義了認證 IT 產品時將評估的**內容**。ST 會被轉換為更具體的**安全性功能要求（SFR）**，用於更詳細地評估 ST。

共同準則（CC）還包括**安全性保障要求**。一種常見的認可指標是**評估保證等級（EAL）**。EAL 會與頻繁出現的 SAR 集群組在一起，可以在 PP 和 ST 中加以指定，以支援可比較性。

許多舊版 PP 已封存，並即將由專為特定解決方案和環境所制訂的針對式 PP 取代。為齊力確保所有 CCRA 會員之間能持續相互認可，國際技術社群（iTC）已經成立，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）。相關的利害關係人將繼續開發以 CCRA 以外之使用者群組和相互認可協議為對象的 PP。

從 2015 年初開始，Apple 便開始依據更新的 CCRA（包含特定 cPP）致力取得認證。此後，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 提供的安全性保障。

Apple 在專門進行行動安全技術評估的技術社群中扮演著積極角色，這些社群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，其他憑證也已核發，以證明部分市場的特定安全要求。

安全隔離區處理器的安全性認證

安全隔離區認證背景

硬體加密編譯模組（**Apple SEP Secure Key Store 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 Intel 架構式 Mac 電腦所採用的 T 系列安全晶片。

在 2018 年，Apple 將軟體加密編譯模組的驗證與 2017 年發佈的作業系統（iOS 11、macOS 10.13、tvOS 11 和 watchOS 4）加以同步化。SEP 硬體加密編譯模組（被識別為「Apple SEP Secure Key Store 加密編譯模組 v1.0」）最初是根據 FIPS 140-2 安全性層級 1 的要求完成驗證。

在 2019 年，Apple 根據 FIPS 140-2 安全性層級 2 要求驗證了硬體模組，並將模組版本識別碼更新為 v9.0，以便與對應的 Corecrypto「使用者」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 Apple 致力取得驗證以符合 FIPS 140-3，並針對 Apple 晶片（A13、A14、S6 和 M1 晶片）額外取得實體安全性需求的安全性層級 3 保證。

Apple 也針對作業系統每個主要版本積極參與 Corecrypto「使用者」和 Corecrypto「核心」模組的驗證。符合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畫（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」分成四個階段來追蹤 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作業。
  - **協調**：實驗室和 CMVP 正在解決發現的所有問題。
  - **最終處理**：與簽發憑證有關的作業和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性憑證，並將其加到已驗證的加密編譯模組列表中。這包含：
  - 標示為作用中（Active）的已驗證模組。
  - 5 年過後，模組會標示為歷史（Historical）。
  - 如果模組憑證因某些原因遭撤銷時，則會標示為已撤銷（Revoked）。

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 Secure Key Store (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) 使用者空間、核心空間和 Secure Key Store 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	憑證/文件	模組資訊
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (A9-A14、T2、M1、S3-S6) **整體安全性層級：**2
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (A13、A14、S6、M1) **整體安全性層級：**2 **實體安全性層級：**3
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (A9-A14、T2、M1、S3-S6) **整體安全性層級：**2
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (A13、A14、S6、M1) **整體安全性層級：**2 **實體安全性層級：**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	憑證/文件	模組資訊
作業系統發佈日期：2019 **驗證日期：**2021/2/5	**憑證：**3811 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v10.0 **作業系統：**macOS 10.15 Catalina 的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2018 **驗證日期：**2019/9/10	**憑證：**3523 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v9.0 **作業系統：**macOS 10.14 Mojave 的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2017 **驗證日期：**2019/9/10	**憑證：**3223 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v1.0 **作業系統：**macOS 10.13 High Sierra 的 sepOS **類型：**硬體 **安全性層級：**2

共同準則 (CC) 認證

Apple 積極參與具有適當保護剖繪可涵蓋 Apple 技術之安全性功能的共同準則評估。

共同準則 (CC) 認證狀態

由 NIAP 運作的 U.S. 架構維護著一份評估產品列表，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」(或同等狀態) 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) 下相互認可的認證。共同準則入口網站可以將產品保留在認證產品列表中 5 年，記錄則會由共同準則入口網站保留以備存檔認證。

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	架構 ID/文件	標題/保護剖繪
作業系統：sepOS **認證日期：**—	**架構 ID：**尚未通過認證 **文件：** 憑證 安全性目標 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 **硬體：**安全隔離區 (A9-A14、M1、T2、S3-S6) **軟體：**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	憑證/文件	模組資訊
作業系統發佈日期：2020 **驗證日期：**2019/12/7 到 2022/12/26	**憑證：**CFNR201902910002（P.R.China：移動金融技術服務認證） 中文版 英文版	**標題：**行動終端可信執行環境 **作業系統：**iOS 13.5.1 **規格：**JR/T 0156-2017

Apple T2 安全晶片的安全性認證

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 內嵌軟體和硬體模組的驗證。符合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 安全晶片，該晶片是以 Apple 晶片為基礎的系統單晶片（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 使用者模組（由 Intel 架構式 Mac 電腦的 macOS 使用）
- Intel 適用的 Corecrypto 核心模組（由 Intel 架構式 Mac 電腦的 macOS 使用）
- ARM 適用的 Corecrypto 使用者模組（由 T2 晶片使用）
- ARM 適用的 Corecrypto 核心模組（由 T2 晶片使用）
- Secure Key Store 加密編譯模組（由 T2 晶片中的內嵌「安全隔離區」副處理器使用）

【注意】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畫（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」分成四個階段來追蹤 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作業。
  - **協調：**實驗室和 CMVP 正在解決發現的所有問題。
  - **最終處理：**與簽發憑證有關的作業和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性憑證，並將其加到已驗證的加密編譯模組列表中。這包含：
  - 標示為作用中（Active）的已驗證模組。
  - 5 年過後，模組會標示為歷史（Historical）。
  - 如果模組憑證因某些原因遭撤銷時，則會標示為已撤銷（Revoked）。

FIPS 140-3 認證

目前狀態

使用者空間、核心空間和 Secure Key Store 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)。

使用者空間、核心空間和 Secure Key Store 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	憑證/文件	模組資訊
作業系統發佈日期：2021 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、使用者、軟體 **類型**：軟體 **安全性層級**：1
作業系統發佈日期：2021 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、軟體 **類型**：軟體 **安全性層級**：1
作業系統發佈日期：2021 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、Secure Key Store、硬體 **類型**：硬體 (T2) **安全性層級**：2
作業系統發佈日期：2020 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、使用者、軟體 **類型**：軟體 **安全性層級**：1
作業系統發佈日期：2020 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、軟體 **類型**：軟體 **安全性層級**：1
作業系統發佈日期：2020 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 Crypto Officer 指引	**標題**：Apple Corecrypto 模組 v11.1 **作業系統**：Intel 架構式 macOS 11 Big Sur 的 sepOS **環境**：Apple 晶片、Secure Key Store、硬體 **類型**：硬體 **安全性層級**：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	憑證/文件	模組資訊
作業系統發佈日期：2019 **驗證日期：**2021/3/23	**憑證：**3856 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v10.0 **作業系統：**macOS 10.15 Catalina 的 sepOS **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**2021/3/23	**憑證：**3855 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**2021/2/5	**憑證：**3811 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto Secure Key Store 加密編譯模組 v10.0 **作業系統：**macOS 10.15 Catalina 的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2018 **驗證日期：**2019/4/23	**憑證：**3438 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v9.0 **作業系統：**macOS 10.14 Mojave 的 sepOS **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2018 **驗證日期：**2019/4/11	**憑證：**3433 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2018 **驗證日期：**2019/9/10	**憑證：**3523 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v9.0 **作業系統：**macOS 10.14 Mojave 的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2017 **驗證日期：**2018/3/9、2018/5/22、2018/7/6	**憑證：**3148 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v8.0 **作業系統：**macOS 10.13 High Sierra 的 sepOS **類型：**軟體 **安全性層級：**1

日期	憑證/文件	模組資訊
作業系統發佈日期：2017 **驗證日期：**2018/3/9、2018/5/17、2018/7/3	**憑證：**3147 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2017 **驗證日期：**2018/7/10	**憑證：**3223 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v1.0 **作業系統：**macOS 10.13 High Sierra 的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2016 **驗證日期：**2017/2/1	**憑證：**2828 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2016 **驗證日期：**2017/2/1	**憑證：**2827 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1

作業系統安全性認證

Apple 作業系統安全性認證概覽

Apple 為 sepOS 和 T2 韌體維護聯邦資訊處理標準（FIPS）140-2/-3 符合性驗證憑證以及其他認證。Apple 從**認證基本要件**開始著手，這些基本要件可在適用情況下跨多個平台廣泛應用。其中一個基本要件就是 Corecrypto 的驗證，其用於 Apple 所開發作業系統內的軟硬體加密編譯密模組開發。第二個基本要件是安全隔離區（內嵌在許多 Apple 裝置內）的認證。第三個則是 Secure Element 的認證，應用於配備 Touch ID 的 Apple 裝置和配備 Face ID 的裝置。這些硬體認證基本要件為更廣泛的平台安全性認證形成了基礎。

加密演算法驗證

驗證許多加密演算法和相關安全性功能的導入正確性，是 FIPS 140-3 驗證和支援其他認證的先決條件。驗證由 NIST 加密演算法驗證程式（CAVP）管理。您可使用 CAVP 搜尋工具來找到 Apple 導入的驗證憑證。

加密編譯密模組驗證：FIPS 140-2/3（ISO/IEC 19790）

自 2012 年起，每個主要作業系統發佈後，「加密編譯模組驗證計畫」（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 每年都針對以軟體為基礎的模組（macOS 的 Corecrypto 模組（Intel）和 Corecrypto Kernel 模組（Intel））達到**安全性層級 1**。若是 Apple 晶片，模組「Corecrypto 模組（ARM）」和「Corecrypto Kernel 模組（ARM）」適用於 iOS、iPadOS、tvOS、watchOS 以及 Mac 電腦所配備 Apple T2 安全晶片內嵌的韌體。

2019 年，Apple 已針對嵌入式硬體加密編譯模組（稱為「Apple Corecrypto 模組：安全鑰匙儲存」）實現第一個 FIPS 140-2 **安全性層級 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體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訊。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。因為該評估程序的長度可能有所變動，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，用來當作 IT 產品安全性評估的基礎。

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，相互承認受 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安全性標準，以明確可靠地評估資訊科技產品的安全性功能。「共同準則認證」會對產品能否符合安全性標準進行獨立評估，以讓客戶提升對資訊科技產品安全性的信心，進而根據充足的資訊作出決策。

透過 CCRA，各會員國家已同意抱持相同的信心度，承認該資訊技術產品認證。認證之前需要進行的評估相當廣，包括：

- 保護剖繪（PP）
- 安全性目標（ST）
- 安全性功能要求（SFR）
- 安全性保障要求（SAR）
- 評估保證等級（EAL）

「保護剖繪」（PP）是一種明定各項安全性需求的文件，適用於特定的裝置型態分類（例如「行動性」），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，皆只須取得單一認證，並得到任何 CCRA 簽署者的認可。

安全性目標（ST）定義了認證 IT 產品時將評估的**內容**。ST 會被轉換為更具體的**安全性功能要求（SFR）**，用於更詳細地評估 ST。

共同準則（CC）還包括**安全性保障要求**。一種常見的認可指標是**評估保證等級（EAL）**。EAL 會與頻繁出現的 SAR 集群組在一起，可以在 PP 和 ST 中加以指定，以支援可比較性。

許多舊版 PP 已封存，並即將由專為特定解決方案和環境所制訂的針對式 PP 取代。為齊力確保所有 CCRA 會員之間能持續相互認可，國際技術社群（iTC）已經成立，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）**。相關的利害關係人將繼續開發以 CCRA 以外之使用者群組和相互認可協議為對象的 PP。

從 2015 年初開始，Apple 便開始依據更新的 CCRA（包含特定 cPP）致力取得認證。此後，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 提供的安全性保障。

Apple 在專門進行行動安全技術評估的技術社群中扮演著積極角色，這些社群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，其他憑證也已核發，以證明部分市場的特定安全要求。

iOS 的安全性認證

iOS 認證背景

Apple 針對作業系統每個主要版本積極參與 Apple 內嵌軟體和硬體模組的驗證。符合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畫 (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」分成四個階段來追蹤 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作業。
  - **協調：**實驗室和 CMVP 正在解決發現的所有問題。
  - **最終處理：**與簽發憑證有關的作業和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性憑證，並將其加到已驗證的加密編譯模組列表中。這包含：
  - 標示為作用中 (Active) 的已驗證模組。
  - 5 年過後，模組會標示為歷史 (Historical)。
  - 如果模組憑證因某些原因遭撤銷時，則會標示為已撤銷 (Revoked)。

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) 使用者空間、核心空間和 Secure Key Store 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) 使用者空間、核心空間和 Secure Key Store 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	憑證/文件	模組資訊
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v12 **作業系統：**iOS 15 **環境：**Apple 晶片、使用者、軟體 **類型：**軟體 **整體安全性層級：**1
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v12 **作業系統：**iOS 15 **環境：**Apple 晶片、核心、軟體 **類型：**軟體 **整體安全性層級：**1
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (A9-A14) **整體安全性層級：**2
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (A13、A14、A15) **整體安全性層級：**2 **實體安全性層級：**3
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v11.1 **作業系統：**iOS 14 **環境：**Apple 晶片、使用者、軟體 **類型：**軟體 **整體安全性層級：**1
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、軟體 **類型：**軟體 **整體安全性層級：**1

日期	憑證/文件	模組資訊
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (A9-A14) **整體安全性層級：**2
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (A13-A14) **整體安全性層級：**2 **實體安全性層級：**3

FIPS 140-2 認證

下表顯示實驗室目前正在測試且已經過測試符合 FIPS 140-2 的加密編譯模組。

日期	憑證/文件	模組資訊
作業系統發佈日期：2019 **驗證日期：**2021/3/23	**憑證：**3856 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v10.0 **作業系統：**iOS 13 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**2021/3/23	**憑證：**3855 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**2021/2/5	**憑證：**3811 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v10.0 **作業系統：**與 iOS 13 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2018 **驗證日期：**2019/4/23	**憑證：**3438 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2018 **驗證日期：**2019/4/11	**憑證：**3433 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v9.0 **作業系統：**iOS 12 **類型：**軟體 **安全性層級：**1

日期	憑證/文件	模組資訊
作業系統發佈日期：2018 **驗證日期：**2019/9/10	**憑證：**3523 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v9.0 **作業系統：**與 iOS 12 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2017 **驗證日期：**2018/3/9、2018/5/22、2018/7/6	**憑證：**3148 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v8.0 **作業系統：**iOS 11 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2017 **驗證日期：**2018/3/9、2018/5/17、2018/7/3	**憑證：**3147 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2017 **驗證日期：**2019/9/10	**憑證：**3223 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v1.0 **作業系統：**與 iOS 11 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2016 **驗證日期：**2017/2/1	**憑證：**2828 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple iOS Corecrypto 核心模組 v7.0 **作業系統：**iOS 10 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2016 **驗證日期：**2017/2/1	**憑證：**2827 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple iOS Corecrypto 核心模組 v7.0 **作業系統：**iOS 10 **類型：**軟體 **安全性層級：**1

先前版本

超過 5 年的憑證會由 CMVP 列出，並具有歷史記錄狀態。以下先前的 iOS 版本具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 U.S. 架構維護著一份評估產品列表，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」（或同等狀態）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）下相互認可的認證。共同準則入口網站可以將產品保留在認證產品列表中 5 年，記錄則會由共同準則入口網站保留以備存檔認證。

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。如需最新資訊，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	架構 ID/文件	標題/保護剖繪
作業系統：iOS 15 **認證日期**：—	**架構 ID**：尚未通過認證 **文件**：—	**標題**：Apple iOS 15：iPhones **保護剖繪**：行動裝置基礎（PP 模組待確認）
作業系統：iOS 14 **認證日期**：2021/9/1	**架構 ID**：11146 **文件**： 憑證 安全性目標 指引 驗證報告 保證作業報告	**標題**：Apple iOS 14：iPhones **保護剖繪**：行動裝置基礎、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**：2020/11/6	**架構 ID**：11036 **文件**： 憑證 安全性目標 指引 驗證報告 保證作業報告	**標題**：iPhone 上的 Apple iOS 13 **保護剖繪**：行動裝置基礎、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	架構 ID/文件	標題/保護剖繪
作業系統：iOS 12 **認證日期：**2019/3/14	**架構 ID：**10937 **文件：** 安全性目標 指引	**標題：** iOS 12 的 iPhone **保護剖繪：**行動裝置基礎、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：**2018/7/17	**架構 ID：**10851 **文件：** 安全性目標 指引	**標題：**Apple iOS 11 **保護剖繪：**行動裝置基礎、無線 LAN 用戶端 EP、MDM 代理程式 EP
作業系統：iOS 10 **認證日期：**2017/7/27	**架構 ID：**10782 **文件：**安全性目標、指引	**標題：**iPhone 和 iPad 裝置上的 iOS 10.2 **保護剖繪：**行動裝置基礎、無線 LAN 用戶端 EP、MDM 代理程式 EP
作業系統：iOS 10 **認證日期：**2017/7/27	**架構 ID：**10792 **文件：**安全性目標、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：**2016/10/14	**架構 ID：**10725 **文件：**安全性目標、指引	**標題：**iOS 9.3.2 搭配 MDM 代理程式 **保護剖繪：**行動裝置基礎、MDM 代理程式 EP
作業系統：iOS 9 **認證日期：**2016/10/13	**架構 ID：**10714 **文件：**安全性目標、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：**2016/1/28	**架構 ID：**10695 **文件：**安全性目標、指引	**標題：**iOS 9 **保護剖繪：**行動裝置基礎

iPadOS 的安全性認證

iPadOS 認證背景

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

【注意】在 2019 年，iPad 裝置的作業系統改以 iPadOS 的名稱推出。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畫 (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」分成四個階段來追蹤 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作業。
  - **協調：**實驗室和 CMVP 正在解決發現的所有問題。
  - **最終處理：**與簽發憑證有關的作業和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性憑證，並將其加到已驗證的加密編譯模組列表中。這包含：
  - 標示為作用中 (Active) 的已驗證模組。
  - 5 年過後，模組會標示為歷史 (Historical)。
  - 如果模組憑證因某些原因遭撤銷時，則會標示為已撤銷 (Revoked)。

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) 使用者空間、核心空間和 Secure Key Store 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) 使用者空間、核心空間和 Secure Key Store 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	憑證/文件	模組資訊
作業系統發佈日期：2021 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 Crypto Officer 指引	**標題**：Apple Corecrypto 模組 v12 **作業系統**：iPadOS 15 **環境**：Apple 晶片、使用者、軟體 **類型**：軟體 **整體安全性層級**：1
作業系統發佈日期：2021 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 Crypto Officer 指引	**標題**：Apple Corecrypto 模組 v12 **作業系統**：iPadOS 15 **環境**：Apple 晶片、核心、軟體 **類型**：軟體 **整體安全性層級**：1
作業系統發佈日期：2021 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、Secure Key Store、硬體 **類型**：硬體 (A9-A14、M1) **整體安全性層級**：2
作業系統發佈日期：2021 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、Secure Key Store、硬體 **類型**：硬體 (A9-A14、M1) **整體安全性層級**：2 **實體安全性層級**：3
作業系統發佈日期：2020 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 Crypto Officer 指引	**標題**：Apple Corecrypto 模組 v11.1 **作業系統**：iPadOS 14 **環境**：Apple 晶片、使用者、軟體 **類型**：軟體 **整體安全性層級**：1
作業系統發佈日期：2020 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、軟體 **類型**：軟體 **整體安全性層級**：1

日期	憑證/文件	模組資訊
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (A9-A14、M1) **整體安全性層級：**2
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (A9-A14、M1) **整體安全性層級：**2 **實體安全性層級：**3

FIPS 140-2 認證

下表顯示實驗室目前正在測試且已經過測試符合 FIPS 140-2 的加密編譯模組。

日期	憑證/文件	模組資訊
作業系統發佈日期：2019 **驗證日期：**2021/3/23	**憑證：**3856 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v10.0 **作業系統：**iPadOS 13 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**2021/3/23	**憑證：**3855 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**2021/2/5	**憑證：**3811 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto Secure Key Store 加密編譯模組 v10.0 **作業系統：**與 iPadOS 13 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2018 **驗證日期：**2019/4/23	**憑證：**3438 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2018 **驗證日期：**2019/4/11	**憑證：**3433 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v9.0 **作業系統：**iOS 12 **類型：**軟體 **安全性層級：**1

日期	憑證/文件	模組資訊
作業系統發佈日期：2018 **驗證日期：**2019/9/10	**憑證：**3523 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v9.0 **作業系統：**與 iOS 12 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2017 **驗證日期：**2018/3/9、2018/5/22、2018/7/6	**憑證：**3148 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v8.0 **作業系統：**iOS 11 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2017 **驗證日期：**2018/3/9、2018/5/17、2018/7/3	**憑證：**3147 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2017 **驗證日期：**2019/9/10	**憑證：**3223 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v1.0 **作業系統：**與 iOS 11 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2016 **驗證日期：**2017/2/1	**憑證：**2828 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple iOS Corecrypto 核心模組 v7.0 **作業系統：**iOS 10 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2016 **驗證日期：**2017/2/1	**憑證：**2827 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple iOS Corecrypto 核心模組 v7.0 **作業系統：**iOS 10 **類型：**軟體 **安全性層級：**1

先前版本

超過 5 年的憑證會由 CMVP 列出，並具有歷史記錄狀態。以下先前的 iOS 版本具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 U.S. 架構維護著一份評估產品列表，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」（或同等狀態）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）下相互認可的認證。共同準則入口網站可以將產品保留在認證產品列表中 5 年，記錄則會由共同準則入口網站保留以備存檔認證。

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。如需最新資訊，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	架構 ID/文件	標題/保護剖繪
作業系統：iPadOS 15 **認證日期：**2019/3/14	**架構 ID：**— **文件：** 憑證 安全性目標 指引 驗證報告 保證作業報告	**標題：**iOS 12 的 iPad **保護剖繪：**行動裝置基礎、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：**2021/9/1	**架構 ID：**11147 **文件：** 憑證 安全性目標 指引 驗證報告 保證作業報告	**標題：**Apple iPadOS 14：iPad **保護剖繪：**行動裝置基礎、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：**2020/11/6	**架構 ID：**11036 **文件：** 憑證 安全性目標 指引 驗證報告 保證作業報告	**標題：**iPad 行動裝置上的 iPadOS 13 **保護剖繪：**行動裝置基礎、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（架構 ID：10937）
- iOS 11（架構 ID：10851）
- iOS 10（架構 ID：107782、10792）
- iOS 9（架構 ID：10725、10714、10695）

macOS 的安全性認證

macOS 認證背景

Apple 會使用適合的合作保護剖繪和 FIPS 140-3 安全性層級，針對其作業系統的每個主要版本積極參與驗證。符合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畫 (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」分成四個階段來追蹤 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作業。
  - **協調：**實驗室和 CMVP 正在解決發現的所有問題。
  - **最終處理：**與簽發憑證有關的作業和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性憑證，並將其加到已驗證的加密編譯模組列表中。這包含：
  - 標示為作用中 (Active) 的已驗證模組。
  - 5 年過後，模組會標示為歷史 (Historical)。
  - 如果模組憑證因某些原因遭撤銷時，則會標示為已撤銷 (Revoked)。

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 安全晶片的 Mac 電腦	採用 Intel 架構而未配備 Apple T2 安全晶片的 Mac 電腦
Apple 晶片使用者空間	✓		
Apple 晶片核心	✓		
Intel 使用者空間		✓	✓
Intel 核心		✓	✓
Secure Key Store	✓	✓	

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 晶片或採用 Intel 架構的 Mac 電腦的適用性。

【注意】許多採用 Intel 架構的 Mac 電腦都包含 Apple T2 安全晶片。如需 T2 晶片認證的相關資訊，請參閱 Apple T2 安全晶片的安全性認證。

macOS ssh 用戶端

OpenSSH 可設定為使用 FIPS 140-3 已驗證模組來處理特定 FIPS 140-3 演算法。組織可以執行 Apple 所提供經簽署與公證的安裝程式（密碼為 FIPS140Mode）。安裝程式會在 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受 NIST 驗證的加密方式，並確保 OpenSSH 用戶端是使用由平台提供且經過驗證的加密編譯模組。管理者也可以製作自己的檔案。如需更多資訊，請參閱 macOS 12.0.1 或以上版本的 `apple_ssh_and_fips` man 頁面。

目前狀態

macOS 11 Big Sur 使用者空間、核心空間和 Secure Key Store 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 使用者空間、核心空間和 Secure Key Store 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	憑證/文件	模組資訊
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、使用者、軟體 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、軟體 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、使用者、軟體 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、軟體 **類型：**軟體 **安全性層級：**1

日期	憑證/文件	模組資訊
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v12.0 **作業系統：**Apple 晶片上與 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 **環境：**Apple 晶片、Secure Key Store、硬體 **類型：**硬體 (M1 和 T2) **安全性層級：**2
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v12.0 **作業系統：**Apple 晶片上與 macOS 12 Monterey 一起發佈的 sepOS **環境：**Apple 晶片、Secure Key Store、硬體 **類型：**硬體 (M1) **安全性層級：**2 **實體安全性層級：**3
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v11.1 **作業系統：**Intel 上的 macOS 11 Big Sur **環境：**Intel、使用者、軟體 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v11.1 **作業系統：**Intel 上的 macOS 11 Big Sur **環境：**Intel、核心、軟體 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v11.1 **作業系統：**Apple 晶片上的 macOS 11 Big Sur **環境：**Apple 晶片、使用者、軟體 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v11.1 **作業系統：**Apple 晶片上的 macOS 11 Big Sur **環境：**Apple 晶片、核心、軟體 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v11.1 **作業系統：**Apple 晶片上與 macOS 11 Big Sur 一起發佈的 sepOS、Intel 上與 macOS 11 Big Sur 一起發佈的 sepOS **環境：**Apple 晶片、Secure Key Store、硬體 **類型：**硬體 (M1) **安全性層級：**2

日期	憑證/文件	模組資訊
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v11.1 **作業系統：**Apple 晶片上與 macOS 11 Big Sur 一起發佈的 sepOS **環境：**Apple 晶片、Secure Key Store、硬體 **類型：**硬體 (M1) **安全性層級：**2 **實體安全性層級：**3

FIPS 140-2 認證

下表顯示實驗室目前正在測試且已經過測試符合 FIPS 140-2 的加密編譯模組。

macOS 10.15 Catalina 使用者空間、核心空間和 Secure Key Store 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)。

【注意】許多採用 Intel 架構的 Mac 電腦都包含 Apple T2 安全晶片。如需 T2 晶片認證的相關資訊，請參閱 Apple T2 安全晶片的安全性認證。

日期	憑證/文件	模組資訊
作業系統發佈日期：2019 **驗證日期：**2021/3/24	**憑證：**3859 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Intel (ccv10) 適用的 Apple Corecrypto 使用者空間模組 **作業系統：**macOS 10.15 Catalina **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**2021/3/24	**憑證：**3858 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Intel (ccv10) 適用的 Apple Corecrypto 核心模組 v10.0 **作業系統：**macOS 10.15 Catalina **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2018 **驗證日期：**2019/4/12	**憑證：**3402 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Intel 適用的 Apple Corecrypto 使用者模組 v9.0 **作業系統：**macOS 10.14 Mojave **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2018 **驗證日期：**2019/4/12	**憑證：**3431 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2017 **驗證日期：**2018/3/22	**憑證：**3155 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Intel 適用的 Apple Corecrypto 使用者模組 v8.0 **作業系統：**macOS 10.13 High Sierra **類型：**軟體 **安全性層級：**1

日期	憑證/文件	模組資訊
作業系統發佈日期：2017 **驗證日期**：2018/3/22	**憑證**：3156 **文件**： 憑證 安全性規則 Crypto Officer 指引	**標題**：Intel 適用的 Apple Corecrypto 核心模組 v8.0 **作業系統**：macOS 10.13 High Sierra **類型**：軟體 **安全性層級**：1

先前版本

以下先前的 OS X 和 macOS 版本具有加密編譯模組驗證。超過 5 年的版本會由 CMVP 列出，並具有歷史記錄狀態：

- 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 U.S. 架構維護著一份評估產品列表，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」(或同等狀態) 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) 下相互認可的認證。共同準則入口網站可以將產品保留在認證產品列表中 5 年，記錄則會由共同準則入口網站保留以備存檔認證。

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。

如需最新資訊，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	架構 ID/文件	標題/保護剖繪
作業系統：macOS 12 Monterey **認證日期：**—	**架構 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：**—	**架構 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：**—	**架構 ID：**尚未通過認證 **文件：** 憑證 安全性目標 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：**—	**架構 ID：**尚未通過認證 **文件：** 憑證 安全性目標 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：**2021/4/29	**架構 ID：**11078 **文件：** 憑證 安全性目標 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：**2020/9/23	**架構 ID：**11077 **文件：** 憑證 安全性目標 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 的安全性認證

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。符合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畫 (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」分成四個階段來追蹤 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作業。
  - **協調**：實驗室和 CMVP 正在解決發現的所有問題。
  - **最終處理**：與簽發憑證有關的作業和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性憑證，並將其加到已驗證的加密編譯模組列表中。這包含：
  - 標示為作用中 (Active) 的已驗證模組。
  - 5 年過後，模組會標示為歷史 (Historical)。
  - 如果模組憑證因某些原因遭撤銷時，則會標示為已撤銷 (Revoked)。

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) 使用者空間、核心空間和 Secure Key Store 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) 使用者空間、核心空間和 Secure Key Store 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	憑證/文件	模組資訊
作業系統發佈日期：2021 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 Crypto Officer 指引	**標題**：Apple Corecrypto 模組 v12 **作業系統**：tvOS 15 **環境**：Apple 晶片、使用者、軟體 **類型**：軟體 **整體安全性層級**：1
作業系統發佈日期：2021 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 Crypto Officer 指引	**標題**：Apple Corecrypto 模組 v12 **作業系統**：tvOS 15 **環境**：Apple 晶片、核心、軟體 **類型**：軟體 **整體安全性層級**：1
作業系統發佈日期：2021 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、Secure Key Store、硬體 **類型**：硬體 (A10、A12) **整體安全性層級**：2
作業系統發佈日期：2020 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 Crypto Officer 指引	**標題**：Apple Corecrypto 模組 v11.1 **作業系統**：tvOS 14 **環境**：Apple 晶片、使用者、軟體 **類型**：軟體 **整體安全性層級**：1
作業系統發佈日期：2020 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、軟體 **類型**：軟體 **整體安全性層級**：1
作業系統發佈日期：2020 **驗證日期**：—	**憑證**：尚未通過認證 **文件**： 憑證 安全性規則 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、Secure Key Store、硬體 **類型**：硬體 (A10、A12) **整體安全性層級**：2

FIPS 140-2 認證

下表顯示實驗室目前正在測試且已經過測試符合 FIPS 140-2 的加密編譯模組。

tvOS 13 (2019) 使用者空間、核心空間和 Secure Key Store 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	憑證/文件	模組資訊
作業系統發佈日期：2019 **驗證日期：**2021/3/23	**憑證：**3856 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v10.0 **作業系統：**tvOS 13 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**2021/3/23	**憑證：**3855 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**2021/2/5	**憑證：**3811 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v10.0 **作業系統：**與 tvOS 13 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2018 **驗證日期：**2019/4/23	**憑證：**3438 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2018 **驗證日期：**2019/4/11	**憑證：**3433 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v9.0 **作業系統：**tvOS 12 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2018 **驗證日期：**2019/9/10	**憑證：**3523 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v9.0 **作業系統：**與 tvOS 12 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2017 **驗證日期：**2018/3/9、2018/5/22、2018/7/6	**憑證：**3148 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v8.0 **作業系統：**tvOS 11 **類型：**軟體 **安全性層級：**1

日期	憑證/文件	模組資訊
作業系統發佈日期：2017 **驗證日期：**2018/3/9、2018/5/17、2018/7/3	**憑證：**3147 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2017 **驗證日期：**2019/9/10	**憑證：**3223 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v1.0 **作業系統：**與 tvOS 11 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2

watchOS 的安全性認證

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。符合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畫 (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」分成四個階段來追蹤 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作業。
  - **協調：**實驗室和 CMVP 正在解決發現的所有問題。
  - **最終處理：**與簽發憑證有關的作業和手續。
- 在通過 CMVP 驗證後，將向模組授予一致性憑證，並將其加到已驗證的加密編譯模組列表中。這包含：
  - 標示為作用中 (Active) 的已驗證模組。
  - 5 年過後，模組會標示為歷史 (Historical)。
  - 如果模組憑證因某些原因遭撤銷時，則會標示為已撤銷 (Revoked)。

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) 使用者空間、核心空間和 Secure Key Store 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) 使用者空間、核心空間和 Secure Key Store 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	憑證/文件	模組資訊
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v12 **作業系統：**watchOS 8 **環境：**Apple 晶片、使用者、軟體 **類型：**軟體 **整體安全性層級：**1
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v12 **作業系統：**watchOS 8 **環境：**Apple 晶片、核心、軟體 **類型：**軟體 **整體安全性層級：**1
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (S3、S4、S5、S6) **整體安全性層級：**2
作業系統發佈日期：2021 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (S6) **整體安全性層級：**2 **實體安全性層級：**3
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Corecrypto 模組 v11.1 **作業系統：**watchOS 7 **環境：**Apple 晶片、使用者、軟體 **類型：**軟體 **整體安全性層級：**1
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、軟體 **類型：**軟體 **整體安全性層級：**1

日期	憑證/文件	模組資訊
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (S3、S4、S5、S6) **整體安全性層級：**2
作業系統發佈日期：2020 **驗證日期：**—	**憑證：**尚未通過認證 **文件：** 憑證 安全性規則 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、Secure Key Store、硬體 **類型：**硬體 (S6) **整體安全性層級：**2 **實體安全性層級：**3

FIPS 140-2 認證

下表顯示實驗室目前正在測試且已經過測試符合 FIPS 140-2 的加密編譯模組。

日期	憑證/文件	模組資訊
作業系統發佈日期：2019 **驗證日期：**—	**憑證：**3856 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v10.0 **作業系統：**watchOS 6 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**—	**憑證：**3855 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2019 **驗證日期：**2021/2/5	**憑證：**3811 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v10.0 **作業系統：**與 watchOS 6 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2018 **驗證日期：**2019/4/23	**憑證：**3438 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2018 **驗證日期：**2019/4/11	**憑證：**3433 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v9.0 **作業系統：**watchOS 5 **類型：**軟體 **安全性層級：**1

日期	憑證/文件	模組資訊
作業系統發佈日期：2018 **驗證日期：**2019/9/10	**憑證：**3523 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v9.0 **作業系統：**與 watchOS 5 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2
作業系統發佈日期：2017 **驗證日期：**2018/3/9、2018/5/22、2018/7/6	**憑證：**3148 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**ARM 適用的 Apple Corecrypto 使用者模組 v8.0 **作業系統：**watchOS 4 **類型：**軟體 **安全性層級：**1
作業系統發佈日期：2017 **驗證日期：**2018/3/9、2018/5/17、2018/7/3	**憑證：**3147 **文件：** 憑證 安全性規則 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：**軟體 **安全性層級：**1
作業系統發佈日期：2017 **驗證日期：**2019/9/10	**憑證：**3223 **文件：** 憑證 安全性規則 Crypto Officer 指引	**標題：**Apple Secure Key Store 加密編譯模組 v1.0 **作業系統：**與 watchOS 4 一起發佈的 sepOS **類型：**硬體 **安全性層級：**2

軟體安全性認證

Apple 軟體安全性認證概覽

Apple 為 sepOS 和 T2 韌體維護聯邦資訊處理標準 (FIPS) 140-2/-3 符合性驗證憑證以及其他認證。Apple 從**認證基本要件**開始著手，這些基本要件可在適用情況下跨多個平台廣泛應用。其中一個基本要件就是 Corecrypto 的驗證，其用於 Apple 所開發作業系統內的軟硬體加密編譯密模組開發。第二個基本要件是安全隔離區 (內嵌在許多 Apple 裝置內) 的認證。第三個則是 Secure Element 的認證，應用於配備 Touch ID 的 Apple 裝置和配備 Face ID 的裝置。這些硬體認證基本要件為更廣泛的平台安全性認證形成了基礎。

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，用來當作 IT 產品安全性評估的基礎。

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，相互承認受 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安全性標準，以明確可靠地評估資訊科技產品的安全性功能。「共同準則認證」會對產品能否符合安全性標準進行獨立評估，以讓客戶提升對資訊科技產品安全性的信心，進而根據充足的資訊作出決策。

透過 CCRA，各會員國家已同意抱持相同的信心度，承認該資訊技術產品認證。認證之前需要進行的評估相當廣，包括：

- 保護剖繪 (PP)
- 安全性目標 (ST)
- 安全性功能要求 (SFR)
- 安全性保障要求 (SAR)
- 評估保證等級 (EAL)

「保護剖繪」(PP) 是一種明定各項安全性需求的文件，適用於特定的裝置型態分類 (例如「行動性」)，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，皆只須取得單一認證，並得到任何 CCRA 簽署者的認可。

安全性目標 (ST) 定義了認證 IT 產品時將評估的**內容**。ST 會被轉換為更具體的**安全性功能要求 (SFR)**，用於更詳細地評估 ST。

共同準則 (CC) 還包括**安全性保障要求**。一種常見的認可指標是**評估保證等級 (EAL)**。EAL 會與頻繁出現的 SAR 集群組在一起，可以在 PP 和 ST 中加以指定，以支援可比較性。

許多舊版 PP 已封存，並即將由專為特定解決方案和環境所制訂的針對式 PP 取代。為齊力確保所有 CCRA 會員之間能持續相互認可，國際技術社群 (iTC) 已經成立，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)。相關的利害關係人將繼續開發以 CCRA 以外之使用者群組和相互認可協議為對象的 PP。

從 2015 年初開始，Apple 便開始依據更新的 CCRA（包含特定 cPP）致力取得認證。此後，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 提供的安全性保障。

Apple 在專門進行行動安全技術評估的技術社群中扮演著積極角色，這些社群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，其他憑證也已核發，以證明部分市場的特定安全要求。

Apple App 的安全性認證

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 的安全性認證。這些評估基於 Apple 已取得的硬體和作業系統認證。

在 2018 年，Apple 對於在 iOS 11 上執行的重要應用程式啟動了應用程式安全性評估，對象為 Safari 瀏覽器和「聯絡人」App。Apple 繼續對在 iOS 12、iOS 13 和 iPadOS 13.1 上執行的 App 進行評估。在 2021 年為 App 將涵蓋範圍擴展至 macOS 11。

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。如需更多資訊，請參閱：iOS 的安全性認證、iPadOS 的安全性認證與 macOS 的安全性認證。

共同準則（CC）認證狀態

由 NIAP 運作的 U.S. 架構維護著一份評估產品列表，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」（或同等狀態）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）下相互認可的認證。共同準則入口網站可以將產品保留在認證產品列表中 5 年，記錄則會由共同準則入口網站保留以備存檔認證。

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	架構 ID/文件	標題/保護剖繪
作業系統：macOS 11 Big Sur **認證日期**：—	**架構 ID**：尚未通過認證 **文件**： 憑證 安全性目標 指引 驗證報告 保證作業報告	**標題**：macOS 11 Big Sur：聯絡人 **保護剖繪**：應用程式軟體的 PP、網頁瀏覽器的 EP
作業系統：macOS 11 Big Sur **認證日期**：—	**架構 ID**：尚未通過認證 **文件**： 憑證 安全性目標 指引 驗證報告 保證作業報告	**標題**：macOS 11 Big Sur：Safari **保護剖繪**：應用程式軟體的 PP、網頁瀏覽器的 EP
作業系統：iOS 14、iPadOS 14 **認證日期**：2021/8/20	**架構 ID**：11191 **文件**： 憑證 安全性目標 指引 驗證報告 保證作業報告	**標題**：Apple iOS 14 和 iPadOS 14：聯絡人 **保護剖繪**：應用程式軟體的 PP、網頁瀏覽器的 EP
作業系統：iOS 14、iPadOS 14 **認證日期**：—	**架構 ID**：11192 **文件**： 憑證 安全性目標 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**：應用程式軟體的 PP、網頁瀏覽器的 EP
作業系統：iOS 13、iPadOS 13 **認證日期**：2020/6/5	**架構 ID**：11060 **文件**： 憑證 安全性目標 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**：應用程式軟體的 PP、網頁瀏覽器的 EP

作業系統/認證日期	架構 ID/文件	標題/保護剖繪
作業系統：iOS 13、iPadOS 13 **認證日期：**2020/6/5	**架構 ID：**11050 **文件：** 憑證 安全性目標 指引 驗證報告 保證作業報告	**標題：**Apple iOS 13 和 iPadOS 13：聯絡人 **保護剖繪：**應用程式軟體的 PP

Apple App 的已封存共同準則認證

作業系統/認證日期	架構 ID/文件	標題/保護剖繪
作業系統：iOS 12 **認證日期：**2019/6/12	**架構 ID：**10960 **文件：** 安全性目標 指引	**標題：**iOS 12 Safari **保護剖繪：**應用程式軟體的 PP、網頁瀏覽器的 EP
作業系統：iOS 12 **認證日期：**2019/2/28	**架構 ID：**10961 **文件：** 安全性目標 指引	**標題：**iOS 12 聯絡人 **保護剖繪：**應用程式軟體的 PP
作業系統：iOS 11 **認證日期：**2018/11/9	**架構 ID：**10916 **文件：** 安全性目標 指引	**標題：**iOS 11 Safari **保護剖繪：**應用程式軟體的 PP、網頁瀏覽器的 EP
作業系統：iOS 11 **認證日期：**2018/9/13	**架構 ID：**10915 **文件：** 安全性目標 指引	**標題：**iOS 11 聯絡人 **保護剖繪：**應用程式軟體的 PP

Apple Internet 服務的安全性認證

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。這些認證針對範圍內系統的 Apple 資訊安全和隱私權作法，為客戶提供了獨立證明。

ISO/IEC 27001 和 ISO/IEC 27018 是國際標準化組織 (ISO) 所發佈之「資訊安全管理系統」(ISMS) 標準系列的一部分。作為Apple ISMS 的一部分，所有附錄 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「資訊安全管理系統」標準，規定了建立、導入、維護和持續改善組織的「資訊安全管理系統」的相關要求。ISO/IEC 27001 標準包括 Apple ISO/IEC 認證所涵蓋的以下安全性領域：

- 資訊安全性規則
- 資訊安全的組織
- 資產管理
- 人力資源安全性
- 物理和環境安全性
- 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
- 資訊安全性事件管理
- 業務連續性管理
- 合規

ISO/IEC 27018

ISO/IEC 27018 是在公有雲環境中保護個人身分資訊（PII）的實行準則。ISO/IEC 27018 標準包括 Apple ISO/IEC 認證所涵蓋的以下安全性領域：

- 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、保留和揭露限制
- 準確性和品質
- 公開、透明和注意
- 個別參與和存取
- 問責
- 資訊安全性
- 隱私合規

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 Business Chat
- Apple Business Manager
- Apple 推播通知服務（APNs）
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iWork 服務
- 管理式 Apple ID
- 課業
- Siri

認證

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

若要檢視 Apple 的認證，請前往英國標準學會 (British Standards Institution，BSI) 網站上的證書與客戶名錄搜尋，在 Company (公司) 搜尋欄位中輸入 Apple，按一下 Search (搜尋) 按鈕，然後選取搜尋結果來檢視證書。

【注意】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訊非經推薦或背書。對於第三方網站或產品的選項、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訊。

macOS 安全性合規專案

macOS 安全性合規專案 (mSCP) 是一項開放原始碼作業，旨在提供程式設計方式以產生安全性指引。這是一項由國家標準技術研究院 (NIST)、美國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 安全人員聯合參與的專案。此專案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專案支援的任何安全性指南。此外，此專案可以用作資源，利用經過測試及驗證的基元動作 (配置設定) 資料庫以輕鬆建立技術安全性控制的自訂安全性基準。此專案會根據所使用的基準輸出自訂文件、指令碼、設定描述檔，以及稽核檢查表。

mSCP 可以產生要與管理和安全工具結合使用的輸出內容，以達成合規性。此專案中的配置設定支援以下指引準則：

組織	支援的準則
國家標準技術研究院 (NIST) 特殊發佈 (SP) 800-53，建議聯邦資訊系統與組織使用的安全控制，修訂版 5	800-53 高、800-53 中、800-53 低
國家標準技術研究院 (NIST) 特殊發佈 (SP) 800-171，保護非聯邦系統與組織中的受管非機密資訊，修訂版 2	800-171
國防通訊局 (DISA) macOS 11 STIG，Apple macOS 11 安全性技術實施指南	STIG
國家安全系統委員會 (CNSSI) 1253，國家安全系統的安全性分類和控制選擇	1253

其他資訊：

- 此處提供的基準可用於檢閱此專案中的所有規則。
- 若要進一步瞭解此專案與使用途，請參閱 macOS 安全性合規專案 wiki。
- 若要設定此專案以使用，請參閱：瞭解 macOS 安全性合規專案第一部分和瞭解 macOS 安全性合規專案第二部分。
- 若您對支援此專案的開發感興趣，請參閱參與者指引。

文件版本記錄

日期	摘要
2021年10月27日	更新主題： • 安全隔離區處理器的安全性認證 • iOS 的安全性認證 • macOS 的安全性認證
2021 年 8 月 17 日	更新主題： • 安全隔離區處理器的安全性認證 • Apple T2 安全晶片的安全性認證 • iOS 的安全性認證 • iPadOS 的安全性認證 • macOS 的安全性認證 • tvOS 的安全性認證 • watchOS 的安全性認證 • Apple App 的安全性認證 • 安全性認證 • macOS 安全性合規專案
2021 年 4 月 26 日	新增主題： • macOS 安全性合規專案 更新主題： • Apple T2 安全晶片的安全性認證：新 FIPS 140-2 認證，3811 • 安全隔離區處理器的安全性認證：新 FIPS 140-2 認證，3811 和其他認證的新表格。 • iOS 的安全性認證：新 FIPS 140-2 認證，3811、iOS 14 架構 ID 11146（評估中） • iPadOS 的安全性認證：新 FIPS 140-2 認證，3811、iPadOS 14 架構 ID 11147（評估中） • macOS 的安全性認證：新 FIPS 140-2 認證，3811。 • tvOS 的安全性認證：新 FIPS 140-2 認證，3811。 • watchOS 的安全性認證：新 FIPS 140-2 認證，3811。 • Apple App 的安全性認證：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畫（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 提供加密編譯功能的硬體、軟體和/或韌體，必須符合規定的加密編譯模組標準，並滿足其要求。

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

共同準則（CC） 此套標準用來建立 IT 安全性評估的一般概念和原則，並指定一般性的評估模型。它採用標準化的語言列出各種型別的安全性要求。

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」。

安全性目標（ST） 指明特定產品的安全性問題和安全性要求的文件。

安全性層級（SL） ISO/IEC 19790 中定義的四個整體安全性層級（1-4），用於描述適用的安全性要求集。層級 4 是最嚴格的。

安全隔離區處理器（SEP） 建構於系統單晶片（SoC）內的副處理器。

行動裝置管理（MDM） 讓使用者可遠端管理已註冊裝置的服務。裝置註冊後，使用者就可以透過網路使用 MDM 服務來在裝置上配置設定及執行其他任務，無需使用者互動。

完整磁碟加密（FDE） 對儲存卷宗上的所有資料所進行的加密程序。

系統單晶片（SoC） 一種積體電路（IC），可將多重元件整合到單片晶片上。

保護剖繪（PP） 指明特定產品類別的安全性問題和安全性要求的文件。

國家資訊保證合作組織（NIAP） 美國政府的組織，負責在美國導入共同準則並管理 NIAP 共同準則評估和驗證計畫（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）的主辦下，負責制定「保護剖繪」或合作「保護剖繪」的小組。

資訊安全管理系統（ISMS） 一套資訊安全性規則和程序，用於管理安全程式的界線，這些程序的目的是在資訊和/或系統的整個生命週期中，可系統性地管理資訊安全性，藉此保護資訊和系統的範疇。

資深官員小組資訊系統安全性（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） 描述安全性控制的文件，這些控制會在 ISMS 範疇內導入以支援 ISMS/IEC 27001 認證。

檢測中的模組（MIP） 目前由 CMVP 驗證程序中的加密編譯模組的加密編譯模組驗證計畫（CMVP）所維護的列表。

聯邦資訊處理標準（FIPS） 由「國家標準技術研究院」在下列時機所制定的發表內容：在法規要求下、或是在聯邦政府對網路安全性提出有力要求時，或兩者同時發生時。

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

Apple Business Manager 是一個易於使用的入口網站，能提供快速、簡化的方式讓 IT 管理者為組織部署直接購自 Apple 或與 Apple 合作之授權經銷商或電信業者的 Apple 裝置。他們可以在其行動裝置管理（MDM）解決方案中自動註冊裝置，使用者無須先取得裝置並實際在裝置上進行操作或準備。

Apple School Manager 是一個易於使用的入口網站，能提供快速、簡化的方式讓 IT 管理者為組織部署直接購自 Apple 或與 Apple 合作之授權經銷商或電信業者的 Apple 裝置。他們可以在其行動裝置管理（MDM）解決方案中自動註冊裝置，使用者無須先取得裝置並實際在裝置上進行操作或準備。

Corecrypto 提供低層級加密編譯原始語言導入的程式庫。請注意，Corecrypto 不會直接為開發人員提供程式設計介面，而是透過提供給開發人員的 API 來使用。Corecrypto 原始碼可公開取得，以驗證其安全性特點和運作正確性。

IPsec VPN 用戶端 「保護剖繪」中的用戶端，用來在實體或虛擬主機平台以及遠端位置之間提供安全的 IPsec 連線。

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，特定 Intel 架構 Mac 電腦中所配備的 Apple 安全晶片。

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

TA028-00499-B