



# Apple 平台保安

2022 年 5 月



# 目錄

<b>Apple 平台保安</b>	<b>5</b>
Apple 平台保安簡介	5
<b>硬件保安與生物特徵識別</b>	<b>7</b>
硬件保安概覽	7
Apple SoC 保安	8
安全隔離區	9
Face ID 和 Touch ID	17
硬件咪高風斷線功能	23
以剩餘電量使用特快卡	23
<b>系統保安</b>	<b>24</b>
系統保安概覽	24
安全啟動	25
iOS、iPadOS 和 macOS 的簽署系統卷宗保安	42
保安軟件更新	43
作業系統完整性	44
其他 macOS 系統保安功能	46
watchOS 的系統保安	54
亂數產生	57
Apple 安全研究裝置	58
<b>加密與資料保護</b>	<b>59</b>
加密與資料保護概覽	59
密碼	60
資料保護	62
檔案保險箱	72
Apple 如何保護用戶的個人資料	75
電子簽署與加密	77

<b>App 保安</b>	<b>78</b>
App 保安概覽	78
iOS 和 iPadOS 中的 App 保安	79
macOS 中的 App 保安	83
「備忘錄」App 的安全功能	86
「捷徑」App 的安全功能	86
<b>服務保安</b>	<b>87</b>
服務保安概覽	87
Apple ID 與管理式 Apple ID	87
iCloud	89
密碼與密碼管理	96
Apple Pay	103
使用 Apple「銀包」	113
iMessage	120
Apple Messages for Business 保安	122
FaceTime 保安	122
尋找	123
接續互通	125
<b>網絡保安</b>	<b>128</b>
網絡保安概覽	128
TLS 保安	128
IPv6 保安	129
虛擬專用網絡 (VPN) 保安	130
Wi-Fi 保安	130
藍牙保安	133
iOS 的超寬頻保安	134
單一登入	134
AirDrop 保安	135
iPhone 和 iPad 的 Wi-Fi 密碼共享保安	136
macOS 的防火牆保安	136
<b>開發者套件保安</b>	<b>137</b>
開發者套件保安概覽	137
HomeKit 保安	137
iOS、iPadOS 和 watchOS 的 SiriKit 保安	141
macOS 的 DriverKit 保安	141
iOS 和 iPadOS 的 ReplayKit 保安	142
iOS 和 iPadOS 的 ARKit 保安	143

<b>安全裝置管理</b>	<b>144</b>
安全裝置管理概覽	144
iPhone 和 iPad 的配對模式保安	144
流動裝置管理	145
Apple Configurator 保安	150
「螢幕使用時間」保安	150
<b>詞彙表</b>	<b>152</b>
<b>文件版本記錄</b>	<b>155</b>
文件版本記錄	155
<b>版權</b>	<b>162</b>

# Apple 平台保安

## Apple 平台保安簡介

Apple 將保安設計融入平台的核心中。以打造全世界最先進之流動作業系統所累積的豐富經驗，Apple 製作出可因應流動裝置、手錶、桌面電腦和家居獨特要求的安全架構。

每款 Apple 裝置都結合了**硬件、軟件和服務**，設計理念皆旨在互相配合，達至高度保安和透明的用戶體驗，以服務保障個人資料安全的最終目標。例如 Apple 設計的晶片與安全硬件具備重要的保安功能；軟件保護的目的是確保作業系統和第三方 App 獲得防護；服務提供安全機制和即時軟件更新，支援受保護的 App 生態系統，並推動安全的通訊及付款方式。因此，Apple 裝置不僅可保護裝置和其資料，也保護着整個生態系統，包含用戶在本機、網絡上和透過重要互聯網服務執行的任何操作。

我們的產品設計理念除了簡單、直覺式和實用性，也重視安全方面。重要的保安功能不會因意外而停用，例如以硬件為基礎的裝置加密。其他功能（如 Face ID 和 Touch ID）則讓裝置的保護更簡單且直覺，提升用戶體驗。而且因為許多保安功能預設便已啟用，因此用戶或 IT 部門無須進行繁複的設定。

本說明文件將詳細介紹 Apple 平台如何運用各種保安技術與功能。其亦協助機構在其本身的政策和程序中結合 Apple 平台保安技術與功能，以滿足特定的保安需求。

內容主要分為以下幾個主題：

- **硬件保安與生物特徵識別**：組成 Apple 裝置保安基礎的晶片與硬件，包括 Apple 晶片、「安全隔離區」、加密編譯引擎、Face ID 和 Touch ID
- **系統保安**：整合式硬件和軟件功能，可確保安全啟動、更新和 Apple 作業系統持續運作
- **加密與資料保護**：如裝置遺失或遭竊，或有未經授權的人員或程序嘗試使用或修改裝置時，對用戶資料進行保護的架構和設計
- **App 保安**：各種提供安全 App 生態系統的軟件和服務，讓 App 安全運作而無損平台完整性
- **服務保安**：Apple 提供的各種服務，用於識別、密碼管理、付款、通訊、和尋找遺失的裝置
- **網絡保安**：對傳輸中的資料提供安全認證和資料加密的業界標準網絡通訊協定
- **開發者套件保安**：用於以安全且隱密的方式管理家庭與健康資料，而且可將 Apple 裝置與服務功能延伸至第三方 App 的一套框架「套件」
- **安全裝置管理**：允許 Apple 裝置管理，協助防止在未經授權的情況下使用裝置，以及在裝置遺失或遭竊時可進行遙距清除的方式

## 對保安的承諾

Apple 致力以最先進的私隱與保安技術保護個人資料，以保障客戶的安全，並採用全方位方式來保護企業環境中的公司資料。Apple 透過提供「Apple 保安獎金」(Apple Security Bounty)，獎勵研究人員為找出漏洞所付出的努力。計劃和獎金類別的詳細資料，可於下列網站取得：<https://developer.apple.com/security-bounty/>。

我們擁有一組專業的保安團隊，專門為所有 Apple 產品提供支援。團隊會為開發階段和已發佈的產品進行保安審核和測試。Apple 團隊亦提供保安工具和訓練，並積極監控新保安問題的威脅及報告。Apple 為「國際網絡安全應急論壇組織」(Forum of Incident Response and Security Teams, FIRST) 的成員。

Apple 不斷求進，在保障安全和私隱上持續努力突破可能的極限。Apple 在整個產品系列使用自製晶片(從 Apple Watch 到 iPhone 和 iPad，再到 Mac 中的 T2 保安晶片和 Apple 晶片)，其不僅支援高效計算，也提供保安。例如，Apple 晶片提供了安全啟動、Face ID 和 Touch ID 以及「資料保護」的基礎。此外，裝置上由 Apple 晶片驅動的保安功能(例如「核心完整保護」、「指標認證碼」和「快速權限取用限制」)，有助阻止常見的網絡攻擊類型。因此，即使攻擊者代碼以某種方式執行，也能大幅地減少其可能造成的損害。

為了充分利用我們平台內建的強大保安功能，我們建議機構審核其 IT 部門和保安規則，以確保可充分使用到這些平台所提供的多重保安技術。

如要深入了解如何向 Apple 回報問題以及訂閱保安通知的相關資料，請參閱：[回報保安或私隱漏洞](#)。

**Apple 相信私隱是基本的人權，並提供許多內置控制項目和選項，讓用戶決定 App 可以如何使用其資料、於何時使用，以及可以使用哪些資料。如需深入了解 Apple 對於私隱的處理方式、Apple 裝置上的私隱控制以及 Apple 私隱政策，請參閱：<https://www.apple.com/hk/privacy>。**

**附註：**除非另有說明，否則本文件適用於下列作業系統版本：iOS 15.4、iPadOS 15.4、macOS 12.3、tvOS 15.4 和 watchOS 8.5。

# 硬件保安與生物特徵識別

## 硬件保安概覽

軟件的保安，必須建基於具有內置保安的硬件上。這正是執行 iOS、iPadOS、macOS、tvOS 和 watchOS 的 Apple 裝置配備採用安全功能設計的晶片之原因。這些功能包含支援系統安全功能的 CPU，以及專用於安全功能的額外晶片。首重保安的硬件以支援有限的離散定義功能為原則，以便將攻擊面縮到最小。這類元件包含 Boot ROM（負責組成用於安全啟動的硬件信任根）、專用 AES 引擎（用於確保有效且安全的加密與解密）以及「安全隔離區」。「安全隔離區」是單晶片系統（SoC），所有近期推出的 iPhone、iPad、Apple Watch、Apple TV 和 HomePod 裝置，以及配備 Apple 晶片和配備 Apple T2 保安晶片的 Mac 上均具有此元件。「安全隔離區」本身遵循與 SoC 相同的設計原則，其中包含自己的離散 Boot ROM 和 AES 引擎。「安全隔離區」也提供了安全產生和儲存加密靜態資料所需密鑰的基礎，且可保護和評估 Face ID 和 Touch ID 的生物識別資料。

儲存空間的加密必須快速而有效，同時無法洩漏用於建立加密密鑰關係的資料（或**密鑰材料**）。AES 硬件引擎可在**檔案寫入或讀取時**執行快速的內嵌式加密與解密，進而解決此問題。「安全隔離區」中的特殊管道可提供必要的密鑰材料給 AES 引擎，而不會向「應用程式處理器」（或 CPU）或整體作業系統洩漏這些資料。這可協助確保 Apple 「資料保護」和「檔案保險箱」技術確實保護用戶的檔案，且無需洩露長效加密密鑰。

Apple 設計安全啟動來保護最低層級的軟件免受竄改，且開機時只會載入 Apple 所信任的作業系統軟件。安全啟動的起點為無法更改的程式碼 Boot ROM，這些程式碼又稱為「**硬件的信任根**」，在製造 SoC 晶片過程中即寫入完成。在配備 T2 晶片的 Mac 電腦上，macOS 安全啟動的信任以 T2 開始。（T2 晶片和「安全隔離區」也會使用他們的獨立 Boot ROM 執行自己的安全啟動程序；這與 A 系列和 M1 晶片系列安全啟動完全相同。）

「安全隔離區」也會處理來自 Apple 裝置上的 Face ID 和 Touch ID 感應器的臉部和指紋資料。這會提供安全認證，同時確保用戶生物特徵辨識資料的私隱及安全。在許多情況下，這也讓用戶可享有較複雜的長密碼帶來的保安，以及存取或購物時享有快速認證的便利。

# Apple SoC 保安

如今 Apple 設計的晶片組成了所有 Apple 產品的通用架構，並為 Mac、iPhone、iPad、Apple TV 和 Apple Watch 提供動力。十多年來，Apple 的世界級晶片設計團隊一直在建構和改良 Apple 單晶片系統 (SoC)。成果是專為所有裝置設計的可擴展架構，在保安功能方面處於業界領先地位。此保安功能的共同基礎只有自行設計晶片以配搭其軟件使用的公司才可能提供。

Apple 晶片的設計和製造旨在專門啟用下方詳述的系統保安功能：

功能	A10	A11、S3	A12、S4	A13、S5	A14、A15、S6、S7	M1 系列
核心完整保護	✓	✓	✓	✓	✓	✓
快速權限取用限制		✓	✓	✓	✓	✓
系統協同處理器 完整保護			✓	✓	✓	✓
指標認證碼			✓	✓	✓	✓
頁面保護層		✓	✓	✓	✓	請參閱下方的附註。

**附註：**「頁面保護層」(PPL) 要求平台只執行已簽署且受信任的程式碼；此保安模式不適用 macOS。

Apple 設計的晶片也會專門啟用下方詳述的「資料保護」功能。

功能	A10	A11、S3	A12、S4	A13、S5	A14、A15、S6、S7、M1 系列
密封密鑰保護 (SKP)	✓	✓	✓	✓	✓
RecoveryOS - 所有 資料保護類別均受到 保護	✓	✓	✓	✓	✓
替用 DFU 開機、診斷 和更新：類別 A、B 和 C 資料受到保護			✓	✓	✓

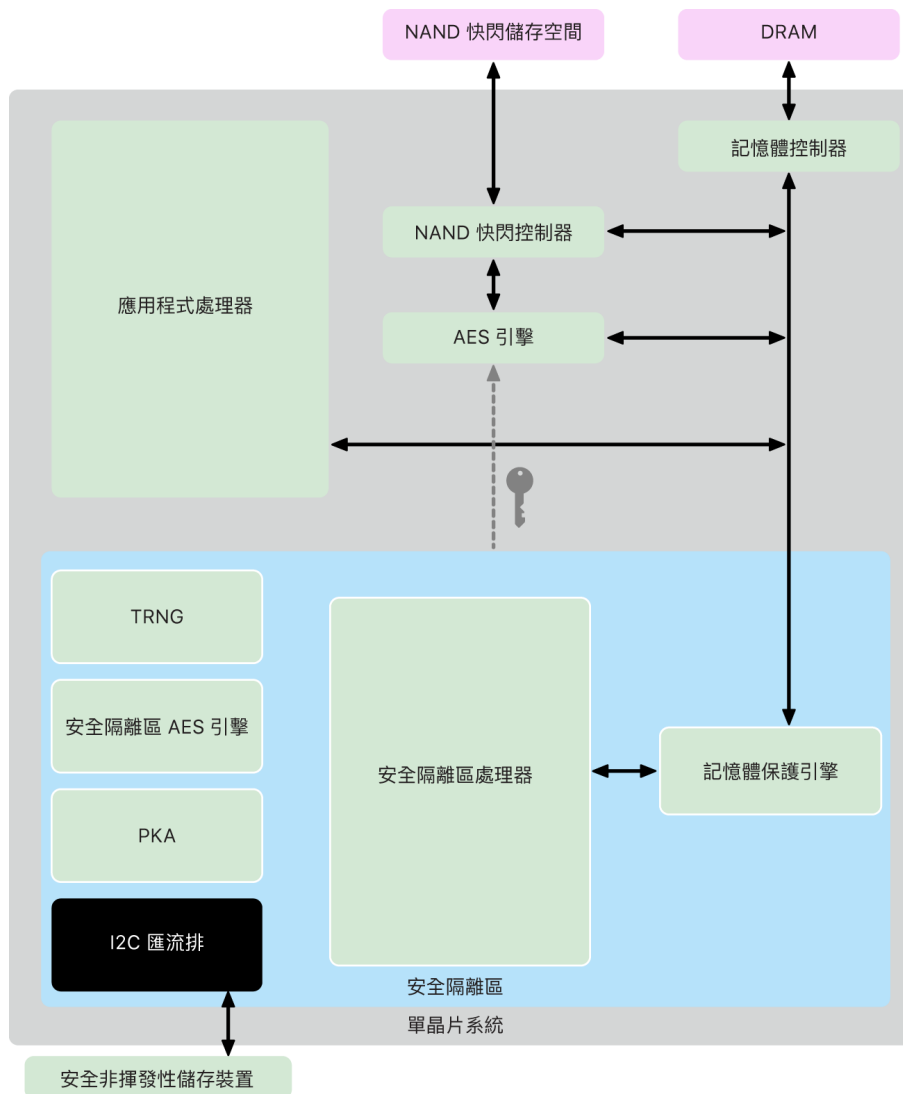


# 安全隔離區

「安全隔離區」是以下最新版本之 iPhone、iPad、iPod touch、Mac、Apple TV、Apple Watch 和 HomePod 的專用安全子系統。

## 概覽

「安全隔離區」是整合在 Apple 單晶片系統 (SoC) 中的專用安全子系統。「安全隔離區」與主要處理器加以隔離，以提供額外的保安，並且即使在「應用程式處理器」核心受到威脅時，也可以確保敏感性用戶資料的安全。其遵循與 SoC 整體相同的設計原則：Boot ROM 用於建立硬件信任根、AES 引擎用於確保有效且安全的加密編譯操作，以及受保護的記憶體。雖然「安全隔離區」不包含儲存空間，但是其具有機制可將資料安全地儲存在外置儲存裝置上 (獨立於「應用程式處理器」和作業系統所使用的 NAND 快閃儲存空間)。



「安全隔離區」是大多數版本 iPhone、iPad、Mac、Apple TV、Apple Watch 和 HomePod 的硬件功能，這些版本為：

- iPhone 5s 或較新型號
- iPad Air 或較新型號
- MacBook Pro 電腦配備觸控欄 (2016 年和 2017 年)，包含 Apple T1 晶片
- 以 Intel 為基礎的 Mac 電腦，包含 Apple T2 保安晶片
- 配備 Apple 晶片的 Mac 電腦
- Apple TV HD 或較新型號
- Apple Watch Series 1 或較新型號
- HomePod 和 HomePod mini

## 安全隔離區處理器

「安全隔離區處理器」為「安全隔離區」提供主要的運算能力。為了提供最強的隔離性，「安全隔離區處理器」專門用於「安全隔離區」。這有助於防止與被攻擊目標軟件共享同一執行核心的惡意軟件從旁進行攻擊。

「安全隔離區處理器」採用 Apple 特製的 L4 microkernel 版本。其設計旨在以較低的時脈高效運行，進而有助於保護其免受時鐘和電源攻擊。自 A11 和 S4 起，「安全隔離區處理器」包含了受記憶體保護的引擎和加密記憶體配搭反重播功能、安全啟動、專用亂數產生器和專屬的 AES 引擎。

## 記憶體保護引擎

「安全隔離區」在裝置 DRAM 記憶體的專用區域內運行。多層保護將「安全隔離區」的受保護記憶體與「應用程式處理器」隔開。

裝置啟動時，「安全隔離區 Boot ROM」會為「記憶體保護引擎」產生隨機的臨時記憶體保護密鑰。每當「安全隔離區」寫入其專用記憶體區域時，「記憶體保護引擎」就會在 Mac XEX (xor-encrypt-xor) 模式下使用 AES 來加密記憶體區塊，並計算該記憶體的密碼型訊息驗證碼 (CMAC) 認證標記。「記憶體保護引擎」將認證標記與加密的記憶體一起儲存。當「安全隔離區」讀取記憶體時，「記憶體保護引擎」便會確認認證標記。如果認證標記相符，則「記憶體保護引擎」將對記憶體區塊進行解密。如果標記不相符，則「記憶體保護引擎」會向「安全隔離區」發出差誤訊號。發生記憶體認證錯誤後，「安全隔離區」會停止接受要求，直到系統重新開機為止。

從 Apple A11 和 S4 SoC 開始，「記憶體保護引擎」為「安全隔離區」記憶體加入了重放保護。為協助防止保安相關重要的資料遭到重播，「記憶體保護引擎」會在認證標記旁邊儲存該記憶體區塊的唯一一次性號碼，稱為**隨機數**。隨機數被用作 CMAC 認證標記的附加調校。所有記憶體區塊的隨機數都使用根植於「安全隔離區」內專用 SRAM 中的完整性樹狀結構進行保護。對於寫入操作，「記憶體保護引擎」將會**更新**隨機數和完整性樹狀結構的每個層級直至 SRAM。對於讀取操作，「記憶體保護引擎」會**驗證**隨機數和完整性樹狀結構的每個層級直至 SRAM。隨機數不相符的處理方式與認證標記不相符的處理方式相似。

在 Apple A14、A15、M1 系列和較新版本 SoC 上，「記憶體保護引擎」支援兩種臨時記憶體保護密鑰。第一種用於「安全隔離區」專用的資料，第二種則用於與「安全神經引擎」共用的資料。

「記憶體保護引擎」對「安全隔離區」直接且透明地運行。「安全隔離區」就像一般未加密的 DRAM 來讀寫記憶體，而「安全隔離區」外部的觀察者只能看到記憶體的加密和認證版本。成果即是強大的記憶體保護，而無須犧牲效能或軟件的複雜度。

## 安全隔離區 Boot ROM

「安全隔離區」包含專用的「安全隔離區 Boot ROM」。類似於「應用程式處理器 Boot ROM」，「安全隔離區 Boot ROM」屬於無法更改的程式碼，用於為「安全隔離區」建立硬件信任根。

系統啟動時，iBoot 會將專用的記憶體區域指定給「安全隔離區」。使用記憶體前，「安全隔離區 Boot ROM」會初始化「記憶體保護引擎」，以提供對「安全隔離區」受保護記憶體的加密保護。

然後，「應用程式處理器」會將 sepOS 映像檔傳送到「安全隔離區 Boot ROM」。將 sepOS 映像檔複製到「安全隔離區」的受保護記憶體後，「安全隔離區 Boot ROM」將會檢查映像檔的加密雜湊值和簽名，以驗證 sepOS 是否已獲得在裝置上執行的授權。如果 sepOS 映像檔已正確簽署以在裝置上執行，則「安全隔離區 Boot ROM」會將控制權轉移到 sepOS。如果簽署無效，則「安全隔離區開機 ROM」的設計會阻止對「安全隔離區」的任何後續使用，直到下一次晶片重置為止。

在 Apple A10 和較新版本的 SoC 上，「安全隔離區 Boot ROM」將 sepOS 的雜湊值鎖定到專用於此用途的註冊器中。「公共密鑰加速器」會將此雜湊值用於作業系統綁定 (OS 綁定) 密鑰。

## 安全隔離區開機監視器

在 Apple A13 和較新版本的 SoC 上，「安全隔離區」包括一個「開機監視器」，其設計用意是確保開機 sepOS 的雜湊值具有更強的完整性。

在系統啟動時，「安全隔離區處理器」的系統協同處理器完整保護 (SCIP) 設定可協助防止「安全隔離區處理器」執行「安全隔離區 Boot ROM」以外的任何程式碼。「開機監視器」可協助防止「安全隔離區」直接修改 SCIP 設定。為了讓載入的 sepOS 可執行，「安全隔離區 Boot ROM」會向「開機監視器」傳送一項要求，其中包含載入之 sepOS 的地址和大小。收到要求後，「開機監視器」將重設「安全隔離區處理器」，對已載入的 sepOS 進行雜湊值處理、更新 SCIP 設定以允許執行已載入的 sepOS，並在新載入的程式碼內開始執行。隨着系統繼續開機，只要有可執行的新程式碼，就會使用相同的程序。每次「開機監視器」都會更新開機程序的執行雜湊值。「開機監視器」也包含執行雜湊值中的重要保安參數。

開機完成後，「開機監視器」將最終確定執行雜湊值，並將其發送到「公共密鑰加速器」以用於 OS 綁定的密鑰。此過程的設計目標是即使「安全隔離區 Boot ROM」中存在漏洞，也無法略過作業系統密鑰的綁定。

## 真隨機數產生器

「真隨機數產生器」(TRNG) 會用來產生安全隨機資料。每當「安全隔離區」產生隨機加密編譯密鑰、隨機密鑰種子或其他熵時，就會使用 TRNG。TRNG 的基礎是使用 CTR\_DRBG (「計數器模式」下以區塊加密為基礎的演算法) 處理後的多個環形振盪器。

## 根加密編譯密鑰

「安全隔離區」包含唯一識別碼 (UID) 根加密編譯密鑰。UID 對每個個別的裝置都是唯一的，並且與裝置上的任何其他識別碼無關。

SoC 於生產時便已植入一個隨機產生的 UID。自 A9 SoC 起，於生產期間「安全隔離區」TRNG 會產生 UID，並使用完全在「安全隔離區」中執行的軟件程序植入其中。這個程序可保護 UID 在生產期間不會在裝置外顯示，因此 Apple 或任何供應商皆無法存取或儲存 UID。

sepOS 會使用 UID 來保護裝置專屬機密資料。UID 允許資料以加密編譯方式與特定裝置綁定。例如，用來保護檔案系統的密鑰階層便包含 UID，因此如將內置 SSD 儲存空間實際從一部裝置移至另一部裝置，檔案則無法存取。其他受保護的裝置專屬機密資料包含 Face ID 或 Touch ID 資料。在 Mac 上，只有與 AES 引擎連結的完全內置儲存空間可獲得這個層級的加密。例如，透過 USB 連接的外部儲存裝置或加到 2019 年 Mac Pro 的 PCIe 式儲存空間都不會由此方式加密。

「安全隔離區」也具有裝備群組 ID (GID)，這對於使用特定 SoC 的所有裝置都是通用的 (例如，所有使用 Apple A15 SoC 的裝置都共享相同的 GID)。

UID 和 GID 無法透過聯合測試工作群組 (JTAG) 或其他除錯介面來使用。

## 安全隔離區 AES 引擎

「安全隔離區 AES 引擎」是一個硬件區塊，用於依據 AES 密碼執行對稱加密編譯。「AES 引擎」的設計用意在於針對使用定時和「靜態功率分析」(SPA) 攻擊阻止資料洩漏。從 A9 SoC 開始，「AES 引擎」也包括對「動態功率分析」(DPA) 攻擊的反制措施。

「AES 引擎」支援硬件和軟件密鑰。硬件密鑰衍生自「安全隔離區」的 UID 或 GID。這些密鑰位於「AES 引擎」中，即使在 sepOS 軟件中也不可見。雖然軟件可以要求使用硬件密鑰進行加密和解密作業，但其無法截取密鑰。

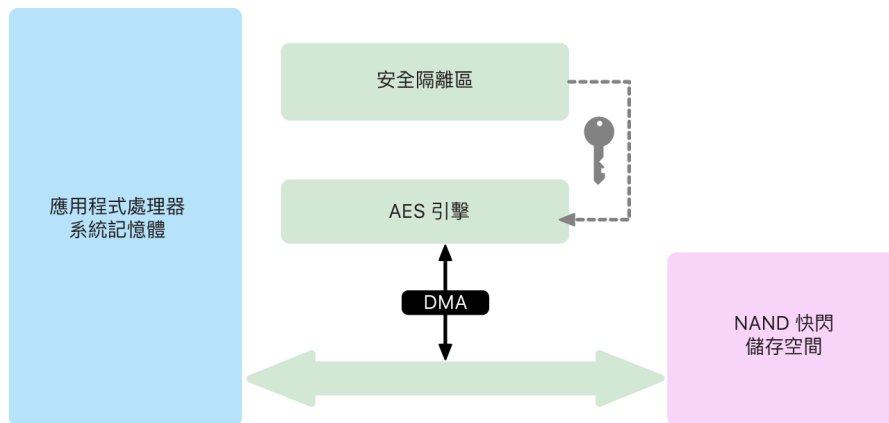
在 Apple A10 和更新的 SoC 上，「AES 引擎」包括可鎖定的種子位元，這些種子位元會讓從 UID 或 GID 衍生的密鑰更多元。這樣就可以根據裝置的操作模式來限制資料的存取。例如，當從裝置韌體更新 (DFU) 模式開機時，可鎖定的種子位元便會用於拒絕存取受密碼保護的資料。如需更多資料，請前往：[密碼](#)。

## AES 引擎

每部具有「安全隔離區」的 Apple 裝置都配備專用的 AES256 加密編譯引擎（「AES 引擎」），其內置於 NAND（非揮發性）快閃儲存空間與主系統記憶體間的「直接記憶體存取」（DMA）路徑中，可讓檔案加密具備高度效率。在 A9 或較新版本 A 系列處理器上，快閃儲存子系統位於獨立的匯流排上，此匯流排擁有的存取權有限，只能存取包含用戶資料的記憶體（透過 DMA 加密編譯引擎）。

在開機時，sepOS 會使用 TRNG 產生臨時包裝密鑰。「安全隔離區」使用專用線路將此密鑰傳輸到「AES 引擎」，此設計是防止「安全隔離區」以外的任何軟件對其進行存取。sepOS 可以使用臨時包裝密鑰來包裝檔案密鑰，以供「應用程式處理器」檔案系統驅動程式使用。當檔案系統驅動程式讀取或寫入檔案時，它會將包裝的密鑰傳送到「AES 引擎」，藉此解開密鑰。「AES 引擎」絕對不會向軟件洩漏解封的密鑰。

**附註：**「AES 引擎」是獨立於「安全隔離區」和「安全隔離區 AES 引擎」的元件，但是其操作與「安全隔離區」環環相扣，如下所示。



## 公共密鑰加速器

「公共密鑰加速器」（PKA）是一個硬件區塊，用於執行非對稱加密作業。PKA 支援 RSA 和 ECC（橢圓曲線加密技術）簽名和加密演算法。PKA 的用意在於針對 SPA 和 DPA 之類的定時和從旁攻擊阻止資料洩漏。

PKA 支援軟件和硬件密鑰。硬件密鑰衍生自「安全隔離區」的 UID 或 GID。這些密鑰位於 PKA 中，即使在 sepOS 軟件中也不可見。

從 A13 SoC 開始，已使用正式的驗證技術證明 PKA 的加密實在數理上是正確的。

在 Apple A10 和更新版 SoC 上，PKA 支援與 OS 綁定的密鑰，也稱為「密封密鑰保護」（SKP）。這些密鑰是使用裝置的 UID 和裝置上執行的 sepOS 雜湊值的組合產生的。雜湊值由「安全隔離區 Boot ROM」或 Apple A13 和較新版本的 SoC 上的「安全隔離區開機監視器」提供。這些密鑰也用於在向某些 Apple 服務送出要求時驗證 sepOS 版本，以及用來在沒有用戶授權的狀態下進行重要系統變更時，協助防止密鑰材料遭存取，藉此改善受密碼保護的資料之保安。

## 安全非揮發性儲存裝置

「安全隔離區」配備了專用的安全非揮發性儲存裝置。安全非揮發性儲存裝置使用專用 I2C 匯流排連接到「安全隔離區」，因此只能由「安全隔離區」對其進行存取。所有用戶資料加密密鑰均基於儲存在「安全隔離區」非揮發性儲存裝置中的熵。

在配備 A12、S4 和較新版本 SoC 的裝置上，「安全隔離區」會與「安全儲存元件」配對，以用於熵儲存空間。「安全儲存元件」本身的設計包含無法更改的 ROM 程式碼、硬件亂數產生器、依設備的唯一加密密鑰、加密編譯引擎，以及物理篡改偵測。「安全隔離區」和「安全儲存元件」使用經過加密和認證的協定進行通訊，以提供對熵的唯一存取。

最早於 2020 年秋季發布的裝置或更新版本均配備了第二代「安全儲存元件」。第二代「安全儲存元件」加入了計數器密碼箱。每個計數器密碼箱都儲存一個 128 位元鹽值、一個 128 位元密碼驗證器、一個 8 位元計數器和一個 8 位元最大嘗試值。對計數器密碼箱的存取會透過經過加密和認證的協定進行。

計數器密碼箱含有解鎖受密碼保護用戶資料所需的熵。如要存取這些用戶資料，配對的「安全隔離區」必須從用戶的密碼和「安全隔離區」的 UID 衍生正確的密碼熵值。從配對的「安全隔離區」以外的其他來源所傳送的解鎖嘗試，無法得知用戶的密碼。如果次數超過了密碼嘗試限制（例如，在 iPhone 上嘗試 10 次），「安全儲存元件」會完全清除受密碼保護的資料。

為了建立計數器密碼箱，「安全隔離區」會向「安全儲存元件」傳送密碼熵值和最大嘗試值。「安全儲存元件」會使用其亂數產生器來產生鹽值。接着會衍生出密碼驗證器值和所提供密碼熵的密碼箱熵值。「安全儲存元件」的唯一加密密鑰以及鹽值。「安全儲存元件」使用計數 0、所提供的最大嘗試值、衍生的密碼驗證器值和鹽值來初始化計數器密碼箱。「安全儲存元件」接着會將產生的密碼箱熵值傳回到「安全隔離區」。

之後如要從計數器密碼箱中取回密碼箱熵值，「安全隔離區」會向「安全儲存元件」傳送密碼熵。「安全儲存元件」會先遞增密碼箱的計數器。如果遞增的計數器超過最大嘗試值，則「安全儲存元件」會完全清除計數器密碼箱。如果計數尚未達到嘗試次數最大值，「安全儲存元件」會透過用於建立計數器密碼箱的同一組演算法，嘗試衍生密碼驗證器值和密碼箱熵值。如果衍生的密碼驗證器值與儲存的密碼驗證器值相符，「安全儲存元件」就會將密碼箱熵值傳回「安全隔離區」，並將計數器重置為 0。

用來存取受密碼保護的資料的密鑰根植於儲存在計數器密碼箱內的熵。如需更多資料，請前往：[「資料保護」概覽](#)。

安全非揮發性儲存裝置可用於「安全隔離區」中的所有反重播服務。「安全隔離區」上的反重播服務用於在發生標記反重播邊界的情形時撤銷資料，包括但不限於以下情形：

- 密碼更改
- 啟用或停用 Face ID 或 Touch ID
- 加入或移除 Face ID 容貌或 Touch ID 指紋
- Face ID 或 Touch ID 重設
- 加入或移除 Apple Pay 卡片
- 清除所有內容和設定

在沒有採用「安全儲存元件」的架構上，會利用 EEPROM（電子清除式可程式化唯讀記憶體）來為「安全隔離區」提供安全儲存服務。如同「安全儲存元件」，EEPROM 只能透過「安全隔離區」連接和存取，不過 EEPROM 中不包含專用的硬件保安功能，也不保證對熵的專有存取權限（除了其實體連接特性之外），也不提供計數器密碼箱功能。

## 安全神經引擎

在配備 Face ID 的裝置上，「安全神經引擎」將 2D 影像和深度圖轉換為用戶容貌的數學表徵。

在 A11 至 A13 SoC 上，「安全神經引擎」已整合到「安全隔離區」中。「安全神經引擎」使用直接記憶體存取 (DMA) 來取得高效能。在 sepOS 核心控制下的輸入輸出記憶體管理單元 (IOMMU) 限制了對授權記憶體區域的直接存取。

從 A14 和 M1 系列開始，「安全神經引擎」在「應用程式處理器」的「神經引擎」中作為安全模式進行運作。專用的硬件保安控制器在「應用程式處理器」和「安全隔離區」任務之間切換，在每次轉換時重設「神經引擎」狀態，以確保 Face ID 的資料安全。專用引擎會進行記憶體加密、認證和存取控制，同時使用單獨的加密密鑰和記憶體範圍將「安全神經引擎」限制在授權的記憶體區域中。

## 電源和時鐘監視器

所有電子裝置均設計為在有限的電壓和頻率範圍內操作。超出此範圍進行操作時，電子裝置可能會發生故障，然後可能會繞過安全控制。為協助確保電壓和頻率保持在安全範圍內，「安全隔離區」設計有監控電路。這些監控電路的作業範圍要比「安全隔離區」的其餘部份大得多。如果監視器偵測到非法的作業點，則「安全隔離區」中的時鐘會自動停止並且直到下一次 SoC 重設才會重新起動。

## 安全隔離區功能摘要

附註：2020 年秋季首次發布的 A12、A13、S4 和 S5 產品配備第二代「安全儲存元件」，而以這些 SoC 為基礎的較早產品則配備第一代「安全儲存元件」。

SoC	記憶體保護引擎	安全儲存	AES 引擎	PKA
A8	加密和認證	EEPROM	是	否
A9	加密和認證	EEPROM	DPA 保護	是
A10	加密和認證	EEPROM	DPA 保護和可鎖定的種子位元	作業系統鎖定的密鑰
A11	加密、認證和重放預防	EEPROM	DPA 保護和可鎖定的種子位元	作業系統鎖定的密鑰
A12 (2020 年秋季之前發布的 Apple 裝置)	加密、認證和重放預防	安全儲存元件 (第一代)	DPA 保護和可鎖定的種子位元	作業系統鎖定的密鑰
A12 (2020 年秋季之後發布的 Apple 裝置)	加密、認證和重放預防	安全儲存元件 (第二代)	DPA 保護和可鎖定的種子位元	作業系統鎖定的密鑰
A13 (2020 年秋季之前發布的 Apple 裝置)	加密、認證和重放預防	安全儲存元件 (第一代)	DPA 保護和可鎖定的種子位元	作業系統綁定的密鑰和「開機監視器」
A13 (2020 年秋季之後發布的 Apple 裝置)	加密、認證和重放預防	安全儲存元件 (第二代)	DPA 保護和可鎖定的種子位元	作業系統綁定的密鑰和「開機監視器」
A14、A15	加密、認證和重放預防	安全儲存元件 (第二代)	DPA 保護和可鎖定的種子位元	作業系統綁定的密鑰和「開機監視器」
S3	加密和認證	EEPROM	DPA 保護和可鎖定的種子位元	是
S4	加密、認證和重放預防	安全儲存元件 (第一代)	DPA 保護和可鎖定的種子位元	作業系統鎖定的密鑰
S5 (2020 年秋季之前發布的 Apple 裝置)	加密、認證和重放預防	安全儲存元件 (第一代)	DPA 保護和可鎖定的種子位元	作業系統鎖定的密鑰

SoC	記憶體保護引擎	安全儲存	AES 引擎	PKA
S5 (2020 年秋季之後發佈的 Apple 裝置)	加密、認證和重放預防	安全儲存元件 (第二代)	DPA 保護和可鎖定的種子位元	作業系統鎖定的密鑰
S6、S7	加密、認證和重放預防	安全儲存元件 (第二代)	DPA 保護和可鎖定的種子位元	作業系統鎖定的密鑰
T2	加密和認證	EEPROM	DPA 保護和可鎖定的種子位元	作業系統鎖定的密鑰
M1 系列	加密、認證和重放預防	安全儲存元件 (第二代)	DPA 保護和可鎖定的種子位元	作業系統綁定的密鑰和「開機監視器」



# Face ID 和 Touch ID

## Face ID 和 Touch ID 保安

密碼對於 Apple 裝置的保安至關重要。同時，用戶需要能夠方便取用其裝置，每日甚至會超過 100 次。生物識別認證提供了一種方式，可以保留高強度密碼的保安，甚至可以增強密碼，因為不需要手動輸入密碼，同時還提供了透過手指按壓或注視螢幕來快速解鎖的便利性。Face ID 與 Touch ID 不會取代密碼，但是在大部份的情況下，它們確實可以讓取用裝置的動作變得更快、更輕鬆。

Apple 的生物識別安全架構有賴於生物識別感應器與「安全隔離區」之間嚴格的責任劃分，以及兩者之間的安全連線。感應器會截取生物識別影像並將其安全地傳輸到「安全隔離區」。在註冊過程中，「安全隔離區」會處理、加密和儲存對應的 Face ID 和 Touch ID 範本資料。在比對期間，「安全隔離區」會將來自生物識別感應器的傳入資料與儲存的範本進行比較，以確定是否要解鎖裝置或回應比對有效（適用於 Apple Pay、App 內購買以及 Face ID 與 Touch ID 的其他用途）。此架構支援包含感應器和「安全隔離區」的裝置（如 iPhone、iPad 和許多 Mac 系統），以及將感應器實體分離到周邊裝置的功能，其之後會將周邊裝置安全地配對到配備 Apple 晶片的 Mac 中的「安全隔離區」。

### Face ID 保安

只要看一眼，Face ID 便會安全地解鎖支援的 Apple 裝置。此技術透過原深感測鏡頭系統提供了直覺且安全的認證方式，運用先進技術來精確對比臉部幾何結構。Face ID 會使用神經網絡來判斷螢幕注視、比對和防止造假，用戶在使用支援的裝置時，便可以透過注視螢幕來解鎖手機（即使戴上口罩）。Face ID 會自動適應外表變化，並嚴密保護用戶生物特徵識別資料的私隱與安全。

Face ID 的設計用意為確認用戶注視螢幕、提供比對錯誤率低的穩固認證方式，以及減少電子和物理性造假。

原深感測鏡頭會在以下情況自動尋找用戶的面孔：當用戶喚醒配備 Face ID 的 Apple 裝置時（拿起裝置或點按螢幕）；當這些裝置嘗試取得用戶的認證以顯示收到的通知時；或是當支援的 App 要求 Face ID 認證時。當偵測到面孔時，Face ID 會辨認用戶的眼睛是張開的並注視裝置，以確認螢幕注視和進行解鎖的意圖；針對輔助使用功能，當啟用「旁白」時會停用此功能，並可在需要時個別停用 Face ID 注意檢查。戴上口罩使用 Face ID 時，一律需要偵測注視。

在原深感測鏡頭確偵測到注視螢幕的面孔後，會發出並讀取數千個紅外線光點以形成面孔的深度圖，包含 2D 紅外線影像。此資料用於製作一系列的 2D 影像和深度圖，經過電子簽署後傳送到「安全隔離區」。為了防止電子和物理性造假，原深感測鏡頭會隨機排序截取到的一系列 2D 影像和深度圖，並發出裝置特定的隨機圖形。「安全神經引擎」的一部份神經引擎（受「安全隔離區」保護）會將這些資料轉換為數學表徵，並將這些表徵與登記的面孔資料進行比對。這個登記的面孔資料本身為以多種姿勢捕捉的用戶面孔之數學表徵。

### Touch ID 保安

Touch ID 是指紋感應系統，有助於更快、更輕鬆地對支援的 Apple 裝置進行安全的存取。此技術可從任何角度來讀取指紋，隨着感應器每次使用時識別出其他重疊的節點而持續擴大指紋圖，逐漸提高對用戶指紋識別的能力。

配備 Touch ID 感應器的 Apple 裝置可透過指紋解鎖。Touch ID 不會取代系統對裝置密碼或用戶密碼的需求，在裝置啟動、重新開機或在登出（在 Mac 上）後，仍會要求這些密碼。在部份 App 中，Touch ID 亦可用來取代裝置密碼或用戶密碼，例如在「備忘錄」App 中解鎖受密碼保護的備忘錄、解鎖受鑰匙圈保護的網站，以及解鎖受支援的 App 的密碼。但是，在部份情況下系統總是會要求裝置密碼或用戶密碼（例如更改現有的裝置密碼或用戶密碼，或移除現有或建立新的指紋登記）。

當指紋感應器偵測到手指觸碰時，它會觸發進階成像陣列來掃描手指，並將結果傳送到「安全隔離區」。用來確保此連線安全的頻道會有所不同，這取決於 Touch ID 感應器是內置於配有「安全隔離區」的裝置中，還是位於單獨的周邊裝置中。

對指紋掃描執行向量化以進行分析時，光柵掃描會暫時儲存在「安全隔離區」的加密記憶體中，然後便會遭捨棄。此分析使用皮下指紋紋路角度對應，這是一種有損性的程序，重建用戶實際指紋所必需的精細資料會在分析完成後刪除。在註冊過程中，最後產生的節點圖會以加密格式儲存，該加密格式只能由「安全隔離區」讀取為範本，以便針對未來比對項目進行比較，但不含任何識別資料。此資料絕對不會流出裝置，不會傳送至 Apple，也不會納入裝置備份中。

## 內置 Touch ID 頻道保安

「安全隔離區」與內置的 Touch ID 感應器之間的通訊是透過序列周邊介面匯流排來執行。處理器會將資料轉送至「安全隔離區」，但處理器本身無法讀取這些資料。資料會藉由作業階段密鑰進行加密與認證，該作業階段密鑰是透過每個 Touch ID 感應器出廠時配置的共享密鑰及其相應的「安全隔離區」進行交涉。共享密鑰的每個 Touch ID 感應器保安極高、具隨機性，且都不同。作業階段密鑰的交換會使用 AES 密鑰進行封裝，並由兩端提供一隨機密鑰，用來建立作業階段密鑰並使用提供認證和機密性的傳輸加密 (使用 AES-CCM)。

## 配備 Touch ID 的精妙鍵盤

配備 Touch ID 的精妙鍵盤 (和配備 Touch ID 與數字鍵盤的精妙鍵盤) 在外置鍵盤中提供了 Touch ID 感應器，可搭配任何配備 Apple 晶片的 Mac 使用。配備 Touch ID 的精妙鍵盤具備生物識別感應器的角色；其不會儲存生物識別範本、執行生物識別比對或執行保安規則 (例如，必須在 48 小時未有解鎖後輸入密碼)。必須先將配備 Touch ID 的精妙鍵盤中的 Touch ID 感應器與 Mac 上的「安全隔離區」嚴密配對，然後才能使用配備 Touch ID 的精妙鍵盤，接著「安全隔離區」會執行註冊和比對作業，並以針對內置 Touch ID 感應器相同的方式來執行保安規則。Apple 在出廠時對 Mac 隨附之配備 Touch ID 的精妙鍵盤進行了配對處理。如有需要，配對作業也可以由用戶執行。配備 Touch ID 的精妙鍵盤一次只能與一部 Mac 安全地配對，但是 Mac 最多可以與五個配備 Touch ID 的精妙鍵盤維持安全配對。

配備 Touch ID 的精妙鍵盤與內置 Touch ID 感應器相容。如果在配備 Touch ID 的精妙鍵盤上出現了內置 Mac Touch ID 感應上的手指，則 Mac 中的「安全隔離區」將會成功處理比對作業，反之亦然。

為了支援安全配對，進而支援 Mac「安全隔離區」和配備 Touch ID 的精妙鍵盤之間的通訊，該鍵盤配備了硬件「公共密鑰加速器 (PKA)」區塊，以提供證明以及配對硬件式鍵盤來執行必要的操作加密編譯過程。

## 安全配對

在配備 Touch ID 的精妙鍵盤可用於 Touch ID 操作之前，需要將其安全地與 Mac 配對。如要配對，Mac 上的「安全隔離區」和配備 Touch ID 的精妙鍵盤中的 PKA 區塊會交換公共密鑰 (根植於受信任的 Apple Ca)，並且它們使用硬件持有的證明密鑰和臨時 ECDH 來安全地證明其身份。在 Mac 上，此資料受「安全隔離區」保護；在配備 Touch ID 的精妙鍵盤上，此資料則受 PKA 區塊保護。安全配對後，Mac 和配備 Touch ID 的精妙鍵盤之間的所有 Touch ID 資料通訊都將由 AES-GCM 使用 256 位的密鑰長度加密，並依據儲存的識別身份使用 NIST P-256 曲線的臨時 ECDH 密鑰進行加密。(與任何藍牙鍵盤一樣，一般按鍵會使用藍牙保安進行交換。)

## 確定配對意圖

如要首次執行某些 Touch ID 操作 (例如，註冊新的指紋)，用戶必須實際確認其想要在 Mac 上使用配備 Touch ID 的精妙鍵盤的意圖。透過在用戶介面指示時按兩下 Mac 電源按鈕，或透過成功比對先前已在 Mac 上註冊的指紋，可以確認實際意圖。如需更多資料，請前往：[安全意圖以及與「安全隔離區」的連線](#)。

Apple Pay 交易可以使用 Touch ID 比對進行授權，或者輸入 macOS 用戶密碼並在配備 Touch ID 的精妙鍵盤上按兩下 Touch ID 按鈕。後者可讓用戶即使沒有進行 Touch ID 比對，也可以確認實際意圖。

## 配備 Touch ID 的精妙鍵盤的頻道保安

為協助確保配備 Touch ID 的精妙鍵盤中的 Touch ID 感應器與配對的 Mac 上的「安全隔離區」之間的通訊頻道安全，需要執行以下項目：

- 配備 Touch ID 的精妙鍵盤 PKA 區塊和「安全隔離區」之間的安全配對 (如上所述)
- 配備 Touch ID 感應器的精妙鍵盤與其 PKA 區塊之間的安全頻道

配備 Touch ID 感應器的巧控鍵盤與其 PKA 區塊之間的安全頻道是在出廠時，使用兩者之間共享的唯一密鑰來建立的。(對於內置 Touch ID 的 Mac 電腦，這與在 Mac 上的「安全隔離區」及其內置感應器之間建立安全頻道，所使用的技術相同。)

## Face ID、Touch ID 和密碼

如要使用 Face ID 或 Touch ID，用戶必須將裝置設定為需用密碼來解鎖。當 Face ID 或 Touch ID 偵測到成功的比對時，用戶的裝置便會自動解鎖，無需輸入裝置密碼。這讓使用更長、更複雜的密碼變得更為實用，因為用戶無須經常輸入密碼。Face ID 和 Touch ID 並不會取代用戶的密碼，反而是在周全的界限和時間限制內提供更簡便的存取裝置方式。這一點很重要，因為高強度的密碼是構成 iPhone、iPad、Mac 或 Apple Watch 加密保護用戶資料的基礎。

### 甚麼時候需使用裝置密碼

用戶可以隨時使用其密碼來代替 Face ID 或 Touch ID，但有些情況不允許使用生物識別。以下高度要求保安的作業一律會要求輸入密碼：

- 更新軟件
- 清除裝置
- 檢視或更改密碼設定
- 安裝設定描述檔
- 在 Mac 上的「系統偏好設定」解鎖「保安與私隱」面板
- 在 Mac 上的「系統偏好設定」解鎖「用戶與群組」面板（如「檔案保險箱」已開啟）

如裝置處於以下任何一種狀態，也需要使用密碼：

- 裝置剛開機或重新啟動。
- 用戶已登出其 Mac 帳戶（或尚未登入）。
- 用戶超過 48 小時未解鎖裝置。
- 用戶在 156 小時（六日半）內未使用密碼來解鎖裝置，並且在 4 小時內未使用生物識別技術來解鎖裝置。
- 裝置收到了遙距鎖定命令。
- 用戶透過同時按住音量按鈕和睡眠/喚醒按鈕 2 秒，然後按下「取消」來離開關機/緊急求助 SOS。
- 生物識別配對失敗五次後（雖然為兼顧可用性，該裝置可能會在較少次數的失敗後要求輸入密碼取代生物識別）。

在 iPhone 上啟用戴着口罩使用 Face ID 時，其在以下其中一項用戶動作後的 6.5 小時內可供使用：

- 嘗試配對 Face ID 成功（佩戴或未有佩戴口罩）
- 裝置密碼驗證
- 使用 Apple Watch 解鎖裝置

執行以上任何一項動作都會將期限延長 6.5 小時。

當 iPhone 或 iPad 上的 Face ID 或 Touch ID 啟用時，按下睡眠/喚醒按鈕時裝置會立即鎖定裝置，每當裝置進入睡眠時也會鎖定。每次喚醒裝置時，Face ID 和 Touch ID 便需要成功的配對（或是選擇輸入密碼）。

人群中隨機一人可使用 Face ID 解鎖用戶的 iPhone 或 iPad 的機率為百萬分之一（包括開啟戴着口罩使用 Face ID 時）。至於用戶的配備 Touch ID 的 iPhone、iPad、Mac 型號，以及已與精妙鍵盤配對的 Mac 型號，此率低於五萬分之一。此機率會隨着登記多個指紋（五個指紋的機率會增至一萬分之一）或面孔（兩個面孔的機率會增至五十萬分之一）而增加。為了進一步保護裝置，Face ID 和 Touch ID 皆只允許五次配對失敗，其後便需要輸入密碼才能取用用戶的裝置或帳戶。使用 Face ID，在以下情況下錯誤比對的機率更高：

- 雙胞胎或長相與用戶相似的兄弟姊妹
- 13 歲以下孩子（因為他們的獨特臉部特徵發展可能尚未成熟）

在這兩種情況下戴着口罩使用 Face ID 時，機率可能會進一步增加。如用戶對比對錯誤存有疑慮，Apple 建議使用密碼來認證。

## 面孔比對保安

系統會在「安全隔離區」內利用專為此目的訓練的神經網絡進行面孔比對。為了開發面孔比對神經網絡，Apple 使用了超過十億張影像，其中包括在參與者知情同意下進行的研究中所收集的紅外線 (IR) 和深度圖。Apple 遂與世界各地的參與者合作，考量性別、年齡、種族和其他因素，讓具代表性的一群人參與其中。我們視必要性擴大了研究範圍，以便為多元用戶提供更高的準確度。Face ID 設計為可在用戶戴着帽子、圍巾、眼鏡、隱形眼鏡和各式太陽眼鏡時使用。Face ID 亦在 iPhone 12 及 iOS 15.4 或以上版本的 iPhone 裝置上戴着口罩解鎖。此外，在室內、室外甚至是完全黑暗的環境下也都能正常使用。專為偵測和防止造假而訓練的一個額外神經網絡，可防範有心人士企圖以相片或面具解鎖裝置。Face ID 資料 (包括用戶面孔的數學表徵) 經過加密，且僅供「安全隔離區」使用。此資料絕對不會流出裝置，不會傳送至 Apple，也不會納入裝置備份中。下列經儲存和加密的 Face ID 資料僅供「安全隔離區」在一般操作期間使用：

- 登記期間對用戶的面孔進行計算所產生的數學表徵
- 某幾次嘗試解鎖時對用戶的面孔進行計算所產生的數學表徵 (如果 Face ID 認為可用於增強未來配對效果)

系統不會儲存一般操作期間捕捉的面孔影像，而是會在為了登記或與登記的 Face ID 資料進行配對而計算了數學表徵後，立即捨棄這些面孔影像。

## 改進 Face ID 配對

為了改善配對效能，以及跟進面孔和外貌的自然變化，Face ID 會逐漸擴增它所儲存的數學表徵。成功配對時，如果新計算的數學表徵品質夠好，Face ID 可能會在捨棄該資料前，使用有關資料來進行有限次數的額外配對。相反地，如果 Face ID 無法識別面孔，但是比對品質高於特定標準，且用戶在失敗後立即輸入密碼，Face ID 會再次捕捉面孔，並以新計算出的數學表徵擴增登記的 Face ID 資料。如果用戶停止用這項新的 Face ID 資料進行比對，或是在進行有限次數的比對後，系統會捨棄這項資料；選擇重設 Face ID 選項時，新資料也會遭捨棄。這些增強程序可讓 Face ID 跟進用戶鬍子或妝容的顯著變化，同時將誤判而接受的情況減到最少。

# Face ID 和 Touch ID 的用途

## 解鎖裝置或用戶帳戶

如 Face ID 或 Touch ID 已關閉，在裝置或帳戶鎖定時，系統會捨棄保留在「安全隔離區」中最高「資料保護」類別的密鑰。除非用戶輸入密碼來解鎖裝置或帳戶，否則便無法存取該類別的檔案和鑰匙圈項目。

如 Face ID 或 Touch ID 已開啟，則不會在裝置或帳戶鎖定時捨棄這些密鑰，而是透過提供給「安全隔離區」中 Face ID 或 Touch ID 子系統的密鑰進行封裝。當用戶嘗試解鎖裝置或帳戶時，如裝置偵測到成功的配對，它便會提供密鑰來解除封裝「資料保護」密鑰，裝置或帳戶便會解鎖。此流程透過要求「資料保護」和 Face ID 或 Touch ID 子系統合作來解鎖裝置，因此提供了額外的保護。

當裝置重新啟動時，Face ID 或 Touch ID 解鎖裝置或帳戶時所需的密鑰會消失；每當符合任何需要輸入密碼的條件時，「安全隔離區」就會捨棄這些密鑰。

## 使用 Apple Pay 安全地進行消費

Face ID 和 Touch ID 也可以配搭 Apple Pay 使用，方便用戶在商店、App 內和網站上輕鬆且安全地進行購買：

- **在商店中使用 Face ID：**如要使用 Face ID 授權店內付款，用戶必須先按兩下側邊按鈕確認付款意圖，此按兩下的動作使用直接連結到「安全隔離區」的物理動作來取得用戶的意圖，且可防止惡意的偽造程序。用戶之後便可使用 Face ID 進行授權，再將裝置靠近非接觸式付款讀卡器。通過 Face ID 認證後可選擇另一種 Apple Pay 付款方式，這需要進行重新認證，不過不用再按兩下側邊按鈕。
- **在 App 內和在網站上使用 Face ID：**如要在 App 內和網站上付款，用戶必須先按兩下側邊按鈕確認其付款意圖，然後使用 Face ID 進行認證以授權付款。如果用戶沒有在按兩下側邊按鈕後 60 秒內完成 Apple Pay 交易，就必須再按兩下側邊按鈕重新確認付款意圖。
- **使用 Touch ID：**如為 Touch ID，付款意圖是透過啟用 Touch ID 感應器並成功比對用戶指紋的手勢來完成確認。

## 使用系統提供的 API

第三方 App 可使用系統提供的 API 來要求用戶透過 Face ID、Touch ID 或密碼進行認證，且支援 Touch ID 的 App 無需任何變更就可自動支援 Face ID。使用 Face ID 或 Touch ID 時，App 只會收到認證是否成功的通知，無法存取 Face ID、Touch ID 或已登記之用戶的相關資料。

## 保護鑰匙圈項目

Face ID 或 Touch ID 也可用來保護鑰匙圈項目，只有在「安全隔離區」比對成功或裝置密碼或帳戶密碼正確時才將鑰匙圈項目釋出。要求以 Face ID、Touch ID 或密碼解鎖鑰匙圈項目前，App 開發者可透過 API 確認用戶已設定密碼。App 開發者可執行以下任何操作：

- 要求「認證 API」的作業不得使用 App 密碼或裝置密碼來當作備用認證方式。他們可以查詢用戶是否已登記 Face ID 或 Touch ID，以便允許在對保安有高度要求的 App 中將 Face ID 或 Touch ID 當作第二個驗證條件。
- 在「安全隔離區」內產生和使用可由 Face ID 或 Touch ID 保護的橢圓曲線加密技術 (ECC) 密鑰。「安全隔離區」授權使用這些密鑰後，這些密鑰的相關操作會一律在「安全隔離區」內執行。

## 進行及允許購買

用戶也可設定 Face ID 或 Touch ID 以用來核准從 iTunes Store、App Store、Apple Books 等服務購買項目，如此一來便無需輸入 Apple ID 密碼。購買後，「安全隔離區」會驗證是否進行了生物識別認證，然後核發用於簽署商店要求的 ECC 密鑰。

## 安全意圖以及與「安全隔離區」的連線

安全意圖提供了一種無需與作業系統或「應用程式處理器」進行任何互動，即可確認用戶意圖的方式。該連線是從實體按鈕到「安全隔離區」的實體連結，可在以下裝置使用：

- iPhone X 或較新型號
- Apple Watch Series 1 或較新型號
- iPad Pro (所有型號)
- iPad Air (2020 年)
- 配備 Apple 晶片的 Mac 電腦

有了此連線，用戶可以確認他們打算以某種方式完成操作的意圖，因此即使具有根特權或核心中執行的軟件也不會遭欺騙。

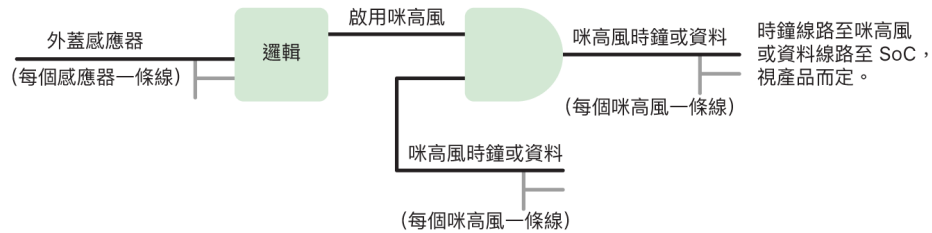
此功能用於 Apple Pay 交易過程中以及在將配備 Touch ID 的精妙鍵盤與配備 Apple 晶片的 Mac 配對完成時，確認用戶的意圖。當用戶介面提示時，按兩下相對應的按鈕 (Face ID) 或指紋掃描 (Touch ID) 可發出確認用戶意圖的訊號。如需更多資料，請前往：[使用 Apple Pay 安全地進行消費](#)。配備 Apple T2 保安晶片且沒有觸控欄的 MacBook 型號，支援以「安全隔離區」和 T2 韌體為基礎的類似機制。

## 硬件咪高風斷線功能

所有配備 Apple 晶片的 Mac 手提電腦和以 Intel 為基礎並配備 Apple T2 保安晶片的 Mac 手提電腦，均具有硬件斷線功能，可在合上上蓋時停用咪高風。在所有配備 T2 晶片的 13 吋 MacBook Pro 和 MacBook Air 手提電腦、所有配備 T2 晶片的 MacBook 手提電腦（2019 年和較新型號）以及所有配備 Apple 晶片的 Mac 手提電腦上，這個斷線功能只在硬件上執行。此斷線功能的設計用意是防止任何軟件（即使具有 macOS 中的根或核心權限，以及 T2 晶片上的軟件或其他韌體）在上蓋合上時使用咪高風。（硬件相機不會斷線，因為其視野會完全被合上的上蓋遮蔽。）

2020 年開始的 iPad 型號也配備硬件咪高風斷線功能。當 iPad 裝入 MFI 認證的護殼（包含 Apple 所發售的）並合上時，硬件中的咪高風就會中斷連線。其設計用意是防止系統允許任何軟件使用咪高風音訊資料，即使該軟件具有 iPadOS 的根或核心權限，或是任何裝置韌體，也具保護作用。

根據以下電路圖，本節中的保護會直接透過硬件邏輯執行：



在具有硬件咪高風截斷功能的每項產品中，一或多個外蓋感應器會使用互動的某些物理屬性（例如，霍爾效應感應器或鉸鏈角度感應器）來偵測外蓋或護殼的實際閉合程度。對於需要校正的感應器，在裝置生產期間會設定參數，並且校正過程包括不可逆轉的硬件鎖定，以防止對感應器上敏感參數進行任何後續變更。這些感應器發出直接的硬件訊號，該訊號通過一組簡單、不可重新編寫程式的硬件邏輯。這些邏輯提供去抖動、滯後作用和/或最多 500ms 的延遲，然後再停用咪高風。視產品的不同，可以藉由停用在咪高風和單晶片系統 (SoC) 之間傳輸資料的線路或藉由停用咪高風模組中使其處於作用狀態的其中一條輸入線路，例如時鐘線路或類似的有效控制，來執行此訊號。

## 以剩餘電量使用特快卡

如果 iOS 因為 iPhone 需要充電而未運作，電池中可能仍有足夠的電力以支援「特快卡」交易。支援的 iPhone 裝置會自動對以下票證提供此功能：

- 專為「特快交通卡」設計的付款卡或交通卡
- 已開啟「特快模式」的學生證
- 已開啟「特快模式」的車匙
- 已開啟「快速模式」的家居鎖匙
- 已開啟「快速模式」的酒店或公司識別證

按下側邊按鈕（或在 iPhone SE 第二代上按下主畫面按鈕），會顯示電力不足的圖像，以及表示可使用「特快卡」的文字。此時 NFC 控制器仍會執行「特快卡」交易，如同 iOS 仍在正常運作一般，差別在於交易只會以觸覺通知（不會顯示視覺通知）表示。在 iPhone SE 第二代上，完成的交易可能需要幾秒鐘才能顯示在螢幕上。如是由用戶執行的標準關機，此功能則不會運作。

# 系統保安

## 系統保安概覽

系統保安是以 Apple 硬件的獨特功能為基礎所建置，負責控制對 Apple 裝置中系統資源的存取，且不犧牲可用性。系統保安包含開機程序、軟件更新及保護電腦系統資源，如 CPU、記憶體、磁碟、軟件程式和儲存的資料。

最新版本的 Apple 作業系統是最安全的。Apple 保安的重要部份是**安全啟動**，可以在開機時保護系統免受惡意軟件感染。安全啟動會在硬件中開始，並透過軟件建立信任鏈，交付控制權之前，每個步驟的設計用意都是確認下一個步驟

可正常運作。此安全模式不僅支援 Apple 裝置的預設開機程序，也支援 Apple 裝置上的多種還原和即時更新。T2 晶片和「安全隔離區」等子元件也會執行專屬的安全啟動程序，來確保自己只啟動來自 Apple 的已知安全程式碼。更新系統的設計旨在協助阻止降級攻擊，讓攻擊者不能透過令裝置變回較舊的作業系統版本（攻擊者懂得如何入侵）來盜取用戶資料。

Apple 裝置也包含開機與執行階段保護，因此可在持續運作期間維持完整性。Apple 設計的晶片安裝於 iPhone、iPad、Apple Watch、Apple TV、HomePod 和配備 Apple 晶片的 Mac 上，提供可保護作業系統完整性的通用架構。macOS 也提供延伸且可設定的一組防護功能以支援不同的運算模式，以及所有 Mac 硬件平台支援的功能。



# 安全啟動

## iOS 和 iPadOS 裝置的開機程序

開機程序中每個步驟包含的元件都經過 Apple 加密編譯簽署以啟用其完整性檢查，以在驗證信任鏈結後，每個步驟才能繼續。這些元件包含啟動程式、核心、核心延伸功能和流動網絡基頻韌體。此安全啟動鏈旨在確認底層的軟件未經竄改。

開啟 iOS 和 iPadOS 裝置後，其「應用程式處理器」會立即執行唯讀記憶體（稱為 Boot ROM）中的程式碼。此類無法更改的程式碼（稱為**硬件的信任根**）是在製造晶片時完成設定，且可完全信任。Boot ROM 程式碼包含 Apple Root 憑證授權管理中心（CA）公用密鑰，該公用密鑰用於驗證 iBoot 啟動程式是否經過 Apple 簽署，以決定是否允許其載入。這是信任鏈結中的第一步，信任鏈結中的每個步驟都會檢查下一個步驟是否經由 Apple 簽署。當 iBoot 完成其任務後，便會驗證和執行 iOS 或 iPadOS 核心。如為配備 A9 或較早 A 系列處理器的裝置，會載入額外的底層啟動程式（LLB）階段並由 Boot ROM 加以驗證，接着會載入並驗證 iBoot。

視硬件而定，載入或驗證以下階段失敗的處理方式會有所不同：

- **Boot ROM 無法載入 LLB (較舊裝置)：**裝置韌體升級 (DFU) 模式
- **LLB 或 iBoot：**還原模式

無論哪一種情況下，裝置都必須透過 Finder (macOS 10.15 或較新版本) 或透過 USB 連接到 iTunes (macOS 10.14 或較早版本) 並還原至出廠預設值。

「開機進度暫存器」(BPR) 是「安全隔離區」用來在不同模式中限制用戶資料存取的機制，其會在進入以下模式前更新：

- **DFU 模式：**在配備 Apple A12 或較新版本 SoC 的裝置上透過 Boot ROM 設定
- **還原模式：**在配備 Apple A10、S2 較新版本 SoC 的裝置上透過 iBoot 設定

在具有流動數據連線功能的裝置上，流動網絡基頻子系統會使用已簽署的軟件以及由基頻處理器驗證的密鑰，來執行其他安全啟動操作。

「安全隔離區」也會執行安全啟動，以檢查其軟件 (sepOS) 已經過 Apple 驗證和簽署。

## 記憶體安全執行 iBoot

在 iOS 14 和 iPadOS 14 中，Apple 修改了用來建立 iBoot 啟動程式的 C 編譯器工具鏈以改善其保安。修改後的工具鏈會執行程式碼，其設計目的是防止通常會在 C 程式中遇到的記憶體和型別安全問題。例如，這可協助防止下列類別中大部分的弱點：

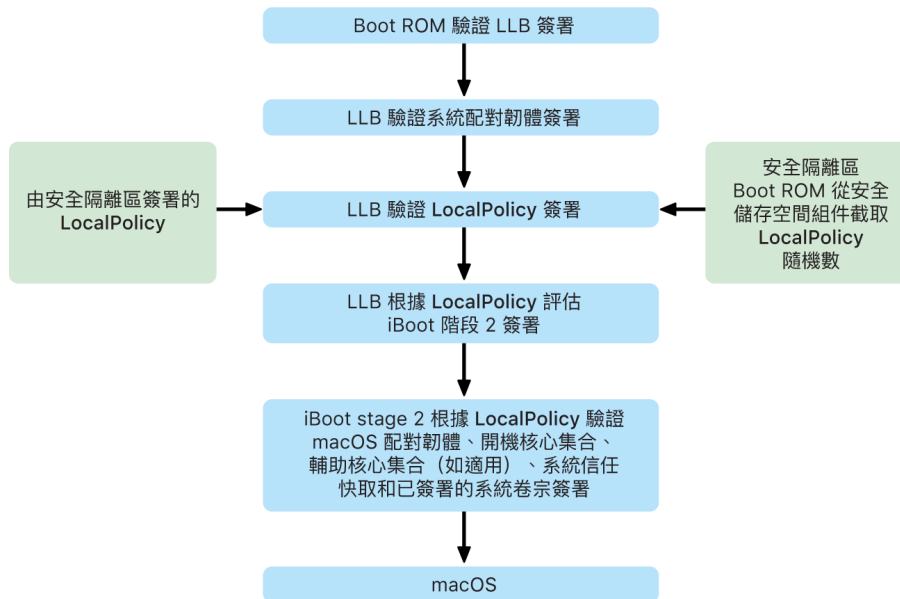
- **緩衝區溢位：**透過確保所有指標都攜帶存取記憶體時通過驗證的界限資料
- **堆積利用：**透過分離堆積資料與其後設資料及正確偵測雙重釋出等錯誤情況
- **型別混淆：**透過確保所有指標都攜帶指標轉換操作期間通過驗證的執行階段型別資料
- **釋出後使用錯誤所造成的型別混淆：**透過靜態型別分隔所有動態記憶體配置

配備 Apple A13 仿生晶片或較新版本的 iPhone，以及配備 A14 仿生晶片的 iPad 均可使用此技術。

# 配備 Apple 晶片的 Mac 電腦

## 配備 Apple 晶片的 Mac 之開機程序

當配備 Apple 晶片的 Mac 開啟時，會執行與 iPhone 和 iPad 非常類似的開機程序。



晶片會在信任鏈的第一個步驟執行 Boot ROM 中的程式碼。配備 Apple 晶片的 Mac 上的 macOS 安全啟動不只會驗證作業系統程式碼本身，也會驗證經授權用戶設定的保安規則甚至是 kext (提供支援，但不建議使用)。

當 LLB (其代表「低階 Bootstrap」) 啟動時，隨即會驗證簽署並為 SoC 內部核心 (例如儲存體、顯示器、系統管理和 Thunderbolt 控制器) 載入系統配對韌體。LLB 也負責載入 LocalPolicy (由「安全隔離區處理器」簽署的檔案)。LocalPolicy 檔案描述用戶針對系統開機和執行階段保安規則選擇的設定。LocalPolicy 的資料結構格式與其他所有開機物件相同，不過會在本機由一個專用密鑰 (只能在特定電腦的「安全隔離區」內存取) 簽署，而非由中央 Apple 伺服器 (例如軟體更新) 簽署。

為協助防止先前的 LocalPolicy 重播，LLB 必須從連接「安全隔離區」的「安全儲存元件」查找隨機數。如要這麼做，其會使用「安全隔離區 ROM」，並確保 LocalPolicy 中的隨機數與「安全儲存元件」中的隨機數相符。這可協助防止進行保安升級後舊版 LocalPolicy (設定的保安可能較低) 重新套用至系統。結果是配備 Apple 晶片的 Mac 上的

安全啟動不僅能防止作業系統版本回滾，也能防止保安規則降級。

LocalPolicy 檔案會截取作業系統是設為「完整保安」、「較低保安」還是「寬鬆保安」。

- **完整保安**：系統的行為就跟 iOS 和 iPadOS 相同，且只允許安裝時已知最新版的開機軟件。
- **較低保安**：系統會指示 LLB 信任與作業系統綁定的「全域」簽署。這會允許系統執行舊版的 macOS。因為舊版 macOS 不可避免地具有未修補的漏洞，此保安模型便被稱為「較低保安」。這也是支援開機核心延伸功能 (kext) 所需的規則層級。
- **寬鬆保安**：系統的行為類似「較低保安」，也使用 iBoot 的全域簽署驗證，不過也會告知 iBoot 應接受某些由「安全隔離區」簽署的開機物件，這些物件的密鑰與用來簽署 LocalPolicy 的密鑰相同。這個規則層級支援用戶建立、簽署和啟動自己的自訂 XNU 核心。

如果 LocalPolicy 向 LLB 指出選取的作業系統正在以「完整保安」執行，則 LLB 會評估 iBoot 的個人化簽署。如果有關作業系統以「較低保安」或「寬鬆保安」執行，則會評估全域簽署。任何簽署驗證錯誤都會導致系統開機至 RecoveryOS 以提供修復選項。

LLB 交給 iBoot 接手之後，會載入與 macOS 配對的韌體，例如「安全神經引擎」、Always On Processor 等的韌體。iBoot 也會查看從 LLB 傳遞給它的 LocalPolicy 相關資料。如果 LocalPolicy 指出應有一個輔助核心集合 (AuxKC)，iBoot 便會在檔案系統上查找 AuxKC，驗證有關 AuxKC 是使用與 LocalPolicy 相同的密鑰由「安全隔離區」簽署，並驗證其雜湊值與 LocalPolicy 中儲存的雜湊值相符。如果 AuxKC 通過驗證，iBoot 會透過「開機核心集合」將 AuxKC 放入記憶體，然後再鎖定整個記憶體區域，這個區域涵蓋開機核心集合和具有系統協同處理器完整保護 (SCIP) 的 AuxKC。如果規則指出應存在一個 AuxKC 但卻找不到，系統便會繼續在沒有 AuxKC 的狀態下開機進入 macOS。iBoot 也負責驗證簽署系統卷宗 (SSV) 的開機雜湊值，以確認將裝載核心的檔案系統完全通過完整性驗證。

## 配備 Apple 晶片的 Mac 之開機模式

配備 Apple 晶片的 Mac 具有下列的開機模式。

模式	按鍵組合	描述
macOS	在開機狀態下按下並 <b>放開</b> 電源按鈕。	<ol style="list-style-type: none"><li>1. Boot ROM 交給 LLB 接手。</li><li>2. LLB 載入系統配對韌體和所選 macOS 的 LocalPolicy。</li><li>3. LLB 將開機進入 macOS 的指示鎖定在「開機進度暫存器」(BPR) 中，然後再接力給 iBoot。</li><li>4. iBoot 載入 macOS 配對韌體、靜態信任快取、裝置樹狀結構以及開機核心集合。</li><li>5. 如果 LocalPolicy 允許，iBoot 會載入第三方 kext 的輔助核心集合 (AuxKC)。</li><li>6. 如果 LocalPolicy 沒有停用此功能，iBoot 會驗證簽署系統卷宗 (SSV) 的根簽署雜湊值。</li></ol>
配對 RecoveryOS	在開機狀態下 <b>按住</b> 電源按鈕。	<ol style="list-style-type: none"><li>1. Boot ROM 交給 LLB 接手。</li><li>2. LLB 載入系統配對韌體和 RecoveryOS 的 LocalPolicy。</li><li>3. LLB 將開機進入配對 RecoveryOS 的指示鎖定在「開機進度暫存器」中，然後再移交給配對 RecoveryOS 的 iBoot。</li><li>4. iBoot 載入 macOS 配對韌體、信任快取、裝置樹狀結構以及開機核心集合。</li><li>5. 如果配對 RecoveryOS 開機失敗，系統會嘗試開機進入備用 RecoveryOS。</li></ol> <p><b>附註：</b>配對 RecoveryOS 的 LocalPolicy 不允許保安降級。</p>
備用 RecoveryOS	在開機狀態下 <b>按兩下</b> 並 <b>按住</b> 電源按鈕。	<ol style="list-style-type: none"><li>1. Boot ROM 交給 LLB 接手。</li><li>2. LLB 載入系統配對韌體和 RecoveryOS 的 LocalPolicy。</li><li>3. LLB 將開機進入配對 RecoveryOS 的指示鎖定在「開機進度暫存器」中，然後再移交給 RecoveryOS 的 iBoot。</li><li>4. iBoot 載入 macOS 配對韌體、信任快取、裝置樹狀結構以及開機核心集合。</li></ol> <p><b>附註：</b>配對 RecoveryOS 的 LocalPolicy 不允許保安降級。</p>
安全模式	按照上述步驟開機至 RecoveryOS，然後在選擇啟動卷宗的同時按住 <b>Shift</b> 鍵。	<ol style="list-style-type: none"><li>1. 按照上述步驟開機至 RecoveryOS。</li><li>2. 選擇卷宗時按住 Shift 鍵會讓 BootPicker App 照常啟動 macOS，其也會設定 nvram 變數，該變數會告知 iBoot 在下次開機時不要載入 AuxKC。</li><li>3. 系統重新開機並開機至目標卷宗，但 iBoot 不會載入 AuxKC。</li></ol>

## 配對 RecoveryOS 的限制

在 macOS 12.0.1 或較新版本中，每次新的 macOS 安裝作業也會將配對版本的 RecoveryOS 安裝到相對應的 APFS 卷宗群組中。這種設計對於以 Intel 為基礎的 Mac 電腦之用戶來說很熟悉，但在配備 Apple 晶片的 Mac 上，它提供了額外的保安和相容性保證。因為現在每次 macOS 安裝作業都有一個專用的配對 RecoveryOS，這有助於確保只有專用的配對 RecoveryOS 才能執行保安降級操作。這有助於保護較新版本 macOS 的安裝作業免受較舊版本 macOS 的篡改，反之亦然。

配對限制會執行如下：

- macOS 11 的所有安裝作業都會與 RecoveryOS 配對。如果選取預設開機進行 macOS 11 安裝作業，則在 v 使用 Apple 晶片的 Mac 上開機時按住電源鍵即可將 RecoveryOS 開機。RecoveryOS 可以降級任何 macOS 11 安裝作業的保安設定，但不能降級 macOS 12.0.1 的任何安裝項目。
- 如果選取預設開機進行 macOS 12.0.1 或較新版本的安裝作業，則在 Mac 啟動時按住電源鍵即可將其配對 RecoveryOS 開機。配對 RecoveryOS 可以為配對的 macOS 安裝項目降級保安設定，但不能為任何其他 macOS 安裝項目降級。

如要讓任何 macOS 安裝項目開機進入配對 RecoveryOS，需要選取該安裝項目作為預設項目，這可以使用「系統偏好設定」中的「啟動磁碟」，或透過啟動任何 RecoveryOS 並在選擇卷宗時按住 Option 鍵來完成。

**附註：**備用 RecoveryOS 無法執行任何 macOS 安裝項目的降級。

## 配備 Apple 晶片的 Mac 之「啟動磁碟」保安規則控制

### 概覽

與以 Intel 為基礎的 Mac 上的保安規則不同，配備 Apple 晶片的 Mac 上的保安規則適用於各個已安裝的作業系統。這表示同一部 Mac 上支援多個不同版本的已安裝 macOS 執行個體和保安規則。因此，**作業系統選擇器**已加入至「開機保安工具程式」。



在配備 Apple 晶片的 Mac 上，「系統保安工具程式」會指出整體用戶設定的 macOS 保安狀態，例如啟動 kext 或「系統完整保護」(SIP) 的設定。如果更改保安設定，會大幅降低保安或導致系統更容易遭入侵，用戶必須按住電源按鈕來進入 RecoveryOS (讓惡意軟件無法觸發訊號，只有可實體操作的人類可以觸發)，才能進行更動。因此，配備 Apple 晶片的 Mac 也不要求 (或支援) 韌體密碼，所有重要的變更都已經透過用戶授權來把關。如需更多 SIP 的資訊，請參閱：[系統完整保護](#)。

「完整保安」和「較低保安」可從 RecoveryOS 使用「開機保安工具程式」來設定。但是「寬鬆保安」只能由接受自己的 Mac 保安會大幅下降的人從命令列工具存取。

## 「完整保安」規則

「完整保安」是預設選項，其行為與 iOS 和 iPadOS 相似。下載軟件準備安裝時，macOS 並非使用軟件隨附的全域簽署，而是與用於 iOS 和 iPadOS 的相同 Apple 簽署伺服器通訊，並重新要求一個新的「個人化」簽署。如簽署要求的一部份包含「唯一晶片識別碼 (ECID)」(此案例中為 Apple CPU 專屬的唯一 ID)，該簽署就是個人化簽署。簽署伺服器傳回的簽署會變為唯一簽署，且只有該特定 Apple CPU 可以使用。當「完整保安」規則生效，Boot ROM 和 LLB 會協助確認指定的簽署不僅是由 Apple 簽署，而且是專為此特定 Mac 簽署，本質上就是將該 macOS 版本與該 Mac 綁定。



相較於典型的全域簽署方式，使用網上簽署伺服器還提供了更好的保護以避免還原攻擊。在全域簽署系統中，保安時間起點可能已回滾很多次，但從未見過最新韌體的系統並不知道。例如，相信其現正處於保安 epoch 1 的電腦，會接受保安 epoch 2 的軟件，即使現時的實際保安 epoch 是 5。透過 Apple 晶片網上簽署系統，簽署伺服器可拒絕為並非屬於最新保安 epoch 的軟件建立簽署。

此外，如果攻擊者在保安 epoch 更改後發現漏洞，便無法直接將屬於舊版 epoch 的有漏洞軟件從系統 A 中挑出，然後套用到系統 B 以進行攻擊。屬於舊版 epoch 的有漏洞軟件是針對系統 A 進行個人化，因而協助避免其遭轉移用以攻擊系統 B。在所有機制通力合作下，可更有效保證攻擊者無法刻意將有漏洞的軟件放到 Mac 上，藉此規避最新軟件提供的防護。但是擁有 Mac 管理者用戶名稱和密碼的用戶可隨時選擇最適合其使用案例的保安規則。

## 「較低保安」規則

「較低保安」類似配備 T2 晶片的 Mac (以 Intel 為基礎) 上的「中等保安」，廠商 (此案例中為 Apple) 會為程式碼產生電子簽署來宣告其為該廠商所提供。這設計可協助防止攻擊者插入未簽署的代碼。Apple 將這類簽署稱為「全域」簽署，因為可在任何 Mac 上使用 (目前已設定「較低保安」規則的 Mac)，且次數不限。「較低保安」本身無法抵禦回滾攻擊 (雖然未授權的作業系統變更可能導致用戶資料變為無法存取。如需更多資料，請前往：[配備 Apple 晶片的 Mac 上的核心延伸功能](#))。



除了允許執行舊版 macOS 之外，其他作業會要求使用「較低保安」，這會為用戶的系統保安帶來風險，例如引入第三方核心延伸功能 (kext)。kext 的權限與核心相同，因此第三方 kext 中的任何漏洞都可能導致作業系統遭全面入侵。正因如此，強烈建議開發者在未來配備 Apple 晶片的 Mac 電腦上移除 macOS 中的 kext 支援前，先採用系統延伸功能。即使第三方 kext 已啟用，仍不能將其載入隨選即用核心中，相反地，kext 會合併到輔助核心集合 (AuxKC) 中，這個集合的雜湊值儲存在 LocalPolicy 內，因此這些 kext 需要重新開機。如需更多有關產生 AuxKC 的資料，請參閱：[macOS 的核心延伸功能](#)。

## 「寬鬆保安」規則

「寬鬆保安」適用於接受讓自己的 Mac 處於極度不安全狀態風險的用戶。此模式與配備 T2 晶片的 Mac (以 Intel 為基礎) 之「無保安」模式不同。如使用「寬鬆保安」, 簽署驗證仍會在整個安全啟動鏈中執行, 但是如將規則設為「寬鬆」, 就會告訴 iBoot 應接受本機「安全隔離區」簽署的開機物件, 例如用戶產生的「開機核心集合」(從自訂 XNU 核心來源建立)。如此一來, 「寬鬆保安」也會提供執行任意「完全不受信任作業系統」核心的架構功能。自訂「開機核心集合」或完全不受信任的作業系統在系統上載入時, 某些解密密鑰會變得無法使用。其設計用意是防止完全不受信任的作業系統存取受信任作業系統中的資料。

**重要事項:** Apple 不提供或支援自訂 XNU 核心。



「寬鬆保安」與配備 T2 晶片的 Mac (以 Intel 為基礎) 之「無保安」模式另一個不同之處: 它現在是過去可獨立控制的某些保安降級的先決條件。最值得注意的是, 如要在配備 Apple 晶片的 Mac 上停用「系統完整保護」(SIP), 用戶必須認知到自己是將系統設為「寬鬆保安」。之所以有這個要求, 是因為停用 SIP 總是會讓系統進入核心非常容易遭入侵的狀態。尤其, 如在配備 Apple 晶片的 Mac 上停用 SIP, 便會在產生 AuxKC 期間停用 kext 簽署強制執行, 因此會允許將任意 kext 載入核心記憶體中。我們已改良配備 Apple 晶片的 Mac 上的 SIP, 規則存放區已移出 NVRAM 並移到 LocalPolicy 中。因此, 現在如要停用 SIP, 必須由擁有 LocalPolicy 簽署密鑰存取權的用戶進入 RecoveryOS (按住電源按鈕) 並進行認證。這使得純軟件攻擊者、甚至是實際在場的攻擊者都很難停用 SIP。

從「開機保安工具程式」App 無法降級為「寬鬆保安」。用戶只能在 RecoveryOS 中從「終端機」執行命令列來降級, 例如 `csrutil` (會停用 SIP)。用戶降級後, 發生的這個事件會反映在「開機保安工具程式」中, 因此用戶可輕鬆將保安設為更安全的模式。

**附註:** 配備 Apple 晶片的 Mac 既不需要亦不支援特定的媒體開機規則, 因為從技術層面來看所有開機都是在本機執行。如果用戶選擇從外置媒體開機, 必須先從 RecoveryOS 使用認證的重新開機對該作業系統版本進行個人化。此重新開機會在內置磁碟上製作一個 LocalPolicy 檔案, 用來從儲存在外置媒體上的作業系統執行受信任的開機。這表示從外置媒體開機的設定一律會在每個作業系統上直接啟用, 且已要求用戶授權, 因此不需要其他安全設定。

## LocalPolicy 簽署密鑰的建立與管理

### 建立

一開始在廠內安裝 macOS 時，或在執行連線式清除安裝時，Mac 會從暫時還原 RAM 磁碟執行程式碼以初始化其預設狀態。在此過程中，還原環境將建立一對新的公用密鑰和專用密鑰，分別保存在「安全隔離區」中。專用密鑰稱為**擁有人身份密鑰 (OIK)**。如有任何 OIK 已經存在，則會在此過程中被銷毀。還原環境還會初始化用於「啟用鎖」的密鑰；**即用戶身份密鑰 (UIK)**。該過程的一部份（這對配備 Apple 晶片的 Mac 而言是專有程序）是在為「啟用鎖」要求 UIK 認證時，會包括一組在驗證時在 LocalPolicy 上強制執行的要求限制。如果裝置無法為「啟用鎖」取得 UIK 認證（例如，由於該裝置目前連繫至「尋找我的 Mac」帳戶並且回報為遺失），則該裝置將無法繼續建立 Local Policy。如果向裝置核發了**用戶身份憑證 (ucrt)**，則該 ucrt 在 X.509 v3 擴充套件中包含伺服器所施加的規則限制和用戶要求的規則限制。

成功取得「啟用鎖」/ucrt 後，它會儲存在伺服器端的資料庫中，且還會傳回到裝置。裝置具有 ucrt 後，與 OIK 對應的公用密鑰認證要求會傳送到**基本認證機構 (BAA)** 伺服器。BAA 會使用儲存在 BAA 可取用資料庫中的 ucrt 中的公用密鑰來確認 OIK 認證要求。如果 BAA 可以確認認證，將會驗證公用密鑰，並傳回**擁有人身份憑證 (OIC)**；OIC 由 BAA 簽署並包含儲存在 ucrt 中的限制。OIC 會被傳送回「安全隔離區」。從那時起，只要「安全隔離區」簽署了新的 LocalPolicy，它就會將 OIC 附加到 Image4。LLB 對 BAA 根憑證具有內置信任，這讓其可信任 OIC，也可讓其信任 LocalPolicy 完整簽署。

### RemotePolicy 限制

所有 Image4 檔案（並非只有 Local Policy）都包含對 Image4 資料檔評估設定的限制。這些限制都會使用分葉憑證中的特殊物件識別碼 (OID) 加以編碼。進行簽署評估時，Image4 驗證庫會在憑證中查找特殊憑證限制 OID，然後機械式評估其中指定的限制。限制的形式有以下幾種：

- X 必須存在
- X 必須不存在
- X 必須有指定值

舉例來說，如為「個人化」簽署，憑證限制就會包含「ECID 必須存在」，而如是「全域」簽署，則會包含「ECID 必須不存在」。這些限制的設計旨在確保由指定的密鑰簽署的所有 Image4 檔案，都必須遵守特定要求，以避免產生錯誤簽署的 Image4 資料檔。

在每個 LocalPolicy 中，這些 Image4 憑證限制稱為 **RemotePolicy**。對於不同開機環境的 LocalPolicy，可以有不同的 RemotePolicy。RemotePolicy 用於限制 RecoveryOS LocalPolicy，讓 RecoveryOS 啟動時，行為只能和以「完整保安」啟動一樣。這提高了對 RecoveryOS 開機環境完整性的信任，可在這個環境中更改規則。RemotePolicy 會將 LocalPolicy 限制為包含產生 LocalPolicy 的 Mac 之 ECID，以及儲存在該 Mac 上「安全儲存元件」中的特定「遙距規則」隨機數雜湊值 (rpnh)。僅當對「尋找我的 Mac」和「啟用鎖」採取了如註冊、取消註冊、遙距鎖定和遙距清除之類的操作時，rpnh 以及 RemotePolicy 才會更改。「遙距規則」限制是在用戶身份密鑰 (UIK) 認證時確定和指定的，並已登入到已核發的「用戶身份憑證」(ucrt)。伺服器確定某些「遙距規則」限制，例如 ECID、ChipID 和 BoardID。其設計用意是防止一部裝置為另一部裝置簽署 LocalPolicy 檔案。裝置可能會指定其他「遙距規則」限制，以協助防止在沒有提供取用目前 OIK 所需的本機驗證和裝置鎖鎖之帳戶的遙距驗證之情況下，讓 Local Policy 的保安降級。

### 配備 Apple 晶片的 Mac 之 LocalPolicy 檔案內容

LocalPolicy 是一個由「安全隔離區」簽署的 Image4 檔案。Image4 為 ASN.1 (抽象語法記法 1) DER 編碼資料結構格式，用於描述 Apple 平台上安全啟動鏈物件的相關資料。在 Image4 安全啟動模式中，安裝軟件時會要求藉由向 Apple 簽署伺服器傳送簽署要求來啟用保安規則。如果規則可接受，簽署伺服器會傳回已簽署的 Image4 檔案，其中包含各種 4 字元代碼 (4CC) 序號。開機時 Boot ROM 或 LLB 這類軟件會評估這些已簽署的 Image4 檔案和 4CC。

## 作業系統間的擁有權移交

對「擁有人身份密鑰」(OIK)的取用權限稱為「擁有權」。需有擁有權才能允許用戶在更改規則或軟件後退出 LocalPolicy。OIK 受到與「密封密鑰保護」(SKP) 中所述相同的密鑰階層保護，同時 OIK 受到與「卷宗加密密鑰」(VEK) 相同的「密鑰加密密鑰」(KEK) 保護。這意味着它通常受用戶密碼以及作業系統和規則測量值的保護。Mac 上的所有作業系統只有一個 OIK。因此，在安裝第二個作業系統時，需要第一個作業系統上的用戶明確同意，才能將擁有權移交給第二個作業系統上的用戶。但是，當安裝程式從第一個作業系統執行時，第二個作業系統的用戶尚不存在。在啟動作業系統並執行「設定輔助程式」前，通常不會產生作業系統中的用戶。因此，在配備 Apple 晶片的 Mac 上安裝第二個作業系統時，需要執行兩個新動作：

- 為第二個作業系統建立 LocalPolicy
- 準備「安裝用戶」以移交擁有權

當執行「安裝輔助程式」並針對第二個空白卷宗鎖定安裝時，提示會詢問用戶是否要將目前卷宗中的用戶複製為第二個卷宗的第一個用戶。如果用戶說「好」，則建立的「安裝用戶」實際上是從所選用戶的密碼和硬件密鑰衍生的 KEK，其接着會在傳遞給第二個作業系統時，用來對 OIK 進行加密。然後，從第二個作業系統「安裝輔助程式」中，提示輸入該用戶的密碼，以允許其取用「安全隔離區」中針對新作業系統的 OIK。如果用戶選擇不複製用戶，則「安裝用戶」仍會以相同的方式建立，但是會使用空白密碼，而非用戶密碼。此第二流程會在某些系統管理方案中出現。但是，想要進行多卷宗安裝並以最安全的方式執行擁有權移交的用戶，應一律選擇將用戶從第一個作業系統複製到第二個作業系統。

## 配備 Apple 晶片的 Mac 上之 LocalPolicy

在配備 Apple 晶片的 Mac 上，本機保安規則控制權已委派給在「安全隔離區」中執行的一個應用程式。這個軟件可利用用戶的憑證和主要 CPU 的開機模式，判斷誰可以更改保安規則，以及從哪個開機環境更改。這有助於協助防止惡意軟件透過將規則降級以取得更多權限，從而利用保安規則控制來影響用戶。

## LocalPolicy 資料檔屬性

LocalPolicy 檔案包含一些架構 4CC，這幾乎在所有 Image4 檔案中都會出現，例如主機板或型號 ID (BORD)、表示特定 Apple 晶片 (CHIP) 或唯一晶片識別碼 (ECID)。但是以下的 4CC 只着重於用戶可設定的保安規則。

**附註：**Apple 使用已配對 **One True RecoveryOS (1TR)** 一詞來表示開機進入配對 RecoveryOS (透過按一下並按住實體電源按鈕)。這與一般的 RecoveryOS 開機不一樣，一般的 RecoveryOS 開機可使用 NVRAM 或按兩下並按住實體電源按鈕進行，或可能在開機出現錯誤時發生。按下特定種類的實體按鈕會增強信任，是侵入 macOS 的純軟件攻擊者無法達到的開機環境。

## LocalPolicy 隨機數雜湊值 (lpmh)

- **類型：**OctetString (48)
- **可變環境：**1TR、RecoveryOS、macOS
- **說明：**lpmh 用於 LocalPolicy 的反重播機制。這是 LocalPolicy 隨機數 (LPN) 的 SHA384 雜湊值，儲存在「安全儲存元件」中，且可使用「安全隔離區 Boot ROM」或「安全隔離區」存取。原始隨機數永遠不會向「應用程式處理器」顯示，僅會對 sepOS 顯示。攻擊者如想說服 LLB 他們先前截取的 LocalPolicy 為有效，需將一個值放入「安全儲存元件」，而這個值必須雜湊值為與他們想重播的 LocalPolicy 中的 lpmh 值相同。通常系統上會有一個有效的 LPN (軟件更新期間除外，同時會有兩個有效的 LPN，以便在發生更新錯誤時還原以啟動舊版軟件)。當任何作業系統的任何 LocalPolicy 更改時，所有規則都會以對應「安全儲存元件」中新 LPN 的新 lpmh 值重新簽署。當用戶更改安全設定或使用新的 LocalPolicy 為每個作業系統建立新的作業系統時，就會發生此變更。



### 「遙距規則」隨機數雜湊值 (rpnh)

- **類型:** OctetString (48)
- **可變環境:** 1TR、RecoveryOS、macOS
- **說明:** rpnh 的行為與 lpnh 相同，但是只會在遙距規則更新時隨之更新，例如更改「尋找」註冊狀態時。用戶在其 Mac 上更改「尋找」狀態時，便會發生此變更。

### RecoveryOS 隨機數雜湊值 (ronh)

- **類型:** OctetString (48)
- **可變環境:** 1TR、RecoveryOS、macOS
- **說明:** 此 ronh 的行為與 lpnh 相同，但是只存在於 RecoveryOS 的 LocalPolicy 中。當系統 RecoveryOS 更新時會隨之更新，例如軟件更新時。使用獨立於 lpnh 和 rpnh 的隨機數，因此當「尋找」將裝置設為停用狀態時，可停用現有的作業系統（透過移除其「安全儲存元件」中的 LPN 和 RPN），同時仍讓系統 RecoveryOS 保持可啟動狀態。以此方式，當系統擁有者證明其擁有系統的控制權（透過輸入其用於「尋找」帳戶的 iCloud 密碼）時，便可重新啟用作業系統。當用戶更新系統 RecoveryOS 或建立新的作業系統時，便會發生此更動。

### 下一階段 Image4 資料檔雜湊值 (nsih)

- **類型:** OctetString (48)
- **可變環境:** 1TR、RecoveryOS、macOS
- **說明:** 此 nsih 欄位代表 Image4 資料檔資料結構的 SHA384 雜湊值，描述已啟動的 macOS。macOS Image4 資料檔包含所有開機物件（例如 iBoot、靜態信任快取、裝置樹狀結構、開機核心集和簽署系統卷宗 (SSV) 根雜湊值）的測量值。當系統指示 LLB 啟動指定的 macOS 時，其設計旨在確保 macOS Image4 資料檔的雜湊值附加至在 LocalPolicy 的 nsih 欄位中截取到的 iBoot 相符項目。如此一來，nsih 便能知道用戶是為了哪個作業系統製作 LocalPolicy。因此用戶可在執行軟件更新時，間接更改 nsih 值。

### 輔助核心集 (AuxKC) 規則雜湊值 (auxp)

- **類型:** OctetString (48)
- **可變環境:** macOS
- **說明:** auxp 是用戶授權 kext 列表 (UAKL) 規則的 SHA384 雜湊值。這用於產生 AuxKC 時，協助確保只有用戶授權的 kext 包含在 AuxKC 中。smb2 是設定此欄位的先決條件。用戶從「系統偏好設定」的「保安與私隱」對話框中核准 kext 來更改 UAKL 時，會間接更改 auxp 值。

### 輔助核心集 (AuxKC) Image4 資料檔雜湊值 (auxi)

- **類型:** OctetString (48)
- **可變環境:** macOS
- **說明:** 系統驗證 UAKL 雜湊值與 LocalPolicy 中的 auxp 欄位相符後，會要求由負責 LocalPolicy 簽署作業的「安全隔離區」處理器應用程式簽署 AuxKC。接著，AuxKC Image4 資料檔簽署的 SHA384 雜湊值會放入 LocalPolicy 中，以避免開機時將先前簽署的 AuxKC 與作業系統混合和比對的可能性。如果 iBoot 在 LocalPolicy 中發現 auxi 欄位，便嘗試從儲存空間載入 AuxKC 並驗證其簽署，也會驗證附加至 AuxKC 的 Image4 資料檔雜湊值與 auxi 欄位相符。如果 AuxKC 因任何理由無法載入，系統會在沒有這個開機物件的情況下繼續開機，因此不會載入任何第三方 kext。auxp 欄位是設定 LocalPolicy 中 auxi 欄位的先決條件。用戶從「系統偏好設定」的「保安與私隱」對話框中核准 kext 來更改 UAKL 時，會間接更改 auxi 值。

#### 輔助核心集合 (AuxKC) 收據雜湊值 (auxr)

- 類型: OctetString (48)
- 可變環境: macOS
- 說明: auxr 是 AuxKC 收據的 SHA384 雜湊值, 表示 AuxKC 中所包含的確切一組 kext。AuxKC 收據可以是 UAKL 的子集, 因為如果已知攻擊者使用過的 kext, 即使已獲用戶授權, 仍可將其排除在 AuxKC 之外。此外, 某些可用來破壞用戶核心邊界的 kext 可能導致功能降低, 例如無法使用 Apple Pay 或播放 4K 和 HDR 內容。用戶如想要這些功能, 可選擇加入限制性更高的 AuxKC 包含項目。auxp 欄位是設定 LocalPolicy 中 auxr 欄位的先決條件。用戶從「系統偏好設定」的「保安與私隱」對話框中建立新的 AuxKC 時, 會間接更改 auxr 值。

#### CustomOS Image4 資料檔雜湊值 (coih)

- 類型: OctetString (48)
- 可變環境: 1TR
- 說明: coih 是 CustomOS Image4 資料檔的 SHA384 雜湊。該資料檔的承載資料是由 iBoot (而非 XNU 核心) 用來移轉控制權。當用戶在 1TR 中使用 kmutil configure-boot 命令列工具時, 會間接地更改 coih 值。

#### APFS 卷宗群組 UUID (vuid)

- 類型: OctetString (16)
- 可變環境: 1TR、RecoveryOS、macOS
- 說明: vuid 指明核心應當作根群組的卷宗群組。此欄位主要作用是提供資料並不會用於保安限制。此 vuid 是在用戶製作新的作業系統安裝時間接設定。

#### 密鑰加密密鑰 (KEK) 群組 UUID (kuid)

- 類型: OctetString (16)
- 可變環境: 1TR、RecoveryOS、macOS
- 說明: kuid 指明開機的卷宗。密鑰加密密鑰通常用於「資料保護」。對於每個 LocalPolicy, 密鑰加密密鑰是用來保護 LocalPolicy 簽署密鑰。kuid 是在用戶製作新的作業系統安裝時間接設定。

#### 配對 RecoveryOS 受信任開機規則測量 (prot)。

- 類型: OctetString (48)
- 可變環境: 1TR、RecoveryOS、macOS
- 說明: 配對 RecoveryOS 受信任開機規則測量 (TBPM) 是對 LocalPolicy 的 Image4 資訊檔進行的特殊反覆 SHA384 雜湊值計算, 排除隨機數, 以便得出不隨時間變動的一致測量 (因為 lpmh 這類隨機數會經常更新)。prot 欄位只存在於每個 macOS LocalPolicy 中, 提供配對以指出對應到 macOS LocalPolicy 的 RecoveryOS LocalPolicy。

#### 「安全隔離區」已簽署 RecoveryOS LocalPolicy (hrlp)

- 類型: 布林值
- 可變環境: 1TR、RecoveryOS、macOS
- 說明: hrlp 指出 prot 值 (上述) 是否為「安全隔離區」所簽署 RecoveryOS LocalPolicy 的測量值。如果不是, 那麼 RecoveryOS LocalPolicy 是由負責簽署 macOS Image4 檔案這類項目的 Apple 網上簽署伺服器所簽署。

### 本機作業系統版本 (love)

- **類型:**布林值
- **可變環境:**1TR、RecoveryOS、macOS
- **說明:**love 表示為其建立 LocalPolicy 的作業系統版本。此版本是在 LocalPolicy 建立期間從下一個階段資料檔取得的,用於強制執行 RecoveryOS 配對限制。

### 安全多重開機 (smb0)

- **類型:**布林值
- **可變環境:**1TR、RecoveryOS
- **說明:**如 smb0 存在且為 true,LLB 會允許全域簽署下一階段 Image4 資料檔,而非要求個人化簽署。用戶可透過「開機保安工具程式」或 bputil 來更改此欄位以降級為「較低保安」。

### 安全多重開機 (smb1)

- **類型:**布林值
- **可變環境:**1TR
- **說明:**如果 smb1 存在且為 true,iBoot 會允許使用與 LocalPolicy 相同的密鑰由「安全隔離區」簽署物件(例如自訂核心集合)。smb0 存在是 smb1 存在的先決條件。用戶可以使用命令列工具(例如 csrutil 或 bputil)來更改此欄位以降級為「較低保安」。

### 安全多重開機 (smb2)

- **類型:**布林值
- **可變環境:**1TR
- **說明:**如果 smb2 存在且為 true,iBoot 會允許使用與 LocalPolicy 相同的密鑰由「安全隔離區」簽署輔助核心集合(AuxKC)。smb0 存在是 smb2 存在的先決條件。用戶可使用「開機保安工具程式」或 bputil 來更改此欄位以降級為「較低保安」和啟用第三方 kext。

### 安全多重開機 (smb3)

- **類型:**布林值
- **可變環境:**1TR
- **說明:**如果 smb3 存在且為 true,表示操作裝置的用戶已選擇加入其系統的流動裝置管理(MDM)控制。此欄位的存在讓控制「安全隔離區」處理器應用程式的 LocalPolicy 接受 MDM 認證,而非要求本機用戶認證。用戶可使用「開機保安工具程式」或 bputil 來更改此欄位以啟用第三方 kext 和軟件更新的管理式控制。(在 macOS 11.2 或較新版本中,如果目前保安模式為「完整完全性」,則 MDM 也可以啟動對最新 macOS 版本的更新作業。)

### 安全多重開機 (smb4)

- **類型:**布林值
- **可變環境:**macOS
- **說明:**如果 smb4 存在且為 true,表示裝置已使用 Apple School Manager、Apple Business Manager 或 Apple Business Essentials 選擇加入作業系統的 MDM 控制。此欄位的存在讓控制「安全隔離區」應用程式的 LocalPolicy 接受 MDM 認證,而非要求本機用戶認證。MDM 解決方案偵測到裝置的序號出現在這些服務的任何一項時,此欄位會更改。

### 系統完整保護 (sip0)

- **類型:**64 位元未簽署整數
- **可變環境:**1TR
- **說明:**sip0 值包含現有「系統完整保護」(SIP) 規則位元 (先前儲存在 NVRAM 中)。新的 SIP 規則位元如果只用於 macOS 而沒有用於 LLB, 便會在此處加入 (而非使用如下所示的幾個 LocalPolicy 欄位)。用戶可以從 1TR 使用 csrutil 來更改此欄位以停用 SIP 和降級為「寬鬆保安」。

### 系統完整保護 (sip1)

- **類型:**布林值
- **可變環境:**1TR
- **說明:**如果 sip1 存在且為 true, iBoot 會允許失敗以驗證 SSV 卷宗根雜湊值。用戶可以從 1TR 使用 csrutil 或 bputil 來更改此欄位。

### 系統完整保護 (sip2)

- **類型:**布林值
- **可變環境:**1TR
- **說明:**如果 sip2 存在且為 true, 則 iBoot 不鎖定會將核心記憶體標示為非可寫的可設定文字唯讀區域 (CTRR) 硬件暫存器。用戶可以從 1TR 使用 csrutil 或 bputil 來更改此欄位。

### 系統完整保護 (sip3)

- **類型:**布林值
- **可變環境:**1TR
- **說明:**如果 sip3 存在且為 true, iBoot 就不會強制執行其 boot-args NVRAM 變數的內置允許列表 (強制執行時會過濾傳送至核心的選項)。用戶可以從 1TR 使用 csrutil 或 bputil 來更改此欄位。

### 憑證和 RemotePolicy

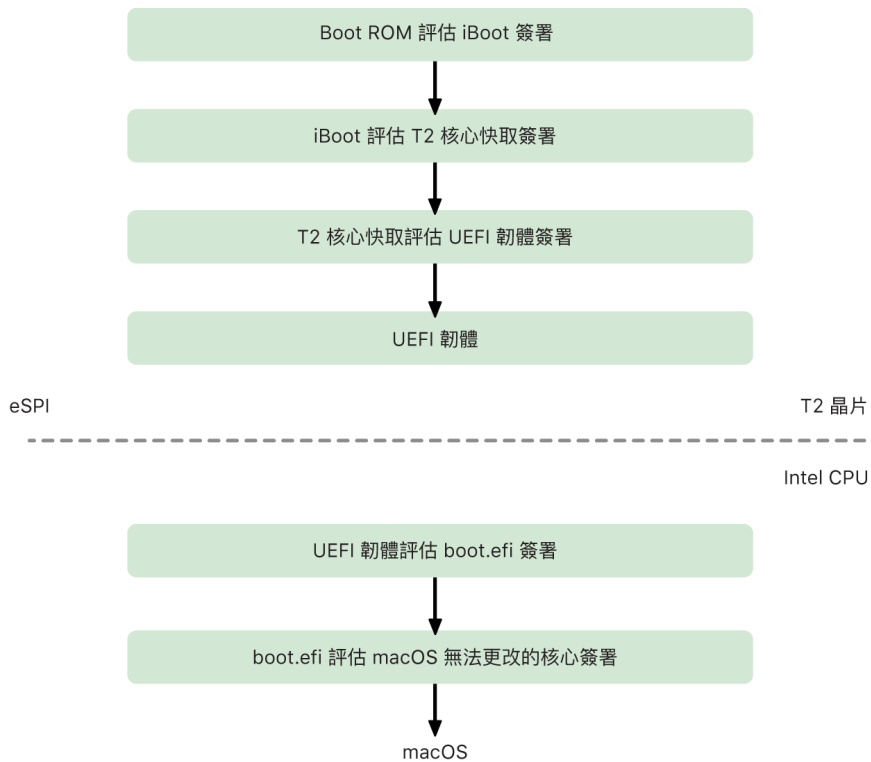
如 [LocalPolicy 簽署密鑰的建立與管理](#) 中所述, LocalPolicy Image4 也包含「擁有人身份憑證」(OIC) 和內嵌 RemotePolicy。

# 以 Intel 為基礎的 Mac 電腦

## 以 Intel 為基礎的 Mac 之開機程序

### 以 Intel 為基礎並配備 Apple T2 保安晶片的 Mac

當以 Intel 為基礎並配備 Apple T2 保安晶片的 Mac 電腦開啟時，晶片會從其 Boot ROM 執行安全啟動，執行方式與 iPhone、iPad 和配備 Apple 晶片的 Mac 相同。這會驗證 iBoot 啟動程式，且是信任鏈中的第一個步驟。iBoot 會檢查 T2 晶片上的核心和核心延伸功能代碼，接着 T2 晶片會檢查 Intel UEFI 韌體。一開始 UEFI 韌體和關聯的簽署只適用於 T2 晶片。



驗證後，UEFI 韌體映像會對映至 T2 晶片記憶體的一部份。此記憶體經由增強型序列周邊介面 (eSPI) 供 Intel CPU 使用。Intel CPU 初次啟動時，會透過 eSPI 從 T2 晶片上已通過完整性檢查、記憶體對映的韌體副本截取 UEFI 韌體。

Intel CPU 上會繼續進行信任鏈評估，由 UEFI 韌體評估 boot.efi (macOS 啟動程式) 的簽署。採用 Intel 技術的 macOS 安全啟動簽署，儲存於與用於 iOS、iPadOS 和 T2 晶片安全啟動相同的 Image4 格式的檔案的程式碼等同於最新 iOS 和 iPadOS 安全啟動實作的強化程式碼。Boot.efi 會驗證稱為 immutablekernel 的新檔案之簽署。當已啟用安全啟動，immutablekernel 檔案代表了啟動 macOS 所需的整套 Apple 核心延伸功能。接手給 immutablekernel 時安全啟動規則會終止，此後 macOS 保安規則 (例如「系統完整保護」和簽署的核心延伸功能) 會生效。

此過程中如發生任何錯誤或失敗，都會導致 Mac 進入還原模式、Apple T2 保安晶片還原模式或 Apple T2 保安晶片裝置韌體升級 (DFU) 模式。

## 以 Intel 為基礎並配備 T2 保安晶片的 Mac 上的 Microsoft Windows

依照預設，支援安全啟動且以 Intel 為基礎的 Mac 只信任 Apple 簽署的內容。但是，為了改進「開機切換」安裝項目的保安，Apple 亦支援 Windows 安全啟動。統一可延伸韌體介面 (UEFI) 韌體包含了 Microsoft Windows Production CA 2011 證書副本，用於認證 Microsoft 啟動程式。

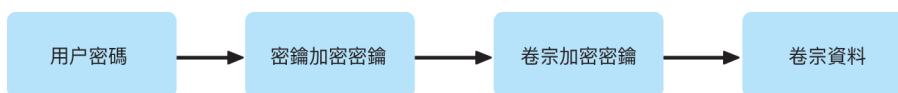
**附註：**目前沒有針對 Microsoft Corporation UEFI CA 2011 (這會允許驗證 Microsoft 合作夥伴所簽署的程式碼) 提供信任。此 UEFI CA 常用於驗證其他作業系統的啟動程式 (如 Linux 變體) 的確實性。

Windows 安全啟動支援並非預設啟用，而是透過「開機切換輔助程式」(BCA) 啟用。當用戶執行 BCA，macOS 會在啟動時重新設定以信任 Microsoft 第一方簽署的程式碼。BCA 完成後，如果 macOS 無法在安全啟動期間通過 Apple 第一方信任評估，UEFI 韌體會嘗試根據 UEFI 安全啟動格式評估物件的信任。如果信任評估成功，Mac 就會繼續執行並啟動 Windows。如果不成功，則 Mac 會進入 RecoveryOS，並通知用戶信任評估失敗。

## 以 Intel 為基礎而未配備 T2 晶片的 Mac 電腦

未配備 T2 晶片並以 Intel 為基礎的 Mac 不支援安全啟動。因此統一可延伸韌體介面 (UEFI) 韌體會從檔案系統載入 macOS 開機程式 (boot.efi) 而不進行驗證，而開機程式會從檔案系統載入核心 (prelinkedkernel) 而不進行驗證。為了保護啟動鏈的完整性，用戶應啟用以下所有保安機制：

- **系統完整保護 (SIP)：**預設啟用，以保護開機程式和核心，防止來自正在運行的 macOS 的惡意寫入。
- **檔案保險箱：**可透過以下兩者啟用檔案保險箱：用戶或流動裝置管理 (MDM) 的管理員。此機制可抵禦實際在場的攻擊者以「目標磁碟模式」來覆寫開機程式。
- **韌體密碼：**啟用方式有兩種：由用戶或 MDM 管理員啟用。這有助防止能防止實際在場的攻擊者啟動替用開機模式，例如 RecoveryOS、單一用戶模式或目標磁碟模式，這些模式可覆寫開機程式。同時也可協助防止從替用媒體開機，如以此方式開機，攻擊者便可執行程式碼來覆寫開機程式。



## 以 Intel 為基礎並配備 Apple T2 保安晶片的 Mac 之開機模式

以 Intel 為基礎並配備 Apple T2 晶片的 Mac 具備多種開機模式，按下 UEFI 韌體或開機程式可識別的按鍵組合便可在開機時進入這些模式。除非在「開機保安工具程式」中將保安規則更改為「無保安」，否則部份開機模式如「單一用戶」模式會無法運作。

模式	按鍵組合	描述
macOS 開機	無	UEFI 韌體會接手至 macOS 開機磁碟 (UEFI 程式) 再接手至 macOS 核心。在啟用「檔案保險箱」的標準 Mac 開機程序中，macOS 開機程式會顯示「登入視窗」介面，並會使用密碼將儲存空間解密。
開機管理程式	Option (⌥)	UEFI 韌體會啟動內置的 UEFI 應用程式，而這個應用程式會向用戶顯示開機裝置選取介面。
目標磁碟模式 (TMD)	T	UEFI 韌體會啟動內置的 UEFI 應用程式，而這個應用程式會將內置儲存裝置顯示為透過 FireWire、Thunderbolt、USB 或三者任意組合 (視 Mac 型號而定) 連接的區塊式原始儲存裝置。
單一用戶模式	Command (⌘) + S	macOS 核心在 launchd 的引數向量中傳送 <code>-s</code> 旗標，然後 launchd 在「系統監視程式」App 的 TTY 建立單一用戶 Shell。 <b>附註：</b> 如果用戶退出 Shell，macOS 會繼續啟動「登入」視窗。
RecoveryOS	Command (⌘) + R	UEFI 韌體在內置儲存裝置上從已簽署的磁碟映像 (.dmg) 檔案載入最小化的 macOS。

模式	按鍵組合	描述
互聯網 RecoveryOS	Option (⌥) + Command (⌘) + R	使用 HTTP 從互聯網下載已簽署的磁碟映像檔。
診斷	D	UEFI 韌體在內置儲存裝置上從已簽署的磁碟映像檔載入最小化的 UEFI 診斷環境。
互聯網診斷	Option (⌥) + D	使用 HTTP 從互聯網下載已簽署的磁碟映像檔。
啟動 Windows	無	如果已使用「開機切換」安裝 Windows，UEFI 韌體會接手給 Windows 開機程式，然後再接手給 Windows 核心。

## 配備 Apple T2 保安晶片的 Mac 之開機保安工具程式

### 概覽

在以 Intel 為基礎並配備 Apple T2 保安晶片的 Mac 上，「開機保安工具程式」會處理許多保安規則設定。開機進入 RecoveryOS 並從「工具程式」選單中選取「開機保安工具程式」，即可取用此工具程式，並保護受支援的保安設定，避免遭攻擊者輕鬆操控。



即使處於「還原」模式也需要認證才能更改重要規則。首次開啟「開機保安工具程式」時，會提示用戶輸入管理員密碼，此密碼必須來自已安裝的主要 macOS，而且此份 macOS 必須連繫至目前啟動的 RecoveryOS。如沒有管理員，必須先建立一個管理員才能更改規則。T2 晶片需要 Mac 電腦在開機當下進入 RecoveryOS，且必須透過以「安全隔離區」支援的憑證進行認證，才能更改規則。保安規則更動有兩個間接要求，RecoveryOS 必須：

- 從直接連接至 T2 晶片的儲存裝置啟動，因為其他裝置上的分割區沒有將「安全隔離區」支援憑證網綁至內置儲存裝置。
- 位處基於 APFS 的卷宗，因為僅在磁碟中「預開機」APFS 卷宗上才會提供支援，來儲存「還原」憑證中傳送至「安全隔離區」的「認證」。HFS plus 格式的卷宗無法使用安全啟動。

此規則只會顯示於以 Intel 為基礎並配備 T2 保安晶片的 Mac 上的「開機保安工具程式」中。雖然大多數使用案例應該都不需要更改安全啟動規則，不過用戶最終可控制其裝置設定，且可根據需要選擇停用或降級 Mac 上的安全啟動功能。

從這個 App 中進行的安全啟動規則變更，只會套用到 Intel 處理器上進行驗證的信任鏈評估。「安全啟動 T2 晶片」選項永遠有效。

安全啟動規則可選用以下三項設定的其中之一：「完整保安」、「中等保安」及「無保安」。「無保安」會徹底停用 Intel 處理器上的安全啟動評估，且允許用戶以其所想的任何方式開機。

### 「完整保安」開機規則

「完整保安」是預設的開機規則，其行為與 iOS 和 iPadOS 或配備 Apple 晶片的 Mac 上的「完整保安」十分相似。下載軟件並準備安裝時，作為簽署要求的一部份，會在簽署中包含唯一晶片識別碼 (ECID) (此案例中為 T2 晶片專屬的唯一 ID)，透過這個簽署進行個人化。簽署伺服器傳回的簽署會變為唯一簽署，且只有該特定 T2 晶片可以使用。統一可延伸韌體介面 (UEFI) 韌體的設計用意是確保在「完整保安」規則生效時，所給予的簽署並非只由 Apple 簽署，而是為此特定的 Mac 簽署，實質上將該版本的 macOS 與此 Mac 相連。這有助於防止回滾攻擊，如同針對配備 Apple 晶片的 Mac 上的「完整保安」說明的情況。

### 中等保安開機規則

「中等保安」開機規則某種程度上類似於傳統 UEFI 安全啟動，廠商 (此例中為 Apple) 會為程式碼產生電子簽署來宣告其為該廠商所提供。這樣可以防止攻擊者插入未簽署的代碼。我們將這類簽署稱為「全域」簽署，因為可在任何 Mac 上使用 (目前已設定「中等保安」規則的 Mac)，且次數不限。無論是 iOS、iPadOS 還是 T2 晶片本身均不支援全域簽署。此設定不會嘗試防止回滾攻擊。

### 媒體開機規則

媒體開機規則只存在於配備 T2 晶片並以 Intel 為基礎的 Mac 上，且獨立於安全啟動規則。因此即便用戶停用安全啟動，也不會更改禁止從非直接連接 T2 晶片的儲存裝置啟動 Mac 的預設行為。(配備 Apple 晶片的 Mac 不需要媒體開機規則。如需更多資料，請參閱：[「啟動磁碟」保安規則控制](#)。)

## 以 Intel 為基礎的 Mac 之韌體密碼保護

以 Intel 為基礎並配備 Apple T2 保安晶片的 Mac 電腦之 macOS，支援使用「韌體密碼」來協助防止在特定 Mac 上對韌體設定進行非故意的修改。「韌體密碼」的設計用意是防止選取替用開機模式，例如開機進入 RecoveryOS 或「單一用戶」模式、從未授權的卷宗開機，或是開機進入「目標磁碟模式」。

**附註：**配備 Apple 晶片的 Mac 不需要韌體密碼，因為其限制的重要韌體功能已移到 RecoveryOS (當「檔案保險箱」啟用時) 中，且 RecoveryOS 要求用戶進行認證才能取用其重要功能。

最基本的韌體密碼模式，在**未配備** T2 晶片並以 Intel 為基礎的 Mac 上，可從 RecoveryOS「韌體密碼工具程式」取用；在以 Intel 為基礎並**配備** T2 晶片的 Mac 上，則需透過「開機保安工具程式」取用。進階選項 (例如每次開機都提示輸入密碼的功能) 可從 macOS 中的 `firmwarepasswd` 命令列工具取用。

設定韌體密碼尤其重要，可降低未配備 T2 晶片並以 Intel 為基礎的 Mac 電腦受到實際在場的攻擊者攻擊之風險。韌體密碼有助於防止攻擊者開機進入 RecoveryOS (如進入便可停用「系統完整保護」(SIP))。透過限制替用媒體啟動，攻擊者便無法從其他作業系統執行有權限的程式碼以攻擊周邊韌體。

提供「韌體密碼」重設機制，以協助忘記密碼的用戶。用戶在開機時按下按鍵組合，就會顯示一組型號專屬的字串，此字串需提供給 AppleCare。AppleCare 會以電子方式簽署通過「統一資源識別碼」(URI) 簽署檢查的資源。如果簽署通過驗證，且內容為特定 Mac 專用，UEFI 韌體便會移除韌體密碼。



如用戶想透過軟件方式親自移除其韌體密碼(而非依靠其他人),`-disable-reset-capability` 選項已加至 macOS 10.15 的 `firmwarepasswd` 命令列工具。設定此選項前,用戶必須了解當忘記密碼且需移除時,用戶需自行承擔達成此目的所需的主機板更換費用。機構如想保護其 Mac 電腦,防禦來自外部攻擊者和員工的攻擊,則必須在組織所屬系統上設定韌體密碼。此操作可在裝置上透過以下任何方式完成:

- 配置時,手動使用 `firmwarepasswd` 命令列工具
- 配備使用 `firmwarepasswd` 命令列工具的第三方管理工具
- 使用流動裝置管理 (MDM)

## 以 Intel 為基礎的 Mac 之 RecoveryOS 和診斷環境

### RecoveryOS

RecoveryOS 與 macOS 主體完全獨立,且所有內容儲存於稱為 `BaseSystem.dmg` 的磁碟映像檔案。同時亦有關聯的 `BaseSystem.chunklist` 用來驗證 `BaseSystem.dmg` 的完整性。區塊列表是 `BaseSystem.dmg` 的 10 MB 區塊的一系列雜湊值。統一可延伸韌體介面 (UEFI) 韌體會評估區塊列表檔案的簽署,然後為 `BaseSystem.dmg` 的區塊雜湊值進行逐個評估。這可協助確保其與區塊列表顯示的簽署內容相符。如果這些雜湊值中有任何一個不相符,便會中止從本機 RecoveryOS 開機,然後 UEFI 韌體會改為嘗試從互聯網 RecoveryOS 開機。

如果驗證成功完成,UEFI 韌體會將 `BaseSystem.dmg` 裝載為 RAM 磁碟,並啟動其中的 `boot.efi` 檔案。UEFI 韌體不需要對 `boot.efi` 執行特定檢查,`boot.efi` 也不需要檢查核心,因為作業系統的完整內容(這些元素只是其子集)已通過完整性檢查。

### Apple 診斷

啟動本機診斷環境的程序大部份與啟動 RecoveryOS 相同。系統會使用獨立的 `AppleDiagnostics.dmg` 和 `AppleDiagnostics.chunklist` 檔案,但是驗證方式與 `BaseSystem` 檔案相同。無需啟動 `boot.efi`,UEFI 韌體會啟動磁碟映像(.dmg 檔案)中的 `diags.efi` 檔案,然後這個檔案會負責呼叫其他各種 UEFI 驅動程式,這些驅動程式可以連接並檢查硬件中的錯誤。

### 互聯網 RecoveryOS 和診斷環境

如果啟動本機還原或診斷環境時發生錯誤,UEFI 韌體會嘗試改從互聯網下載映像檔。(用戶也可使用啟動時按下特殊按鍵序列的方法,指定要求從互聯網載取映像檔)。從「OS 還原伺服器」下載的磁碟映像和區塊列表的完整性驗證方式,與驗證從儲存裝置取得的映像之方式相同。

雖然連線至「OS 還原伺服器」時是使用 HTTP,但下載的完整內容仍會進行上文所說明的完整性檢查,因此受到保護而免於遭擁有網絡控制權的攻擊者操縱。當單獨的區塊沒有通過完整性驗證,系統會先從 OS 還原伺服器重新要求該區塊 11 次,然後再放棄並顯示錯誤。

Mac 電腦的互聯網還原和診斷模式是於 2011 年加入,當時決定最好使用較簡單的 HTTP 傳輸,以及使用區塊列表機制來處理內容認證,而非在 UEFI 韌體中執行較複雜的 HTTPS 功能,因此增加了韌體的攻擊面。

# iOS、iPadOS 和 macOS 的簽署系統卷宗保安

在 macOS 10.15，Apple 引入了唯讀系統卷宗，這是供系統內容專用的隔離卷宗。macOS 11 則為**簽署系統卷宗 (SSV)**的系統內容加入了高強度的加密編譯保護。SSV 具備核心機制，可在執行時驗證系統內容的完整性，以及拒絕沒有 Apple 有效加密編譯簽署的任何資料（程式碼與非程式碼）。從 iOS 15 和 iPadOS 15 開始，iOS 和 iPadOS 裝置上的系統卷宗也取得簽署系統卷宗的加密保護。

SSV 有助於防止竄改屬於作業系統一部份的任何 Apple 軟件，也可讓 macOS 軟件更新更可靠且更安全。且因為 SSV 使用「Apple 檔案系統」(APFS) 快照，如果更新無法執行，可還原舊版系統而不需要重新安裝。

引入此功能後，APFS 在內置儲存裝置上使用非加密編譯總和檢查碼，因此提供了檔案系統後設資料完整性。SSV 加入了加密編譯雜湊值，讓其可延伸至包含檔案資料的所有位元組，因而加強了完整性機制。內置儲存裝置（包括檔案系統後設資料）中的資料在讀取路徑中以加密編譯方式進行雜湊值處理，而雜湊值之後會與檔案系統後設資料中的預期值做比較。如結果不一致，系統會假設資料已遭到竄改，且不會傳回給提出要求的軟件。

每個 SSV SHA256 雜湊值都儲存在主檔案系統後設資料樹狀結構中，而這個樹狀結構本身就經過雜湊值處理。樹狀結構的每個節點都經過遞迴式驗證，驗證其子項目雜湊值的完整性，類似二位元雜湊值 (Merkle) 樹狀結構；因此根節點的雜湊值（稱為**印章**）會包含 SSV 中資料的所有位元組，這表示加密編譯簽署涵蓋整個系統卷宗。

安裝和更新 macOS 期間，印章會從裝置上的檔案系統進行重新運算，並根據 Apple 簽署的測量值驗證其測量結果。在配備 Apple 晶片的 Mac 上，將控制權傳送給核心之前，啟動程式會驗證印章。在以 Intel 為基礎並配備 Apple T2 保安晶片的 Mac 上，啟動程式會將測量值和簽署轉送至核心，然後核心會直接在裝載根檔案系統之前驗證印章。在這兩種情況下，如果驗證失敗，開機程序都會停止，且系統會提示用戶重新安裝 macOS。此程序會在每次開機時重複執行，除非用戶選擇進入較低的保安模式，且已分別選擇停用簽署系統卷宗。

在 iOS 和 iPadOS 軟件更新期間，系統卷宗會以類似的方式準備和重新計算。在允許裝置設備啟動核心之前，iOS 和 iPadOS Bootloader 會驗證印章是否完好無損並且符合 Apple 簽署值。開機時如不相符，系統會提示用戶更新裝置上的系統軟件。用戶無法在 iOS 和 iPadOS 上停用已簽署之系統卷宗的保護機制。

## SSV 和程式碼簽署

程式碼簽署仍存在並由核心強制執行。從內置儲存裝置讀取任何位元組時，簽署系統卷宗可提供保護。相對地，當 Mach 物件記憶體對映到可執行檔時，程式碼簽署可提供保護。SSV 和程式碼簽署都能保護所有讀取和執行路徑上的可執行程式碼。

## SSV 和檔案保險箱

在 macOS 11 中，SSV 為系統內容提供了等效的靜態保護，因此系統卷宗不再需要加密。對靜態檔案系統進行的任何修改，都會在讀取檔案系統時偵測到。如果用戶已啟用「檔案保險箱」，資料卷宗上的用戶內容仍會以用戶提供的密碼加密。

如果用戶選擇停用 SSV，靜態時的系統將變得容易遭到竄改，且此處的竄改可能讓攻擊者得以在系統下次啟動時截取已加密的用戶資料。因此，如果「檔案保險箱」已啟用，系統將不會允許用戶停用 SSV。兩種卷宗的靜態保護功能啟用或停用狀態必須一致。

在 macOS 10.15 或較早版本中，「檔案保險箱」使用密鑰（受到用戶提供的密碼保護）加密用戶和系統內容，藉此保護靜態作業系統軟件。此功能會保護裝置，以防止可實際取用裝置的攻擊者存取或有效地修改包含系統軟件的檔案系統。

## SSV 和配備 Apple T2 保安晶片的 Mac

在配備 Apple T2 保安晶片的 Mac 上，只有 macOS 本身受到 SSV 保護。在 T2 晶片上執行和驗證 macOS 的軟件受到安全啟動保護。

## 保安軟件更新

保安是一個過程；可靠地啟動出廠時安裝的作業系統版本並不足夠，必須存在可快速且安全地取得最新保安更新的機制。Apple 會定期釋出軟件更新以解決新出現的保安顧慮。iOS 和 iPadOS 裝置的用戶會在裝置上收到更新通知。Mac 用戶可於「系統偏好設定」中取用。更新會經無線方式傳送，來迅速採用最新的保安修正。

## 更新程序

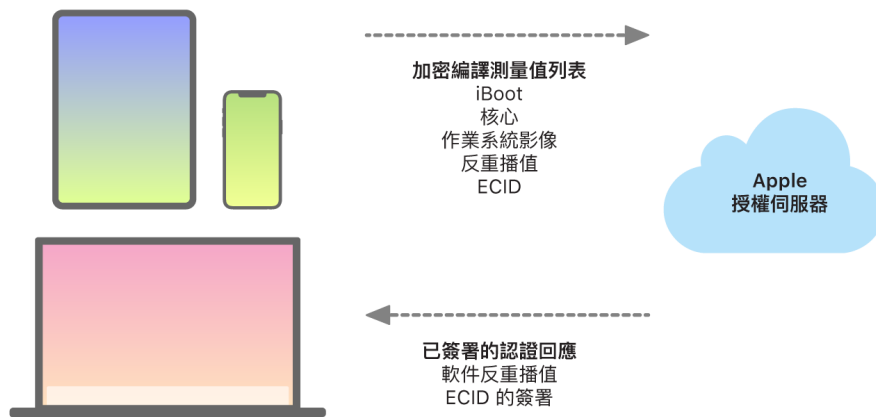
更新程序會使用與安全啟動所用之相同的硬件式信任根，其設計僅會安裝 Apple 簽署的編碼。此外，更新程序也會使用系統軟件授權來確保只有經 Apple 主動簽署的作業系統版本副本才可安裝在 iOS 和 iPadOS 裝置，或是「開機保安工具程式」中「完整保安」設定為安全啟動規則的 Mac 電腦上。有了這些恰當的安全程序，Apple 便可停止簽署包含已知漏洞的較舊作業系統版本，並可協助防止降級的攻擊。

為取得更高的軟件更新保安，當要升級的裝置實際連接到 Mac 時，便會下載 iOS 或 iPadOS 的完整副本並安裝。但是無線傳輸 (OTA) 的軟件更新只會下載完成更新所需的元件而不會下載整個作業系統，藉此改進網絡效率。再者，軟件更新可在執行 macOS 10.13 或較新版本並已開啟「內容快取」的 Mac 上進行快取，如此 iOS 和 iPadOS 裝置便無須透過互聯網重新下載必要的更新。(他們仍需連上 Apple 伺服器來完成更新程序。)

## 個人化的更新程序

在升級和更新期間，會連接 Apple 安裝授權伺服器，並包含以下資料：要安裝之安裝套件中的各部份加密編譯測量值列表 (如 iBoot、核心及作業系統映像檔)、隨機的反重播值 (隨機數) 以及裝置專屬的唯一晶片識別碼 (ECID)。

授權伺服器會將提供的測量值列表與允許安裝的版本進行比較，如找到相符項目，便會將 ECID 加入到測量值中並對結果進行簽署。伺服器會將完整的一組已簽署資料傳遞至裝置，作為升級程序的一部份。加入 ECID 可為要求的裝置「個人化」授權作業。藉由只對已知的測量值授權和簽署，伺服器可協助確保更新的內容與 Apple 所提供的完全相同。



開機時間的信任鏈評估程序會驗證該次簽署是否來自 Apple，並確認從儲存裝置載入之項目測量值在結合裝置的 ECID 後，是否與該簽署所涵蓋的內容相符。這些步驟的設計目的是確保在支援個人化的裝置上，授權是針對特定裝置進行，且較舊的作業系統或韌體版本無法從一部裝置複製到另一部裝置。隨機數可協助阻止攻擊者儲存伺服器的回應，並協助阻止攻擊者使用該回應來破壞裝置，或以其他方式篡改系統軟件。

由於需進行個人化程序，因此任何採用 Apple 設計晶片的裝置一律需要透過網絡連線至 Apple 以進行更新，包含以 Intel 為基礎並配備 Apple T2 保安晶片的 Mac。

最後，用戶的資料卷宗絕不會在軟件更新期間裝載，以協助防止該卷宗在更新期間被讀取或寫入任何項目。

在配備「安全隔離區」的裝置上，硬件會以類似方式使用系統軟件授權來檢查軟件的完整性，且其設計用意是阻止降級安裝作業。

## 作業系統完整性

Apple 設計的作業系統以保安為重點。這樣的設計包硬件信任根 (用來啟用安全啟動) 以及快速且安全的保安軟件更新程序。Apple 作業系統也採用特製的晶片式硬件功能,可協助防止系統執行期間遭到惡意利用。這些執行階段功能可保護受信任程式碼在執行時的完整性。簡而言之,Apple 作業系統軟件可幫助緩解攻擊和善用技術,——無論源自於惡意 App、網絡或經由任何其他管道都能應付。此處列出的防護措施可於採用受支援 Apple 設計 SoC 的裝置上使用,包含 iOS、iPadOS、tvOS、watchOS,現在還有配備 Apple 晶片的 Mac 上的 macOS。

功能	A10	A11、S3	A12、S4	A13、S5	A14、A15、S6、S7	M1 系列
核心完整保護	✓	✓	✓	✓	✓	✓
快速權限取用限制		✓	✓	✓	✓	✓
系統協同處理器完整保護			✓	✓	✓	✓
指標認證碼			✓	✓	✓	✓
頁面保護層		✓	✓	✓	✓	請參閱下方的附註。

附註:「頁面保護層」(PPL) 要求平台只執行已簽署且受信任的程式碼;此保安模式不適用 macOS 上。

### 核心完整保護

作業系統核心完成初始化後,會啟用「核心完整保護」(KIP)以協助防止核心與驅動程式程式碼遭修改。記憶體控制器提供一個受保護的實體記憶體區域,iBoot 會用此區域來載入核心與核心延伸功能。啟動完成後,記憶體控制器會拒絕對受保護的實體記憶體區域進行寫入。「應用程式處理器」的「記憶體管理單元」(MMU)已設定為協助防止從受保護記憶體區域外的實體記憶體對映特權碼,以及協助防止核心記憶體區域內的實體記憶體可寫入對映。

為了防止重新設定,用於啟用 KIP 的硬件會在開機程序完成後被鎖定。

### 快速權限取用限制

自 Apple A11 仿生晶片和 S3 SoC 開始,引入了全新的硬件原語。這個原語(「快速權限取用限制」)包含一個 CPU 暫存器,可快速限制每個執行緒的權限。透過「快速權限取用限制」(又稱為 APRR 暫存器),支援的作業系統可以移除記憶體中的執行權限,而不會造成系統呼叫的額外負荷和分頁表清查或排清。這些暫存器提供了額外一層減緩機制,可應付來自網絡的攻擊,尤其是任何即時編譯(just-in-time compiled)程式碼,因為記憶體在遭讀取和可寫入的同時無法有效執行。

### 系統協同處理器完整保護

協同處理器韌體處理許多重要系統任務,例如「安全隔離區」、影像感應器處理器以及動作協同處理器。因此其保安是整套系統保安的關鍵所在。為避免協同處理器韌體遭修改,Apple 採用**系統協同處理器完整保護(SCIP)**機制。

SCIP 的運作方式很類似「核心完整保護」(KIP):在開機時,iBoot 會將每個協同處理器的韌體載入受保護的記憶體區域(此記憶體區域是預先保留且與 KIP 區域隔離)。iBoot 會設定每個協同處理器的記憶體單元,以協助防止以下情況:

- 受保護的記憶體區域部份外的可執行對映
- 受保護的記憶體區域部份內的可寫入對映

在開機時,如要設定「安全隔離區」的 SCIP,系統會使用「安全隔離區」的作業系統。開機程序完成後,用於啟用 SCIP 的硬件會被鎖定。其設計用意是防止重新設定。

## 指標認證碼

指標認證碼 (PAC) 用於防止記憶體損毀錯誤遭惡意利用。系統軟件和內置的 App 會使用 PAC 來協助防止修改函式指標和傳回地址 (程式碼指標)。PAC 使用五個秘密的 128 位元值來簽署核心指示和資料, 且每個用戶空間程序都有自己的 B 密鑰。系統會對項目進行「加鹽」處理和簽署, 如下所示。

項目	索引鍵	鹽值
函式傳回地址	IB	儲存地址
函式指標	IA	0
區塊調用函式	IA	儲存地址
Objective-C 方法快取	IB	儲存地址 + 類別 + 選擇器
C++ V-Table 輸入項目	IA	儲存地址 + 雜湊值 (雜湊值方法名稱)
計算 Goto 標籤	IA	雜湊值 (函式名稱)
核心討論串狀態	GA	•
用戶討論串狀態暫存器	IA	儲存地址
C++ V-Table 指標	DA	0

簽署值儲存於 64 位元指標上方的未使用填充位元。使用前系統會驗證簽署, 亦會還原填充位元來協助確認指標地址可以執行。驗證失敗會導致中止。此驗證增加了多種攻擊的難度, 例如會試圖操縱儲存在疊放上的函式傳回地址、藉此惡意誘使裝置執行現有程式碼的返回導向程式設計 (ROP) 攻擊。

## 頁面保護層

iOS、iPadOS 和 watchOS 的「頁面保護層」(PPL) 的設計用意是防止用戶空間程式碼在簽署驗證完成後遭修改。PPL 建置在「核心完整保護」和「快速權限取用限制」之上, 可管理分頁表權限覆蓋, 以便確保只有 PPL 可變更包含用戶程式碼和分頁表的受保護頁面。系統可藉由支援全系統程式碼完整性之執行來大幅減少攻擊面, 即使當面對遭入侵的核心也適用。這個防護機制並未在 macOS 上提供, 因為 PPL 只適用於所有執行的程式碼都必須經過簽署的系統。

# 其他 macOS 系統保安功能

## 其他 macOS 系統保安功能

macOS 可在更廣泛的硬件上執行 (例如採用 Intel CPU、採用 Intel CPU 並配搭 Apple T2 保安晶片, 以及配備 Apple 晶片 SoC 的硬件), 且支援各種一般用途運算使用案例。有些用戶僅使用基本的預先安裝 App 或可從 App Store 取得的 App, 而另一些用戶則是核心駭客, 他們需要停用差不多所有平台保護機制, 以便可以最高信任層級來執行和測試其執行程式碼。大部份的用戶則介於兩者之間, 其中有許多人擁有要求不同取用層級的周邊設備和軟件。Apple 設計的 macOS 平台採用了硬件、軟件與服務的整合作法, 此平台的設計為內置保安, 且簡化了設定、部署和管理的操作, 不過也保留了用戶期望的可設定性。macOS 也包含 IT 專業人員所需的重要安全技術, 有助於保護公司資料及在安全的公司網絡環境內進行整合。

下列功能支援和協助保護 macOS 用戶的不同需求。包括:

- 簽署系統卷宗保安
- 系統完整保護
- 信任快取
- 周邊設備保護
- Rosetta 2 (自動轉譯) 支援和配備 Apple 晶片的 Mac 之保安
- DMA 支援與保護
- 核心延伸功能 (kext) 支援與保安
- Option ROM 支援與保安
- 以 Intel 為基礎的 Mac 電腦之 UEFI 韌體保安

## 系統完整保護

macOS 的「**系統完整保護**」(SIP) 功能可利用核心權限來限制重要系統檔案的可寫性。在配備 Apple 晶片的 Mac 上, 這是獨立於硬件式「核心完整保護」(KIP) 的額外功能, 可防止記憶體中的核心遭修改。系統利用強制存取權限控制技術來提供此功能以及其他核心層級保護, 包括「沙盒」和 Data Vault 在內。

### 強制性存取控制

macOS 使用強制存取權限控制 (無法覆蓋的規則, 設定了開發者建立的安全限制)。此方法與自由取用控制不同, 後者允許用戶根據自己的喜好凌駕保安規則。

強制性存取控制不為用戶所見, 但這是幫助啟用多個重要功能的基礎技術, 其中包括沙盒處理、分級保護控制、管理偏好設定、副檔名和「系統完整保護」。

### 系統完整保護

**系統完整保護**會在特定的重要檔案系統位置將元件限制為唯讀, 以協助防止惡意程式碼修改檔案系統。「系統完整保護」是每部電腦專屬的設定, 當用戶升級至 OS X 10.11 或較新版本時預設為啟用。在以 Intel 為基礎的 Mac 上, 如停用此功能會移除實體儲存裝置上對所有分割區的保護。macOS 將此保安規則套用到系統上執行的所有程序, 無論是否以沙盒執行或具有管理權限。

## 信任快取

安全啟動鏈包含的其中一個物件為靜態信任快取，這是由簽署系統卷宗主控的所有 Mach-O 二進位檔的受信任記錄。每個 Mach-O 都以一個程式碼目錄雜湊值代表。為進行有效率的搜尋，這些雜湊值會先經過排序再插入信任快取中。程式碼目錄是 `codesign(1)` 執行的簽署作業所產生的結果。為了強制執行信任快取，SIP 需要保持啟用狀態。如要在配備 Apple 晶片的 Mac 上停用信任快取強制執行，安全啟動必須設為「寬鬆保安」。

當二進位檔執行時（無論是繁衍新程序還是將可執行程式碼對映至現有程序的過程），系統都會截取其程式碼目錄並進行雜湊值處理。如果產生的雜湊值出現在信任快取中，為該二進位檔建立的可執行對映就會獲得平台權限，也就是說，該檔案可能擁有任何授權，且不需要進一步驗證簽署的真實性就能執行。以 Intel 為基礎的 Mac 情況則形成對比，簽署該二進位檔的 Apple 憑證會將平台權限傳達至作業系統內容。（這個憑證不會限制二進位檔可擁有的授權。）

非平台二進位檔（例如通過公證的第三方程式碼）必須具備有效的憑證才能執行，而且其可擁有的授權受限於 Apple 開發者計劃核發給開發者的簽署描述檔。

在 macOS 內遞送的所有二進位檔都是透過**平台識別碼**簽署。在配備 Apple 晶片的 Mac 上，這個識別碼用於指出，即使二進位檔已由 Apple 簽署，其程式碼目錄雜湊值仍必須存在於信任快取中才能執行。在以 Intel 為基礎的 Mac 上，平台識別碼用於對舊版 macOS 中的二進位檔執行針對性撤銷，此針對性撤銷有助於防止這些二進位檔在新版本上執行。

靜態信任快取會將一組二進位檔完全鎖定至指定的 macOS 版本。此行為可協助防止舊版作業系統中 Apple 合法簽署的二進位檔引入新的版本中，讓攻擊者有機可乘。

### 在作業系統之外遞送的平台程式碼

Apple 提供一些非透過平台識別碼簽署的二進位檔，例如 Xcode 和開發工具疊放。即使如此，在配備 Apple 晶片和配備 T2 晶片的 Mac 上，系統仍允許這類二進位檔以平台權限執行。由於這個平台軟件是獨立於 macOS 進行遞送，因此不受限於靜態信任快取所施加的撤銷行為。

### 可載入的信任快取

Apple 透過**可載入的信任快取**遞送某些軟件套件。這些快取的資料結構與靜態信任快取相同。但是儘管只有一個靜態信任快取，且核心早期初始化完成後其內容總是保證鎖定在唯讀範圍中，可載入的信任快取仍會在執行時加入系統中。

認證這些信任快取的機制，與認證開機韌體（使用 Apple 信任的簽署服務作個人化）或全域簽署物件（其簽署不會將其與特定裝置綁定）的機制相同。

個人化信任快取的一個範例是，會隨着配備 Apple 晶片的 Mac 上用於執行診斷的磁碟映像一起提供的快取。這個信任快取經過個人化處理並隨着磁碟映像提供，且會在開機進入診斷模式時載入目標 Mac 電腦的核心中。信任快取可讓磁碟映像內的軟件以平台權限執行。

一個全域簽署信任快取的範例會隨着 macOS 軟件更新一起提供。這個信任快取允許軟件更新中的一個程式碼區塊（**更新核心**）以平台權限執行。主機系統缺乏在不同版本間以相同方式執行的能力，因此交由更新核心執行軟件更新所需的所有工作。

## Mac 電腦的周邊處理器保安

所有現代運算系統均配備多個內置周邊處理器，專門處理網絡、繪圖、電力管理等等。這些周邊處理器通常為單一用途，且功能遠不如主要 CPU 強大。內置的周邊處理器如沒有實施充分的安全機制，就會成為攻擊者的更容易下手的攻擊目標，然後持續感染作業系統。如有周邊處理器韌體感染，攻擊者便能鎖定主要 CPU 上的軟件為目標，或是直接截取敏感資料（例如以太网網絡裝置可查看未加密封包的內容）。

Apple 盡可能地致力減少必要周邊處理器的數量，並避免採用需要韌體的設計。但在獨立處理器必須有專屬韌體的情況下，會採用保護機制來協助確保攻擊者無法持續攻擊該處理器。這可以透過以下兩種方式之一來驗證處理器：

- 執行處理器，讓其在啟動時從主要 CPU 下載經驗證的韌體
- 讓周邊處理器執行專屬的安全啟動鏈，以在每次 Mac 開機時都會驗證周邊處理器韌體

Apple 與廠商合作審核其實施項目，並加強其設計以包括所需的屬性，例如：

- 確保最低加密強度
- 確保強制撤銷已知惡意的韌體
- 停用除錯介面
- 使用儲存在 Apple 控制的「硬件安全模組」（HSM）中的加密密鑰對韌體進行簽署

近年來 Apple 與幾家外部廠商通力合作，採用與 Apple 晶片所使用的相同「Image4」資料架構、驗證碼及簽署基礎架構。

如果無記憶體操作或記憶體加安全啟動都不是選項，則設計會要求在對持久性記憶體進行更新之前，必須對韌體更新進行加密簽署和驗證。

## 配備 Apple 晶片的 Mac 上之 Rosetta 2

配備 Apple 晶片的 Mac 可執行使用 Rosetta 2 轉譯機制來針對 x86\_64 指令集編譯的程式碼。提供兩種類型的轉譯：即時和提前。

### 即時轉譯

即時 (JIT) 轉譯流程中，系統會在映像執行路徑早期階段識別 x86\_64 Mach 物件。遇到這些映像時，核心會將控制權轉移給特殊的 Rosetta 轉譯虛設常式，而非動態連結編輯器 `dylld(1)`。接着這個轉譯虛設常式會在映像執行期間轉譯 x86\_64 頁面。這項轉譯作業完全在程序中進行。核心仍會根據頁面發生錯誤時附加至二進位檔的程式碼簽署，驗證每個 x86\_64 頁面的程式碼雜湊值。如雜湊值不相符，核心就會強制執行適用於該程序的修復規則。

### 提前轉譯

如採用提前 (AOT) 轉譯路徑，系統認為該程式碼的回應能力最佳時，就會從儲存體讀取 x86\_64 二進位檔。轉譯完的成品會作為特殊類型的 Mach 物件檔案寫入儲存體中。該檔案類似可執行的映像，但是系統會將其標記以指出它是轉譯另一個映像所產生的成品。

在這個模式中，AOT 成品會從原始的 x86\_64 可執行映像衍生出所有識別資料。為了強制這種綁定關係，有特殊權限的用戶空間實體會使用裝置專屬的密鑰（受到「安全隔離區」管理）來簽署轉譯成品。這個密鑰只會發佈給有特殊權限的用戶空間實體，而系統會利用受限制的權限來識別這個實體。為了轉譯成品製作的程式碼目錄中，包含原始 x86\_64 可執行映像的程式碼目錄雜湊值。轉譯成品本身上的簽署也稱為**補充簽署**。



AOT 流程的開始方式類似 JIT 流程，核心會將控制權轉移給 Rosetta 執行階段，而非動態連結編輯器 dyld(1)。但是接着 Rosetta 執行階段會傳送程序間通訊 (IPC) 查詢給 Rosetta 系統服務，詢問目前的可執行映像是否有可用的 AOT 轉譯。如果有找到，Rosetta 服務會提供一個控制代碼給該轉譯，再對映到程序中並執行。執行期間，核心會強制執行轉譯成品 (藉由根植在裝置專屬簽署密鑰中的簽署進行認證) 的程式碼目錄雜湊值。這項程序與原始 x86\_64 映像的程式碼目錄雜湊值無關。

轉譯後的成品會儲存在 Data Vault 中；除了 Rosetta 服務以外，任何實體都不能在執行階段存取 Data Vault。Rosetta 服務藉由分發唯讀檔案描述元給個別轉譯成品；這樣可限制存取 AOT 成品快取。這個服務的程序間通訊和從屬的磁碟使用量會刻意維持在極小的範圍內，藉此限制其攻擊面。

如果原始 x86\_64 映像的程式碼目錄雜湊值不符合編碼為 AOT 轉譯成品的簽署，系統就會將此結果視為等同於無效的程式碼簽署，並採取適當的強制措施。

如果遙距程序向核心查詢 AOT 轉譯可執行檔的權限或其他程式碼識別屬性，則會傳回原始 x86\_64 映像的識別屬性。

## 靜態信任快取內容

macOS 11 或較新版本隨附 Mach「厚實」二進位檔，其中包含 x86\_64 和 arm64 電腦程式碼的配量。在配備 Apple 晶片的 Mac 上，用戶可選擇透過 Rosetta 流程執行系統二進位檔的 x86\_64 配量，例如需載入不含原生 arm64 變體的外掛模組。為支援此作法，macOS 隨附的靜態信任快取通常包含每個 Mach 物件檔案的三個程式碼目錄雜湊值。

- arm64 配量的程式碼目錄雜湊值
- x86\_64 配量的程式碼目錄雜湊值
- x86\_64 配量之 AOT 轉譯的程式碼目錄雜湊值

Rosetta AOT 轉譯程序具確定性，因為它會為任何提供的輸入重製相同的輸出，無論轉譯何時執行或是在哪個裝置上執行結果都一樣。

建立 macOS 期間，每個 Mach 物件檔案都會經歷與建立中的 macOS 版本相關聯的 Rosetta AOT 轉譯流程，藉此將程式碼目錄雜湊值記錄在信任快取中。為求效率，實際的轉譯產品不會隨作業系統提供，且會在用戶提出要求時隨需要重新建構。

當 x86\_64 映像配備 Apple 晶片的 Mac 上執行時，如果該映像的程式碼目錄雜湊值位於靜態信任快取中，所產生 AOT 成品的程式碼目錄雜湊值也預期會存在於靜態信任快取中。這類產品沒有經過裝置專屬密鑰簽署，因為簽署管理中心根植在 Apple 安全啟動鏈中。

## 未簽署的 x86\_64 程式碼

配備 Apple 晶片的 Mac 不允許原生 arm64 程式碼在沒有附加有效簽署的情況下執行。這個簽署可以像「隨機操作」程式碼簽署 (cf. codesign(1)) 一樣簡單，不包含來自非對稱式密鑰組秘密部份的任何實際的識別資料 (只是二進位檔的未認證測量值)。

為求二進位檔相容性，系統允許轉譯的 x86\_64 程式碼在沒有簽署的情況下透過 Rosetta 執行。不會有任何識別資料透過裝置專用的「安全隔離區」簽署程序傳達這個程式碼中，且其執行限制與在以 Intel 為基礎的 Mac 上執行的原生未簽署程式碼完全一致。

## Mac 電腦的直接記憶體存取保護

為了達成高速度介面 (例如 PCIe、FireWire、Thunderbolt 和 USB) 的高輸送量，電腦必須支援周邊設備的直接記憶體存取 (DMA)。也就是說，周邊設備必須能讀取和寫入 RAM，而無需 CPU 持續參與。自 2012 年起 Mac 電腦已實施多種技術以保護 DMA，因此具備了個人電腦上最優異、最完善的一套 DMA 保護機制。

### 配備 Apple 晶片的 Mac 的直接記憶體存取保護

Apple 系統單晶片針對系統中的每個 DMA 代理程式都包含一個「輸入/輸出記憶體管理單元」(IOMMU)，包含 PCIe 和 Thunderbolt 連接埠。因為每個 IOMMU 都有專屬的一組地址轉譯表，用於轉譯 DMA 要求，因此透過 PCIe 或 Thunderbolt 連接的周邊設備，只能存取已明確對映供其使用的記憶體。周邊設備無法存取屬於系統其他部份的記憶體 (例如核心或韌體)，或指派給其他周邊設備的記憶體。如果 IOMMU 偵測到有周邊設備嘗試存取並非對映供該周邊設備使用的記憶體，則會觸發核心異常。

### 以 Intel 為基礎的 Mac 上的直接記憶體存取保護

以 Intel 為基礎、並配備適用於導向式 I/O 的 Intel 虛擬化技術 I/O (VT-d) 的 Mac 電腦會初始化 IOMMU，啟用 DMA 對映並在開機程序的極早期中斷重新對映，藉此減輕各種保安漏洞類別的威脅。Apple IOMMU 硬件是依據預設拒絕規則開始作業，因此在系統啟動的當下，就會自動開始阻擋來自周邊設備的 DMA 要求。軟件初始化 IOMMU 後，IOMMU 會開始允許來自周邊設備的 DMA 要求傳至已明確對映供其使用的記憶體區域。

**附註：**在配備 Apple 晶片的 Mac 上，中斷 PCIe 的重新對映並非必要程序，因為每個 IOMMU 都會針對其自己的周邊設備處理 MSI。

從 macOS 11 開始，所有配備 Apple T2 保安晶片的 Mac 電腦都執行 UEFI 驅動程式，當這些驅動程式與外部裝置配對時，它們可以在受限的 ring 3 環境中推行 DMA。此屬性有助於緩解在開機期間，惡意裝置以非預期的方式與 UEFI 驅動程式進行互動時，可能發生的安全漏洞。尤其是，此屬性降低了在處理 DMA 緩衝區的驅動程式中發生漏洞的影響。

## macOS 的核心延伸功能

從 macOS 11 開始，如果第三方核心延伸功能 (kext) 已啟用，就不能按照要求載入核心中。相反地，這些 kext 會合併到一個會在開機程序期間載入的**輔助核心集合 (AuxKC)**中。對於配備 Apple 晶片的 Mac，AuxKC 的測量值已簽署到 LocalPolicy 中 (而對於先前的硬件，AuxKC 則會留在資料卷宗上)。如要重建 AuxKC，需要用戶許可並重新啟動 macOS，以將變更載入核心中，且需要將安全啟動設為「較低保安」。

**重要事項：**我們已不建議在 macOS 中使用 kext。kext 會對作業系統帶來完整性和可靠性風險，Apple 建議用戶應選擇不需要延伸核心的解決方案。

### 配備 Apple 晶片的 Mac 上的核心延伸功能

配備 Apple 晶片的 Mac 必須直接啟用 kext，方式為在開機時按住電源按鈕進入 One True Recovery (1TR) 模式，然後降級為「較低保安」，並別選該別選框來啟用核心延伸功能。此動作還需要輸入管理員密碼以授權降級。1TR 和密碼需求的結合讓純軟件攻擊者很難從 macOS 內部開始將 kext 注入 macOS (他們隨後可藉此取得核心權限)。

在用戶授權 kext 載入後，上述「用戶許可的核心延伸功能載入」流程會用於授權 kext 的安裝。用於上述流程的授權也會用於在 LocalPolicy 中載取用戶授權 kext 列表 (UAKL) 的 SHA384 雜湊值。之後核心管理服務程式 (kmd) 僅負責驗證在 UAKL 中找到的那些包含在 AuxKC 中的 kext。

- 如果啟用了「系統完整保護」(SIP)，則會在將每個 kext 的簽署納入 AuxKC 前，對其進行驗證。
- 如果 SIP 已停用，則不會強制執行 kext 簽署。

這個作法允許「寬鬆保安」為沒有參與 Apple 開發者計劃的開發者或用戶執行流程，在簽署 kext 之前先進行測試。

建立 AuxKC 之後，其測量值將傳送到「安全隔離區」，以進行簽署並納入 Image4 資料結構中，LLB 可以在開機時對其進行評估。作為 AuxKC 結構的一部份，也會產生一筆 kext 收據。這個收據包含實際上納入 AuxKC 中的 kext 列表，因為如果遇到遭禁用的 kext，該集合可能為 UAKL 的子集。LocalPolicy 中包含 AuxKC Image4 資料結構的 SHA384 雜湊值和 kext 收據。iBoot 在開機時會使用 AuxKC Image4 雜湊值進行額外的驗證，以協助確保無法使用更新的 LocalPolicy 啟動由「安全隔離區」簽署的較舊 AuxKC Image4 檔案。ApplePay 等子系統使用 kext 收據來確定目前是否載入了任何 kext，這些 kext 可能會干擾 macOS 的可信度。如果有 kext 已載入，那麼 Apple Pay 功能可能會遭停用。

## kext 的替用項目 (macOS 10.15 或較新版本)

macOS 10.15 可讓開發者能藉由安裝和管理在用戶空間中 (而非核心層級) 執行的系統延伸功能來延伸 macOS 的功能。透過在用戶空間運行，系統延伸功能提高了 macOS 的穩定性和保安。即使 kext 本質上具有整個作業系統的完全存取權，在用戶空間中執行的延伸功能只會獲得執行其指定功能所需的權限。

開發者可使用框架 (包含 DriverKit、EndpointSecurity 和 NetworkExtension) 來寫入 USB 及人性化介面驅動程式、端點安全工具 (例如防止資料遺失或其他端點代理程式) 及 VPN 和網絡工具，而不需要編寫 kext。只有當第三方保安代理程式採用這些 API，或具有移入第三方保安代理程式和移出核心延伸功能的完備藍圖時，才應使用這類代理程式。

## 用戶許可的核心延伸功能載入

為改進保安，需要用戶同意來載入核心延伸功能 (其於 macOS 10.13 安裝的同時或之後安裝)。這個程序稱為 **用戶許可的核心延伸功能載入**。亦需要管理員授權來允許核心延伸功能。在以下情況核心延伸功能無需取得授權：

- 在執行 macOS 10.12 或較早版本時已安裝在 Mac 上
- 用以取代先前允許的延伸功能
- 如使用 Mac 從 RecoveryOS 開機時可用的 `spctl` 命令列工具，無需取得用戶同意便可載入
- 允許使用流動裝置管理 (MDM) 設定來載入

從 macOS 10.13.2 起，用戶可使用 MDM 來指定無需用戶同意亦能載入的核心延伸功能列表。此選項僅適用於系統為 macOS 10.13.2 且已在 MDM 中註冊的 Mac，包括透過 Apple School Manager、Apple Business Manager 或由用戶完成註冊的 MDM。

## macOS 的 Option ROM 保安

**附註：**配備 Apple 晶片的 Mac 目前不支援 Option ROM。

### 配備 Apple T2 保安晶片的 Mac 之 Option ROM 保安

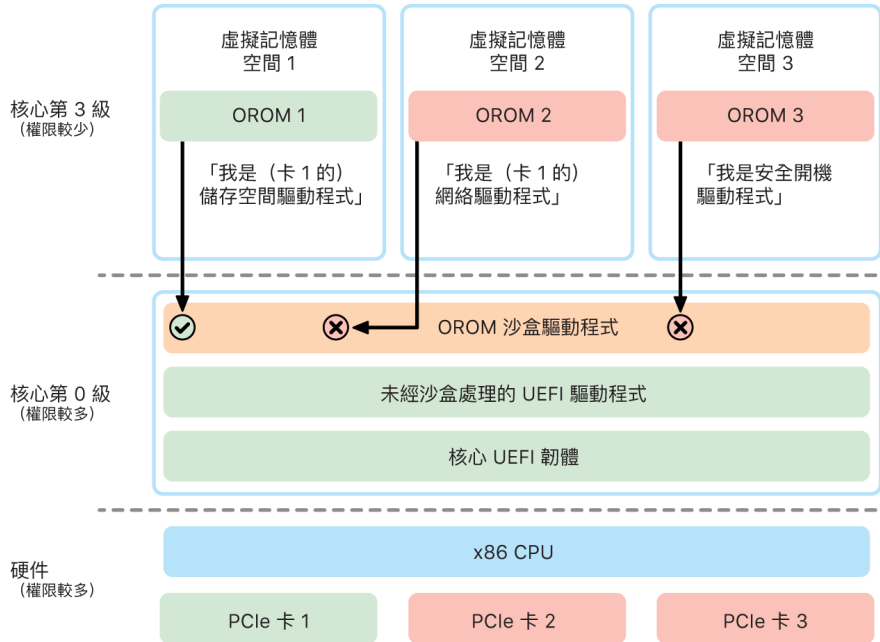
Thunderbolt 和 PCIe 裝置都具有與裝置實體連接的「Option ROM」(OROM)。(這通常不是真正的 ROM，而是儲存着韌體的可寫入晶片。)在 UEFI 架構的系統，該韌體通常是 UEFI 驅動程式，由 UEFI 韌體讀取並執行。執行的代碼應該初始化和設定從中取得的硬件，以便其餘的韌體可以使用該硬件。需要此功能是因為要讓專門的第三方硬件可在早期開機階段載入和運作，例如從外部 RAID 陣列開機。

然而，由於 OROM 通常可重複寫入，如果攻擊者覆寫合法周邊設備的 OROM，攻擊者的程式碼便可在開機程序的早期階段執行，且可竄改執行環境，以及破壞後續載入的軟件完整性。同樣地，如果攻擊者將自己的惡意裝置連接到系統中，他們也可以執行惡意程式碼。

在 macOS 10.12.3 中，2011 年後售出的 Mac 電腦之行為已更改為預設不在 Mac 開機時執行 OROM，除非按下特殊按鍵組合。這種按鍵組合可防止意外將惡意 OROM 引入 macOS 開機流程中。「韌體密碼工具程式」的預設行為也有所更改，當用戶設定韌體密碼時，即使按下按鍵組合也無法執行 OROM。這樣可以防止實際在場的攻擊者故意引入惡意 OROM。已設定韌體密碼的用戶如果仍需執行 OROM，可以使用 macOS 中的 `firmwarepasswd` 命令列工具來設定非預設選項。

## OROM 沙盒保安

在 macOS 10.15 中，UEFI 韌體已更新為包含對 OROM 執行沙盒處理和解除權限的機制。UEFI 韌體通常以最高 CPU 權限層級（稱為 ring 0）執行所有程式碼（包含 OROM 在內），且有一個共享虛擬記憶體空間供所有程式碼和資料使用。ring 0 是 macOS 核心執行所用的權限層級，而 App 執行所用的較低層級權限是 ring 3。OROM 沙盒藉由使用虛擬記憶體分隔（與核心一樣）來解除 OROM 的權限然後讓 OROM 以 ring 3 執行。



沙盒進一步大幅限制 OROM 可呼叫的介面（這十分類似於核心中的系統呼叫過濾）和 OROM 可登記的裝置類型（十分類似於 App 核准）。此設計的優點為惡意 OROM 無法再直接寫入 ring 0 記憶體中的任何一個位置，而是會限制在範圍極窄且定義明確的沙盒介面中。這個受限制的介面大幅縮小了攻擊面，並強迫攻擊者先逃離沙盒再提高權限。

# 以 Intel 為基礎的 Mac 之 UEFI 韌體保安

以 Intel 為基礎並配備 Apple T2 保安晶片的 Mac 使用 UEFI (Intel) 韌體來提供保安。

## 概覽

自 2006 年以來，配備以 Intel 為基礎的 CPU 的 Mac 電腦會使用基於可延伸韌體介面 (EFI) 開發者套件 (EDK) 版本 1 或版本 2 的 Intel 韌體。EDK2 架構的代碼符合統一可延伸韌體介面 (UEFI) 的規範。本節以 **UEFI 韌體** 來稱呼 Intel 韌體。UEFI 韌體是在 Intel 晶片上執行的首個代碼。

如 Mac 未配備 Apple T2 保安晶片並以 Intel 為基礎，UEFI 韌體的信任根則為儲存着韌體的晶片。UEFI 韌體更新是由 Apple 電子簽署，且須由韌體進行驗證後才會更新儲存體。為協助防止回捲攻擊，更新必須一律為比現有版本更新的版本。但是，攻擊者如能實體取用 Mac，便可能以硬體連接韌體儲存晶片並更新該晶片來包含惡意內容。同樣地，如果在 UEFI 韌體的早期開機過程中發現漏洞（在對儲存晶片進行寫入限制之前），這也可能導致 UEFI 韌體持續感染。這個硬件架構限制在大部份以 Intel 為基礎的 PC 上很常見，且所有未配備 T2 晶片並以 Intel 為基礎的 Mac 電腦上均存在此限制。

為了防止破壞 UEFI 韌體的實體攻擊，我們重新設計了 Mac 電腦的架構，以便將信任根放入 T2 晶片 UEFI 韌體內。在這些 Mac 電腦上，UEFI 韌體的信任根具體來說為 T2 韌體；詳情請參閱：[以 Intel 為基礎的 Mac 之開機程序](#)。

## Intel 管理引擎 (ME) 子元件

Intel 管理引擎 (ME) 韌體是儲存在 UEFI 韌體中的子元件。ME 是 Intel 晶片內的獨立處理器和子系統，主要用於只採用 Intel 繪圖晶片的 Mac，以保護音訊和影片的版權。為了縮小此子元件的攻擊面，以 Intel 為基礎的 Mac 會執行自訂的 ME 韌體，其中大部份元件都已移除。因為產生的 Mac ME 韌體小於 Intel 提供的預設精簡版組建，過去曾遭受安全研究人員公開攻擊的許多元件已不存在。

## 系統管理模式 (SMM)

Intel 處理器具有與一般作業不同的特殊執行模式。其被稱為「**系統管理模式**」(SMM)，原本引入來處理時間敏感的操作，例如電源管理。但是，為了執行此類操作，Mac 電腦歷史上一直使用稱為「**系統管理控制器**」(SMC) 的特定微控制器。SMC 不再是獨立的微控制器，而是已整合到 T2 晶片內。

# watchOS 的系統保安

Apple Watch 使用許多 iOS 和 iPadOS 使用的相同硬件式平台保安功能。例如，Apple Watch 會：

- 執行安全啟動和保安軟件更新
- 維持作業系統完整性
- 協助保護裝置上的資料，以及在與配對的 iPhone 和互聯網通訊時保護資料

支援的技術包含「系統保安」中列出的項目（例如 KIP、SKP 和 SCIP）以及「資料保護」、鑰匙圈和網絡技術。

## 更新 watchOS

watchOS 可以設定為隔夜更新。如需深入了解系統如何在更新期間儲存和使用 Apple Watch 密碼，請參閱：[Keybag](#)。

## 手腕偵測

如啟用手腕偵測，在用戶將手錶從手腕取下後會於短時間內自動鎖定裝置。如停用手腕偵測功能，控制中心會提供鎖定 Apple Watch 的選項。在 Apple Watch 鎖定時，用戶只能透過在 Apple Watch 上輸入密碼才能使用 Apple Pay。用戶可以在 iPhone 上的 Apple Watch App 中關閉手腕偵測。此設定也可使用流動裝置管理 (MDM) 解決方案來強制執行。

## 啟用鎖

在 iPhone 上開啟「尋找」後，其配對的 Apple Watch 也會使用「啟用鎖」。「啟用鎖」可讓 Apple Watch 在遺失或遭竊時無法由其他人輕易使用或銷售。「啟用鎖」需要用戶的 Apple ID 和密碼才能取消配對、清除或重新啟用 Apple Watch。

## 與 iPhone 安全配對

Apple Watch 一次只能與一部 iPhone 配對。當 Apple Watch 取消配對時，iPhone 會傳遞指令來清除手錶上的所有內容和資料。

將 Apple Watch 與 iPhone 配對是使用頻外處理加以保護以交換公用密鑰，並透過低耗電藍牙 (BLE) 連結共享密鑰。Apple Watch 會顯示動畫圖形，而用戶必須用 iPhone 上的相機來掃描有關圖形。圖形包含已編碼的密鑰，用於 BLE 4.1 頻外配對。如有需要，「標準 BLE 通行密匙項目」(Standard BLE Passkey Entry) 會用作備用配對方式。

一旦建立 BLE 階段作業並使用「藍牙核心規格」提供的最高層級安全通信協定加密後，iPhone 和 Apple Watch 會使用以下任何一項來交換密鑰：

- 改寫自 Apple 識別服務 (IDS) 的程序，如 [iMessage 保安概覽](#) 中所述。
- 使用 IKEv2/IPsec 的密鑰交換。初始密鑰交換使用藍牙階段作業密鑰 (用於配對情境) 或 IDS 密鑰 (用於作業系統更新情境) 進行認證。每個裝置會產生一個隨機的公共和專用 256 位元 Ed25519 密鑰組，並且在初始密鑰交換過程中，將交換公共密鑰。

**附註：**用於密鑰交換和加密的機制會有所改變，這取決於 iPhone 和 Apple Watch 上的作業系統版本。與執行 watchOS 6 或較新版本的 Apple Watch 配對時，執行 iOS 13 或較新版本的 iPhone 裝置僅使用 IKEv2/IPsec 進行密鑰交換和加密。

在密鑰交換後：

- 藍牙階段作業密鑰會被捨棄，iPhone 和 Apple Watch 之間的所有通訊都使用上述方法之一進行了加密，如加密的藍牙、Wi-Fi 和提供了輔助加密層的流動數據連結。
- (僅 IKEv2/IPsec) 這些密鑰儲存在系統鑰匙圈中，並用於認證裝置之間未來的 IKEv2/IPsec 階段作業。在執行 iOS 15 或較新版本的 iPhone 裝置 (並與執行 watchOS 8 或較新版本的 Apple Watch Series 4 或較新型號配對)，這些裝置之間的進一步通訊使用 AES-256-GCM 或 ChaCha20-Poly1305 (256 位元密鑰) 進行加密和完整性保護。

低耗電藍牙裝置的地址每 15 分鐘便會輪換，以減少他人使用持續性識別碼廣播在本機追蹤裝置的風險。

為了支援需要串流資料的 App，會使用 [FaceTime 保安](#) 中提到的方式來提供加密，過程中會使用由已配對的 iPhone 或直接互聯網連線提供的 Apple 識別服務 (IDS)。

Apple Watch 採用硬件加密儲存體並根據類別保護檔案和鑰匙圈項目。也會一併使用鑰匙圈項目的存取控制 Keybag。Apple Watch 與 iPhone 間通訊所使用的密鑰也會利用類別式保護來確保其保安。如需更多資料，請前往：[「資料保護」的 Keybag](#)。

## 自動解鎖和 Apple Watch

為了在使用多個 Apple 裝置時提供更大的便利性，某些裝置在特定情況下可以自動解鎖其他裝置。「自動解鎖」支援三種用途：

- iPhone 可解鎖 Apple Watch。
- Apple Watch 可解鎖 Mac。
- 偵測到用戶的口鼻被遮蓋時，Apple Watch 可解鎖 iPhone。

所有這三個用途都建立在相同的基本基礎上：相互認證的站對站 (STS) 通訊協定，在啟用功能時交換長期密鑰，並為每個要求協商唯一的臨時階段作業密鑰。無論基礎通訊管道為何，STS 通道都是在兩個裝置中的「安全隔離區」之間直接協商的，所有加密編譯材料都保留在該安全區域內 (未配備安全隔離區的 Mac 電腦除外，其會終止核心中的 STS 通道)。

### 解鎖

完整的解鎖順序可以分為兩個階段。首先，要解鎖的裝置 (「目標」) 會產生一個加密編譯的解鎖密鑰，並將其傳送給執行解鎖的裝置 (「發起方」)。接着，發起方會使用先前產生的密鑰執行解鎖。

為了進行自動解鎖，裝置會使用 BLE 連線互相連接。然後，目標裝置隨機產生的 32 位元解鎖密鑰將透過 STS 通道傳送給發起方。在下一生物識別或密碼解鎖期間，目標裝置將其密碼衍生密鑰 (PDK) 與解鎖密鑰包裝在一起，並從其記憶體中捨棄該解鎖密鑰。

為了執行解鎖，裝置會啟動新的 BLE 連線，然後使用點對點 Wi-Fi 安全地估算彼此之間的距離。如果裝置在指定範圍內，並且滿足所需的保安規則，則發起方會透過 STS 通道將其解鎖密鑰傳送給目標。接着，目標會產生一個新的 32 字元解鎖密鑰並將其傳回給發起方。如果發起方傳送的目前解鎖密鑰成功解密了解鎖記錄，則目標裝置將會被解鎖，並且 PDK 會使用新的解鎖密鑰重新包裝。最後，新的解鎖密鑰和 PDK 會從目標記憶體中捨棄。

### Apple Watch 自動解鎖保安規則

為了增加便利性，首次啟動後，iPhone 可以直接將 Apple Watch 解鎖，用戶無需先在 Apple Watch 本身上輸入密碼。為了達成此目的，會使用隨機解鎖密鑰 (在啟用該功能後的第一個解鎖順序期間生成) 來建立長期託管記錄，該記錄則儲存在 Apple Watch Keybag 中。託管記錄密鑰儲存在 iPhone 鑰匙圈中，並在每次 Apple Watch 重新啟動後用於引導新的階段作業。

## iPhone 自動解鎖保安規則

其他保安規則適用於使用 Apple Watch 的 iPhone「自動解鎖」。Apple Watch 無法用來代替 Face ID 上的 Face ID 進行其他操作，例如 Apple Pay 或 App 授權。當 Apple Watch 成功解鎖配對的 iPhone 時，手錶會顯示一則通知並播放相關的觸覺通知。如果用戶點一下通知中的「鎖定 iPhone」按鈕，則手錶會透過 BLE 向 iPhone 傳送鎖定指令。當 iPhone 收到鎖定指令時，便會鎖定並將 Face ID 和使用 Apple Watch 解鎖的功能停用。下一次的 iPhone 解鎖必須使用 iPhone 密碼執行。

如要從 Apple Watch 成功解鎖配對的 iPhone (啟用後)，需要滿足以下條件：

- 將已連繫的 Apple Watch 放在手腕上並解鎖後，必須使用另一種方法解鎖 iPhone 最少一次。
- 感應器必須能夠偵測到口鼻被遮蓋。
- 測量到的距離必須是 2–3 米或以下
- Apple Watch 不得處於就寢模式。
- Apple Watch 或 iPhone 必須在最近曾被解鎖，或者 Apple Watch 必須經歷過實體動作，表示佩戴者處於活動狀態 (例如，未入睡)。
- iPhone 必須在過去 6.5 個小時內曾被解鎖最少一次。
- iPhone 必須處於允許 Face ID 執行裝置解鎖的狀態。(如需更多資料，請參閱：[Face ID](#)、[Touch ID](#) 和 [密碼](#)。)

## 使用 Apple Watch 在 macOS 中進行核准

啟用了以 Apple Watch 自動解鎖後，Apple Watch 可用於適當位置或配搭 Touch ID 使用，以核准來自以下項目的授權和認證提示：

- 要求授權的 macOS 和 Apple App
- 要求認證的第三方 App
- 儲存的 Safari 密碼
- 安全備註

## 安全使用 Wi-Fi、流動網絡、iCloud 和 Gmail

當 Apple Watch 不在藍牙範圍內時，可改為使用 Wi-Fi 或流動網絡。Apple Watch 會自動加入其配對 iPhone 已加入過的 Wi-Fi 網絡 (網絡的憑證必須在兩部裝置都位於連線範圍內時同步至 Apple Watch)。接着在 Apple Watch 上，便可於「設定」App 的 Wi-Fi 部份中設定個別網絡的「自動加入」動作。如為先前未於任何裝置上加入過的 Wi-Fi 網絡，可在 Apple Watch 上於「設定」App 的 Wi-Fi 部份手動加入。

當 Apple Watch 和 iPhone 在範圍外時，Apple Watch 會直接連接到 iCloud 和 Gmail 伺服器以截取郵件，而不是透過互聯網與配對的 iPhone 同步「郵件」資料。針對 Gmail 帳戶，用戶必須在 iPhone 上 Watch App 的「郵件」部份中向 Google 認證。從 Google 接收的 OAuth 代號會透過 Apple 識別服務 (IDS) 以加密格式傳送到 Apple Watch，即可用來截取郵件。此 OAuth 代號絕不會用來從配對的 iPhone 連接到 Gmail 伺服器。



## 亂數產生

加密編譯偽亂數產生器 (CPRNG) 是安全軟件的重要構成要素。有鑑於此，Apple 提供受信任的軟件 CPRNG，在 iOS、iPadOS、macOS、tvOS 及 watchOS 核心中執行。CPRNG 負責從系統整合原始的熵，並在核心和用戶空間中向消費者提供安全的亂數。

## 熵來源

核心 CPRNG 來自裝置啟動時及整個使用週期的多個熵來源。這些包括 (適用與否視情況而定)：

- 「安全隔離區」硬件 TRNG
- 開機期間收集的時基誤差
- 從硬件中斷收集的熵
- 啟動時用於持續執行熵的種子檔案
- Intel 隨機指令，例如 RDSEED 和 RDRAND (僅適用於以 Intel 為基礎的 Mac)

## 核心 CPRNG

核心 CPRNG 是 Fortuna 衍生的設計，以 256 位元安全層級為目標。它使用下列 API 為用戶空間消費者提供高品質的亂數。

- `getentropy(2)` 系統呼叫
- 隨機裝置 (`/dev/random`)

核心 CPRNG 透過寫入隨機裝置接受用戶供應的熵。

# Apple 安全研究裝置

「Apple 安全研究裝置」是以特殊方式嵌合的 iPhone，讓安全研究人員用於對 iOS 進行研究，而無需破壞或停用 iPhone 的平台保安功能。透過此裝置，研究人員可側載以等同於平台權限執行的內容，進而在更接近生產裝置模型的平台上進行研究。

為協助確保用戶裝置不會受到安全研究裝置執行規則影響，會在 iBoot 變體和「開機核心集合」中實施規則變更。這些無法在用戶硬件上啟動。研究 iBoot 會檢查新的嵌合狀態，且如在非研究嵌合硬件上執行，則會進入異常循環。

cryptex 子系統可讓研究人員載入個人化的信任快取，以及包含對應內容的磁碟映像檔。已採取多種防禦深度措施，其設計用意是確保這個子系統不會在用戶裝置上允許執行：

- 如果 launchd 偵測到正常的客戶裝置，便不會載入 cryptexd launchd 屬性列表。
- 如果 cryptexd 偵測到正常的客戶裝置，便會中止。
- AppleImage4 不會提供用於在正常客戶裝置上驗證研究 cryptex 的隨機數。
- 簽署伺服器拒絕為不在明確允許列表上的裝置個人化 cryptex 磁碟映像檔。

為尊重安全研究人員的私隱，進行個人化期間，只會將可執行檔或核心快取的測量值（例如雜湊值）和安全研究裝置識別碼傳送給 Apple。Apple 不會收到載入到裝置上的 cryptex 內容。

為避免惡意人士企圖將研究裝置偽裝成用戶裝置，欺騙目標進行日常使用，安全研究裝置有下列不同之處：

- 安全研究裝置只會在充電期間開機。可使用 Lightning 連接線和 Qi 相容充電器來進行充電。如果裝置在開機期間沒有在充電，便會進入「還原」模式。如果用戶開始充電並將裝置重新開機，裝置就會正常開機。當 XNU 啟動後，便無需為裝置充電也可繼續操作。
- iBoot 啟動期間，**Security Research Device** (安全研究裝置) 字樣會顯示在 Apple 標誌下方。
- XNU 核心會以詳盡模式啟動。
- 以下資訊會蝕刻在裝置的側面：「Property of Apple. Confidential and Proprietary. Call +1 877 595 1125。」

以下是在軟件中導入的其他措施，會在開機後顯示：

- 設定裝置期間會顯示 **Security Research Device** (安全研究裝置) 字樣。
- **Security Research Device** (安全研究裝置) 字樣會顯示在鎖定畫面上和「設定」App 中。

安全研究裝置為研究人員提供下列功能（用戶裝置不提供），研究人員可以：

- 透過與 Apple 作業系統元件相同權限層級的任意授權，將可執行檔程式碼側載到裝置上
- 開機時啟動服務
- 重新開機後維持內容
- 使用 `research.com.apple.license-to-operate` 授權允許程序為系統上的任何其他程序除錯，包括系統程序。

僅 AppleMobileFileIntegrity 核心延伸功能的 RESEARCH 變體會遵循此 `research.` 命名空間；在簽署驗證期間，任何具有此授權的程序都會在客戶裝置上終止。

- 個人化和還原自訂核心快取

# 加密與資料保護

## 加密與資料保護概覽

安全啟動鏈、系統保安和 App 保安功能都有助於驗證裝置上只執行受信任的程式碼和 App。即使安全基礎架構的其他部份遭入侵 (例如如裝置遺失或執行不受信任的程式碼)，Apple 裝置的額外加密功能可保護用戶資料。這些功能對用戶和 IT 管理員都大有助益，可保護個人與企業的資料，並提供裝置遭竊或遺失時，立即遙距完全清除的方式。

iOS 和 iPadOS 裝置採用名為「**資料保護**」的檔案加密方法，而以 Intel 為基礎的 Mac 上的資料則受到名為「**檔案保險箱**」的卷宗加密技術保護。配備 Apple 晶片的 Mac 會使用支援「資料保護」的混合模式，包含兩項須知：不支援最低的保護層級 (類別 D)，而且預設層級 (類別 C) 會使用卷宗密鑰並運作如同以 Intel 為基礎的 Mac 上的「檔案保險箱」。在所有情況中，密鑰管理階層的根設在「安全隔離區」的專用晶片上，且有專用的「AES 引擎」支援線速加密，以及確保不會向核心作業系統或 CPU 洩漏長效加密密鑰 (它們可能會遭入侵)。(配備 T1 或缺少「安全隔離區」的以 Intel 為基礎的 Mac 不會使用專用晶片來保護其「檔案保險箱」加密密鑰。)

除了使用「資料保護」和「檔案保險箱」來協助防止資料未經授權的存取，Apple 會使用**作業系統核心**來強制執行保護和保安。核心使用對「沙盒」App 的存取控制 (其會限制 App 可存取的資料) 和名為 **Data Vault** 的機制 (與其限制 App 可發出的呼叫，反而是限制所有其他要求的 App 對資料的存取)。

# 密碼

為了保護用戶資料免受惡意攻擊，Apple 會在 iOS 和 iPadOS 中使用密碼，並在 macOS 中使用密碼。密碼越長，強度就越高，並且更容易阻止暴力密碼破解攻擊。為了進一步阻止攻擊，Apple 會強制執行時間延遲（適用於 iOS 和 iPadOS）和有限的密碼嘗試次數（適用於 Mac）。

在 iOS 和 iPadOS 中，設定裝置密碼，用戶就會自動啟用「資料保護」。其他配備 Apple 系單晶片系統 (SoC) 的裝置（例如配備 Apple 晶片的 Mac、Apple TV 和 Apple Watch）也會啟用資料保護。在 macOS 中，Apple 則使用內置卷宗加密程序「檔案保險箱」。

## 高強度密碼和密碼如何加強保安

iOS 和 iPadOS 支援六位數、四位數和任意長度的英數字元密碼。除了用於解鎖裝置外，密碼還為特定加密密鑰提供熵。這表示攻擊者即使拿到裝置，在沒有密碼的情況下也無法存取特定保護類別中的資料。

密碼與裝置的 UID 之間有關聯性，所以只能在受攻擊的裝置上使用暴力破解法。因此，iOS 系統使用較大的反覆運算來延緩每次的嘗試。反覆運算計數已經過測定，每次嘗試會耗時約 80 毫秒。事實上，需要 5 年半以上的時間才能試完 6 位英數字元密碼（包含小寫字母和數字）的所有組合。

用戶密碼的強度越高，加密密鑰就越堅固。且透過使用 Face ID 和 Touch ID，用戶可製作一個更高強度的密碼同時又十分實用。較高強度的密碼增加了對用於「資料保護」的加密密鑰進行保護有效份量的熵，而且不會對一日中多次解鎖裝置的用戶體驗產生負面影響。

如輸入較長的純數字密碼，鎖定畫面上會顯示數字鍵盤而非完整鍵盤。與較短的英數字密碼相比，較長的數字密碼更便於輸入，而且可提供類似的保安。

用戶可在「設定」>「Touch ID 與密碼」或「Face ID 與密碼」選項中選取「自訂英數混合密碼」，來指定較長的英數字元密碼。

## 增加延遲時間如何阻止暴力密碼破解攻擊 (iOS、iPadOS)

在 iOS 和 iPadOS 中，為了進一步阻止暴力密碼破解攻擊，系統會延長在鎖定畫面上輸入無效密碼後的延遲時間，如下表所示。

嘗試次數	強制延遲
1-4	無
5	1 分鐘
6	5 分鐘
7-8	15 分鐘
9	1 小時

如果開啟了「清除資料」選項（在「設定」>「Touch ID 與密碼」中），連續 10 次嘗試輸入密碼錯誤後，將從儲存區中移除所有內容和設定。連續嘗試同一個錯誤密碼不會計入限制。此設定還可透過支援此功能的流動裝置管理 (MDM) 解決方案和透過 Microsoft Exchange ActiveSync 作為管理規則，並可設定為較低的臨界值。

在配備「安全隔離區」的裝置上，「安全隔離區」會強制執行延遲。如裝置在定時延遲期間重新啟動，延遲仍會強制執行，但計時器會從目前期間重新開始。

## 增加延遲時間如何阻止暴力密碼破解攻擊 (macOS)

為協助防止暴力密碼破解攻擊，當 Mac 啟動時，不能在「登入視窗」中或使用「目標磁碟模式」嘗試輸入密碼 10 次以上，且密碼輸入錯誤達指定次數後會逐步增加延遲時間。延遲是由「安全隔離區」強制執行。如 Mac 在定時延遲期間重新啟動，延遲仍會強制執行，但計時器會從目前期間重新開始。

下表顯示在配備 Apple 晶片和配備 T2 晶片的 Mac 上，密碼嘗試次數間的延遲。

嘗試次數	強制延遲
5	1 分鐘
6	5 分鐘
7	15 分鐘
8	15 分鐘
9	1 小時
10	停用

為協助防止惡意軟件藉由嘗試攻擊用戶的密碼造成永久性資料遺失，在用戶成功登入 Mac 後，就不會強制執行這些限制，但是會在重新開機後再次實施。如輸入錯誤密碼已達 10 次，開機進入 RecoveryOS 之後還可嘗試 10 次。如果這十次機會也用完，那麼每次「檔案保險箱」還原機制 (iCloud 還原、「檔案保險箱」還原密鑰和其他機構密鑰) 都會有 10 次機會，最多可嘗試 30 次。用盡那些機會後，「安全隔離區」將不會執行任何解密卷宗或驗證密碼的要求，且裝置上的資料將不可還原。

如要協助保護企業設定的資料，IT 人員應使用 MDM 來定義和強制執行「檔案保險箱」設定原則。機構有多個選項來管理加密的卷宗，包括機構還原密鑰、個人還原密鑰 (可選擇以 MDM 儲存來進行託管)，或將它們混合使用。密鑰轉換亦可設定為 MDM 中的原則。

在配備 Apple T2 保安晶片的 Mac 上，密碼的功能很類似，差別在於產生的密鑰是用於「檔案保險箱」加密而非「資料保護」。macOS 也提供額外的密碼還原選項：

- iCloud 還原
- 「檔案保險箱」還原
- 「檔案保險箱」機構密鑰

# 資料保護

## 「資料保護」概覽

Apple 使用名為「資料保護」的技術，來在配備 Apple SoC 的裝置上保護快閃儲存空間中儲存的資料，例如 iPhone、iPad、Apple Watch、Apple TV 和配備 Apple 晶片的 Mac。有了「資料保護」，裝置可回應如來電之類的常見事件，同時對用戶資料啟用較高層次的加密。特定系統 App（如「訊息」、「郵件」、「日曆」、「通訊錄」、「相片」）和「健康」的資料值都預設使用「資料保護」。第三方 App 會自動獲得這項保護措施。

## 實行方法

「資料保護」是透過建構和管理密鑰階層來實行，並建立在 Apple 裝置內置的硬件加密技術上。「資料保護」藉由將每個檔案指定給某個類別，進而對檔案逐一進行控制；能否存取則按照該類別的密鑰是否已解鎖。APFS（Apple 檔案系統）允許檔案系統依據範圍進一步細分密鑰（一個檔案的不同部份可擁有不同密鑰）。

每次在資料卷宗上製作檔案時，「資料保護」都會製作一個新的 256 位元密鑰（**「檔案專屬」密鑰**），並將其提供給硬件「AES 引擎」，此引擎會使用該密鑰對寫入快閃儲存空間的檔案進行加密。在 A14、A15 和 M1 系列裝置上，加密使用 XTS 模式的 AES-256 來進行，其中 256 位元檔案專屬密鑰會經過「密鑰衍生函數」（NIST 特別出版物 800-108），以衍生 256 位元 Tweak 密鑰和 256 位元加密密鑰。而在 A9 至 A13、S5、S6 以及 S7 代的硬件，則會使用 XTS 模式中的 AES-128 進行，其中 256 位元檔案專屬密鑰會被分割，以提供 128 位元 Tweak 密鑰和 128 位元加密密鑰。

在配備 Apple 晶片的 Mac 上，「資料保護」會預設為「類別 C」（請參閱：[「資料保護」類別](#)），但使用卷宗密鑰而非範圍專屬或檔案專屬密鑰——實際上會為用戶資料重建「檔案保險箱」的安全模型。用戶仍必須選擇使用「檔案保險箱」，才能獲得加密密鑰階層與其密碼纏結的完整保護。開發者也可選擇使用範圍專屬或檔案專屬密鑰這些更高層級保護類別。

## Apple 裝置中的「資料保護」

在具備「資料保護」的 Apple 裝置上，每個檔案都是使用一或多條檔案（或範圍）專屬密鑰來加以保護。依據檔案在甚麼情況下可供存取，使用 NIST AED 密鑰封裝演算法加以封裝的密鑰，會進一步使用其中一個類別密鑰進行封裝。封裝的檔案專屬密鑰然後會儲存在檔案的後設資料中。

使用 APFS 格式的裝置可能支援檔案複製功能（使用寫入時複製技術的零成本複製）。複製檔案後，每份副本會各自獲得一個用於接受傳入寫入的新密鑰，以便透過新密鑰將新資料寫入媒體。隨著時間推移，檔案可能會包含分別對映到不同密鑰的不同範圍（或片段）。但是組成同一個檔案的所有範圍都會受到相同的類別密鑰保護。

當開啟檔案時，系統會使用檔案系統密鑰來解密其後設資料，以呈現封裝的檔案專屬密鑰以及表示其保護類別的記號。檔案專屬（或範圍專屬）密鑰會使用類別密鑰來解除封裝，然後提供給硬件「AES 引擎」，該引擎會在從快閃儲存空間中讀取檔案時，對檔案進行解密。所有封裝檔案的密鑰處理都會在「安全隔離區」中進行；檔案密鑰永遠不會直接提供給「應用程式處理器」。在啟動時，「安全隔離區」會與「AES 引擎」進行協調以獲取臨時密鑰。當「安全隔離區」解除封裝檔案密鑰時，這些密鑰會透過臨時密鑰來重新封裝，並傳送回「應用程式處理器」。

資料卷宗檔案系統中所有檔案的後設資料都使用隨機卷宗密鑰進行加密，該密鑰是在首次安裝作業系統時，或用戶清除裝置時製作而成。此密鑰會以只有「安全隔離區」知道的密鑰封裝密鑰來加密和封裝，以便長期儲存。用戶每次清除裝置時密鑰封裝密鑰都會更改。在 A9（和更新版本）SoCs 上，「安全隔離區」依賴（受到反重播系統支援）來實現可抹除性，以及保護其密鑰封裝密鑰與其他資產。如需更多資料，請前往：[安全非揮發性儲存裝置](#)。

與檔案或範圍專屬密鑰相同，資料卷宗的後設資料密鑰永遠不會直接提供給「應用程式處理器」，而是「安全隔離區」會提供每次啟動時產生的臨時版本。儲存時，系統會使用儲存在可抹除儲存空間中的「可抹除的密鑰」或使用媒體密鑰封裝密鑰（受到「安全隔離區」反重播機制保護），對加密的檔案系統密鑰進行額外封裝。此密鑰不會提供額外的資料機密性，而是可以視需求快速清除（由用戶使用「清除所有內容和設定」選項來清除，或者由用戶或管理員從流動裝置管理 (MDM) 解決方案、Microsoft Exchange ActiveSync 或 iCloud 發出遙距清除指令來清除）。以此方式清除密鑰將會讓裝置上的所有檔案因加密編譯而無法存取。

系統可能會使用一或多條檔案（或範圍）專屬密鑰來加密檔案的內容，這些密鑰使用類別密鑰封裝並儲存在檔案的後設資料中，檔案後設資料接着又使用檔案系統密鑰進行加密。類別密鑰使用硬件 UID 取得保護，而某些類別則透過用戶密碼取得保護。此階層架構同時提供了彈性與效能。例如，更改檔案的類別只需要重新封裝其檔案專屬密鑰，更改密碼只需要重新封裝類別密鑰。

## 「資料保護」類別

在支援「資料保護」的裝置上製作新檔案時，用來製作的 App 會替檔案指定一個類別。每個類別使用不同的規則來決定資料何時可供存取。基本類別和規則會在下面的章節中說明。以 Apple 晶片為基礎的 Mac 電腦不支援類別 D：「無保護」，且安全界線是針對登入與登出建立（並非像 iPhone、iPad 和 iPod touch 上的鎖定或解鎖）。

類別	保護類型
類別 A：完整保護	NSFileProtectionComplete
類別 B：未開啟檔案的保護	NSFileProtectionCompleteUnlessOpen
類別 C：首次用戶認證前的保護 附註：macOS 使用卷宗密鑰來重建「檔案保險箱」保護特性。	NSFileProtectionCompleteUntilFirstUserAuthentication
類別 D：無保護 附註：macOS 不支援。	NSFileProtectionNone

### 完整保護

**NSFileProtectionComplete**：類別密鑰會使用從用戶密碼和裝置 UID 所衍生的密鑰加以保護。用戶鎖定裝置後不久（如「需要密碼」設定為「立即」，則為 10 秒），系統便會捨棄已解密的類別密鑰，如此一來只有在用戶再次輸入密碼或使用 Face ID 或 Touch ID 解鎖（登入）裝置時，才可以存取此類別中的所有資料。

在 macOS 中，上一個用戶登出後不久，系統會捨棄已解密的類別密鑰，如此一來只有當某個用戶再次輸入密碼或使用 Touch ID 登入裝置時，才可以存取此類別中的所有資料。

### 未開啟檔案的保護

**NSFileProtectionCompleteUnlessOpen**：某些檔案可能需要在裝置鎖定或用戶已登出時寫入。其中一個不錯的例子是在背景下載的電郵附件。此行為是藉由使用非對稱橢圓曲線加密技術 (Curve25519 的 ECDH) 來達成。一般的檔案專屬密鑰則是使用 One-Pass Diffie-Hellman Key Agreement (如 NIST SP 800-56A 中所述) 所衍生的密鑰加以保護。

該協議的臨時公用密鑰與封裝的檔案專屬密鑰一起儲存。KDF 是串接密鑰衍生函數 (Approved Alternative 1)，如 NIST SP 800-56A 的 5.8.1 節中所述。AlgorithmID 已忽略。PartyUInfo 和 PartyVInfo 則分別為臨時和靜態公用密鑰。SHA256 則用於雜湊值函式。檔案一旦關閉，檔案專屬密鑰便會從記憶體中清除。如要再次開啟檔案，系統會使用「未開啟檔案的保護」類別的專用密鑰和檔案的臨時公用密鑰來重新製作共享密鑰；該密鑰會用於解除封裝檔案專屬密鑰，然後再用來解密檔案。

在 macOS 中，系統上的任何用戶只要登入或經過認證，就能取用 NSFileProtectionCompleteUnlessOpen 的私密部份。

## 首次用戶認證前的保護

**NSFileProtectionCompleteUntilFirstUserAuthentication**: 此類別與「完整保護」類別的行為方式相同，只是在鎖定裝置或用戶已登出時，已解密的類別密鑰不會從記憶體中移除。此類別中的保護和桌面電腦完整卷宗的加密有類似的屬性，可防止資料因重新啟動而遭到攻擊。對於未指定至「資料保護」類別的所有第三方 App 資料，這是預設類別。

在 macOS 中，此類別會使用卷宗密鑰，只要裝載卷宗就能取用這個卷宗密鑰，且其功用與「檔案保險箱」相同。

## 無保護

**NSFileProtectionNone**: 此類別密鑰僅受到 UID 的保護，並且儲存在可抹除儲存空間中。因為解密此類別中檔案所需的所有密鑰都儲存在裝置上，因此這種加密方式只有在快速遙距清除時才具有效益。檔案即使未有被分派「資料保護」類別，仍會以加密形式儲存（就像 iOS 及 iPadOS 裝置上的所有資料一樣）。

macOS 不支援此功能。

**附註**: 在 macOS 中，針對沒有與啟動的作業系統對應的卷宗，只要裝載卷宗就能取用所有資料保護類別。預設資料保護類別為 **NSFileProtectionCompleteUntilFirstUserAuthentication**。Rosetta 2 和原生 App 均可使用範圍專屬密鑰功能。

## 「資料保護」的 Keybag

系統會收集檔案和鑰匙圈「資料保護」類別的密鑰，並在 iOS、iPadOS、watchOS 和 tvOS 的 Keybag 內加以管理。這些作業系統會使用以下的 Keybag：用戶、裝置、備份、託管和「iCloud 備份」。

### 用戶 Keybag

用戶 Keybag 是裝置一般操作中使用的封裝類別密鑰的儲存位置。例如，輸入密碼後，會從用戶 Keybag 中載入 **NSFileProtectionComplete** 並解除封裝。這是儲存在「無保護」類別的二進位屬性列表 (.plist) 檔案。

在配備 A9 之前版本 SoC 的裝置上，.plist 檔案內容會以保留在「可抹除儲存空間」的密鑰加密。為了對 Keybag 提供更高的保安，用戶每次更改密碼時，系統都會清除並重新產生此密鑰。

在配備 A9 或較新版本 SoC 的裝置上，.plist 檔案中包含一個密鑰，指出 Keybag 儲存在保存庫中，這個保存庫受到「安全隔離區」所控制的反重播隨機數保護。

「安全隔離區」會管理用戶 Keybag，並可用於查詢裝置的鎖定狀態。只有當用戶 Keybag 中的所有類別密鑰都可存取且已成功解除封裝，「安全隔離區」才會報告裝置已解鎖。

### 裝置 Keybag

裝置 Keybag 是用來儲存操作相關裝置特定資料的封裝類別密鑰。設定為共用的 iPadOS 裝置有時候需要存取憑證，才能讓用戶登入，因此需要未受用戶密碼保護的 Keybag。

iOS 及 iPadOS 不支援用戶專屬檔案系統內容的加密編譯區分，即系統將使用來自裝置 Keybag 的類別密鑰來封裝檔案專屬密鑰。不過，鑰匙圈會使用來自用戶 Keybag 的類別密鑰來保護用戶鑰匙圈裏的項目。在針對單一用戶（預設設定）設定的 iOS 及 iPadOS 裝置上，裝置 Keybag 和用戶 Keybag 是同一個相同的 Keybag，且受用戶的密碼保護。



## 備份 Keybag

備份 Keybag 是在 Finder (在 macOS 10.15 或較新版本) 或 iTunes (在 macOS 10.14 或較早版本) 進行加密備份時製作，儲存在為裝置進行備份的電腦中。新 Keybag 是使用一組新的密鑰製作而成，備份的資料會以這些新密鑰來重新加密。如前面所述，不可遷移的鑰匙圈項目仍會使用 UID 衍生的密鑰加以封裝，以使其可以回復到最初用於備份的裝置上，但在其他裝置上則無法存取。

Keybag 受到密碼組保護，且執行了一千萬次密鑰衍生函數 PBKDF2 的反覆運算。雖然反覆運算的次數很多，但 Keybag 並未與特定裝置綁定，因此理論上可嘗試在多部電腦上對備份 Keybag 進行暴力密碼破解攻擊。而保安夠高的密碼可以降低此威脅。

如用戶選擇不加密備份，那麼無論檔案屬於哪一種「資料保護」類別，檔案都不會加密，但鑰匙圈仍會使用 UID 衍生的密鑰獲得保護。這就是只有在設定備份密碼時，才能將鑰匙圈項目遷移到新裝置的原因。

## 託管 Keybag

託管 Keybag 用於與 Finder (macOS 10.15 或較新版本) 或透過 USB 與 iTunes (macOS 10.14 或較早版本) 同步，以及同步和流動裝置管理 (MDM)。此 Keybag 允許 Finder 或 iTunes 執行備份和同步，讓用戶無須輸入密碼，還允許 MDM 解決方案遙距清除用戶密碼。此 Keybag 儲存在用於透過 Finder 或 iTunes 進行同步的電腦，或者遙距管理裝置的 MDM 解決方案上。

託管 Keybag 改善了裝置同步期間的用戶體驗，此期間內可能需要存取所有類別的資料。當使用密碼鎖定的裝置首次連接到 Finder 或 iTunes 時，會提示用戶輸入密碼。然後，裝置會製作託管 Keybag，其中包含的類別密鑰與裝置上使用的完全相同，該 Keybag 由新產生的密鑰保護。系統會將託管 Keybag 與用於保護它的密鑰分別存放在裝置和主機或伺服器上，其資料則以「首次用戶認證前的保護」類別儲存在裝置上。這就是重新啟動後首次使用 Finder 或 iTunes 進行備份之前，必須輸入裝置密碼的原因。

如果是進行無線 (OTA) 軟件更新，在一開始進行更新時，系統會提示用戶輸入密碼。這會用來安全地建立一次性解鎖代號，其會在更新後解鎖用戶 Keybag。如未輸入用戶的密碼，便無法產生此代號，且如用戶密碼有所更改，任何先前產生的代號都會失效。

不同的一次性解鎖代號分別適用於手動和自動軟件更新安裝情形。它們會使用「安全隔離區」中單純計數器目前值所衍生的密鑰、Keybag 的 UUID 和「安全隔離區」UID 來進行加密。

在 A9 (和較新版本) SoC 上，一次性鎖定代號不再依賴計數器或「可抹除儲存空間」，而是受到由「安全隔離區」控制的反重播隨機數保護。

手動軟件更新的一次性解鎖代號會在 20 分鐘後過期。在 iOS 13 和 iPadOS 13.1 或較新版本中，代號儲存在受到「安全隔離區」保護的保存庫中。在 iOS 13 以前，此代號可從「安全隔離區」輸出，並寫入「可抹除儲存空間」中，或受到「安全隔離區」反重播機制保護。如裝置在 20 分鐘內未重新開機，規則計時器會遞增計數器。

當以下其中一種情況發生，而且系統偵測到有可用更新時，軟件更新將會自動執行：

- 已在 iOS 12 或較新版本中設定自動更新。
- 用戶在收到更新通知時選擇「稍後安裝」。

用戶輸入密碼後，系統會產生一次性解鎖代號，在「安全隔離區」中效力長達 8 小時。如果尚未執行更新，每次鎖定裝置時系統便會銷毀此一次性解鎖代號，並在其後每一次解鎖時重新建立。每次解鎖都會重計 8 小時。8 小時過後，規則計時器將會使一次性解鎖代號失效。

## 「iCloud 備份」Keybag

「iCloud 備份」Keybag 與備份 Keybag 類似。此 Keybag 中的所有類別密鑰皆為非對稱式 (與「未開啟檔案的保護」資料保護類別一樣，使用 Curve25519)。非對稱式 Keybag 也可用於「iCloud 鑰匙圈」其相關鑰匙圈還原作業的備份中。

## 替用開機模式保護密鑰的機制

「資料保護」的用途是限定只在成功驗證後，才會提供用戶資料存取權限給經授權的用戶。「資料保護」類別的設計目的是支援各種使用案例，例如即使裝置被鎖定（但需在初次解鎖後）仍可讀取和寫入某些資料的能力。處於替用開機模式期間，系統會執行其他步驟來保護用戶資料的存取，例如用於裝置韌體升級（DFU）模式、「還原」模式、「Apple 診斷」或軟件更新期間使用的模式。這些功能的基礎是硬件和軟件功能的組合，並隨着 Apple 設計的晶片發展而擴展。

功能	A10	A11、S3	A12、S4	A13、S5	A14、A15、S6、S7、M1 系列
還原：所有「資料保護」類別都受保護	✓	✓	✓	✓	✓
DFU 模式、「還原」和軟件更新的替用開機：類別 A、B 和 C 資料受保護		✓	✓	✓	✓

「安全隔離區 AES 引擎」配備可鎖定的軟件種子位元。從 UID 建立密鑰時，這些種子位元會包含在密鑰衍生函數中以建立其他密鑰階層。種子位元的使用方式因單晶片系統而異：

- 自 Apple A10 和 S3 SoC 起，種子位元專門用於區分受用戶密碼保護的密鑰。種子位元是為了需要用戶密碼的密鑰而設（包含「資料保護類別 A」、「類別 B」和「類別 C」密鑰），而無需用戶密碼的密鑰（包含檔案系統後設資料密鑰和「類別 D」密鑰）則會清除種子位元。
- 此外，在系統為 iOS 13 或較新版本和 iPadOS 13.1 或較新版本，且配備 A10 或較新版本的裝置上，當裝置開機進入「診斷模式」時，所有用戶資料都會因加密編譯而無法存取。方法為引入額外的種子位元，其設定管控着媒體密鑰的存取權，需使用此媒體密鑰才能存取以「資料保護」加密的資料卷宗上的後設資料（亦因此包括所有檔案的內容）。此保護涵蓋所有類別（A、B、C、D）所保護的檔案，而不只需要用戶密碼的檔案。
- 在 A12 SoC 上，如果「應用程式處理器」已進入裝置韌體升級（DFU）模式或還原模式，「安全隔離區 Boot ROM」會鎖定密碼種子位元。當密碼種子位元鎖定時，系統不會允許任何更改作業。其設計用意是防止存取受用戶密碼保護的資料。

在裝置進入 DFU 模式後進行還原，可讓裝置回到已知的正常狀態，該狀態可確保只會有未經修改且由 Apple 簽署的程式碼。DFU 模式可透過手動方式進入。

請參閱以下關於如何令裝置進入 DFU 模式的 Apple 支援文章：

裝置	文章
iPhone、iPad、iPod touch	<a href="#">如果忘記了 iPhone 密碼</a>
Apple TV	<a href="#">如果 Apple TV 顯示警告符號</a>
配備 Apple 晶片的 Mac	<a href="#">喚醒或回復配備 Apple 晶片的 Mac</a>

## 受攻擊時保護用戶資料

企圖截取用戶資料的攻擊者，通常會嘗試多種手法：將加密的資料截取到另一個媒介上，以進行暴力密碼破解攻擊；操縱作業系統版本；或是更改或弱化裝置的保安規則以便發動攻擊。如要攻擊裝置上的資料，通常需要使用實體介面（例如 Lightning 或 USB）來與裝置通訊。Apple 裝置提供的功能有助於抵禦這類攻擊。

Apple 裝置支援「**密封密鑰保護**」(SKP) 技術，其設計用意是確保加密編譯材料一旦離開裝置，或是如果作業系統版本或保安設定在無適當用戶授權的情況下被操縱，便無法進行存取。這個功能**並非**由「安全隔離區」提供，而是由位於較低層級的硬件暫存器支援，以便為解密非「安全隔離區」相關之用戶資料所需的密鑰，提供額外一層保護。

附註：SKP 只在配備 Apple 設計 SoC 的裝置上提供。

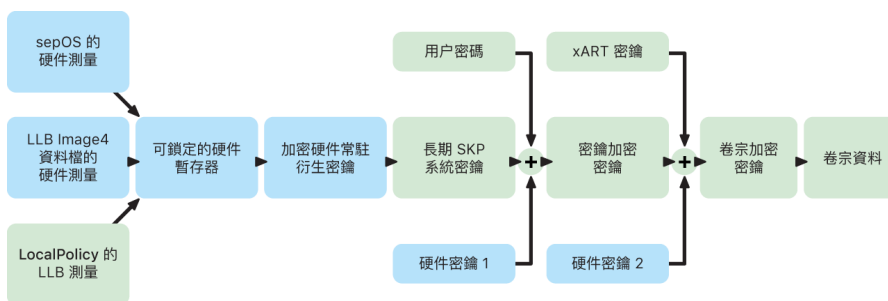
功能	A10	A11、S3	A12、S4	A13、S5	A14、A15、S6、S7、M1 系列
密封密鑰保護	✓	✓	✓	✓	✓

iPhone 和 iPad 也可以設定為只在更可能顯示裝置仍受到授權擁有者實體控制的情況下啟用資料連線。

## 密封密鑰保護 (SKP)

在支援「資料保護」的 Apple 裝置上，密鑰加密密鑰 (KEK) 受到系統上軟件的測量值保護 (或密封)，也與只能從「安全隔離區」取用的 UID 綁定。在配備 Apple 晶片的 Mac 上，整合了有關系統保安規則的資料，進一步強化了 KEK 的保護機制，因為 macOS 支援其他平台不支援的重要保安規則變更 (例如，停用安全啟動或 SIP)。在配備 Apple 晶片的 Mac 上，這個保護機制包含「**檔案保險箱**」密鑰，因為「檔案保險箱」是使用「資料保護」(類別 C) 來執行的。

衍生自用戶密碼、長期 SKP 密鑰和硬件密鑰 1 (「安全隔離區」的 UID) 的密鑰稱為**密碼衍生密鑰**。此密鑰用於保護用戶 Keybag (在所有受支援的平台上) 和 KEK (只在 macOS 上)，然後啟用生物識別解鎖或使用其他裝置 (如 Apple Watch) 來自動解鎖。



「安全隔離區開機監視器」會截取已載入「安全隔離區 OS」的測量值。當「應用程式處理器」的「Boot ROM」測量值附加至 LLB 的 Image4 資料檔時，該資料檔中也會包含其他所有已載入系統配對韌體的測量值。LocalPolicy 包含已載入 macOS 的核心保安設定。LocalPolicy 也包含 `nsih` 欄位，這是 macOS Image4 資料檔的雜湊值。macOS Image4 資料檔包含所有 macOS 配對韌體和核心 macOS 開機物件 (例如「開機核心集合」或簽署系統卷宗 (SSV) 根雜湊值) 的測量值。

如果攻擊者能未預期地更改任何上述任何測量韌體、軟件或保安設定元件，便會修改儲存在硬件暫存器中的測量值。修改測量值會造成由加密硬件衍生的**系統測量根密鑰 (SMRK)** 衍生出不同的值，實際上會破壞密鑰階層上的印章。而這會導致無法存取**系統測量裝置密鑰 (SMDK)**，進而導致無法存取 KEK 和資料。

然而，當系統未有受到攻擊，其必須根據合法軟件更新進行調適，這些更新會更改韌體測量值及 LocalPolicy 中的 nsih 欄位以指向新的 macOS 測量值。在其他企圖整合韌體測量值但沒有已知真實來源的系統中，用戶必須停用保安、更新韌體，然後再重新啟用，這樣才能截取新的測量基準。這大幅提高了攻擊者在軟件更新期間可能竄改韌體的風險。Image4 資料檔包含所需的一切測量值，對系統有所幫助。正常開機期間測量值相符時透過 SMRK 解密 SMDK 的硬件，也可以將 SMDK 加密為建議的未來 SMRK。藉由指定軟件更新後預期的測量值，硬件可以加密可在目前作業系統中存取的 SMDK，如此一來在未來作業系統中它仍保持可存取狀態。同樣地，當客戶合法更改 LocalPolicy 中的保安設定時，必須根據 LLB 電腦下次重新啟動時會運算的 LocalPolicy 測量值將 SMDK 加密為未來的 SMRK。

## 在 iOS 和 iPadOS 中安全啟用資料連線

在 iOS 或 iPadOS 裝置上，如果最近沒有建立任何資料連線，用戶必須使用 Face ID、Touch ID 或密碼，透過 Lightning、USB 或智慧型接點介面來啟用資料連線。這可限制實體連接裝置（例如惡意充電器）的攻擊面，但仍可在合理的時間限制內使用其他配件。如 iOS 或 iPadOS 裝置鎖定或終止配件的數據連線超過一小時，裝置便不會允許建立任何新數據連線，直到裝置解鎖。在這一小時期間，能允許的資料連線只有先前在裝置解鎖狀態下連接過的配件。這些配件在上次連接後會記住 30 日。如此期間有未知配件嘗試開啟數據連線，將會停用所有透過 Lightning、USB 和智慧型接點的配件數據連線，直到裝置再次解鎖。這一小時期間：

- 協助確保經常連接 Mac 或 PC、配件或連線至 CarPlay 的用戶無需在每次連接裝置時輸入密碼
- 為必要的，因為配件生態系統並不會在建立數據連線前提供加密方面可靠的方式來識別配件

此外，如果建立配件的數據連線超過 3 日，裝置會在鎖定後立即拒絕新的數據連線。此用意為替不常使用此類配件的用戶增加防護。當裝置處於需要密碼以重新啟用生物識別認證的狀態時，透過 Lightning、USB 和智慧型接點的數據連線也會被停用。

用戶可以在「設定」中選擇將數據連線的狀態重新啟用為「總是開放的」（設定部份輔助裝置會自動執行此操作）。

## 「Apple 檔案系統」的角色

「Apple 檔案系統」（APFS）是以加密為基礎所設計的專利檔案系統。APFS 可在所有 Apple 的平台上運作，如 iPhone、iPad、iPod touch、Mac、Apple TV 和 Apple Watch。此檔案系統針對快閃/SSD 儲存裝置最佳化，具備高強度加密、後設資料「寫入時複製」機制、空間共享、檔案與目錄複製、快照、快速目錄大小調整、原子化安全儲存基本型別，以及改良的檔案系統基礎，而且獨特的寫入時複製設計採用 I/O 聯合處理，以提供最高效能，同時確保資料可靠性。

### 空間共享

APFS 會按需要分配儲存空間。當單一 APFS 容器有多個卷宗時，該容器的可用空間會被分享，並可按需要分配至任何獨立的卷宗。每個卷宗只會使用整個容器中的一部份，所以可用空間為容器的總容量，減去容器中所有卷宗已使用的空間。

### 多個卷宗

在 macOS 10.15 或較新版本中，用來啟動 Mac 的 APFS 容器必須包含至少五個卷宗，而用戶無法看見前三個卷宗：

- **預開機卷宗**：此卷宗未有加密，並包含啟動容器中每個系統卷宗所需的資料。
- **VM 卷宗**：此卷宗未有加密，macOS 使用其來儲存加密的交換檔案。
- **還原卷宗**：此卷宗未有加密，必須在不解鎖系統卷宗的情況下使用，才能在 RecoveryOS 中啟動。
- **系統卷宗**：包含以下項目：
  - 所有啟動 Mac 必須的檔案
  - 所有 macOS 原生安裝的 App（原置於 /應用程式資料夾的 App 現置於「/系統/應用程式」）

- **附註:** 在預設情況下, 沒有任何程序可以寫入「系統」卷宗, 即使是 Apple 系統程序亦不可以。
- **資料卷宗:** 包含可以變更的資料, 例如:
  - 用戶資料夾內的任何資料, 包括相片、音樂、影片和文件
  - 用戶安裝的 App 包括 AppleScript、Automator 應用程式
  - 用戶、機構或第三方 App 安裝的自訂框架和服務程式
  - 用戶擁有且可寫入的其他位置, 如 /應用程式、/資源庫、/用戶、/Volumes、/usr/local、/private、/var 以及 /tmp

每當容器新增一個系統卷宗, 就會有一個資料卷宗隨之新增。Preboot、VM 和還原卷宗都是共享卷宗, 不能複製。

在 macOS 11 或較新版本中, 系統會儲存系統卷宗的快照。作業系統會從系統卷宗的快照啟動, 而不是從可變系統卷宗的唯讀裝載啟動。

在 iOS 和 iPadOS 中, 儲存空間分為至少兩個 APFS 卷宗:

- 系統卷宗
- 資料卷宗

## 鑰匙圈資料保護

許多 App 需要處理密碼和其他簡短但較為敏感的資料位元, 如密鑰和登入代號。鑰匙圈提供了儲存這些項目的安全方式。不同的 Apple 作業系統使用不同機制來強制執行連繫至不同鑰匙圈保護類別的保證。在 macOS 中 (包括配備 Apple 晶片的 Mac), 不會直接使用「資料保護」來強制執行這些保證。

### 概覽

「鑰匙圈」項目會使用兩種不同的 AES-256-GCM 密鑰進行加密: 資料表密鑰 (後設資料) 和資料列表密鑰 (秘密密鑰)。「鑰匙圈」後設資料 (kSecValue 以外的所有屬性) 會以後設資料密鑰加密來加速搜尋, 而密碼值 (kSecValueData) 會以秘密密鑰加密。後設資料密鑰受「安全隔離區」保護, 但會從「應用程式處理器」中快取, 以允許快速查詢鑰匙圈。秘密密鑰一律需要在「安全隔離區」中來回處理。

鑰匙圈是以儲存在檔案系統中的 SQLite 資料庫的方式導入。資料庫只有一個, 且 securityd 服務程式會決定哪些鑰匙圈項目可供各個處理程序或 App 存取。「鑰匙圈存取 API」會對服務程式發出呼叫, 進而查詢 App 的「Keychain-access-groups」、「application-identifier」和「application-group」權限。各個存取群組皆允許鑰匙圈項目在 App 間共享, 而不會將存取權限制於單一處理程序。

鑰匙圈項目只能在來自同一開發者的 App 間共享。為了共享鑰匙圈項目, 第三方 App 會使用加上前置碼的存取群組, 此前置碼是由 Apple Developer Program (Apple 開發者計劃) 透過應用程式群組所分配。對前置碼的要求和應用程式群組唯一性, 是透過程式碼簽署、配置描述檔和 [Apple Developer Program \(Apple 開發者計劃\)](#) 強制執行。

系統用來保護「鑰匙圈」資料的類別結構, 與檔案「資料保護」中使用的類別結構相似。這些類別具有與檔案「資料保護」類別相同的行為, 但使用的密鑰和功能不同。

可用性	檔案資料保護	鑰匙圈資料保護
未鎖定時	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
鎖定時	NSFileProtectionCompleteUnlessOpen	N/A
首次解鎖後	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
總是可以	NSFileProtectionNone	kSecAttrAccessibleAlways
已啟用密碼時	N/A	kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

使用背景重新整理服務的 App 可將 **kSecAttrAccessibleAfterFirstUnlock** 用於背景更新期間需要存取的鑰匙圈項目。

類別 **kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly** 的行為與 **kSecAttrAccessibleWhenUnlocked** 相同；不過只有在裝置已設定密碼時才能使用。此類別只存在於系統 Keybag 中，且具有以下特性：

- 不會同步到 iCloud 鑰匙圈
- 不會進行備份
- 不會納入託管 Keybag 中

如密碼遭移除或重設，系統便會捨棄類別密鑰，這些項目也變得無法使用。

其他鑰匙圈類別都有對應的「僅限本裝置」項目，其在備份期間從裝置複製時一律受到 UID 保護，因此如回復到其他裝置，將會無法使用。Apple 依據所保護資料的類型和 iOS 和 iPadOS 需要這些資料的時間來選擇鑰匙圈類別，妥善地在保安與可用性之間取得平衡。例如，VPN 證書必須隨時可供使用，這樣裝置才能保持連續的連線，但 VPN 證書被分類為「不可遷移」類別，因此無法將其移至另一部裝置。

## 「鑰匙圈」資料類別保護

系統會為鑰匙圈項目強制執行下列的類別保護：

項目	可存取
Wi-Fi 密碼	首次解鎖後
郵件帳戶	首次解鎖後
Microsoft Exchange ActiveSync 帳戶	首次解鎖後
VPN 密碼	首次解鎖後
LDAP、CalDAV、CardDAV	首次解鎖後
社交網絡帳戶代號	首次解鎖後
「接手」廣播加密密鑰	首次解鎖後
iCloud 代號	首次解鎖後
iMessage 密鑰	首次解鎖後
家庭共享密碼	未鎖定時
Safari 密碼	未鎖定時

項目	可存取
Safari 書籤	未鎖定時
Finder/iTunes 備份	未鎖定時, 不可遷移
由設定描述檔所安裝的專用密鑰	未鎖定時, 不可遷移
VPN 證書	總是可以, 不可遷移
Bluetooth® 密鑰	總是可以, 不可遷移
Apple 推送通知服務 (APNs) 代號	總是可以, 不可遷移
iCloud 證書和專用密鑰	總是可以, 不可遷移
SIM PIN	總是可以, 不可遷移
由設定描述檔所安裝的憑證	總是可以
「尋找」代號	總是可以
留言信箱	總是可以

### 「鑰匙圈」存取權限控制

「鑰匙圈」可使用連線權限控制列表 (ACL) 來設定能否存取和認證需求的規則。項目可以設定在哪些條件下必須由用戶親身進行認證, 方法是指定使用 Face ID、Touch ID 或輸入裝置密碼進行認證, 否則無法存取。如要進一步限制項目存取權限, 可指明 Face ID 或 Touch ID 的登記內容在該項目加入後沒有經過更改。此限制有助於防止攻擊者加入自己的指紋來存取鑰匙圈項目。ACL 會在「安全隔離區」中進行評估, 只有符合其指定的限制條件時, 才匯出到核心中。

### 在 macOS 中的「鑰匙圈架構」

macOS 也提供鑰匙圈的存取權限, 可方便且安全地儲存用戶名稱和密碼、電子識別身份、加密密鑰和安全備註。在「/應用程式/工具程式/」中開啟「鑰匙圈存取」App 便可存取。使用鑰匙圈讓用戶不需要輸入 (甚至記住) 每項資源的憑證。系統已為每位用戶建立初始的預設鑰匙圈, 但用戶可為特定用途建立其他鑰匙圈。

除了仰賴用戶鑰匙圈外, macOS 還需要許多系統層級的鑰匙圈, 以維護不屬於特定用戶的認證資產, 如網絡憑證和公用密鑰基礎架構 (PKI) 識別身份。其中一種鑰匙圈為無法變更的「系統根」, 它儲存了互聯網 PKI 根憑證授權管理中心 (CA) 的憑證, 可讓網絡銀行業務和電子商務等常見作業更加順利。用戶能以類似方式將內部配置的 CA 憑證部署到受管理的 Mac 電腦上, 以協助驗證內部站台和服務。

# 檔案保險箱

## 在 macOS 中使用「檔案保險箱」進行卷宗加密

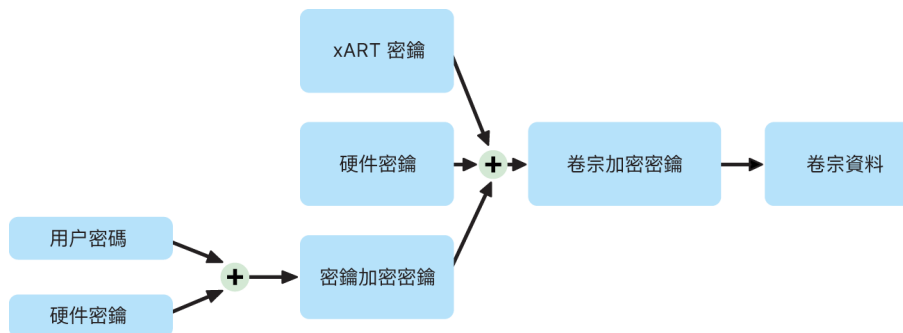
Mac 電腦會提供「檔案保險箱」，這是內置的加密功能，用以保護所有靜態資料。「檔案保險箱」使用 AES-XTS 資料加密演算法來保護在內置及可移除的儲存裝置中的完整卷宗。

配備 Apple 晶片的 Mac 上的「檔案保險箱」，執行時是使用「資料保護」的「類別 C」（採用卷宗密鑰）。在配備 Apple T2 保安晶片的 Mac 以及配備 Apple 晶片的 Mac 上，直接連接「安全隔離區」的加密內置儲存裝置會使用其硬件安全功能以及 AES 引擎的功能。用戶在 Mac 上啟用「檔案保險箱」後，需在開機程序進行期間提供其憑證。

### 「檔案保險箱」啟用時的內置儲存裝置

即使實體儲存裝置已卸除並連接其他電腦，如沒有提供有效的登入憑證資料或加密還原密鑰，內部 APFS 卷宗會維持加密狀態並禁止未經授權的存取。在 macOS 10.15 中，這還包含系統卷宗和資料卷宗。從 macOS 11 開始，系統卷宗藉由簽署系統卷宗 (SSV) 功能受到保護，但資料卷宗仍以加密保護。在配備 Apple 晶片以及配備 T2 晶片的 Mac 上，內部卷宗加密的實行方式為建構和管理密鑰階層結構，並以晶片上內置的硬件加密技術為基礎來建置。這個密鑰階層結構的設計目的為同時達到四個目標：

- 要求用戶密碼來進行解密
- 保護系統免受針對從 Mac 上移除的儲存空間媒體的暴力密碼破解攻擊
- 提供快捷及安全的方法以透過刪除必要的加密編譯材料來清除內容
- 讓用戶更改其密碼（亦因此更改了用於保護其檔案的加密編譯密鑰），無需將整個卷宗重新加密

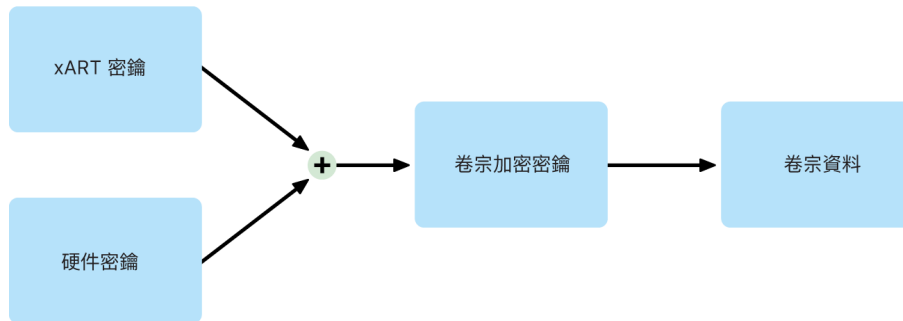


在配備 Apple 晶片以及配備 T2 晶片的 Mac 上，所有「檔案保險箱」密鑰的處理作業會在「安全隔離區」中進行；系統永不會向 Intel CPU 直接提供加密密鑰。所有 APFS 卷宗預設以卷宗加密密鑰製作。卷宗及後設資料內容會以此卷宗加密密鑰來加密，此卷宗加密密鑰使用類別密鑰封裝。當「檔案保險箱」已啟用時，類別密鑰受用戶密碼和硬件 UID 的合併保護。



## 「檔案保險箱」關閉時的內置儲存裝置

如在配備 Apple 晶片以及配備 Apple T2 保安晶片的 Mac 上，「檔案保險箱」在初始「設定輔助程式」步驟中未有啟用，卷宗仍會維持加密，但卷宗加密密鑰只會由「安全隔離區」中的硬件 UID 保護。



如稍後「檔案保險箱」被啟用（在檔案被加密後的即時步驟）重播機制會協助防止舊密鑰（只以硬件 UID 為基礎）被用於解密卷宗。卷宗之後會受用戶密碼和之前提及的硬件 UID 的合併保護。

## 刪除「檔案保險箱」卷宗

刪除卷宗時，其卷宗加密密鑰會由「安全隔離區」安全地刪除。這有助防止未來再以此密鑰存取卷宗，即使是「安全隔離區」也無法辦到。此外，所有卷宗加密密鑰都會以媒體密鑰封裝。媒體密鑰不會提供額外的資料機密性，不過其設計目標是讓資料能快捷及安全地刪除，因為如沒有此密鑰將不可能解密。

在配備 Apple 晶片以及配備 T2 晶片的 Mac 上，保證會透過「安全隔離區」的支援技術（例如遙距 MDM 指令）來清除媒體密鑰。以此方式清除媒體密鑰，會讓卷宗因加密編譯而無法存取。

## 可移除的儲存裝置

可移除的儲存裝置的加密不會使用「安全隔離區」的保安功能，其加密方式與沒有配備 T2 晶片的以 Intel 為基礎的 Mac 的方式相同。

## 在 macOS 中管理檔案保險箱

在 macOS 中，機構可以使用 SecureToken 或「Bootstrap 代號」來管理「檔案保險箱」。

### 使用安全代號

macOS 10.13 或較新版本中的「Apple 檔案系統」(APFS) 更改了產生「檔案保險箱」加密密鑰的方式。在舊版 macOS 的 CoreStorage 卷宗上，「檔案保險箱」加密程序中使用的密鑰，是在用戶或機構於 Mac 上啟用「檔案保險箱」時所製作。在 APFS 卷宗上的 macOS 中，密鑰則是在建立用戶期間、設定第一位用戶的密碼或 Mac 用戶的首次登入期間產生的。這種加密密鑰實行方式、產生時間，以及儲存方式皆為「安全代號」的功能之一部份。具體來說，安全代號是封裝版本的密鑰加密密鑰 (KEK)，受用戶的密碼保護。

在 APFS 上部署「檔案保險箱」時，用戶可繼續：

- 使用現有工具和程序，例如可以流動裝置管理 (MDM) 解決方案儲存的個人還原密鑰 (PRK) 進行託管
- 建立和使用機構還原密鑰 (IRK)
- 延遲啟用「檔案保險箱」，直至用戶登入或登出 Mac

在 macOS 11 中，為 Mac 上的第一位用戶設定初始密碼會讓該用戶取得安全代號。在某些工作流程中，這可能不是你期望的行為，就像以前一樣，授予第一個安全代號應當需要登入用戶帳戶。為了避免此情況發生，請在設定用戶的密碼前，先將 `;DisabledTags;SecureToken` 加入程式所建立的用戶 `AuthenticationAuthority` 屬性中。

```
sudo dscl . append /Users/<user name> AuthenticationAuthority  
";DisabledTags;SecureToken"
```

### 使用 Bootstrap 代號

macOS 10.15 引入了新功能「Bootstrap 代號」，以協助將安全代號授予流動帳戶和透過註冊建立的選擇性裝置管理員帳戶（「受管理的管理員」）。在 macOS 11 中，Bootstrap 代號可以向登入到 Mac 電腦的任何用戶（包括本機用戶帳戶）授予安全代號。使用 macOS 10.15 或更新版本的「Bootstrap 代號」功能有以下要求：

- 使用 Apple School Manager 或 Apple Business Manager 在 MDM 中註冊 Mac，這樣會讓 Mac 受監管
- MDM 廠商支援

如果 MDM 解決方案支援此功能，在 macOS 10.15.4 或較新版本中，任何已啟用安全代號的用戶初次登入時，系統會產生 Bootstrap 代號並交由 MDM 託管。如有需要，也可使用 `profiles` 命令列工具來產生 Bootstrap 代號並交由 MDM 託管。

在 macOS 11 中，Bootstrap 代號除了用來將安全代號授予用戶帳戶外還有其他用途。在配備 Apple 晶片的 Mac 上，如果使用 MDM 進行管理，則 Bootstrap 代號（如果可用）可用來授權安裝核心延伸功能和軟件更新項目。

# Apple 如何保護用戶的個人資料

## 保護 App 對用戶資料的存取

除了對靜態資料進行加密外，Apple 裝置會使用包含 Data Vault 在內的各種技術來防止 App 在未授權下存取用戶的個人資料。用戶可以在 iOS 和 iPadOS 的「設定」和 macOS 的「系統偏好設定」中，查看哪些 App 有權存取特定資料，亦可授予或撤銷往後的任何存取權。下列項目獲強制存取權限：

- iOS、iPadOS 及 macOS：日曆、相機、通訊錄、咪高風、相片、提醒事項、語音識別
- iOS 及 iPadOS：藍牙、家居、媒體、「媒體」App 及 Apple Music、動態與健身
- iOS 和 watchOS：健康
- macOS：輸入監察（例如，鍵盤筆劃）、提示、螢幕錄製（例如，靜態螢幕截圖及錄影）、系統偏好設定

在 iOS 13.4 或較新版本和 iPadOS 13.4 或較新版本中，所有第三方 App 都會自動以 Data Vault 保護其資料。Data Vault 有助於防止資料遭未經授權存取，即使程序本身未經過沙盒處理也一樣。iOS 15 或較新版本中的其他類別包括「本地網絡」、「四周互動」、「研究感應器與使用狀況資料」以及「專注模式」。

如果用戶登入 iCloud，在 iOS 和 iPadOS 中預設便會授予 App 存取「iCloud 雲碟」的權限。用戶可以在「設定」中的 iCloud 下方控制每個 App 的存取權限。iOS 和 iPadOS 也會提供存取限制，其設計用意是防止資料在流動裝置管理 (MDM) 解決方案和用戶所安裝的 App 和帳戶之間移動。

## 保護對用戶健康資料的存取

HealthKit 為 iPhone 和 Apple Watch 上的健康和健身資料提供了一個中央儲存庫。HealthKit 也可直接用於健康與健身裝置，如相容的低耗電藍牙 (BLE) 心率監視器以及許多 iOS 裝置內置的動作協同處理器。所有與健康與健身 App、醫療機構，和健康與健身裝置的 HealthKit 互動都需要用戶的許可。此資料會以「未開啟檔案的保護」的「資料保護」類別來儲存。裝置鎖定後 10 分鐘便會捨棄資料存取權限，當用戶下次輸入密碼或使用 Face ID 或 Touch ID 來解鎖裝置時，即可再次存取資料。

### 收集和儲存健康與健身資料

HealthKit 也會收集和儲存管理資料，如 App 的存取權限、連接 HealthKit 的裝置名稱及排程資料（用來在新資料可用時啟動 App）。此資料會以「首次用戶認證前的保護」的「資料保護」類別來儲存。臨時日誌檔會儲存當裝置鎖定時產生的健康記錄（例如當用戶運動時）。這些臨時日誌檔會以「未開啟檔案的保護」的「資料保護」類別來儲存。當裝置解鎖時，會將臨時日誌檔輸入主要的健康資料庫中，然後在合併作業完成時刪除。

健康資料可儲存在 iCloud 中。「健康」資料的點對點加密需要 iOS 12 或較新版本及雙重認證。否則，用戶的資料仍會在儲存與傳輸期間加密，但不會以點對點加密。用戶開啟雙重認證並更新至 iOS 12 或較新版本後，其健康資料會轉移到點對點加密。

如用戶以 Finder (macOS 10.15 或較新版本) 或 iTunes (macOS 10.14 或較早版本) 備份裝置，只有備份經過加密的情況下才會儲存健康資料。

### 臨床健康記錄

用戶可以在「健康」App 內登入支援的健康系統，以取得一份臨床健康記錄。將用戶連接到健康系統時，用戶需使用 OAuth 2 用戶端憑證進行驗證。連線成功後，便會使用 TLS 1.3 受保護的連線直接從醫療機構下載臨床健康記錄資料。下載資料後，臨床健康記錄會安全地與其他健康資料一起儲存。

## 「健康」資料完整性

儲存在資料庫中的資料包含追蹤每筆資料記錄出處的后設資料。此後設資料包含 App 識別碼，可識別哪個 App 儲存了該記錄。此外，選擇性的后設資料項目可包含記錄的電子簽署副本。此用意是提供記錄（由受信任之裝置所產生）的資料完整性。用於電子簽署的格式為 [RFC 5652](#) 中所指定的加密編譯訊息語法 (Cryptographic Message Syntax, CMS)。

## 第三方 App 存取的健康資料

對 HealthKit API 的存取是使用授權來控制，而 App 必須符合資料使用方式的限制。例如，App 不允許將健康資料用於廣告用途。App 也必須提供私隱權政策給用戶，並詳述其對健康資料的使用方式。

App 對健康資料的存取權限是受用戶的「私隱」設定所控制。當 App 要求存取健康資料時（類似於「通訊錄」、「相片」和其他 iOS 資料來源），系統會要求用戶授予存取權限。然而，使用健康資料時，App 會獲得讀取和寫入資料的獨立存取權，以及各種類型健康資料的獨立存取權限。用戶可以在「設定」>「健康」>「資料存取及裝置」中檢視和撤銷他們授予存取健康資料的權限。

如 App 取得寫入資料的權限，便也可讀取其寫入的資料。如 App 取得讀取資料的權限，App 便可讀取所有來源所寫入的資料。然而，App 無法判定其他 App 被授予的存取權限。此外，App 無法確切得知它們是否已獲得健康資料的讀取存取權限。當 App 沒有讀取權時，所有查詢並不會傳回資料，就如同空白資料庫會傳回的相同回應一樣。其設計用意是避免 App 藉由得知用戶正在追蹤的資料類型，來推測用戶的健康狀態。

## 用戶的「醫療檔案」

「健康」App 可讓用戶選擇填寫「醫療檔案」表單，內有發生緊急醫療事故時所需的重要資料。此資料是手動輸入或更新，並不會與健康資料庫中的資料進行同步。

你可點一下鎖定畫面上的「緊急服務」按鈕來檢視「醫療檔案」資料。此資料會使用「無保護」的「資料保護」類別來儲存於裝置上，如此一來無須輸入裝置密碼即可存取。「醫療檔案」是選擇性的功能，可讓用戶決定如何同時在安全和私隱考慮上取得平衡。此資料在 iOS 13 或較早版本中會備份在「iCloud 備份」中。在 iOS 14 中，「醫療檔案」會使用 CloudKit 在裝置間同步，並具有與其餘健康資料相同的加密特性。

## 健康分享

在 iOS 15 中，「健康」App 為用戶提供了與其他用戶分享「健康」資料的選項。「健康」資料會使用點對點 iCloud 加密在兩位用戶之間分享，而 Apple 無法取用透過「健康」分享所傳送的資料。如要使用此功能，傳送的用戶和接收的用戶都必須執行 iOS 15 或較新版本，並已啟用雙重認證。

用戶也可以選擇使用「健康」App 中的「與提供者分享」功能，與他們的醫療保健提供者分享他們的「健康」資料。使用此功能分享的資料僅供用戶使用點對點加密所選的醫療機構使用，Apple 並不會維護或取用加密密鑰來解密、檢視或以其他方式取用透過「與提供者分享」功能所分享的「健康」資料。如要進一步了解此服務的設計如何保護用戶的「健康」資料，請參閱 Apple 醫療服務組織註冊指南 (Apple Registration Guide for Healthcare Organizations) 的「[保安與私隱](#)」章節。

# 電子簽署與加密

## 連線權限控制列表

鑰匙圈資料會被分割並使用連線權限控制列表 (ACL) 加以保護，因此由第三方 App 所儲存的認證並無法由其他識別身份的 App 存取，除非用戶明確核准那些 App。此保護措施能針對機構在 Apple 裝置中使用的各種應用程式與服務提供保護認證身份的機制。

## 郵件

在「郵件」App 中，用戶可以傳送經電子簽署及加密的訊息。「郵件」會在相容智慧卡中所附加的「個人識別驗證」(PIV) 代號上，於電子簽署和加密憑證上自動搜索適用的 [RFC 5322](#) (區分大小寫) 電郵地址主旨或主旨替代名稱。如果設定的電郵帳戶符合附加 PIV 代號上電子簽署和加密憑證中的電郵地址，「郵件」就會自動在新訊息視窗的工具列中顯示簽名按鈕。如果「郵件」具有收件人的電郵加密憑證或可在 Microsoft Exchange 的全域通訊清單 (GAL) 找到有關憑證，解鎖圖像便會顯示在新郵件的工具列中。鎖住的鎖頭圖像表示將以收件人的公用密鑰加密訊息後再傳送。

## 個別訊息專屬 S/MIME

iOS、iPadOS 及 macOS 支援個別訊息專屬 S/MIME。這代表 S/MIME 用戶可選擇預設總是簽署及加密每個訊息，或簽署及加密個別訊息。

配合 S/MIME 使用的身份可使用設定描述檔、流動裝置管理 (MDM) 解決方案、簡易證書註冊協定 (SCEP) 或 Microsoft Active Directory 證書授權單位傳送到 Apple 裝置。

## 智慧卡

macOS 10.12 或較新版本包括對 PIV 卡的原生支援。這些卡廣泛用於商業和政府機構的雙重認證、電子簽署和加密用途。

智慧卡包含一或多個電子身份識別，具有成對的公用和專用密鑰及綁定的憑證。使用個人識別碼 (PIN) 解鎖智慧卡便可存取用於認證、加密和簽署作業的專用密鑰。憑證決定了密鑰的用途、哪些屬性與其有關聯，以及是否經過憑證授權管理中心 (CA) 驗證 (簽署)。

智慧卡可用於雙重認證。解鎖卡的兩個元素為「用戶所有」(該卡) 及「用戶所知」(PIN)。macOS 10.12 或較新版本亦對智慧卡「登入視窗」驗證，及在 Safari 上對網站的用戶端證書驗證提供原生支援。另亦支援使用密鑰組 (PKINIT) 的 Kerberos 驗證來進行單一登入至支援 Kerberos 的服務。如要進一步了解有關智慧卡和 macOS 的更多資料，請參閱「[Apple 平台部署](#)」中的 [智慧卡整合簡介](#)。

## 加密磁碟映像檔

在 macOS 中，加密的磁碟映像用作安全容器，用戶可在其中儲存或傳送敏感文件及其他檔案。加密的磁碟映像使用位於「/應用程式/工具程式」中的「磁碟工具程式」製作。磁碟映像可使用 128 位元或 256 位元 AES 加密來加密。因為已裝載的磁碟映像被視為連接 Mac 的本機卷宗，用戶可以複製、移動及開啟在其中儲存的檔案及資料夾。如同「檔案保險箱」，磁碟映像會被實時加密及解密。使用加密的磁碟映像，用戶可透過將加密的磁碟映像儲存至可卸除式媒體來安全地交換文件、檔案及資料夾；將其以電郵訊息附件傳送；或將其儲存在遙距伺服器。如需加密磁碟映像檔的詳細資料，請參閱 [磁碟工具程式使用手冊](#)。

# App 保安

## App 保安概覽

App 是現在安全架構最關鍵的要素之一。雖然 App 可顯著提高用戶的生產力，但如處理不當，也可能對系統保安、穩定性和用戶資料產生負面影響。

因此 Apple 提供多層保護，以協助確保 App 沒有包含已知的惡意軟件且未遭竄改，更有額外的保護機制強制要求謹慎協調 App 對用戶資料的存取。這些保安控制項目為 App 提供了穩定且安全的平台，讓成千上萬的開發者能夠為 iOS、iPadOS 及 macOS 提供數十萬款的 App，當中無一會影響系統的完整性。用戶可以在其 Apple 裝置上存取這些 App，無須過度擔心病毒、惡意軟件或未經授權的攻擊。

在 iPhone、iPad 和 iPod touch 上，所有 App 需經由 App Store 取得，且所有 App 都經過沙盒技術限制，以提供最嚴格的控制項目。

在 Mac 上，許多 App 是從 App Store 取得，但是 Mac 用戶也可以從互聯網下載並使用 App。為了安全支援互聯網下載，macOS 提供多層額外控制。首先，在 macOS 10.15 或較新版本的預設狀態下，所有 Mac App 均需要經由 Apple 公證才能啟動。此要求有助於確保這些 App 中不含已知的惡意軟件，同時讓這些 App 可以不透過 App Store 來提供。此外，macOS 包含最先進的防毒保護機制，可封鎖惡意軟件並在必要時予以移除。

作為額外的控制存取平台，沙盒處理可協助保護用戶資料，避免 App 未經授權存取。在 macOS 中，重要區域中的資料本身就受到保護，因此可有助於確保用戶保留針對所有 App 對「桌面」、「文件」、「下載項目」或其他區域中的檔案之存取控制權，無論嘗試存取的 App 本身是否以沙盒技術限制。

原生能力	第三方的對應功能
不獲批准的外掛模組列表，不獲批准的 Safari 延伸功能列表	病毒/惡意軟件定義
檔案隔離	病毒/惡意軟件定義
XProtect/YARA 簽名	病毒/惡意軟件定義；端點防護
守衛	端點防護：在 App 上強制執行程式碼簽名，以協助確保僅執行受信任的軟件。
efiheck (未配備 Apple T2 保安晶片的 Mac 必備)	端點防護：rootkit 偵測
應用程式防火牆	端點防護；防火牆
封包過濾器 (pf)	防火牆解決方案
系統完整保護	內置於 macOS

原生能力	第三方的對應功能
強制性存取控制	內置於 macOS
kext 排除列表	內置於 macOS
強制性 App 程式碼簽署	內置於 macOS
App 公證	內置於 macOS

## iOS 和 iPadOS 中的 App 保安

### iOS 和 iPadOS 的 App 保安簡介

與其他流動平台不同，iOS 和 iPadOS 不允許用戶從網站下載安裝可能有惡意性質且未經簽署的 App，或者執行不受信任的 App。執行時，會在載入所有可執行記憶體頁面後對其進行程式碼簽名檢查，以協助確保 App 自安裝或上次更新後未遭修改過。

確認 App 來自核准的來源後，iOS 和 iPadOS 會強制執行相關的安全措施，以防止該 App 危害其他 App 或系統的其他部份。

### iOS 和 iPadOS 的 App 程式碼簽署程序

在 iOS 和 iPadOS 中，Apple 透過強制程式碼簽署、嚴格的開發者登入程序等方式來提供 App 保安。

#### 強程式碼簽署

iOS 或 iPadOS 核心啟動後，會控制哪些用戶程序和 App 可執行。為了協助確保所有 App 均來自核准的已知來源且未經竄改，iOS 及 iPadOS 會要求所有可執行的程式碼均使用 Apple 核發的證書進行簽署。裝置所隨附的 App (如「郵件」和 Safari) 則由 Apple 簽署。第三方 App 也必須使用 Apple 核發的證書進行驗證和簽署。強制性程式碼簽署將信任鏈的概念從作業系統延伸至 App，可有助於防止第三方 App 載入未簽署的程式碼資源，或使用自行修改的程式碼。

#### 開發者如何簽署其 App

開發者可以透過憑證驗證 (透過 Apple Developer Program (Apple 開發者計劃)) 對他們的 App 進行簽署。他們亦可以將程式碼嵌入 App，並以 Apple 核發的證書驗證其程式碼 (透過團隊識別碼字串)。

- **證書驗證：**如要在 iOS 或 iPadOS 裝置中開發並安裝 App，開發者必須向 Apple 註冊並加入 Apple Developer Program (Apple 開發者計劃)。Apple 會先驗證每位開發者 (無論是個人或企業) 的真實身份，然後再核發憑證。開發者可使用該憑證對 App 進行簽署，並將其提交至 App Store 進行發佈。因此，App Store 中的所有 App 都是由身份可識別的個人或機構提交的，藉此阻止製作惡意 App。這些 App 都經過 Apple 審核，以協助確保它們一般可以如所述方式執行，且沒有明顯的程式錯誤或其他顯著的問題。除了已討論過的技術外，此挑選過程還會讓用戶對所購買的 App 的品質更加放心。
- **程式碼簽署驗證：**iOS 及 iPadOS 允許開發者將程式碼嵌入 App 中，以便供 App 本身或 App 內嵌入的延伸功能使用。為了保護系統並防止其他 App 在其地址空間中載入第三方的程式碼，系統將會為啟動程序時所連結的所有動態資料庫執行程式碼簽署驗證。此驗證過程透過團隊識別碼 (Team ID) 來達成，該識別碼取自 Apple 核發的證書。團隊識別碼是 10 個字元的英數字元字串，例如 1A2B3C4D5F。程式碼可透過連結到隨系統發佈的任何資料庫平台，或其程式碼簽署中具有相同團隊識別碼的資料庫平台來成為主要執行檔。因為作為系統一部份發佈的可執行檔不具有團隊識別碼，所以只能連結到隨系統本身發佈的資料庫。

## 驗證專有的內部 App

合資格的企業也可以編寫供機構內部使用之專有的內部 App，並分發給員工。企業和機構可以請加入 Apple Developer Enterprise Program (ADEP, Apple 開發者企業計劃)。如需更多資料並檢閱資格要求，請參閱：[Apple Developer Enterprise Program 網站](#)。機構成為 ADEP 的成員後，便可註冊以獲得一個配置描述檔，該描述檔允許專有的內部 App 在其授權的裝置上執行。

用戶必須安裝配置描述檔才能執行這些 App。這有助於確保只有機構要求的用戶能夠將 App 載入到其 iOS 及 iPadOS 裝置上。透過流動管理裝置 (MDM) 安裝的 App 會間接獲得信任，因為機構與裝置間的關係已建立。在其他情況下，用戶必須在「設定」中核准 App 的配置描述檔。機構也可以限制用戶，不允許其核准來自未知開發者的 App。第一次啟動任何專有的內部 App 時，裝置必須從 Apple 收到允許執行 App 的肯定確認。

## iOS 及 iPadOS 中的執行階段的保安

iOS 和 iPadOS 藉由使用「沙盒」、宣告授權及地址空間配置隨機載入 (ASLR) 來協助確保執行階段的保安。

### 沙盒處理

所有第三方的 App 均會以沙盒技術限制，因此在存取其他 App 儲存的檔案或對裝置進行變更時會受到限制。沙盒處理的設計用意是防止 App 收集或修改其他 App 儲存的資料。每個 App 都有用於存放其檔案的唯一主目錄，主目錄是在安裝 App 時隨機指定的。如果第三方的 App 需要存取除了本身資料以外的其他資料，只能透過 iOS 及 iPadOS 明確提供的服務來執行。

系統檔案和資源也會與用戶的 App 加以區隔。大部份的 iOS 和 iPadOS 系統檔案和資源會執行為非特權用戶「流動裝置」，如同所有第三方 App。整個作業系統分割區會裝載為唯讀。不必要的工具 (如遙距登入服務) 並未包含在系統軟件中，且 API 不允許 App 提升自己的特殊權限來修改其他 App 或 iOS 和 iPadOS 本身。

### 使用授權

系統使用宣告的授權來控制第三方 App 對用戶資料與功能 (如 iCloud 和延伸功能) 的存取權限。授權 (Entitlement) 是簽署到 App 中的成對密鑰值，允許對執行階段因素以外的內容 (如 UNIX 用戶 ID) 進行認證。授權已經過電子簽署，因此無法更改。系統 App 和服務程式廣泛使用授權來執行特定權限的操作，如果不使用授權，則需要以根用戶身份執行程序。這大幅降低了遭入侵的系統 App 或服務程式提升權限的可能性。

此外，App 只能透過系統提供的 API 來執行背景處理。這讓 App 能夠繼續執行，而不會降低效能或大幅影響電池壽命。

### 地址空間佈局隨機化

地址空間佈局隨機化 (ASLR) 有助於防止利用記憶體損壞錯誤的攻擊。內置 App 會使用 ASLR 來協助確保啟動時隨機安排所有記憶體區域。除了在啟動時運作，ASLR 會隨機安排可執行檔程式碼、系統資料庫和相關程式設計結構的記憶體地址，進一步降低遭到許多攻擊的可能性。例如，「return-to-libc」攻擊試圖藉由操縱疊放和系統資源庫的記憶體地址來誘使裝置執行惡意的程式碼。隨機安排這些項目的位置便能增加執行攻擊的難度，尤其是對多部裝置的攻擊。Xcode 以及 iOS 或 iPadOS 開發環境，可自動編譯啟用了 ASLR 支援的第三方 App。

### Execute Never 功能

iOS 和 iPadOS 使用 ARM 的 Execute Never (XN) 功能來提供進一步的保護，該功能會將記憶體頁面標示為不可執行。App 如要使用標示為可寫入和可執行的記憶體頁面，須符合以下受嚴格控制的條件：核心會檢查 Apple 專屬的動態程式碼簽署授權是否存在。即使如此，也只有單個 mmap 呼叫能用於要求一個可執行且可寫入的記憶體頁面 (系統為其指定了隨機地址)。Safari 就是將此功能用於 JavaScript Just-in-Time (JIT) 編譯器。



## iOS、iPadOS 和 macOS 中的支援延伸功能

iOS、iPadOS 和 macOS 讓 App 可透過延伸功能來對其他 App 增加功能。延伸功能是具有特殊用途的已簽署可執行二進位程式碼，封裝在 App 內。安裝期間，系統會自動偵測延伸功能，並讓使用相符系統的其他 App 使用這些延伸功能。

### 延伸點

支援延伸功能的系統區域稱為**延伸點**。每個延伸點都提供 API，並為該區域強制執行規則。系統依據延伸點特定的比對規則來決定哪些延伸功能可供使用。系統會自動視需要啟動延伸功能程序，並管理這些程序的生命週期。授權可用來限制特定系統 App 的延伸功能可用性。例如，「今日」顯示方式小工具只會在「通知中心」內顯示，而共享的延伸功能則只能從「共享」面板中使用。舉例來說，「今日」小工具、「分享」、「動作」、「相片編輯」、「檔案提供程式」和「自訂鍵盤」都是延伸點。

### 延伸功能的通訊方式

延伸功能會在自己的地址空間中執行。App 與其啟動的延伸功能之間的通訊使用由系統架構所協調的程序間通訊。它們無法存取彼此的檔案或記憶體空間。延伸功能的設計旨在將它們彼此區隔、與包含該延伸功能的 App 區隔，並且與使用它們的 App 加以區隔。與其他第三方 App 類似，延伸功能也以沙盒技術限制，且擁有的容器會與包含 App 的容器隔開。不過，延伸功能與其容器 App 對私隱控制具有相同的存取權限。因此，如用戶對 App 授予「通訊錄」的存取權限，該 App 中嵌入的延伸功能也會獲得此許可權，但由 App 啟動的延伸功能則不具有該許可權。

### 自訂鍵盤的使用方式

自訂鍵盤是一種特殊類型的延伸功能，因為它是由用戶啟用並適用於整個系統。在其啟用後，該鍵盤延伸功能將會用於所有的文字欄位，但密碼輸入和任何安全文字的顯示方式除外。為了限制用戶資料的傳送，在預設情況下自訂鍵盤是在一個十分受限的沙盒中執行，該沙盒會阻止連接網絡、阻止代表程序執行網絡操作的服務，並阻止可允許延伸功能暗中導出輸入資料的 API。自訂鍵盤的開發者可以要求其延伸功能擁有「開放存取」的權限，讓系統在得到用戶的同意後在預設的沙盒中執行延伸功能。

### MDM 及延伸功能

對於在流動管理裝置 (MDM) 解決方案中註冊的裝置，文件和鍵盤延伸功能將遵循「受管理的開啟方式」規則。例如，MDM 解決方案可協助阻止用戶將受管理 App 中的文件輸出到未受管理的「文件提供者」，或協助阻止他們在受管理的 App 中使用未受管理的鍵盤。此外，App 開發者可防止在其 App 中使用第三方的鍵盤延伸功能。

## iOS 及 iPadOS 中的 App 保護及 App 群組

在 iOS 和 iPadOS 中，機構可以使用 iOS SDK 並透過在 Apple Developer Portal (Apple 開發者入口網站) 上加入 App 群組，安全地保護 App。

### 在 App 中採用「資料保護」功能

iOS 和 iPadOS 的 iOS 軟件開發套件 (SDK) 提供全套 API，讓第三方和企業內部開發者能夠輕鬆地採用「資料保護」功能，有助於確保在 App 中享有最高層級的保護。「資料保護」適用於檔案和資料庫 API，包括 `NSFileManager`、`CoreData`、`NSData` 和 `SQLite`。

「郵件」App 資料庫 (包括附件)、受管理的書籍、Safari 書籤、App 啟動影像和位置資料也將加密儲存，而加密密鑰會以用戶裝置上的密碼進行保護。「日曆」(不包括附件)、「通訊錄」、「提醒事項」、「備忘錄」、「訊息」和「相片」會執行「資料保護」授權的「首次用戶認證前的保護」。

沒有選擇加入某個特定「資料保護」類別且由用戶安裝的 App 預設會接受「首次用戶認證前的保護」。

## 加入「App 群組」

指定開發者帳戶所擁有的 App 和延伸功能在設定為「App 群組」的一部份後，便可共享內容。開發者可決定是否在 Apple Developer Portal (Apple 開發者入口網站) 上製作適合的群組，並納入想要的 App 和延伸功能。將 App 設定為「App 群組」的一部份後，便可存取以下內容：

- 只要安裝了 App 群組內的至少一個 App，卷宗上共享的儲存容器就會一直保留在裝置上
- 共享的偏好設定
- 共享的鑰匙圈項目

Apple Developer Portal (Apple 開發者入口網站) 可協助保證 App 群組 ID (GID) 在整個 App 生態系統中均不重複。

## 驗證在 iOS 及 iPadOS 中的配件

Made for iPhone, iPad, and iPod touch (MFi) 授權計劃允許經過審查的配件製造商存取「iPod 配件通訊協定」(iAP) 和必要的支援硬件元件。

當 MFi 配件使用 Lightning 或 USB-C 接頭或透過藍牙與 iOS 或 iPadOS 裝置進行通訊時，裝置會要求配件使用 Apple 提供的憑證 (裝置會對此憑證進行驗證) 進行回應，以證明配件經過 Apple 授權。然後，裝置會傳送一項質詢，配件必須使用已簽署的回應來回應。這個過程完全由 Apple 提供給經核准配件製造商的自訂集成電路 (IC) 處理，而且對於配件本身是透明的。

配件可以要求存取不同的傳輸方式和功能；例如透過 Lightning 或 USB-C 連接線存取數碼音訊串流，或透過藍牙存取位置資料。認證集成電路的設計用意是確保只有經過核准的配件才能取得對裝置的完全存取權限。如果配件不支援認證，其存取權限僅限於類比音訊和一小部份的序列 (UART) 音訊播放控制。

AirPlay 也會利用認證集成電路來驗證接收器已經過 Apple 核准。AirPlay 音訊和 CarPlay 視訊串流採用 MFi-SAP (安全關聯通訊協定)，此通訊協定使用 AES128 在計數器 (CTR) 模式下對配件和裝置之間的通訊進行加密。臨時密鑰則使用 ECDH 密鑰交換 (Curve25519) 進行交換，並使用認證集成電路的 1024 位元 RSA 密鑰來簽署，以作為站對站 (STS) 通訊協定的一部份。

# macOS 中的 App 保安

## macOS 的 App 保安簡介

macOS 的 App 保安包含層層堆疊的保護，首先是可選擇只執行來自 App Store 的已獲簽署且受信任的 App。此外，macOS 提供多層保護機制，可協助確保從互聯網下載的 App 不含已知的惡意軟件。macOS 提供偵測和移除惡意軟件的技術，以及專為防止不受信任的 App 存取用戶資料而設計的額外保護。Apple 服務（例如「公證」和 XProtect）設計旨在協助阻止惡意軟件安裝。在必要時，這些服務會找到一開始躲過偵測的惡意軟件，再快速且有效地移除之。最後，macOS 確保用戶可在對其適用的安全模式中任意操作，包含執行完全未簽署和不受信任的程式碼。

## macOS 的 App 程式碼簽署程序

所有來自 App Store 的 App 皆經過 Apple 簽署。這簽署的設計用意是確保 App 沒有遭到竄改或變更。Apple 會簽署 Apple 裝置隨附的所有 App。

在 macOS 10.15 中，所有在 App Store 以外分發的 App 均須由開發者使用 Apple 核發的開發者 ID 證書（以及其專用密鑰）進行簽署，並由 Apple 進行公證，以在裝置的預設「守衛」設定下執行。機構內部開發的 App 也應使用 Apple 核發的開發者 ID 簽署，以使用戶可驗證其完整性。

在 macOS 上，基於不同目標，程式碼簽署和公證作業獨立進行，且可由不同執行者執行。開發者需使用其開發者 ID 憑證（Apple 所核發）來簽署程式碼，而對此簽名進行驗證可向用戶證明，自開發者建置並簽署軟件以來，該軟件未曾遭竄改。公證可由軟件分銷鏈中的任何人執行，證明已提供檢查惡意軟件的程式碼複製給 Apple，且沒有發現任何已知惡意軟件。公證的輸出形式為票證，會儲存在 Apple 伺服器上，可選擇裝訂到 App 中（任何人皆可進行），而不會使開發者的簽署無效。

強制存取控制項目（MAC）需要有程式碼簽署才能啟用受系統保護的授權。例如，如 App 需要透過防火牆存取，就必須使用適當的 MAC 授權進行程式碼簽署。

## macOS 中的「守衛」和執行階段保護

macOS 提供「守衛」技術和執行階段保護，可協助確保用戶的 Mac 上只會執行受信任的軟件。

### 守衛

macOS 包含名為「守衛」的保安技術，其設計旨在協助確保用戶的 Mac 上只會執行受信任的軟件。當用戶下載並開啟來自 App Store 以外的 App、外掛模組或安裝程式套件時，「守衛」會驗證該軟件來自已識別的開發者，經過 Apple 公證不含已知惡意內容，且未曾遭變更。第一次開啟軟件時，「守衛」也會要求用戶許可，以確認用戶沒有受到詐騙而執行其認為單純為資料檔案的可執行程式碼。

依照預設，「守衛」會協助確認所有下載的軟件均已由 App Store 簽署，或由已登錄的開發者簽署並由 Apple 公證。App Store 審核程序及公證流程的設計用意是確保 App 不含任何已知惡意軟件。因此，依照預設，**無論軟件透過何種方式安裝在 Mac 上，macOS 中的所有軟件第一次開啟時，系統都會檢查是否包含已知的惡意內容。**

用戶和機構可選擇只允許安裝來自 App Store 的軟件。或者，用戶可以凌駕「守衛」的規則以開啟任何軟件，除非受到流動裝置管理（MDM）解決方案限制。機構可使用 MDM 來設定「守衛」設定，包括允許使用其他身份簽署的軟件。必要時，也可完全停用「守衛」。

「守衛」可防止惡意外掛模組隨着良性 App 發佈。這種方式會在用戶不知情的狀況下使用 App 觸發器載入惡意的外掛模組。必要時，「守衛」會在一個隨機唯讀位置開啟 App。其設計用意是防止自動載入伴隨 App 分發的外掛模組。

### 執行階段保護

系統檔案、資源與核心會與用戶的 App 空間加以區隔。來自 App Store 的所有 App 皆以沙盒模式執行，無法存取其他 App 所儲存的資料。如果來自 App Store 的 App 需要存取來自其他 App 的資料，便只能使用由 macOS 提供的 API 與服務來進行。

## 在 macOS 中防範惡意軟件

Apple 進行一套威脅情報程序，可快速識別和阻擋惡意軟件。

### 三層防禦

惡意軟件防禦具有三層結構：

1. 防止惡意軟件啟動或執行：App Store 或與「公證」結合的「守衛」
2. 阻止惡意軟件在客戶系統上執行：「守衛」、「公證」和 XProtect
3. 緩解已執行的惡意軟件：XProtect

第一層防禦機制設計用於遏制惡意軟件傳播，以及讓惡意軟件一次也無法啟動；這是 App Store 和結合「守衛」與「公證」的目標。

下一層防禦機制是為了協助確保如果惡意軟件出現在 Mac 上，系統可快速識別並阻擋，同時阻止傳播以及修復已遭惡意軟件染指的 Mac。XProtect 配搭「守衛」和「公證」為這層防禦機制的助力。

最後，XProtect 的用途是修復已成功執行的惡意軟件。

這些在下方會進一步說明的防護機制結合在一起，成為抵禦病毒和惡意軟件最佳做法的強力後盾。其他還有許多防護措施（尤其在配備 Apple 晶片的 Mac 上）可限制成功執行的惡意軟件造成的可能損害。請參閱[保護 App 對用戶資料的存取](#)以了解 macOS 如何協助保護用戶資料不受惡意軟件侵害，並參閱[作業系統完整性](#)以了解 macOS 如何限制惡意軟件可在系統上執行的動作。

### 公證

「公證」為 Apple 提供的惡意軟件掃描服務。要在 App Store 之外發佈 macOS 版 App 的開發者，可提交其 App 以進行掃描，作為發佈程序的一環。Apple 會掃描這個軟件是否包含已知的惡意軟件，如果沒有發現任何惡意軟件，就會核發「公證」票證。通常開發者會將這個票證附加至其 App，讓「守衛」即使離線也可驗證並啟動該 App。

Apple 也可針對已知惡意的 App（即使先前已通過公證）核發撤銷票證。macOS 會定期檢查新的撤銷票證，以便讓「守衛」接收最新資訊且可阻止這類檔案啟動。這個程序可非常快速地阻擋惡意 App，因為它在背景執行的更新頻率，相較於推送新 XProtect 簽署的背景更新高出許多。此外，這個防護機制可套用至先前已通過及尚未通過公證的 App。

### XProtect

macOS 的內置防毒技術 XProtect 可根據簽章偵測和移除惡意軟件。系統使用 YARA 簽署，此工具用於對惡意軟件執行以簽署為基礎的偵測，Apple 會定期對其進行更新。Apple 會監視新的惡意軟件感染與病種，並自動更新簽署（獨立於系統更新），以協助 Mac 防止惡意軟件感染。XProtect 會自動偵測並阻止執行已知的惡意軟件。在 macOS 10.15 或較新版本中，XProtect 會在下列情況就已知惡意內容進行檢查：

- 首次執行 App
- App 經過變更（在檔案系統中）
- XProtect 簽署更新

當 XProtect 偵測到已知惡意軟件時，會立即封鎖該軟件，並通知用戶可選擇將軟件移至「垃圾桶」。

**附註：**「公證」對於已知檔案（或檔案雜湊值）來說很有效，且可在先前已啟動的 App 上使用。XProtect 以簽署為基礎的偵測比特定檔案雜湊值更通用，因此可找出 Apple 未曾見過的變體。XProtect 只會掃描經過變更或首次啟動的 App。

如果惡意軟件成功入侵 Mac，XProtect 所包含的技術也可對病毒感染進行補救。例如，其包含一個引擎，可根據 Apple 自動提供的更新（作為系統資料檔案自動更新和保安更新的一部份）補救感染。其也會在收到更新資料時移除惡意軟件，並持續定期檢查是否有感染。XProtect 不會自動重新啟動 Mac。

## 自動化 XProtect 保安更新

Apple 會自動根據最新的可用威脅情報來核發 XProtect 的更新。根據預設，macOS 每日都會檢查這些更新。「公證」更新是使用 CloudKit 同步來發佈，其頻率高出許多。

## Apple 發現惡意軟件時的回應方式

發現新的惡意軟件時，系統會執行幾個步驟：

- 任何相關的開發者 ID 憑證都會被撤銷。
- 針對所有檔案 (App 和相關檔案) 核發「公證」撤銷票證。
- 開發並發佈 XProtect 簽署。

這些簽署也可以追溯方式套用至先前通過公證的軟件，且偵測到任何新的惡意軟件都會引發以上一或多項動作。

最後，偵測到新的惡意軟件後會在接下來數秒、數小時和數日內啟動一系列步驟，將可能的最佳防護措施傳播給 Mac 用戶。

## 在 macOS 中控制 App 對檔案的存取

Apple 認為用戶對於哪些 App 正使用其資料，應能一目瞭然、經過同意和擁有控制權。在 macOS 10.15 中，系統會強制執行此模式，以協助確保所有 App 都必須取得用戶的同意，才能取用「文件」、「下載項目」、「桌面」、「iCloud 雲碟」和網絡卷宗內的檔案。在 macOS 10.13 或較新版本中，如 App 需要整個儲存裝置的存取權限，就必須在「系統偏好設定」中明確加入。此外，輔助使用和自動化功能亦需要用戶許可，以協助確保在執行時不會繞過其他保護措施。根據存取規則，用戶可能會被詢問或要求在「系統偏好設定」>「保安與私隱」>「私隱」中更改設定：

項目	用戶收到 App 的提示	用戶必須編輯系統私隱設定
輔助使用		✓
整個內部儲存裝置的存取權限		✓
檔案和資料夾 附註：包括「桌面」、「文件」、「下載項目」、網絡卷宗和可移除卷宗	✓	
自動化 (Apple Event)	✓	

用戶的「垃圾桶」中的項目受到保護，免於被任何使用「完整磁碟取用」的 App 存取；用戶不會收到 App 取用提示。用戶如要讓 App 存取檔案，必須將檔案從「垃圾桶」移到另一個位置。

如用戶在 Mac 上啟用了「檔案保險箱」，系統會要求提供有效的憑證，才能繼續進行啟動程序和取得特殊啟動模式的存取權限。如沒有有效的登入憑證或還原密鑰，即使將儲存裝置的實物移除並連接另一台電腦，整個卷宗仍會保持加密狀態，以防止未經授權的存取。

如要在企業設定中保護資料，IT 人員應使用流動裝置管理 (MDM) 定義及強制執行「檔案保險箱」設定原則。機構有多個選項來管理加密的卷宗，包括機構還原密鑰、個人還原密鑰 (可選擇以 MDM 儲存來進行託管)，或將它們混合使用。密鑰轉換亦可設定為 MDM 中的原則。

## 「備忘錄」App 的安全功能

「備忘錄」App 包含安全備註功能，在 iPhone、iPad、Mac 和 iCloud 網站上，都可讓用戶保護特定備忘錄的內容。用戶也可以安全地與其他人共享備忘錄。

### 安全備註

安全備註是以用戶提供的密語進行點對點加密，為檢視 iOS、iPadOS、macOS 裝置和 iCloud 網站上的備忘錄所需。每個 iCloud 帳戶（包含「在我的」裝置帳戶）都能使用獨立的密語。

當用戶加密備忘錄時，會從用戶的密語透過 PBKDF2 和 SHA256 衍生出 16 位元組的密鑰。備忘錄及其所有附件均使用 Galois/計數器模式下的 AES (AES-GCM) 加密。系統會在 Core Data 和 CloudKit 中建立新記錄，以儲存已加密的備忘錄、附件、標籤和初始化向量。建立新記錄後，原來未加密的資料會被刪除。支援加密的附件包含影像、圖畫、表格、地圖和網站。包含其他類型附件的備忘錄無法加密，不支援的附件無法加入安全備註。

如要檢視安全備註，用戶必須輸入密語，或者使用 Face ID 或 Touch ID 進行認證。用戶成功通過認證後，無論要檢視或製作安全備註，「備忘錄」都會開啟安全作業階段。安全作業階段開啟時，用戶可以檢視或保護其他備忘錄，不需要進行再次認證。不過，安全作業階段僅會套用至使用已提供的密語保護的備忘錄。對於受不同密語保護的備忘錄，用戶仍然需要進行認證。安全作業階段會在以下情況關閉：

- 用戶點一下「備忘錄」中的「現在鎖定」按鈕時
- 「備忘錄」切換至背景超過 3 分鐘時（在 macOS 中為 8 分鐘）
- iOS 或 iPadOS 裝置鎖

如要更改安全備註的密語，用戶必須輸入目前的密語，因為更改密語時無法使用 Face ID 和 Touch ID。選擇密語後，「備忘錄」App 會在同一個帳戶中重新封裝所有現時以先前的密語加密的備忘錄之密鑰。

如果用戶連續打錯密語三次，「備忘錄」就會顯示用戶提供的提示（如用戶在設定時有提供）。如用戶仍無法想起密語，可以在「備忘錄」的設定中重設。此功能可讓用戶以新的密語製作新的安全備註，但不允許他們查看先前保護的備忘錄。先前保護的備忘錄仍可以在想起舊的密語時檢視。重設密語需要用戶的 iCloud 帳戶密語。

### 共享的備忘錄

未使用密語進行端到端加密的備忘錄，可以與他人共享。用戶加入共享的備忘錄中的任何文字或附件均為 CloudKit 加密資料類型。資產一律使用在 CKRecord 中加密的密鑰進行加密。建立和修改日期等後設資料未經加密。CloudKit 會管理參與者可加密及解密彼此資料的程序。

## 「捷徑」App 的安全功能

在「捷徑」App 中，你可選擇使用 iCloud 將捷徑同步到不同 Apple 裝置上。你也可透過 iCloud 與其他用戶分享捷徑。捷徑會以加密格式儲存在本機。

自訂捷徑包羅萬象，類似於指令碼或程式。從互聯網下載捷徑時，系統會警告用戶該捷徑尚未經過 Apple 審核，且會被予以檢驗該捷徑的機會。為了抵禦惡意捷徑，系統會在執行時下載更新版惡意軟件定義，以便識別惡意捷徑。

如從共享工作表啟動，自訂捷徑也可在 Safari 中對網站執行用戶指定的 JavaScript。為了抵禦惡意 JavaScript（例如誘騙用戶在社交媒體上執行會收集其資料的指令碼），JavaScript 會針對惡意軟件定義進行認證。用戶第一次在網域上執行 JavaScript 時，系統會提示用戶允許包含 JavaScript 的捷徑在該網域的目前網頁上執行。

# 服務保安

## 服務保安概覽

Apple 建立了一套強大的服務來協助用戶更充份發揮裝置效能和提升生產力。這些服務提供雲端儲存、同步、密碼儲存、認證、付款、訊息、通訊等強大的功能，同時保護用戶的私隱及其資料的安全。

本章介紹 iCloud、「使用 Apple 登入」、Apple Pay、iMessage、Apple Messages for Business、FaceTime、「尋找」和「接續互通」中使用的保安技術。

**附註：**部份 Apple 服務與內容不適用於部份國家或地區。

## Apple ID 與管理式 Apple ID

### Apple ID 保安概覽

Apple ID 是用來登入 Apple 服務的帳戶。對用戶而言，安全保護其 Apple ID 以協助防止帳戶遭未經授權的存取十分重要。為有助保障安全，Apple ID 需要高強度密碼：

- 長度必須最少為八個字元
- 必須包括字母及數字
- 不得包括三個或以上的連續相同字元
- 不能為常用的密碼

我們鼓勵用戶超越此規則，加入更多的字元和標點符號，來讓密碼變得更為安全。

在對帳戶進行重要更改（例如密碼或帳單資料變更），或使用 Apple ID 來在新裝置上登入時，Apple 也會透過電郵或推送通知，或者同時透過此兩者來通知用戶。如有任何異常情況，Apple 會指示用戶立即更改其 Apple ID 密碼。

此外，Apple 運用多種規則和程序，旨在保護用戶的帳戶。這包括限制重試登入和密碼重設的次數、積極監視詐騙以協助在攻擊發生時進行識別，以及定期檢查規則，讓 Apple 可因應任何可能影響客戶安全的新資訊採取行動。

**附註：**管理式 Apple ID 密碼規則需由管理員在 Apple School Manager 或 Apple Business Manager 中設定。

## 雙重認證

為協助用戶進一步保護其帳戶，Apple 預設會使用**雙重認證**，為 Apple ID 提供另一道安全防線。其設計目標在於確保即使有其他人知道密碼，仍只有帳戶的持有人可以存取帳戶。如使用雙重認證，透過受信任的其中一部裝置或受信任的電話號碼完成驗證後，用戶的帳戶就只能在受信任的裝置上使用，例如用戶的 iPhone、iPad、iPod touch、Mac 或其他裝置。如要在任何新裝置上首次登入，將需要兩項資料：Apple ID 密碼，以及顯示在用戶信任裝置上，或傳送到信任電話號碼的六位數驗證碼。透過輸入驗證碼，用戶可確認他們信任新裝置且可安全登入裝置。由於單靠密碼已不足以取用用戶帳戶，雙重認證能提升用戶 Apple ID 的保安，以及他們透過 Apple 儲存的所有個人資料的保安。雙重認證已直接整合至 iOS、iPadOS、macOS、tvOS、watchOS 和 Apple 網站使用的認證系統。

當用戶使用網頁瀏覽器登入 Apple 網站時，第二個驗證條件要求會傳送至與用戶 iCloud 帳戶關聯的所有信任裝置，要求核准網頁作業階段。如果用戶在信任裝置上從瀏覽器登入 Apple 網站，會在所使用的裝置上看到本機顯示的驗證碼。當用戶在裝置上輸入驗證碼時，便會核准網頁作業階段。

## 密碼重設和帳戶還原

如果忘記 Apple ID 帳戶密碼，用戶可以在受信任的裝置上重設密碼。如果無法使用受信任的裝置但密碼已知，用戶可以使用受信任的電話號碼，透過 SMS 驗證的方式進行驗證。此外，為了立即還原 Apple ID，先前使用的密碼可以和 SMS 驗證一起用來重置。如果無法實現這些選項，則必須遵循帳戶還原的處理程序。如需更多資料，請參閱 Apple 支援文章：[無法重設 Apple ID 密碼時如何使用帳戶還原功能](#)。

## 管理式 Apple ID 保安

「管理式 Apple ID」的功能類似於 Apple ID，但是由企業或教育組織所持有和控制。這些組織可以重設密碼、限制購買和通訊（如 FaceTime 和「訊息」），以及替員工、職員、教師和學生設定以角色為基礎的權限。

如使用管理式 Apple ID，某些服務會停用（例如 Apple Pay、iCloud 鑰匙圈、HomeKit 和「尋找」）。

## 檢查「管理式 Apple ID」

「管理式 Apple ID」亦支援**檢查**，可讓機構遵守法律和私隱法規。Apple School Manager 的管理員、經理或教師可以檢閱特定的管理式 Apple ID 帳戶。

檢閱者只能監察組織階層中層級低於自己的帳戶。例如，教師可以監察學生；經理可以檢查教師和學生；管理員可以檢查經理、教師和學生。

在使用 Apple School Manager 要求檢查憑證時，系統會核發一個特殊帳戶，其只能取用要求檢查的「管理式 Apple ID」。檢查者可以讀取並修改用戶儲存在 iCloud 或已啟用 CloudKit 功能的 App 中的內容。每個審核取用的要求都會記錄在 Apple School Manager 中。記錄會顯示誰是檢查者、檢查者要求取用的「管理式 Apple ID」、要求的時間，以及是否有執行檢查。

## 「管理式 Apple ID」和個人裝置

「管理式 Apple ID」也可以配搭個人擁有的 iOS 裝置、iPadOS 裝置和 Mac 電腦使用。學生可以使用機構核發的「管理式 Apple ID」和額外的家用密碼（用作 Apple ID 雙重認證程序的第二個元素）來登入 iCloud。當學生在個人裝置上使用管理式 Apple ID 時，「iCloud 鑰匙圈」會無法使用，且機構可能會限制 FaceTime 或「訊息」等其他功能。任何由學生在登入時製作的 iCloud 文件都可能會被審核，如本節前文所述。



# iCloud

## iCloud 保安概覽

iCloud 會儲存用戶的聯絡人、日曆、相片、文件和更多項目，並在其所有裝置間自動保持最新的資料。iCloud 也可供第三方 App 用來儲存和同步文件以及開發者定義的 App 資料密鑰值。用戶透過使用 Apple ID 登入並選擇他們想要使用的服務來設定 iCloud。IT 管理員可使用[流動裝置管理 \(MDM\)](#) 設定描述檔來停用部份 iCloud 功能，例如「iCloud 雲碟」和「iCloud 備份」。

iCloud 會使用高強度保安方式並採取嚴格的政策來保護用戶的資料。大部份 iCloud 資料會先在用戶的裝置上加密，其會使用裝置產生的 iCloud 密鑰，然後才會上傳到 iCloud 伺服器。針對非點對點加密的資料，用戶的裝置會安全地將這些 iCloud 密鑰上傳到 Apple 資料中心中的「iCloud 硬件保安模組」。這樣能讓 Apple 協助用戶進行資料還原，並在用戶需要使用資料時代表用戶解密資料（例如當用戶在新裝置上登入、從備份還原，或者在網上取用其 iCloud 資料）。在用戶的裝置和 iCloud 伺服器間移動的資料在傳輸過程中都會透過 TLS 來分別加密，且 iCloud 伺服器會以額外一層靜態保護來儲存用戶的資料。

加密密鑰（在 Apple 可用的情況下）會保存在 Apple 資料中心。在處理儲存在第三方資料中心的資料時，只有在安全伺服器上執行的 Apple 軟件可以取用這些加密密鑰，並且只能在進行必要的處理時取用。為了加強私隱和保安，許多 Apple 服務都會使用點對點加密，這代表只有用戶才能取用他們的 iCloud 資料，並且只能在使用用戶的 Apple ID 登入之受信任裝置上取用那些資料。

Apple 會提供兩個選項來讓用戶加密和保護儲存在 iCloud 中的資料：

- **標準資料保護 (預設設定)**：用戶的 iCloud 資料會被加密，加密密鑰會保存在 Apple 資料中心，且 Apple 可以協助還原資料和帳戶。只有特定 iCloud 資料（14 個資料類別，包括「健康」資料和「iCloud 鑰匙圈」中的密碼）會被點對點加密。
- **iCloud 進階資料保護**：提供 Apple 最高層級的雲端資料保安之可選用設定。如用戶選擇開啟「進階資料保護」，他們的受信任裝置會保有用戶大部份 iCloud 資料的加密密鑰之獨有取用權限，從而使用點對點加密來保護這些資料。當你開啟「進階資料保護」時，使用點對點加密的資料類別會增至 23 個，其中包括你的「iCloud 備份」、「相片」、「備忘錄」等等。

以點對點加密保護的指定 iCloud 資料類別列於 Apple 支援文章：[iCloud 資料保安概覽](#)。

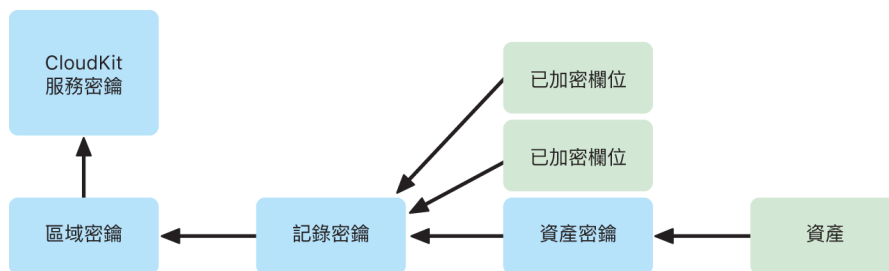
## iCloud 加密

iCloud 中的資料加密與資料儲存模型環環相扣，從允許 App 和系統軟件代表用戶將資料儲存在 iCloud 中的 CloudKit 架構和 API 開始，並讓所有內容在裝置之間和網上保持在最新狀態。

### CloudKit 加密

CloudKit 架構可讓 App 開發者在 iCloud 中儲存密鑰值資料、結構資料和資產（與資料庫分開儲存的大型資料，例如影像或影片）。CloudKit 同時支援公用和專用資料庫，其會以容器來分組。公用資料庫會與全域分享，此資料庫專門供一般資產使用，且不會被加密。專用資料庫則會儲存各個用戶的 iCloud 資料。

CloudKit 會使用符合資料架構的密鑰階層。各個容器的專用資料庫都會由一個密鑰階層保護，該密鑰階層根值於名為「CloudKit 服務」密鑰的非對稱式密鑰。這些密鑰對各個 iCloud 用戶都是獨一無二，並且都是在用戶的受信任裝置上產生。資料寫入 CloudKit 時，系統在上載任何資料前都會先在用戶的受信任裝置上產生所有記錄密鑰，並將密鑰封裝到適當的密鑰階層。



許多 Apple 服務 (Apple 支援文章 [iCloud 資料保安概覽](#) 中詳盡列出) 都使用點對點加密，並搭配受到「iCloud 鑰匙圈」同步功能保護的 CloudKit 服務密鑰。對於這些 CloudKit 容器，服務密鑰會儲存在用戶的「iCloud 鑰匙圈」中，並擁有與「iCloud 鑰匙圈」相同的保安特徵；服務密鑰只能在用戶受信任的裝置上使用，且 Apple 或任何第三方均無法取用。在遺失裝置的情況下，用戶可以透過使用「iCloud 鑰匙圈」安全還原、「帳戶還原聯絡人」或「帳戶還原密鑰」來還原他們的「iCloud 鑰匙圈」資料。

### 加密密鑰管理

CloudKit 中的加密資料之保安有賴於對應的加密密鑰之保安。CloudKit 服務密鑰會分兩個類別：點對點加密和認證後可使用。

- **點對點加密服務密鑰：**針對點對點加密的 iCloud 服務，Apple 伺服器永遠無法取用相關 CloudKit 服務專用密鑰。服務密鑰組（包括專用密鑰）會在用戶受信任的裝置上於本機製作，並會使用「iCloud 鑰匙圈」保安來傳送到用戶的其他裝置。雖然「iCloud 鑰匙圈」還原和同步流程都是由 Apple 伺服器協調，這些伺服器皆會以加密編譯方式來避免取用用戶的任何鑰匙圈資料。在失去「iCloud 鑰匙圈」的取用權限及所用還原機制的最差情況下，就會失去 CloudKit 中的點對點加密資料。Apple 無法協助還原此資料。
- **認證後可使用服務密鑰：**針對其他服務（例如「相片」和「iCloud 雲碟」），服務密鑰會儲存在 Apple 資料中心的「iCloud 硬件安全模組」，並可透過部份 Apple 服務取用。當用戶在新裝置上登入 iCloud 並認證其 Apple ID，Apple 伺服器就可以取用這些密鑰，無需進一步的用戶互動或輸入。例如，在登入 iCloud.com 後，用戶就可以即時在網上檢視其相片。這些服務密鑰就是**認證後可使用密鑰**。

## iCloud 進階資料保護

iCloud 進階資料保護為非必要設定，其會提供 Apple 最高層級的雲端資料保安。用戶開啟「進階資料保護」時，他們的受信任裝置會保有用戶大部份 iCloud 資料的加密密鑰之獨有取用權限，從而透過**點對點加密**來保護這些資料。針對開啟「進階資料保護」的用戶，受點對點加密保護的資料類別總數會由 14 個增加至 23 個，其中包括「iCloud 備份」、「相片」、「備忘錄」等等。

「iCloud 進階資料保護」將會在 2022 年底向美國用戶提供，並會在 2023 年初開始在世界各地推出。

從概念上來說，「進階資料保護」十分簡單：所有在裝置上產生，並在之後上載到 Apple 資料中心中的**認證後可使用**「iCloud 硬件安全模組」(HSM) 的「CloudKit 服務」密鑰都會從那些 HSM 上刪除，並改為完全保存在帳戶的「iCloud 鑰匙圈」保護網域。這些密鑰的處理方式類似現有的**點對點加密**服務密鑰，代表 Apple 無法再讀取或取用這些密鑰。

「進階資料保護」亦會自動保護第三方開發者選擇標記為加密的 CloudKit 欄位，以及所有 CloudKit 資產。

### 啟用「進階資料保護」

用戶開啟「進階資料保護」時，用戶的受信任裝置會執行兩項動作：第一，裝置會將用戶開啟「進階資料保護」的意圖傳達至用戶其他參與點對點加密的裝置。裝置會透將新值（由裝置本機密鑰簽署）寫入至其「iCloud 鑰匙圈」裝置後設資料來執行此操作。在此證明與用戶的其他裝置進行同步期間，Apple 伺服器無法移除或修改此證明。

第二，裝置會開始將**認證後可使用**服務密鑰從 Apple 資料中心移除。由於這些密鑰是由 iCloud HSM 保護，此刪除動作會即時進行，且為永久及不可改變。密鑰被刪除後，Apple 就無法再取用**任何**由用戶的服務密鑰保護的資料。此時，裝置會開始異步密鑰輪換操作，該操作會為各項之前向 Apple 伺服器提供密鑰的服務製作新的服務密鑰。如因為網絡中斷或任何其他錯誤導致密鑰輪換失敗，裝置會重試密鑰輪換直至成功為止。

服務密鑰輪換成功後，就無法以舊的服務密鑰解密寫入該服務的新資料。資料會以新的密鑰保護，該密鑰只會由用戶的受信任裝置控制，且 Apple 永遠無法取用該密鑰。

### 「進階資料保護」和 iCloud.com 網上存取功能

在用戶首次開啟「進階資料保護」後，用戶資料在 iCloud.com 的網上存取功能會自動關閉。這是因為 iCloud 網站伺服器不能再取用解密和顯示用戶資料所需的密鑰。用戶可以選擇再次開啟網上存取功能，並使用受信任裝置的參與來在網上存取已加密的 iCloud 資料。

開啟網上存取功能後，用戶每次到訪 iCloud.com 時都需要在受信任的裝置上授權網上登入。授權可以讓裝置為網上存取「作好準備」。在接下來的一小時，此裝置會接受來自特定 Apple 伺服器的要求以上載個別服務密鑰，但只限對應到在 iCloud.com 上一般可取用服務的許可服務列表。換言之，即使用戶授權網絡登入，伺服器要求仍無法誘使用戶的裝置上載不能在 iCloud.com 上檢視的資料（例如「健康」資料或「iCloud 鑰匙圈」中的密碼）之服務密鑰。Apple 伺服器只會要求解密用戶要求在網上存取的指定資料所需的服務密鑰。每次上載服務密鑰時，密鑰會以綁定到用戶已授權的網頁作業階段的臨時密鑰來加密，而且用戶的裝置上亦會顯示通知，顯示暫時向 Apple 伺服器提供資料的 iCloud 服務。

### 保留用戶選擇的權利

「進階資料保護」和 iCloud.com 網上存取功能設定只可以由用戶修改。這些值會儲存在用戶的「iCloud 鑰匙圈」裝置後設資料，並只可以在用戶其中一部受信任的裝置上進行更改。Apple 伺服器無法代表用戶修改這些設定，或將其變回之前的設定。

## 共享和共同編輯涉及的保安

在大部份情況下，當用戶共享內容來與他人進行共同編輯（例如共享「備忘錄」、共享「提醒事項」、「iCloud 雲碟」中的共享資料夾，或者「iCloud 共享相片圖庫」），且所有用戶都有開啟「進階資料保護」，Apple 伺服器只會用於建立共享，但無法取用共享資料的加密密鑰。內容仍會以點對點加密，並只可以在參與者的受信任裝置上存取。針對每項共享操作，Apple 可能會以標準資料保護來儲存共享的標題和相應的縮圖，以向收到的用戶顯示預覽。

在啟用共同編輯時選擇「擁有連結的用戶」選項，會讓 Apple 伺服器可以使用的內容使用標準資料保護，因為伺服器需要向所有開啟該 URL 的用戶提供內容的取用權限。

iWork 共同編輯和「相片」中的「共享相簿」功能不支援「進階資料保護」。當用戶在 iWork 文件上進行共同編輯，或從「iCloud 雲碟」開啟 iWork 文件，文件的加密密鑰會安全地上載到 Apple 資料中心中的 iWork 伺服器。這是因為 iWork 中的即時共同編輯需要伺服器端進行協調，以配合各個參與者間的文件變更。加至「共享相簿」的相片會以標準資料保護來儲存，因為該項功能允許在網絡上公開分享相簿。

## 停用「進階資料保護」

用戶可以隨時關閉「進階資料保護」。如用戶決定這樣做：

1. 用戶的裝置會先將用戶的新選擇記錄在「iCloud 鑰匙圈」參與後設資料，然後此設定會安全地同步到用戶的所有裝置。
2. 用戶的裝置會安全地將所有**認證後可使用**服務的服務密鑰上載到 Apple 資料中心中的 iCloud HSM。這操作永不包括在標準資料保護下為點對點加密的服務，例如「iCloud 鑰匙圈」和「健康」。

裝置會上載在開啟「進階資料保護」前所產生的原有服務密鑰，以及在用戶開啟該功能後產生的新服務密鑰。這樣可以讓這些服務中的所有資料在認證後都可供存取，並將帳戶回復為標準資料保護，這樣 Apple 可以再次協助用戶將大部份無法取用的資料還原。

## 「進階資料保護」未涵蓋的 iCloud 資料

由於需要全域電郵、通訊錄和日曆系統交互操作，「iCloud 郵件」、「通訊錄」和「日曆」無法使用點對點加密。

即使「進階資料保護」已開啟，iCloud 仍會在不使用用戶專屬 CloudKit 服務密鑰保護的方式儲存部份資料。「CloudKit 記錄」欄位必須在容器架構中明確宣告為「加密」才會受到保護，且讀取和寫入加密欄位都需要使用專用的 API。系統會使用修改檔案或物件的日期和時間會來排列用戶的資料，以及使用檔案和相片資料的總和檢查碼協助 Apple 刪除重覆項目，並最佳化用戶的 iCloud 和裝置儲存空間，這兩項操作都無需檔案和相片本身的取用權限。特定資料類別使用加密的方式之詳細資料，可於 Apple 支援文章 [iCloud 資料保安概覽](#)上取得。

將總和檢查碼用於刪除重覆項目（名為**聚合加密**的著名技術）等決定是 iCloud 服務推出時的原始設計之一部份。此後設資料總是會被加密，但加密密鑰會由 Apple 以標準資料保護儲存。為了繼續加強所有用戶的保安保護措施，Apple 承諾確保在「進階資料保護」開啟時將更多資料（包括這類後設資料）以點對點方式加密。

## 「進階資料保護」的需求

開啟「iCloud 進階資料保護」的需求包括以下各項：

- 用戶的帳戶必需支援點對點加密。點對點加密需要用戶的 Apple ID 使用雙重認證，以及在用戶受信任的裝置上設定密碼。如需更多資料，請參閱 Apple 支援文章：[Apple ID 雙重認證](#)。
- 用戶使用 Apple ID 登入的裝置必需更新至 iOS 16.2、iPadOS 16.2、macOS 13.1、tvOS 16.2、watchOS 9.2，以及最新版本的 Windows 版 iCloud。此需求可避免較舊版本的 iOS、iPadOS、macOS、tvOS 或 watchOS 以不當方式處理新製作的服務密鑰，在被誤導的還原帳戶狀態嘗試中，將服務密鑰重新上傳到認證後可使用的 HSM。
- 用戶必須設定至少一種替用還原方式（一個或多個還原聯絡人或還原密鑰），讓用戶可以在無法取用帳戶時用來還原 iCloud 資料。

如果還原方式失敗，例如還原聯絡人資料已過時，或用戶忘記有關資料，Apple 無法協助還原用戶的點對點加密 iCloud 資料。

「iCloud 進階資料保護」只可以為 Apple ID 開啟。「管理式 Apple ID」和兒童帳戶（因國家或地區而異）都不受支援。

## 「iCloud 備份」的保安

iCloud 每日會透過 Wi-Fi 備份資料（包括裝置設定、App 資料、「相機菲林」中的相片和影片，以及「訊息」App 中的對話）。系統只會在裝置已鎖定、連接到電源，並可透過 Wi-Fi 連接互聯網時，才會進行「iCloud 備份」。注意到 iOS 和 iPadOS 中所使用的儲存加密技術，「iCloud 備份」的設計，既可保護資料安全，又能容許增量、自發式的備份和還原動作。依照預設，「iCloud 備份」服務密鑰會安全地備份在 Apple 資料中心的「iCloud 硬件保安模組」，並且是認證後可使用資料類別的一部份。針對開啟「iCloud 進階資料保護」的用戶，「iCloud 備份」服務密鑰會以點對點加密方式保護，並且只可以由用戶在其受信任裝置上使用。

如果檔案製作時採用的「資料保護」類別令其無法在裝置鎖定時存取，其檔案專屬密鑰會使用「iCloud 備份」Keybag 中的類別密鑰進行加密，並以其原始加密狀態將檔案備份至 iCloud。所有檔案都會在傳送時加密，且在儲存時，會使用以帳戶為基礎的密鑰（如 [CloudKit 加密](#) 中所述）加密。

「iCloud 備份」Keybag 包含「資料保護」類別的非對稱式（Curve25519）密鑰，當裝置被鎖定時，該密鑰無法被取用。備份集儲存於用戶的 iCloud 帳戶中，由用戶的檔案副本和「iCloud 備份」Keybag 組成。「iCloud 備份」Keybag 受到會與備份集一起儲存的隨機密鑰所保護。用戶的 iCloud 密碼不會用於加密，因此更改 iCloud 密碼不會使現有的備份資料失效。

還原後，將會從用戶的 iCloud 帳戶取回備份的檔案、「iCloud 備份」Keybag 和 Keybag 的密鑰。「iCloud 備份」Keybag 使用其密鑰進行解密，然後 Keybag 中的檔案專屬密鑰則用於解密備份集內的檔案，這些檔案會以新檔案的形式寫入檔案系統，並根據其「資料保護」類別對其重新加密。

以下內容會使用「iCloud 備份」來備份：

- 已購買的音樂、電影、電視節目、App 和書籍的相關記錄。用戶的「iCloud 備份」包含用戶裝置上現有已購買內容的相關資料，但不包括已購買的內容本身。當用戶從「iCloud 備份」還原時，其已購買的內容會自動從 iTunes Store、App Store、Apple TV App 或 Apple Books 下載。部分類型的內容在部份國家或地區不會自動下載，且在內容已退款或相關的商店不再提供內容時，可能無法取得先前的購買項目。完整購買記錄會連繫至用戶的 Apple ID。
- 用戶裝置上的相片與影片。請注意，如用戶在 iOS 8.1 或較新版本、iPadOS 13.1 或較新版本，或是 OS X 10.10.3 或較新版本中開啟「iCloud 相片」，其相片與影片便已儲存在 iCloud 中，因此不會包含在用戶的「iCloud 備份」中。
- 通訊錄、日曆行程、提醒事項和備忘錄
- 裝置設定
- App 資料

- 主畫面和 App 整理方式
- HomeKit 設定
- 醫療檔案資料
- 「留言信箱」密碼 (如有需要, 必需裝有備份期間所使用的實體 SIM 卡)
- 「訊息」、Apple Messages for Business、短訊 (SMS) 與 MMS 訊息 (如有需要, 必需裝有備份期間所使用的實體 SIM 卡)

「iCloud 備份」亦會用於備份本機裝置鑰匙圈, 其會使用裝置的 Secure Enclave UID 根加密編譯密鑰衍生的密鑰來加密。此密鑰為裝置獨有, 且 Apple 不會知道此密鑰。這樣可讓資料庫只能還原至原先產生它的同一部裝置, 這代表任何人 (包括 Apple) 都無法讀取。如需更多資料, 請前往: [安全隔離區](#)。

## iCloud 雲端「訊息」

iCloud 雲端「訊息」可讓用戶的整個訊息記錄保持更新, 並可在所有裝置上取用。

配搭標準資料保護, iCloud 雲端「訊息」在「iCloud 備份」關閉時會使用點對點加密。「iCloud 備份」開啟時, 備份會包括 iCloud 雲端「訊息」加密密鑰的副本, 因此即使用戶無法取用「iCloud 鑰匙圈」和受信任的裝置, Apple 也可以協助用戶還原訊息。如用戶關閉「iCloud 備份」, 用戶的裝置上會產生新的密鑰, 以保護之後的 iCloud 雲端「訊息」。新的密鑰只會儲存在「iCloud 鑰匙圈」, 只有用戶可以在受信任的裝置上取用該密鑰, 而寫入容器的新資料無法使用舊的容器密鑰來解密。

配搭「進階資料保護」, iCloud 雲端「訊息」總是會使用點對點加密。「iCloud 備份」開啟時, 其中的所有內容都會使用點對點加密, 包括 iCloud 雲端「訊息」加密密鑰。當用戶開啟「進階資料保護」, 「iCloud 備份」服務密鑰以及 iCloud 雲端「訊息」容器密鑰都會變換。如需更多資料, 請參閱 Apple 支援文章: [iCloud 資料保安概覽](#)。

## 帳戶還原聯絡人保安

用戶最多可以將五位他們信任的人員加入帳戶還原聯絡人, 以協助他們還原其 iCloud 帳戶和資料, 包括所有點對點加密資料 (不論他們是否已開啟「進階資料保護」)。Apple 和還原聯絡人都沒有可用來獨立解密用戶的點對點加密 iCloud 資料之必要資料。

「還原聯絡人」的設計相當重視用戶的私隱。Apple 不會知道用戶選擇的還原聯絡人。只有在用戶向還原聯絡人求助, 且該聯絡人開始實際協助進行還原的情況下, Apple 伺服器才會在還原嘗試的較後階段知道關於還原聯絡人的資料。完成還原後, 該項資料不會被保留。

## 還原聯絡人保安程序

用戶設定「帳戶還原聯絡人」時, 用於取用用戶 iCloud 資料 (包括點對點加密的 CloudKit 資料) 的密鑰會以高強度隨機密鑰加密。之後此隨機密鑰會分別存放於還原聯絡人和 Apple。在還原時, 只當有兩個密鑰部份重新結合才能還原原始密鑰並取用其用戶的 iCloud 資料。

如要設定「帳戶還原聯絡人」, 用戶的裝置要與 Apple 伺服器通訊, 以上傳 Apple 持有那部份的密鑰資料。然後其會與還原聯絡人建立點對點加密的 CloudKit 容器, 以分享還原聯絡人所需的部份。Apple 和還原聯絡人也會收到同一個來自用戶的授權密鑰, 之後的還原會需要該密鑰。邀請和接受還原聯絡人的通訊是透過相互認證的 IDS 頻道進行。還原聯絡人會自動將收到的資料儲存在他們的「iCloud 鑰匙圈」中。Apple 無法取用 CloudKit 容器的內容, 或儲存此資料的「iCloud 鑰匙圈」。在進行分享時, Apple 伺服器只會檢視還原聯絡人的匿名識別碼。

之後, 當用戶需要還原他們的帳戶和 iCloud 資料時, 可以向他們的還原聯絡人要求協助。屆時, 還原聯絡人的裝置會產生一個還原代碼, 還原聯絡人便可於頻外 (例如親自或透過電話) 將其提供給用戶。然後用戶在他們的裝置上輸入還原代碼, 以使用 SPAKE2+ 通訊協定在裝置間建立安全連線, Apple 無法取用其中的內容。此互動由 Apple 伺服器協調, 但 Apple 無法啟動還原程序。

建立安全連線並完成所有必要的安全檢查後，還原聯絡人的裝置會將他們那部份的密鑰資料以及之前建立的授權密鑰，傳回給要求還原的用戶。用戶向 Apple 伺服器出示此授權密鑰，其會將取用 Apple 儲存的密鑰資料之取用權限授予用戶。提供授權密鑰也會授權重設帳戶密碼以還原帳戶取用權限。

最後，用戶的裝置會結合從 Apple 和「帳戶還原聯絡人」接收的密鑰資料，並使用有關資料來解密和還原用戶的 iCloud 資料。

系統會實施保護機制來防止還原聯絡人在未得到用戶的同意下啟動還原，這些保護機制包括在用戶帳戶上進行活動性分析。如果帳戶正被積極使用，就會需要知道最近使用的裝置密碼或「iCloud 安全碼」才能使用「還原聯絡人」進行還原。

## 遺產聯絡人保安

如果用戶希望讓指定受益人在用戶死後可以取用其 iCloud 資料，他們可以在其帳戶上設定「遺產聯絡人」。「遺產聯絡人」受益人會獲得取用去世者所有 iCloud 資料的權限（包括幾乎所有點對點加密資料，但不包括帳戶密碼等「iCloud 鑰匙圈」資料）。「遺產聯絡人」的技術基礎類似「還原聯絡人」的運作方式：將一個高強度隨機密鑰分別存放於 Apple 和遺產聯絡人手上，因此雙方都無法自行解密任何資料。不論用戶有沒有開啟「進階資料保護」，受益人都會收到同類別的資料。

受益人收到的密鑰資料在面向用戶的文件中被稱為取用密鑰，其會自動儲存在支援的裝置上，但也可以列印和儲存以供離線使用。如需更多資料，請參閱 Apple 支援文章：[如何為你的 Apple ID 加入「遺產聯絡人」](#)。

用戶去世後，「遺產聯絡人」可以登入 Apple 聲明網站以啟動取用權限。這需要死亡證明，並會使用前文提到的授權密鑰進行授權。完成所有保安檢查後，Apple 會為新帳戶核發用戶名稱和密碼，並將必要的密鑰資料釋出給「遺產聯絡人」。

為了在需要時更輕鬆地輸入取用密鑰，其會顯示為含有相關二維碼的英數代碼。輸入後，對去世者 iCloud 資料的取用權限則會恢復。這可以在裝置上執行，也可以在網上建立取用權限。如需更多資料，請參閱 Apple 支援文章：[以「遺產聯絡人」身分要求取用 Apple 帳戶](#)。

## 「iCloud 私密轉送」保安

「iCloud 私密轉送」主要會在使用 Safari 瀏覽網頁時協助保護用戶，但其也包括所有 DNS 名稱解析要求。這有助確保任何一方（甚至 Apple）都無法將用戶的 IP 位址連繫至其的瀏覽活動。其透過使用不同的代理來做到這一點：由 Apple 管理的輸入代理和由內容供應商所管理的輸出代理。如要使用「iCloud 私密轉送」，用戶必須執行 iOS 15、iPadOS 15 或 macOS 12.0.1 或較新版本，並使用其 Apple ID 登入 iCloud+ 帳戶。然後便可在「設定」>「iCloud」或「系統設定」>「iCloud」中開啟「iCloud 私密轉送」。

如需更多資料，請參閱：[iCloud 私密轉送概覽](#)。

# 密碼與密碼管理

## 密碼保安概覽

iOS、iPadOS 及 macOS 讓用戶輕鬆驗證使用密碼的第三方 App 及網站。管理密碼的最佳方式就是根本不需要使用密碼。「使用 Apple 登入」讓用戶不需要建立和管理額外的帳戶或密碼，即可登入第三方 App 和網站，同時透過其 Apple ID 雙重認證程序保護登入資料。針對不支援「使用 Apple 登入」的網站，「自動使用高強度密碼」功能可讓用戶的裝置於網站和 App 中自動建立、同步和輸入不重複的高強度密碼。在 iOS 和 iPadOS 中，密碼會儲存至特別的「自動填寫密碼」鑰匙圈中，這個鑰匙圈由用戶控制，且可在 iOS 和 iPadOS 中前往「設定」>「密碼」管理。

在 macOS 中，已儲存的密碼可在 Safari 的「密碼」偏好設定中管理。這個同步系統也可以用來同步用戶手動建立的密碼。

## 「使用 Apple 登入」保安

對其他單一登入系統而言，「使用 Apple 登入」是可保護私隱的替用方式。它提供了一鍵式登入的便利和效率，同時為用戶提供了更高的透明度和對個人資料的控制權。

「使用 Apple 登入」讓用戶可設定一個帳戶，然後使用原有的 Apple ID 登入 App 和網站，且提供更完善的個人資料控制權。App 在設定帳戶時，只能詢問用戶的名稱和電郵地址，而且用戶總是有選擇權：可以與 App 分享自己的個人電郵地址，或是選擇將個人電郵地址保密，改用 Apple 新推出的私隱電郵轉送服務。此電郵轉送服務會分享一個不重複的匿名電郵地址，而其電郵會轉送至用戶的個人地址，因此用戶仍可收到來自開發者的通訊內容，同時保留一定程度的私隱和個人資料控制權。

「使用 Apple 登入」為內置的安全功能。使用「使用 Apple 登入」的所有用戶都必須為其 Apple ID 啟用雙重認證。雙重認證不止有助保護用戶的 Apple ID，也能保護他們使用 App 建立的帳戶。此外，Apple 還開發出可保護私隱的防詐騙訊號，並整合到「使用 Apple 登入」中。這讓開發者具有信心，能確保獲得的新用戶皆為真人，而非機械人或執行指令的帳戶。

## 自動使用高強度密碼

當「iCloud 鑰匙圈」已啟用，iOS、iPadOS 及 macOS 會在用戶於 Safari 中的網站上註冊或變更密碼時，製作高強度、隨機的唯一密碼。在 iOS 和 iPadOS 中，自動產生高強度密碼的功能也可用於 App。用戶必須作出選擇，才可以停止使用高強度密碼。產生的密碼會儲存在鑰匙圈中，並在已啟用「iCloud 鑰匙圈」的各個裝置上保持最新狀態。

按照預設，iOS 及 iPadOS 產生的密碼長度為 20 字元。其中包括一個數字、一個大寫字元、兩個連字號和 16 個小寫字元。這些產生的密碼皆為高強度，且包括 71 位元的熵。

密碼會根據放發法產生，其可判斷密碼欄位使用體驗是否適用於製作密碼。如果放發法無法識別製作密碼時使用的內容限定密碼，App 開發者可以在文字欄位上設定 `UITextContentType.newPassword`，而網頁開發者可以在 `<input>` 元素中設定 `autocomplete="new-password"`。

為協助確保產生的密碼與相關的服務相容，App 及網站可提供規則。開發者使用 `UITextInputPasswordRules` 或輸入元素中的 `passwordrules` 屬性來提供規則。然後裝置會產生可滿足這些規則的最高強度密碼。



## 「自動填寫密碼」保安

「自動填寫密碼」會自動填寫儲存在「鑰匙圈」中的憑證。「iCloud 鑰匙圈」密碼管理員和「自動填寫密碼」提供以下功能：

- 在 App 和網站中填入憑證
- 產生高強度密碼
- 儲存在 App 和 Safari 中的網站之密碼
- 以安全方式將密碼分享給用戶的聯絡人
- 提供密碼給附近要求憑證的 Apple TV

於 App 內產生及儲存密碼，以及向 Apple TV 提供密碼的功能只適用於 iOS 和 iPadOS。

### 在 App 中「自動填寫密碼」

iOS 和 iPadOS 允許用戶在 App 內的憑證相關欄位中，輸入已儲存的用戶名稱和密碼，其操作方式類似 Safari 中的「自動填寫密碼」功能。在 iOS 和 iPadOS 中，用戶需點一下軟件鍵盤「快速輸入」列中的直觀功能按鍵。在 macOS 中，針對使用 Mac Catalyst 製作的 App，在憑證相關欄位下會顯示「密碼」下拉式選單。

當 App 使用相同的 App 網站連繫機制（透過同一個 apple-app-site-association 檔案驅動）來與網站建立高強度連繫時，如果有任何憑證已儲存至「自動填寫密碼」鑰匙圈，iOS 和 iPadOS 的「快速輸入」列及 macOS 的下拉式選單就會直接建議該 App 的憑證。如此一來用戶就可選擇向使用相同安全屬性的 App 提供 Safari 儲存的憑證，但這些 App 不需要採用 API。

「自動填寫密碼」不會向 App 提供任何憑證資料，除非用戶同意向 App 釋出憑證。系統會從 App 的程序中提取或顯示憑證列表。

當 App 和網站具有受信任關係，且用戶在 App 中提交了憑證，iOS 和 iPadOS 可能會提示用戶將這些憑證儲存至「自動填寫密碼」鑰匙圈供日後使用。

## App 對已儲存密碼的存取權限

iOS、iPadOS 和 macOS App 可以要求「自動填寫密碼」鑰匙圈協助使用

ASAuthorizationPasswordProvider 和 SecAddSharedWebCredential 讓用戶登入。密碼提供者和其要求可配搭「使用 Apple 登入」使用，因此會呼叫相同的 API 以協助用戶登入 App，無論用戶的帳戶採用密碼，還是透過「使用 Apple 登入」所建立。

只有 App 開發者和網站管理員核准且用戶同意後，App 才能存取已儲存的密碼。App 開發者藉由在其 App 中包含授權，讓系統知悉他們需要存取 Safari 已儲存的密碼。授權會列出相關網站的完整網域名稱，且網站必須在其伺服器上放置一個檔案，列出經 Apple 核准 App 的唯一 App 識別碼。

在安裝帶有 com.apple.developer.associated-domains 授權的 App 後，iOS 和 iPadOS 會向每個列出的網站發出 TLS 要求，以索取以下其中一個檔案：

- apple-app-site-association
- .well-known/apple-app-site-association

如檔案中列出了要安裝之 App 的識別碼，iOS 和 iPadOS 才會將網站和 App 標示為具有信任關係。只有在具有信任關係的情況下，才會呼叫這兩個 API 並向用戶發出提示，經用戶同意後，才會將密碼核發給 App、更新或刪除。

## 密碼保安建議

iOS、iPadOS 和 macOS 中「自動填寫密碼」的密碼列表，會指出用戶已儲存的密碼中有哪些將**重複用於**其他網站、哪些密碼的**強度不足**，以及哪些密碼因**資料洩漏**而遭洩。

### 概覽

將相同的密碼用於多個服務可能會導致那些帳戶容易受到憑證填充攻擊。如果服務遭入侵且密碼洩漏，攻擊者可能會嘗試對其他服務使用相同的憑證，藉此入侵其他帳戶。

- 如果看到同一個密碼用於不同網域中的多個已儲存密碼，則會將密碼標記為**重複使用**。
- 如密碼易於被攻擊者猜中，系統會將其標記為**弱**。iOS、iPadOS 和 macOS 會偵測用於製作易記密碼的常用模式，例如使用字典中的單字、常用字元替換（例如使用「p4ssw0rd」代替「password」），在鍵盤上找到的模式（例如 QWERTY 鍵盤上的「q12we34r」）或重複的序列（例如「123123」）。這些模式通常用於建立滿足服務最低密碼要求的密碼，但是也常被攻擊者用來嘗試以暴力取得密碼。

由於許多服務特別要求輸入四位或六位 PIN 碼，因此短密碼會使用不同規則來評估強度。PIN 碼如為最常見的 PIN 碼、遞增或遞減數列（例如「1234」或「8765」）或依循重複模式（例如「123123」或「123321」），就會視為強度弱。

- 如果「密碼監測」功能可以證明密碼已存在於資料洩漏中，則會將密碼標記為**洩漏**。如需更多資料，請前往：[密碼監測](#)。

弱、重複使用和已洩漏的密碼會在密碼列表 (macOS) 中被指明或顯示於專用的「保安級別建議」介面 (iOS 和 iPadOS) 中。如果用戶在 Safari 中使用先前儲存且強度極弱、或已因資料洩漏而遭洩的密碼登入網站，系統會顯示提示，強烈建議升級為自動高強度密碼。

### 升級 iOS 和 iPadOS 中的帳戶認證保安

導入了「帳戶認證修改延伸功能」（位於「認證服務」架構中）的 App 可為採用密碼的帳戶提供輕鬆的一鍵式升級，也就是可以切換為使用「使用 Apple 登入」或自動高強度密碼。這個延伸點可用於 iOS 和 iPadOS。

如果 App 使用了延伸點並已安裝在裝置上，則用戶在「設定」的「iCloud 鑰匙圈」密碼管理員中檢視與該 App 關聯的憑證「保安級別建議」時，便會看到擴充升級的選項。當用戶使用有風險的憑證登入到 App 時，系統也會提供升級選項。App 能告訴系統在登入後不要提示用戶升級選項。使用新的 AuthenticationServices API，App 也可以呼叫其擴充功能並自行執行升級，理想情況是從 App 中的帳戶設定或帳戶管理畫面進行。

App 可以選擇支援高強度密碼升級、「使用 Apple 登入」或同時支援這兩者。在高強度密碼升級中，系統將會為用戶產生自動高強度密碼。如有需要，App 可在產生新密碼時，提供要遵循的自訂密碼規則。當用戶將帳戶從使用密碼切換為使用「使用 Apple 登入」時，系統會向該擴充程序提供新的「使用 Apple 登入」憑證，以將該帳戶與其相關聯。用戶的 Apple ID 電郵不會作為憑證的一部份提供。成功進行「使用 Apple 登入」升級後，系統將從用戶的鑰匙圈中刪除以前使用的密碼憑證（如果已儲存在其中）。

「帳戶認證修改擴充」有機會在執行升級之前執行額外的用戶認證。對於在密碼管理員中啟動的升級或登入到 App 後啟動的升級，擴充程序將會為要升級的帳戶提供用戶名稱和密碼。如為 App 內升級，則只會提供用戶名稱。如果延伸功能需要進一步的用戶認證，則可在繼續升級之前要求顯示自訂用戶介面。顯示此用戶介面的預期用途是讓用戶輸入第二重認證來授權升級。

## 密碼監測

「密碼監測」是一項功能，可將儲存在用戶的「自動填寫密碼」鑰匙圈中的密碼與不斷更新和整理的密碼列表（已知已暴露於不同網上組織的洩漏資料中）進行比對。如果啟用了此功能，則監測通訊協定會持續將用戶的「自動填寫密碼」鑰匙圈密碼與整理的列表相比對。

### 監測功能的運作方式

用戶裝置會連續對用戶密碼進行循環檢查，並以不受用戶密碼或其密碼管理程式使用模式影響的時間間隔進行查詢。這有助確保驗證狀態與洩漏密碼的目前最新整理列表保持最新狀態。為協助防止洩漏用戶擁有多少個專屬密碼的相關資料，要求會批次且並行執行。每次檢查都會並行確認固定數量的密碼，並且如果用戶擁有的數量少於此數量，則會產生隨機密碼並將其加入到查詢中以彌補差異。

### 密碼的比對方式

密碼比對過程分為兩部份。最常洩露的密碼包含在用戶裝置的本機列表中。如果用戶的密碼出現在此列表中，則會立即通知用戶，而無需進行任何外部互動。其設計用意是確保不會洩露因密碼洩露而讓用戶產生最大風險的相關密碼資料。

如果該密碼未包含在最頻繁洩漏的列表中，則其與洩漏頻率較低的密碼比對。

### 將用戶密碼與指定列表進行比較

確認本機列表中不存在的密碼是否相符，會涉及與 Apple 伺服器的一些互動。為協助確保不會將合法用戶的密碼傳送給 Apple，我們部署了一種加密的**私密集交叉作業**，將用戶的密碼與大量洩露的密碼進行比較。其設計用意是確保，對於侵害風險較低的密碼，與 Apple 共享更少的資料。對用戶的密碼而言，此資料的限制為加密雜湊值的15 位元前置碼。使用最經常洩露的密碼的本機列表來從此互動過程中刪除最經常洩露的密碼，會減少網絡服務儲存貯體中密碼的相對頻率變化，從這些查詢中推測用戶密碼是徒勞的。

此底層協定將整理的密碼列表劃分為  $2^{15}$  個不同的儲存桶，其中的密碼在撰寫本文時包含大約 15 億個密碼。密碼所屬的儲存桶是依據密碼的 SHA256 雜湊值的前 15 位元而定。此外，每個洩漏的密碼 (pw) 與 NIST P256 曲線上的橢圓曲線點相關聯： $P_{pw} = \alpha \cdot H_{SWU}(pw)$ ，其中  $\alpha$  是僅 Apple 所知的秘密隨機密鑰，而  $H_{SWU}$  是根據 Shallue-van de Woestijne-Ulas 方法將密碼映射到曲線點的隨機 oracle 函數。此轉換的設計用意是透過計算隱藏密碼的值，並透過「密碼監測」協助防止揭露新洩漏的密碼。

為了計算私密集的交集，用戶裝置會使用  $\lambda$  (SHA256(upw) 的 15 位元前置碼) 來決定用戶密碼所屬的儲存桶，其中 upw 是其中一個用戶密碼。裝置產生自己的隨機常數  $\beta$ ，並將點  $P_c = \beta \cdot H_{SWU}(upw)$  以及與  $\lambda$  對應的儲存桶要求傳送到伺服器。 $\beta$  在此處隱藏了有關用戶密碼的資料，並且將從密碼向 Apple 揭露的資料限制為  $\lambda$ 。最後，伺服器取得用戶裝置所傳送的點，計算出  $\alpha P_c = \alpha \beta \cdot H_{SWU}(upw)$ ，並將其連同相關的點之儲存桶—— $B_\lambda = \{ P_{pw} \mid \text{SHA256}(pw) \text{ 以前置碼 } \lambda \text{ 開頭} \}$ ——傳回至裝置。

傳回的資料讓裝置可以計算  $B'_\lambda = \{ \beta \cdot P_{pw} \mid P_{pw} \in B_\lambda \}$ ，如果  $\alpha P_c \in B'_\lambda$ ，則確定用戶密碼已遭洩漏。

## 傳送密碼給其他用戶或 Apple 裝置

Apple 會使用 AirDrop 以及在 Apple TV 上將密碼安全地傳送給其他用戶或 Apple 裝置。

### 使用 AirDrop 將憑證儲存到另一部裝置

啟用 iCloud 後，用戶可以使用 AirDrop 將儲存的憑證傳送到另一部裝置。憑證包括用戶名稱和密碼以及為其被儲存以用於哪些網站。無論用戶的設定為何，透過 AirDrop 傳送憑證只會在「只限聯絡人」模式下進行。在接收裝置上，用戶同意後便會將憑證儲存在用戶的「自動填寫密碼」鑰匙圈中。

### 在 Apple TV 上的 App 中填入憑證

「自動填寫密碼」可用於在 Apple TV 上的 App 中填寫憑證。當用戶於螢幕上停留在 tvOS 上的用戶名稱或密碼文字欄位時，Apple TV 會開始透過低功耗藍牙 (BLE) 傳播「自動填寫密碼」要求。

附近的任何 iPhone、iPad 或 iPod touch 會顯示提示，邀請用戶與 Apple TV 分享一組憑證。

建立加密方式的方法如下：

- 如果裝置和 Apple TV 使用相同的 iCloud 帳戶，兩部裝置間的加密會自動進行。
- 如裝置登入的 iCloud 帳戶與 Apple TV 所用的不同，系統會提示用戶透過使用 PIN 碼建立加密連線。如要接收提示，必須解鎖 iPhone 並將其靠近與該 Apple TV 配對的「Apple TV Remote」。

使用 BLE 連結加密技術建立加密的連線後，系統會將憑證傳送至 Apple TV，並自動填入 App 上的相關文字欄位。

## 憑證提供者延伸功能

在 iOS、iPadOS 和 macOS 中，用戶可以將參與的第三方 App 指定為憑證提供者，位置在「密碼」設定 (iOS 和 iPadOS) 中的「自動填寫密碼」或在「系統偏好設定」(macOS) 中的「延伸功能」設定。這個機制建立在 App 延伸功能之上。憑證提供者延伸功能必須提供選擇憑證的畫面，且延伸功能可選擇性提供有關已儲存憑證的後設資料，以便直接在「快速輸入」列上 (iOS 和 iPadOS) 或在自動完成建議中 (macOS) 提供。後設資料包含憑證的網站和相關用戶名稱，但不包含其密碼。用戶選擇將憑證填入 App 中或 Safari 中的網站上時，iOS、iPadOS 和 macOS 會與延伸功能通訊以取得密碼。憑證後設資料存放在憑證提供者的 App 的容器內，且 App 解除安裝時會自動移除。

## iCloud 鑰匙圈

### 「iCloud 鑰匙圈」保安概覽

iCloud 可讓用戶在 iOS 與 iPadOS 裝置和 Mac 電腦之間安全地同步其密碼，不會將此資料提供給 Apple。除了強大的私隱保護和保安，易用性和回復鑰匙圈功能這兩個目的對「iCloud 鑰匙圈」的設計和架構也具有重要影響。

「iCloud 鑰匙圈」由兩項服務組成：鑰匙圈同步和鑰匙圈還原。

Apple 設計的「iCloud 鑰匙圈」和鑰匙圈還原可確保用戶的密碼在下列情況下仍然受到保護：

- 用戶的 iCloud 帳戶被盜。
- 外部攻擊者或員工危害了 iCloud 的保安。
- 第三方取用用戶帳戶。

### iCloud 鑰匙圈與密碼管理員的整合

iOS、iPadOS 和 macOS 可以自動產生具有加密編譯強度的隨機字串，以用作 Safari 中的帳戶密碼。iOS 和 iPadOS 也可為 App 產生高強度密碼。產生的密碼會儲存在鑰匙圈中並同步到其他裝置。鑰匙圈項目透過 Apple 伺服器在不同的裝置之間傳輸，但會嚴格進行加密，Apple 和其他裝置均無法讀取其內容。

## 鑰匙圈安全同步

當用戶第一次啟用「iCloud 鑰匙圈」時，裝置將建立信任圈並為自己製作同步身份。同步身份包括專用密鑰和公用密鑰，並會儲存在裝置的鑰匙圈中。同步身份的公用密鑰會置於信任圈中，該信任圈已經過兩次簽署：第一次由同步身份的專用密鑰簽署，第二次由用戶 iCloud 帳戶密碼所衍生的非對稱橢圓密鑰（使用 P-256）簽署。連同信任圈一起儲存的還有參數（隨機鹽值和反覆運算次數），用於製作以用戶 iCloud 密碼為基礎的密鑰。

對於雙重認證帳戶，會建立額外的類似同步信任圈並將其儲存在 CloudKit 中。此系統中的裝置身份由兩對非對稱橢圓金鑰（使用 P-384）組成，也儲存在鑰匙圈中。每部裝置都會維護其本身的信任身份列表，並使用其中一個身份密鑰對該列表進行簽署。

### 同步信任圈的 iCloud 儲存

已簽署的同步信任圈會存放於用戶的 iCloud 密鑰值儲存區域。如果不知道用戶的 iCloud 密碼，就無法讀取該同步信任圈，而如果沒有該同步信任圈成員同步身份的專用密鑰，就無法進行有效修改。

對於雙重認證帳戶，每部裝置的同步列表會儲存在 CloudKit 中。如果不知道用戶的 iCloud 密碼，就無法讀取這些列表，而如果沒有該持有裝置的專用密鑰，就無法對這些列表進行修改。

### 用戶的其他裝置如何加入到同步信任圈

新裝置在登入 iCloud 時，會透過以下兩種方式之一加入「iCloud 鑰匙圈」的同步信任圈：與現有「iCloud 鑰匙圈」裝置配對並由其贊助，或使用「iCloud 鑰匙圈」還原。

在配對流程中，申請裝置為同步信任圈和同步列表（用於雙重認證帳戶）建立新的同步身份，並將其顯示給贊助者。贊助者會將新成員的公用密鑰加入到同步信任圈，並使用其同步身份和來自用戶 iCloud 密碼的密鑰再次簽署。新的同步信任圈會置於 iCloud 中，該信任圈的新成員會以類似方式進行簽名。在雙重認證帳戶中，贊助者裝置也會向加入的裝置提供由其身份密鑰簽署的憑證，表示應信任申請裝置。然後，其會更新其受信任同步身份的個別列表以納入申請者。

現在簽名信任圈有兩個成員，並且每個成員擁有其同伴裝置的公用密鑰。他們現在開始透過 iCloud 密鑰值儲存空間來交換個別的鑰匙圈項目，或他們會儲存在 CloudKit 中（以最適用者為主）。如果兩個信任圈成員都對同一個項目進行更新，選擇其中一個或另一個，都會產生最終的一致性。每個同步的項目都會經過加密，因此只能由用戶信任圈中的裝置進行解密；其他任何裝置或 Apple 均無法解密。

當新裝置加入同步信任圈時，請重複此「加入程序」。例如，當第三部裝置加入時，它可以與任何一部現有裝置進行配對。每當有新的同伴裝置加入，每部同伴裝置都會與新裝置進行同步。其設計用意是確保所有成員擁有相同的鑰匙圈項目。

### 只有特定項目會進行同步

部份鑰匙圈項目是用於特定裝置，例如 iMessage 密鑰，因此必須保留在裝置上。因此，每個要同步的項目都必須用 `kSecAttrSynchronizable` 屬性明確標示。

Apple 已經為 Safari 用戶資料（包括用戶名稱、密碼和信用卡卡號），以及 Wi-Fi 網絡密碼、HomeKit 加密密鑰和其他支援點對點 iCloud 加密的鑰匙圈項目設定了此屬性。

此外，依照預設，第三方 App 所加入的鑰匙圈項目不會進行同步。將項目加入到鑰匙圈時，開發者必須設定 `kSecAttrSynchronizable` 屬性。

## 「iCloud 鑰匙圈」安全還原

「iCloud 鑰匙圈」會將用戶鑰匙圈交由 Apple 託管，但不允許 Apple 讀取密碼和鑰匙圈包含的其他資料。即使用戶只有一部裝置，鑰匙圈還原也可以提供安全網來防止資料遺失。如果使用了 Safari 來為網頁帳戶隨機產生高強度密碼，鑰匙圈還原就顯得格外重要，因為只有鑰匙圈會記錄這些密碼。

鑰匙圈還原包含兩大基本要素：輔助認證和安全託管服務，後者是 Apple 專為支援此功能而建立的服務。用戶的鑰匙圈會使用高強度密碼進行加密，只有在滿足一組嚴格的條件時，託管服務才會提供鑰匙圈副本。

### 使用第二個認證

建立高強度密碼的方式有以下幾種：

- 如用戶的帳戶已啟用雙重認證，便會使用裝置密碼來還原託管的鑰匙圈。
- 如未設定雙重認證，則會要求用戶提供六位數的密碼以製作 iCloud 安全碼。或者，在不使用雙重認證的情況下，用戶可自行指定較長的安全碼，或讓裝置以加密編譯方式製作隨機編碼，方便用戶自行記錄和保存。

### 鑰匙圈託管程序

建立密碼後，鑰匙圈便會交由 Apple 託管。iOS、iPadOS 或 macOS 裝置會先匯出用戶的鑰匙圈副本，然後加密封裝至非對稱式 Keybag 的密鑰中，並將其放置在用戶的 iCloud 密鑰值儲存區域中。Keybag 會以用戶的 iCloud 安全碼和儲存託管記錄的硬件安全模組 (HSM) 叢集公用密鑰進行封裝。這會變成用戶的 **iCloud 託管記錄**。如為雙重認證帳戶，鑰匙圈也儲存在 CloudKit 中，包裝為僅可使用 iCloud 託管記錄內容來還原的中間鑰匙，進而提供同等級的保護。

託管記錄的內容還允許還原裝置以重新加入「iCloud 鑰匙圈」，向任何現有裝置證明還原裝置已順利執行託管過程，並因此得到帳戶持有人的授權。

**附註：**如果用戶決定接受隨機加密編譯的安全碼，而不自行指定或使用四位數值，則不再需要託管記錄。相反地，iCloud 安全碼會用來直接封裝隨機密鑰。

除了建立安全碼，用戶也須註冊一個電話號碼。這提供了進行鑰匙圈還原期間的第二層認證機制。用戶會收到一則 SMS 短訊，必須回覆才能繼續進行還原。

## 「iCloud 鑰匙圈」的託管保安

iCloud 為鑰匙圈託管提供了安全的基礎架構，可協助確保只有經過授權的用戶和裝置能進行還原。iCloud 背後部署的是硬件保安模組 (HSM) 叢集，可保護託管記錄。如前文所述，叢集的每位成員都有一個密鑰，用來對其監管的託管記錄進行加密。

如要還原鑰匙圈，用戶必須使用其 iCloud 帳戶和密碼進行身份認證，當訊息傳送至所註冊的電話號碼時，用戶必須進行回覆。回覆完成後，用戶必須輸入其 iCloud 安全碼。HSM 叢集會使用「安全遙距密碼」(SRP) 通訊協定來驗證用戶是否知道其 iCloud 安全碼；安全碼本身不會傳送給 Apple。叢集的每個成員都會單獨驗證用戶是否未超過載取記錄所允許的最多嘗試次數，如以下所述。如果多數成員同意，叢集會將託管記錄解除封裝並將其傳送至用戶的裝置。

接着，裝置會使用 iCloud 安全碼來將用於加密用戶鑰匙圈的隨機密鑰解除封裝。系統會使用該密鑰來解密鑰匙圈（從 iCloud 密鑰值儲存區域和 CloudKit 中取回）並還原到裝置上。iOS、iPadOS 和 macOS 只允許嘗試認證和取回託管記錄 10 次。數次嘗試失敗後記錄將會被鎖定，用戶必須聯絡「Apple 支援」才能進行更多次嘗試。第 10 次嘗試失敗後，HSM 叢集將銷毀託管記錄，且鑰匙圈將永久消失。這種方式以犧牲鑰匙圈資料為代價，防止有心人士嘗試透過暴力密碼破解攻擊來載取記錄。

這些規則已寫入 HSM 韌體程式碼中。允許更改韌體的管理取用卡已銷毀。任何嘗試更改韌體或取用專用密鑰的操作，都會導致 HSM 叢集刪除專用密鑰。萬一發生這種情況，受叢集保護的所有鑰匙圈擁有者會收到訊息，通知他們已失去其託管記錄。他們之後可以選擇重新註冊。

# Apple Pay

## Apple Pay 保安概覽

使用 Apple Pay，用戶可以使用受支援的 iPhone、iPad、Mac 和 Apple Watch 裝置來以簡單、安全又保密的方式，在商店、App 和 Safari 的網頁上進行付款。用戶也可將支援 Apple Pay 功能的交通卡、學生證和識別證加入 Apple「銀包」。Apple Pay 對於用戶來說相當簡單易用，且在硬件和軟件方面皆具備整合性的安全措施。

Apple Pay 的目標也在於保護用戶的個人資料。Apple Pay 不會收集任何可追蹤用戶的交易資料。付款交易只於用戶、商戶和發卡機構之間進行。

## Apple Pay 元件保安

Apple Pay 使用多種硬件和軟件功能來提供安全可靠的購買體驗。

### Secure Element

Secure Element 是執行 Java Card 平台，且符合業界標準和受認證的晶片，其符合金融業的電子付款要求。Secure Element IC 和 Java Card 平台均通過 EMVCo 安全評估程序的認證。成功完成安全評估後，EMVCo 會核發不重複的 IC 和平台認證。

Secure Element IC 已按照「共同準則」的標準認證。如需更多資料，請參閱「Apple 平台認證」中的[安全隔離區處理器保安認證](#)。

### NFC 控制器

NFC 控制器處理「近場通訊」通訊協定並傳送「應用程式處理器」與 Secure Element 之間的通訊，以及 Secure Element 與銷售點終端機之間的通訊。

### Apple「銀包」

Apple「銀包」App 可用來加入和管理信用卡、扣帳卡和商店卡，以及使用 Apple Pay 付款。用戶可以在 Apple「銀包」中檢視其卡，同時或可檢視發卡機構提供的其他資料，例如發卡機構的私隱政策，以及近期交易等。用戶也可在以下位置將卡加入 Apple Pay：

- iOS 和 iPadOS 上的「設定輔助程式」和「設定」
- 用來設定 Apple Watch 的「手錶」App
- 配備 Touch ID 的 Mac「系統偏好設定」中的「銀包與 Apple Pay」

此外，用戶也可用 Apple「銀包」來加入和管理交通卡、獎勵卡、登機證、票券、禮品卡、學生證、識別證等票證。

### 安全隔離區

在 iPhone、iPad、Apple Watch、配備 Touch ID 的 Mac 電腦，以及配備 Apple 晶片且使用配備 Touch ID 之精妙鍵盤的 Mac 電腦上，「安全隔離區」會管理認證過程並允許進行付款交易。

在 Apple Watch 上，裝置必須解鎖，而用戶必須按兩下側邊按鈕。系統會偵測按兩下的動作並直接傳遞到 Secure Element 或「安全隔離區」（根據適用情況），不會經過「應用程式處理器」。

### Apple Pay 伺服器

Apple Pay 伺服器會管理 Apple「銀包」中信用卡、扣帳卡、交通卡、學生證和識別證的設定與配置。伺服器也會管理儲存在 Secure Element 中的「裝置帳戶號碼」。Apple Pay 伺服器會與裝置和付款網絡或發卡機構伺服器進行通訊。Apple Pay 伺服器也負責為 App 內和網絡上的付款重新加密付款憑證。

# Apple Pay 如何保護用戶的購買項目

## Secure Element

Secure Element 主控着一種特殊設計的 Applet 來管理 Apple Pay。其中也包含經過付款網絡或發卡機構認證的 Applet。已加密的信用卡、扣帳卡和預付卡資料會從付款網絡和發卡機構傳送到這些 Applet，期間會使用只有付款網絡或發卡機構和 Applet 的安全網域知悉的密鑰。此資料會儲存在這些 Applet 中，並受到 Secure Element 的保安功能保護。在交易期間，終端機會經由專用硬件匯流排，透過近場通訊 (NFC) 控制器直接與 Secure Element 進行通訊。

## NFC 控制器

作為 Secure Element 的閘道，NFC 控制器會協助確保所有非接觸式付款交易均使用接近該裝置的銷售點終端機進行。NFC 控制器只會將來自內場終端機的付款要求標示為非接觸式付款交易。

卡片持有人使用 Face ID、Touch ID 或密碼，或在解鎖的 Apple Watch 上按兩下側邊按鈕來授權信用卡、扣帳卡或預付卡 (包含商店卡) 付款，Secure Element 內由付款 Applet 準備的非接觸式付款回應會由控制器專門傳送至 NFC 磁場。因此，非接觸式付款交易的付款授權詳細資料會限制在本機 NFC 磁場內，且絕對不會向「應用程式處理器」揭露。相反地，App 內和網站上付款的付款授權詳細資料會傳送至「應用程式處理器」，但在此之前會先由 Secure Element 將資料加密至 Apple Pay 伺服器。

## 信用卡、扣帳卡及預付卡

### 卡配置的保安概覽

當用戶加入信用卡、扣帳卡或預付卡 (包含商店卡) 到 Apple「銀包」時，Apple 會以安全的方式將卡資料及用戶帳戶和裝置的其他資料，傳送到發卡機構或發卡機構授權的服務供應商。發卡機構會使用此資料來判定是否要核准將該卡加入 Apple「銀包」。作為卡配置程序的一部份，Apple Pay 使用三種伺服器端呼叫來傳送和接收與發卡機構或網絡之間的通訊：

- 必填的欄位
- 卡檢查
- 連結和配置

發卡機構或網絡會使用這些呼叫來驗證、核准卡以及將卡加入 Apple「銀包」。這些用戶端伺服器作業階段使用 TLS 1.2 來傳輸資料。

完整卡號不會儲存在裝置或 Apple Pay 伺服器上。反之，系統會建立一個獨有的「裝置帳戶號碼」，並對其加密，然後儲存在 Secure Element 中。這個獨有的「裝置帳戶號碼」會以 Apple 無法取用的方式加密。「裝置帳戶號碼」是獨有號碼，且與大部份信用卡或扣帳卡號不同，發卡機構或付款網絡可以防止將此號碼用於磁條卡、電話或網站。Secure Element 中的「裝置帳戶號碼」絕對不會儲存在 Apple Pay 伺服器上，也不會備份至 iCloud，且與 iOS、iPadOS 和 watchOS 裝置以及配備 Touch ID 的 Mac 電腦隔離。

配搭 Apple Watch 使用的卡，是使用 iPhone 上的 Apple Watch App 或在發卡機構的 iPhone App 中配置給 Apple Pay。將卡加入 Apple Watch 會要求手錶必須位於藍牙通訊範圍內。卡會特別註冊以配搭 Apple Watch 使用且具有專屬的「裝置帳戶號碼」，此資料會儲存在 Apple Watch 上的 Secure Element 內。

在使用相同 iCloud 帳戶登入的裝置上執行「設定輔助程式」期間，已加入的信用卡、扣帳卡或預付卡 (包含商店卡) 會在卡列表中顯示。只要在至少在一部裝置上為啟用狀態，這些卡就會保留在這個列表上。從所有裝置上移除卡 7 日後，該卡就會從此列表中移除。此功能需要對該 iCloud 帳戶啟用雙重認證。



## 將信用卡或扣帳卡加入 Apple Pay

可手動將信用卡加入 Apple 裝置中的 Apple Pay。

### 手動加入信用卡或扣帳卡

如要手動加入卡，需要提供姓名、卡號、到期日和 CVV 以執行配置程序。從「設定」、Apple「銀包」或 Apple Watch App 中，用戶可以透過打字方式或使用裝置上的相機來輸入該資料。當相機截取到卡資料時，Apple 會嘗試填入姓名、卡號和到期日。相片並不會儲存在裝置上或相片圖庫中。所有欄位均填妥後，「卡檢查」程序會驗證 CVV 以外的欄位。所有資料然後會經過加密並傳送到 Apple Pay 伺服器。

如「卡檢查」程序傳回使用條款 ID，Apple 會下載發卡機構的使用條款及細則，並顯示給用戶閱覽。如果用戶接受使用條款，Apple 便會將所接受條款的 ID 連同 CVV 傳送至「連結和配置」程序。此外，作為「連結和配置」程序的一部份，Apple 會與發卡機構或網絡分享裝置的資料。這包括像是 (a) 用戶 iTunes 和 App Store 帳戶活動的相關資料 (例如用戶是否在 iTunes 內有長期的交易記錄)、(b) 用戶裝置 (例如電話號碼、裝置名稱及裝置型號，以及任何設定 Apple Pay 所需的輔助 Apple 裝置)，以及 (c) 加入卡時的大約位置 (如用戶已啟用「定位服務」)。發卡機構會使用此資料來判斷是否要核准將該卡加入 Apple Pay。

「連結和配置」程序會產生兩個結果：

- 裝置會開始下載代表信用卡或扣帳卡的 Apple「銀包」票證檔案。
- 裝置會開始將卡連繫至 Secure Element。

票證檔案包含 URL，可供下載卡圖片、與卡相關的後設資料 (例如聯絡資料)、相關發卡機構 App 和支援的功能。票證檔案也包含票證狀態，其中的資料包含 Secure Element 的個人化是否已完成、卡目前是否已遭發卡銀行停用，或在卡可以配搭 Apple Pay 進行付款前，還需要進行哪些其他驗證。

### 從 iTunes Store 帳戶加入信用卡或扣帳卡

如要使用向 iTunes 登記的信用卡或扣帳卡，用戶可能需要重新輸入其 Apple ID 密碼。系統會從 iTunes 取得卡號，並隨之啟動「卡檢查」程序。如果卡符合使用 Apple Pay 的資格，裝置會下載並顯示使用條款，並連帶條款 ID 和卡安全碼傳送至「連結和配置」程序。iTunes 帳戶存檔的卡資料可能需要額外驗證。

### 從發卡機構的 App 加入信用卡或扣帳卡

App 註冊與 Apple Pay 配搭使用時，系統便會為 App 和發卡機構伺服器建立密鑰。這些密鑰用來加密傳送給發卡機構的卡資料。其設計用意是避免資料遭 Apple 裝置讀取。此配置流程類似於上述手動加入卡所使用的流程，除了會使用一次性密碼而非 CVV。

### 從發卡機構的網站加入信用卡或扣帳卡

某些發卡機構提供了直接從其網站為 Apple「銀包」啟動卡配置流程的功能。在這種情況下，用戶透過在發卡機構的網站上選取要配置的卡來啟動操作。然後，系統會將用戶引導至獨立的 Apple 登入體驗 (包含在 Apple 的網域中)，並要求使用其 Apple ID 登入。成功登入後，用戶接着選擇一部或多部裝置來配置卡，並需要在每個個別的目標裝置上確認配置結果。

### 加入額外驗證

發卡機構有權決定信用卡或扣帳卡是否需要額外驗證。視發卡機構提供的選項而定，用戶可能有多種額外驗證選項，例如短訊、電郵、致電客戶服務熱線，或經核准的第三方 App 所提供的方法來完成驗證。如使用短訊或電郵，用戶需從發卡機構存檔的聯絡資料中選擇。接着系統會傳送一組代碼，用戶必須將其輸入 Apple「銀包」、「設定」或 Apple Watch App 中。如使用客戶服務熱線或 App 驗證，發卡機構會執行其自有的通訊流程。

## Apple Pay 付款授權

在具有「安全隔離區」的裝置上，只有在收到來自「安全隔離區」的授權後，才能進行付款。在 iPhone 或 iPad 上，此操作則包含確認用戶已透過 Face ID、Touch ID 或裝置密碼進行認證。Face ID 或 Touch ID (如適用) 為預設方法；但用戶隨時都可以使用密碼。在三次嘗試比對指紋失敗後，或是兩次嘗試配對面孔失敗後，會自動建議改用密碼；而嘗試失敗五次後，則必須輸入密碼。當用戶未設定 Face ID 或 Touch ID，或是沒有針對 Apple Pay 啟用 Touch ID 或 Face ID 時，也需要輸入密碼。如要在 Apple Watch 上進行付款，必須使用密碼解鎖裝置，且必須按兩下側邊按鈕。

### 使用共享的配對密鑰

「安全隔離區」和 Secure Element 之間的通訊會在序列介面上進行，Secure Element 會連接到 NFC 控制器，接着再連接到「應用程式處理器」。即使未直接連接，「安全隔離區」和 Secure Element 也可以使用共享的配對密鑰來安全地通訊，此配對密鑰是在生產過程中配置的。通訊的加密和認證是基於 AES，兩端的通訊方皆會使用加密編譯隨機數來防止重播攻擊。配對密鑰是從「安全隔離區」內的 UID 密鑰和 Secure Element 的唯一識別碼產生。配對密鑰接着會安全地從「安全隔離區」傳送至工廠內的硬件安全模組 (HSM)，其中包含所需的密鑰材料，再將配對密鑰植入 Secure Element。

### 授權安全交易

當用戶授權交易時 (包括直接與「安全隔離區」通訊的物理動作)，「安全隔離區」會將認證類型的簽署資料和交易類型的詳細資料 (非接觸式或 App 內付款) 傳送至 Secure Element，繫結至「授權隨機」(AR) 值。當用戶首次配置信用卡並於 Apple Pay 啟用時保存，便會在「安全隔離區」內產生 AR 值，此值受到「安全隔離區」的加密和反回滾機制保護。它會藉由運用配對密鑰安全地傳送到 Secure Element。在接收到新的 AR 值時，Secure Element 會將任何先前加入過的卡標記為已刪除。

### 使用付款密碼來達成動態保安

來自付款 Applet 的付款交易包含付款密碼及「裝置帳戶號碼」。這組密碼是一次性安全碼，計算方式是使用交易計數器和密鑰。交易計數器會隨每筆交易遞增。該密鑰是在進行個人化期間於付款 Applet 中配置，且付款網絡或發卡機構或此二者皆知道該密鑰。視付款方案而定，也可能會使用其他資料來進行計算，包括：

- Terminal Unpredictable Number (適用於近場通訊 (NFC) 交易)
- Apple Pay 伺服器隨機數 (適用於 App 內交易)

這些安全碼會提供給付款網絡和發卡機構，供發卡機構驗證每筆交易。這些安全碼的長度會視交易的類型而有所不同。

## 使用 Apple Pay 用卡付款

Apple Pay 可用來在商店、App 內和網站上購買商品。

### 在商店使用卡付款

如果 iPhone 或 Apple Watch 已開機且偵測到 NFC 磁場，便會向用戶顯示要求的卡（如該卡已開啟自動選取功能），或顯示「設定」中管理的預設卡。用戶也可前往 Apple「錢包」並選擇卡，或當裝置鎖定時，可以：

- 在配備 Face ID 的裝置上按兩下側邊按鈕
- 在配備 Touch ID 的裝置上按兩下主畫面按鈕
- 使用允許從鎖定畫面支付 Apple Pay 的輔助使用功能

接着，在發送付款資料前，用戶必須使用 Face ID、Touch ID 或其密碼來授權。當 Apple Watch 解鎖時，按兩下側邊按鈕來啟用付款的預設卡。所有付款資料皆需經過用戶認證始得發送。

用戶認證完成後，在處理付款時便會使用「裝置帳戶號碼」和因交易而異的動態安全碼。無論是 Apple 或用戶的裝置，皆不會將完整的信用卡或扣帳卡號碼傳送給商戶。Apple 可能會接收到匿名的交易資料，如交易的大約時間和位置，這可協助改進 Apple Pay 及其他的 Apple 產品和服務。

### 在 App 內使用卡付款

Apple Pay 也可以用來在 iPhone、iPad、Mac 及 Apple Watch App 內進行付款。當用戶在 App 內使用 Apple Pay 付款時，Apple 會收到加密的交易資料。在該資料傳送給開發商或商戶前，Apple 會以開發者特定密鑰再次加密該交易。Apple Pay 會保留匿名的交易資料，例如約略購買金額。此資料無法用來追蹤用戶，且絕不包含用戶購買的商品資料。

當 App 開始進行 Apple Pay 付款交易時，Apple Pay 伺服器會比商戶先收到來自裝置的加密資料。Apple Pay 伺服器接着會以商戶特定密鑰將交易再次加密，才會將交易傳遞給商戶。

當 App 要求付款時，會呼叫 API 以判別裝置是否支援 Apple Pay，以及用戶所使用的信用卡或扣帳卡是否可在商戶認可的付款網絡上進行付款。App 會要求取得任何所需的資料，以處理及完成交易，例如帳單和送貨地址，以及聯絡資料。App 接着會要求 iOS、iPadOS 或 watchOS 出示 Apple Pay 表單，其會要求 App 的資料以及其他必要資料，例如要使用的卡。

此時，系統已向 App 提供城市、區和郵政編碼等資料以計算最終運費。直到用戶以 Face ID、Touch ID 或裝置密碼授權付款，所要求的全部資料才會提供給 App。付款一經授權，Apple Pay 表單內出示的資料便會傳送給商戶。

### App 付款授權

當用戶授權付款時，系統會呼叫 Apple Pay 伺服器以取得加密編譯隨機數，這與進行店內交易時 NFC 終端機傳回的數值類似。隨機數和其他交易資料會傳遞到 Secure Element 以計算付款憑證，此付款憑證會以 Apple 密鑰進行加密。加密的付款憑證會傳回到 Apple Pay 伺服器，伺服器會解密憑證、比對憑證中的隨機數與原來由 Apple Pay 伺服器發送的隨機數，然後使用與「商戶 ID」綁定的商戶密鑰重新加密付款憑證。接着付款憑證會傳回裝置，透過 API 傳送回 App。App 接下來會將付款憑證傳遞到商戶系統進行處理。商戶便可以使用其專用密鑰解鎖付款憑證以進行處理。這會結合來自 Apple 伺服器的簽名，允許商戶驗證交易是針對此特定商戶所進行的。

API 會要求一項授權，此授權用來指定支援的「商戶 ID」。App 也可能包含要傳送至 Secure Element 進行簽署的其他資料（例如訂單號碼或客戶身份），以確保交易無法轉移到其他客戶。此程序需由 App 開發者執行，其能指定 PKPaymentRequest 上的 applicationData。此資料的雜湊值會包含在加密的付款資料中。商戶接着會負責驗證其 applicationData 雜湊值是否與付款資料內包含的雜湊值相符。

## 在網站上使用卡付款

你可在 iPhone、iPad、Apple Watch 以及 Mac 電腦 (配備 Touch ID) 上, 使用 Apple Pay 在網站進行付款。Apple Pay 交易也可在 Mac 上進行, 並在使用相同 iCloud 帳戶且已啟用 Apple Pay 的 iPhone 或 Apple Watch 上完成。

網絡上的 Apple Pay 服務會要求所有參與的網站向 Apple 註冊。網域註冊後, 只會在 Apple 核發 TLS 用戶端憑證後, 才執行網域名稱驗證。支援 Apple Pay 的網站需要透過 HTTPS 來提供內容服務。針對每次付款交易, 網站需要使用 Apple 發出的 TLS 用戶端證書來向 Apple 伺服器取得安全且唯一的商戶作業階段。商戶作業階段資料則會由 Apple 加以簽署。商戶作業階段簽名經過驗證後, 網站便可查詢用戶是否具有支援 Apple Pay 的裝置, 以及這些裝置上是否已啟用信用卡、扣帳卡或預付卡。任何其他細節皆不會共享。如果用戶不想要共享此資料, 他們可以在 iPhone、iPad 和 Mac 裝置上的 Safari 隱私設定中停用 Apple Pay 查詢。

商戶作業階段經過驗證後, 所有隱私與保安措施皆與用戶在 App 內付款時相同。

如用戶將付款相關資料從 Mac 傳送到 iPhone 或 Apple Watch, Apple Pay 的「接手」功能會使用點對點的加密 Apple 識別服務 (IDS) 通訊協定, 在用戶的 Mac 與授權裝置間傳輸付款的相關資料。Mac 上的 IDS 用戶端會利用用戶的裝置密鑰來執行加密, 因此任何其他裝置皆無法解密此資料, 而這些密鑰不會提供予 Apple。為 Apple Pay 「接手」進行的裝置搜尋包含用戶信用卡的類型與唯一識別碼, 以及部份後設資料。用戶卡的特定裝置帳戶號碼不會共享, 且會安全地繼續保留在用戶的 iPhone 或 Apple Watch 上。Apple 也會透過「iCloud 鑰匙圈」安全地傳送用戶最近使用過的聯絡資料、送貨及帳單地址。

用戶使用 Face ID、Touch ID 或密碼, 或在 Apple Watch 上按兩下側邊按鈕來授權付款後, 針對每個網站商戶憑證進行專屬加密的付款代號就會安全地從用戶的 iPhone 或 Apple Watch 傳輸到他們的 Mac, 然後傳遞到商戶的網站。

只有鄰近的裝置可要求和完成付款。鄰近位置是透過低耗電藍牙 (BLE) 廣播來加以判定。

## Apple Pay 中的非接觸式票證

為了將資料從支援的票證傳輸到相容的 NFC 終端機, Apple 使用「Apple 增值服務」(Apple VAS) 通訊協定。VAS 通訊協定可在非接觸式終端機上或在 iPhone App 上執行, 並使用 NFC 來與支援的 Apple 裝置進行通訊。VAS 通訊協定可間隔一小段距離使用, 且可用來單獨出示非接觸式票證, 或作為 Apple Pay 交易的一部份。

將裝置拿近 NFC 終端機時, 終端機會藉由發送票證要求來起始接收票證資料的程序。如用戶擁有帶有票證供應商識別碼的票證, 系統會要求用戶透過 Face ID、Touch ID 或密碼授權使用。票證資料、時間戳記及一次性隨機 ECDH P-256 密鑰會與票證供應商的公用密鑰一起使用, 以便為票證資料衍生一個加密密鑰, 並將此密鑰傳送至終端機。

從 iOS 12.0.1 至 (包含) iOS 13, 用戶可手動選擇票證再向商戶的 NFC 終端機出示。在 iOS 13.1 或較新版本, 票證供應商可設定手動選擇票證是否需要用戶認證或無需認證。

## 透過 Apple Pay 讓卡無法使用

只有在 Secure Element 使用與加入卡時相同的配對密鑰和「授權隨機」(AR) 值出示授權時, 才能使用加入到 Secure Element 的信用卡、扣帳卡和預付卡。在接收到新的 AR 值時, Secure Element 會將任何先前加入過的卡標記為已刪除。這會使作業系統在下列情況發出指令, 讓「安全隔離區」將 AR 副本標記為無效, 讓卡變為無法使用的狀態:

方式	裝置
密碼停用。	iPhone、iPad、Apple Watch
密碼停用。	Mac
用戶登出 iCloud。	iPhone、iPad、Mac、Apple Watch
用戶選擇「清除所有內容和設定」。	iPhone、iPad、Mac、Apple Watch
裝置從「還原模式」還原。	iPhone、iPad、Mac、Apple Watch
取消配對時	Apple Watch

### 停用、移除和清除卡

用戶可以使用「尋找」來將裝置設為「遺失模式」, 藉此在 iPhone、iPad 及 Apple Watch 上停用 Apple Pay。用戶也可以使用「尋找」、iCloud.com 或直接在裝置上使用 Apple「銀包」來清除 Apple Pay 中的卡。在 Apple Watch 上, 可以使用 iCloud 設定、iPhone 上的 Apple Watch App 移除卡, 或直接在手錶上移除卡。在裝置上使用卡來進行付款的功能將會由發卡機構或個別付款網絡在 Apple Pay 中停用或移除, 即使裝置處於離線狀態且未連線至流動數據或 Wi-Fi 網絡也能進行。用戶也可致電其發卡機構來從 Apple Pay 停用或移除卡。

當用戶透過「清除所有內容和設定」、使用「尋找」或將裝置還原來清除全部裝置時, iPhone、iPad、iPod touch、Mac 和 Apple Watch 會指示 Secure Element 將所有卡標記為已刪除。這會立即將卡更改為無法使用的狀態, 直到可聯絡到 Apple Pay 伺服器來從 Secure Element 完全清除卡為止。除此之外, 「安全隔離區」會將 AR 標記為無效, 使先前登記的卡無法進行進一步的付款授權。當裝置為在線狀態時, 會嘗試聯絡 Apple Pay 伺服器, 以協助確保 Secure Element 中的所有卡皆已清除。

# Apple Card 保安

在支援的 iPhone 和 Mac 型號上，用戶可以安全地申請 Apple Card。

## Apple Card 申請

在 iOS 12.4 或較新版本、macOS 10.14.6 或較新版本以及 watchOS 5.3 或較新版本中，可配搭 Apple Pay 使用 Apple Card 來在商店、App 內和網站上進行付款。

如要申請 Apple Card，用戶必須在與 Apple Pay 相容的 iOS 或 iPadOS 裝置上登入自己的 iCloud 帳戶，並已為 iCloud 帳戶設定雙重認證。申請獲批後，用戶就可在已登入其 Apple ID 的任何合資格裝置上，於 Apple「銀包」或「設定」>「銀包與 Apple Pay」中取用 Apple Card。

當用戶申請 Apple Card 時，Apple 的身份提供者合作夥伴會以安全方式驗證用戶的身份資料，然後基於身份與信用評估目的與 Goldman Sachs Bank USA 共享這些資訊。

申請過程中提供的社會安全碼或身份證明文件圖像之類的資料將安全地傳傳輸到 Apple 的身份服務供應商合作伙伴和/或 Goldman Sachs Bank USA，過程中資料會以其各自擁有的密鑰加密。Apple 無法解密此資料。

在申請過程中提供的收入資料以及用於支付帳單的銀行帳戶資料會安全地傳傳輸到 Goldman Sachs Bank USA，並使用其密鑰進行加密。銀行帳戶資料會儲存在鑰匙圈中。Apple 無法解密此資料。

將 Apple Card 加入到 Apple「銀包」時，可能會與 Apple 合作夥伴銀行 Goldman Sachs Bank USA 及 Apple Payments Inc. 共享用戶加入信用卡或扣帳卡時相同的資料。此資料只用於排解疑難、防範詐騙和法規用途。

在 iOS 14.6 或較新版本、iPadOS 14.6 或較新版本以及 watchOS 7.5 或較新版本中，擁有 Apple Card 的 iCloud 家庭的組織者可以與 13 歲以上的 iCloud 家庭成員共享他們的卡。需要用戶認證才能確認邀請。Apple「銀包」使用「安全隔離區」中的密鑰來計算綁定持有人和受邀者的簽署。該簽署會在 Apple 伺服器上驗證。

組織者可以選擇為成員設定交易上限。成員的卡也可以透過 Apple「銀包」隨時加以鎖定以暫停消費。當 18 歲以上的共同持有人或成員接受邀請並提出申請時，他們將按照 Apple「銀包」中 Apple Card 申請部份中定義的相同申請流程進行申請。

## Apple Card 使用

用戶可透過 Apple「銀包」中的 Apple Card 要求實體卡。用戶收到實體卡後，需使用裝着實體卡的對摺信封內的 NFC 標籤來啟用卡。該標籤為每張卡獨有，不能用於啟用用戶的其他卡。或者，也可在 Apple「銀包」設定中手動啟用卡。此外，用戶也可隨時透過 Apple「銀包」選擇鎖定或解鎖實體卡。

## Apple Card 付款及 Apple「銀包」票證詳細資料

用戶可以使用 Apple Cash 和銀行帳戶，透過 iOS 中的 Apple「銀包」繳付 Apple Card 帳戶的應繳款項。可以將帳單付款安排為定期付款，也可以安排為在特定日期使用 Apple Cash 和銀行帳戶一次付款。用戶付款時將呼叫 Apple Pay 伺服器以獲得類似於 Apple Cash 的加密隨機數。隨機數和付款設定詳細資料會傳遞到 Secure Element 以計算簽署。簽署則會傳回到 Apple Pay 伺服器。付款的認證、完整性和正確性會由 Apple Pay 伺服器透過簽名和隨機數驗證，並將訂單傳遞給 Goldman Sachs Bank USA 進行處理。

Apple「銀包」透過提供憑證來載取 Apple Card 卡號。Apple Pay 伺服器會驗證憑證以確認密鑰是在「安全隔離區」中產生，然後使用此密鑰對 Apple Card 卡號進行加密，接著將其傳回到 Apple「銀包」，這樣只有要求 Apple Card 卡號的 iPhone 才能解密。解密後，Apple Card 卡號會儲存在「iCloud 鑰匙圈」中。

如要使用 Apple「銀包」在票證中顯示 Apple Card 卡號詳細資料，需透過 Face ID、Touch ID 或密碼進行用戶認證。用戶可在卡資料部份取代及停用之前的詳細資料。

## 進階詐騙防範

在 iOS 15 或較新版本以及 iPadOS 15 或較新版本中，Apple Card 用戶可以在 Apple「銀包」中啟用「進階詐騙防範」。啟用後，「卡安全碼」每隔幾日會重新整理一次。

## Apple Cash 保安

在 iOS 11.2 或較新版本、iPadOS 13.1 或較新版本及 watchOS 4.2 或較新版本上，可在 iPhone、iPad 或 Apple Watch 上使用 Apple Pay 向其他用戶付款、收款和要求付款。用戶收款時，款項會加入 Apple Cash 帳戶中，且可在用戶已用 Apple ID 登入的合資格裝置上，前往 Apple「銀包」或「設定」>「錢包與 Apple Pay」使用該款項。

在 iOS 14、iPadOS 14 和 watchOS 7 中，已向 Apple Cash 驗證身份的 iCloud 家庭組織者可以為 18 歲以下的家庭成員啟用 Apple Cash。組織者可以選擇將這些用戶的匯款功能限制為僅限家庭成員或僅限聯絡人。如果 18 歲以下的家庭成員進行 Apple ID 帳戶還原，則家庭的組織者必須手動為該用戶重新啟用 Apple Cash 卡。如果 18 歲以下的家庭成員不再屬於 iCloud 家庭，則其 Apple Cash 餘額將自動轉移到組織者的帳戶中。

用戶設定 Apple Cash 時，某些資料可能會與我們的合作銀行 Green Dot Bank 和 Apple Payments Inc. 共享，這些資料與用戶在加入信用卡或扣帳卡時所提供的相同。Apple Payments Inc. 是我們專為保護用戶的私隱而成立的全資子公司，其儲存和處理資料的過程獨立於 Apple 與其餘子公司，且方法完全保密。此資料只用於排解疑難、防範詐騙和法規用途。

### 在 iMessage 中使用 Apple Cash

如要使用個人對個人付款和 Apple Cash，用戶必須在與 Apple Cash 相容的裝置上登入自己的 iCloud 帳戶，並為 iCloud 帳戶設定雙重認證。用戶間的要求付款和轉帳程序可從「訊息」App 內啟動或要求 Siri 執行。用戶嘗試付款時，iMessage 會顯示 Apple Pay 表單。系統一律會先使用 Apple Cash 餘額。如有必要，會從用戶加入 Apple「銀包」中的第二信用卡或扣帳卡提取額外款項。

### 在商店、App 內和在網站上使用 Apple Cash

Apple「銀包」中的 Apple Cash 卡可配搭 Apple Pay 使用，以便在商店、App 內和網站上進行付款。Apple Cash 帳戶中的錢也可以轉帳到銀行帳戶中。除了收取其他用戶所付的款項，也可使用 Apple「銀包」中的扣帳卡或預付卡為 Apple Cash 帳戶增值。

一旦交易完成，基於疑難排解、防範詐騙或法規目的，Apple Payments Inc. 會儲存且可能使用用戶的交易資料。Apple 與其餘子公司無從得知用戶的付款、收款對象或使用 Apple Cash 卡購物的地點。

當你透過 Apple Pay 付款、將款項加入 Apple Cash 帳戶中，或是轉帳至銀行帳戶時，系統會呼叫 Apple Pay 伺服器以取得加密編譯隨機數，這個隨機數與 App 中針對 Apple Pay 傳回的數值類似。隨機數和其他交易資料會傳遞到 Secure Element 以計算付款簽署。簽署會傳回到 Apple Pay 伺服器。Apple Pay 伺服器會透過付款簽名和隨機數驗證交易的認證、完整性和正確性。接著就會啟動轉帳程序，並在交易完成時通知用戶。

如果交易牽涉以下項目：

- 對 Apple Cash 儲值的扣帳卡
- 如果 Apple Cash 餘額不足，則提供補充金額

也會產生加密的付款憑證，並將其傳送到 Apple Pay 伺服器，類似於 Apple Pay 在 App 和網站中的運作方式。

Apple Cash 帳戶的餘額超過一定金額後，或當偵測到異常活動，系統就會提示用戶驗證其身份。社會安全碼或問題的回答（例如確認用戶先前居住地址的街道名稱）等提供用於驗證用戶身份的資料，都會以安全的方式傳輸給 Apple 的合作廠商，並使用其密鑰進行加密。Apple 無法解密此資料。如果用戶執行了 Apple ID 帳戶還原，則系統將提示用戶再次驗證其身份，然後才能重新取用其 Apple Cash 餘額。

## Tap to Pay on iPhone 的保安

iOS 15.4 中提供的 Tap to Pay on iPhone 允許美國商戶使用 iPhone 和支援合作夥伴的 iOS App 接受 Apple Pay 和其他非接觸式支付。透過這項服務，擁有受支援的 iPhone 裝置的用戶可以安全地接受非接觸式支付和支援 Apple Pay NFC 的票卡。透過 Tap to Pay on iPhone，商戶無需額外的硬件即可接受非接觸式支付。

Tap to Pay on iPhone 的設計旨在保護付款人的個人資料。此服務不會收集可追蹤付款人的交易資料。信用卡/扣帳卡號 (PAN) 等付款卡資料由 Secure Element 保護，商戶無法使用。付款卡資料會保留在商戶的支付服務供應商、付款人和發卡機構之間。此外，Tap to Pay 服務不會收集付款人的姓名、地址或電話號碼。

Tap to Pay on iPhone 已由認證的安全實驗室進行外部評估，並獲得 American Express、Discover、Mastercard 和 Visa 的許可。

### 非接觸式支付元件的保安

- **Secure Element:** Secure Element [Apple Pay Secure Element 部份的連結] 託管用於讀取和保護非接觸式付款卡的資料之付款核心。
- **NFC 控制器:** NFC 控制器處理「近場通訊」通訊協定並傳送「應用程式處理器」與 Secure Element 之間的通訊，以及 Secure Element 與非接觸式付款卡之間的通訊。
- **Tap to Pay on iPhone 伺服器:** Tap to Pay on iPhone 伺服器會管理裝置中付款核心的設定和配置。這些伺服器還以與付款卡產業安全標準委員會 (PCI SSC) 的 COTS 非接觸式支付 (CPoC) 標準相容的方式監控 iPhone 裝置上的 Tap to Pay 保安，並且符合 PCI DSS。

## Tap to Pay 如何讀取信用卡、扣帳卡和預付卡

### 配置保安概覽

首次使用足夠授權的 App 來使用 Tap to Pay on iPhone 時，Tap to Pay on iPhone 伺服器會確定裝置是否符合裝置型號、iOS 版本以及是否設定了密碼等資格標準。此驗證完成後，系統會從 Tap to Pay on iPhone 伺服器下載付款接受 applet 並將其安裝在 Secure Element 上，也會一併安裝相關的付款核心設定。此操作會在 Tap to Pay on iPhone 伺服器和 Secure Element 之間安全地執行。Secure Element 在安裝前會驗證此資料的完整性和真實性。

### 卡讀取的保安概覽

當 Tap to Pay on iPhone App 要求從 ProximityReader 架構讀取卡時，會顯示一份由 iOS 控制的工作表並提示用戶感應付款卡。iOS 會初始化付款卡讀卡機，然後要求 Secure Element 中的付款核心啟動卡讀取。

此時，Secure Element 在「閱讀器模式」下接管 NFC 控制器。此模式僅允許透過 NFC 控制器在付款卡和 Secure Element 之間交換卡的資料。只有在此模式下才能讀取付款卡。

Secure Element 上的付款接受 applet 完成讀卡後，會對卡的資料進行加密和簽署。卡片資料在到達支付服務供應商之前會一直保持加密和已認證的狀態。只有 App 用來要求讀卡的支付服務供應商才能解密卡的資料。支付服務供應商必須從 Tap to Pay on iPhone 伺服器要求解密卡資料的密鑰。Tap to Pay on iPhone 伺服器會在驗證資料的完整性和真實性，以及在裝置上讀取卡的時間在 60 秒內完成後，向支付服務供應商發送解密密鑰。

此模型有助於確保卡的資料不會遭支付服務供應商以外的任何人解密，支付服務供應商會為商戶處理此交易。



# 使用 Apple「銀包」

## 使用 Apple「銀包」通行

在支援的 iPhone 和 Apple Watch 裝置上的 Apple「銀包」中，用戶可以儲存他們的家居、汽車和酒店房間鎖匙。他們甚至可以儲存公司識別證和學生證。當用戶抵達門口時，系統會自動顯示正確的鎖匙，讓他們使用近場通訊 (NFC)，只需輕觸一下即可進入。

### 用戶便利性

如將鎖匙、票證、學生證和公司識別證加入 Apple「銀包」，系統就會預設開啟「特快模式」。處於「特快模式」的卡能與接受該證件的終端機互動，不需要使用 Face ID、Touch ID、密碼認證或按兩下 Apple Watch 的側邊按鈕。如要停用此功能，用戶可以點一下 Apple「銀包」中卡正面的「更多」按鈕來關閉「特快模式」。如要重新開啟「特快模式」，他們必須使用 Face ID、Touch ID 或密碼。

### 私隱和保安

Apple「銀包」中的鎖匙充分利用了 iPhone 和 Apple Watch 內置的私隱和保安。用戶使用 Apple「銀包」中的鎖匙的時間和地點，永遠不會與 Apple 分享或儲存在 Apple 伺服器上，並且憑證會安全地儲存在受支援裝置的 Secure Element (SE) 中。SE 會託管專門設計的 applet 來安全地管理和儲存鎖匙，確保無法截取鎖匙。

在配置任何鎖匙前，用戶必須在相容的 iPhone 上登入其 iCloud 帳戶，並為其 iCloud 帳戶開啟雙重認證，但不包括學生證，學生證不需要雙重認證即可開啟。

當用戶啟動配置程序時，會發生與信用卡和扣帳卡配置中所涉及的類似步驟，例如[連結和配置](#)。在交易期間，讀卡機會使用已建立的安全通道，透過近場通訊 (NFC) 控制器直接與 Secure Element 進行通訊。

可以配置鎖匙的裝置數量 (包括 iPhone 和 Apple Watch) 由每個合作夥伴定義和控制，並且可能因合作夥伴而異。這種方法允許每個合作夥伴控制每種裝置類型配置鎖匙的上限，以滿足其特定需求。為此目的，Apple 會向合作夥伴提供裝置類型和匿名裝置識別碼。由於私隱與保安的緣故，每個合作夥伴的識別碼都不一樣。

可透過以下方式停用或移除鎖匙：

- 透過「尋找」遙距清除裝置
- 透過「尋找」啟用「遺失模式」
- 接收流動裝置管理 (MDM) 遙距清除指令
- 從 Apple ID 帳戶頁面移除所有卡
- 從 iCloud.com 移除所有卡
- 從 Apple「銀包」中移除所有卡
- 在發卡機構的 App 中移除卡

在 iOS 15.4 或較新版本中，當用戶按兩下配備 Face ID 的 iPhone 上的側邊按鈕，或按兩下配備 Touch ID 的 iPhone 上的主畫面按鈕時，在他們向裝置進行認證前，系統不會顯示他們的票證和鎖匙的詳細資料。在票證特定資料 (包括酒店預訂詳細資料) 在 Apple「銀包」中顯示之前，需要進行 Face ID、Touch ID 或密碼認證。

## 存取憑證類型

Apple「銀包」提供不同類型的存取權限，例如酒店、公司識別證、學生證、家居鎖匙和車匙。

### 酒店

Apple「銀包」中的酒店房間鑰匙有助於提供從入住到退房的輕鬆、非接觸式體驗，有別於傳統塑膠酒店房卡，其可以為客人提供額外的私隱與保安優勢。在受支援地點的酒客人可以在相容的 iPhone 和 Apple Watch Series 4 或較新型號上，使用 Apple「銀包」中的房間鎖匙輕觸解鎖。

Apple「銀包」中的功能專為減少客戶的不便而設計：

- 從酒店 App 進行抵達前的配置，以便在入住前將票證加入 Apple「銀包」中
- 入住票證方格，用於從 Apple「銀包」啟動登記入住和房間分配
- 配置後鎖匙更新，以支援延長或修改目前的住宿天數
- Apple「銀包」中單一票證可支援多間房間的鎖匙
- Apple「銀包」中會自動封存過期鎖匙

### 公司識別證

受支援合作夥伴的員工識別證可以加至 iPhone 和 Apple Watch 上的 Apple「銀包」，讓世界各地的員工能夠以非接觸方式進入他們的工作場所。如要加入識別證，員工必須為其用於登入其僱主所提供之 App 的帳戶啟用多重認證。

員工識別證使用 Apple 的取用功能，允許用戶：

- 透過推送配置自動將員工識別證加至已配對的 Apple Watch，無需安裝合作夥伴的 App
- 使用特快模式無縫取用辦公設施
- 即使 iPhone 耗盡電量，也可以進入工作場所

### 學生證

在 iOS 12 或較新版本中，參與方案的院校所屬教職員生可將其學生證或在校相關證件在支援的 iPhone 和 Apple Watch 型號上加至 Apple「銀包」，以便進出校園設施及在接受其證件的地方付款。

用戶需透過學生證發卡機構或參與學校提供的 App，將其學生證加至 Apple「銀包」。此操作的技術程序，與從發卡機構的 App 加入信用卡或扣帳卡中所述的程序相同。此外，發卡機構的 App 必須支援對保護其學生證存取權的帳戶使用雙重認證。最多可同時在以相同 Apple ID 登入的任何兩部支援 Apple 裝置上設定同一張卡。

### 多戶住宅

受支援合作夥伴設施的租戶和員工可以使用他們在 Apple「銀包」中的家居鎖匙進入他們的建築物、單位和公共區域。你可以從合作夥伴提供的 App 中配置家居鎖匙。對於支援便利配置的合作夥伴，物業經理可以向租戶傳送連結以使用他們偏好的通訊管道（例如電郵或 SMS）來啟動配置，租戶只需按一下該連結即可兌換鎖匙。「輕巧版 App」也能提供安全無縫的體驗，無需安裝合作夥伴的 App 即可配置鎖匙。如需更多資料，請參閱 Apple 支援文章：[在 iPhone 上使用「輕巧版 App」](#)。

## 家居鎖匙

只需點一下 iPhone 或 Apple Watch，即可將 Apple「銀包」中的家居鎖匙與支援 NFC 的門鎖配搭使用。如需有關用戶如何設定和使用家居鎖匙的更多資料，請參閱 Apple 支援文章：[在 iPhone 上使用家居鎖匙解除門鎖](#)。

當用戶設定家居鎖匙時，他們家中的所有住戶也會自動收到家居鎖匙。如要進一步共享家居鎖匙或刪除共享家居的成員，家居擁有者可以使用「家居」App 來管理邀請和成員。當用戶選擇接受邀請以使用家居鎖匙加入家居時，這會啟動將家居鎖匙配置到其裝置上的 Apple「銀包」中的操作。如果用戶選擇離開家居或家居擁有者撤回他們的取用權限，這些動作也會從 Apple「銀包」中移除家居鎖匙。

## 車匙

受支援的 iPhone 裝置和已配對的 Apple Watch 裝置中已原生支援在 Apple「銀包」中以數碼方式儲存車匙。車匙在 Apple「銀包」中會顯示為票證（由 Apple 代表汽車製造商製作），並支持完整的 Apple Pay 卡生命週期（iCloud「遺失模式」、「遙距清除」、本機票證刪除以及「清除所有內容和設定」）。除了標準的 Apple Pay 卡管理之外，還可以從車主的 iPhone、Apple Watch 和車輛人機介面（HMI）中刪除共享的車匙。

「車匙」可用於解鎖和鎖定車輛，以及發動引擎或將車輛設為行駛模式。「標準作業」提供相互認證，且對於發動引擎來說是強制性的。在需要講求效率表現時，解鎖和鎖定操作可能會使用「快速作業」。

鑰匙是透過將 iPhone 與自有和支援的車輛配對來製作。所有鑰匙都是基於橢圓曲線（NIST P-256）卡片鑰匙生成（ECC-OBKG）在嵌入式 Secure Element 上製作的，密鑰永遠不會離開 Secure Element。裝置與車輛之間的通訊使用 NFC 或藍牙 LE 與 UWB 結合，而鎖匙管理則使用具有相互認證 TLS 的 Apple 對汽車製造商伺服器的 API。將鑰匙與 iPhone 配對後，與該 iPhone 配對的任何 Apple Watch 也會收到鑰匙。在車輛或裝置上刪除鑰匙後，將無法還原。遺失或遭竊裝置上的鑰匙可將其暫停或恢復，但是在新裝置上重新配置鑰匙則需要重新配對或共享。

## iOS 中的車匙保安

在受支援的 iPhone 和已配對的 Apple Watch 上，開發者能支援無須鎖匙且安全的方式以取用車輛。

### 車主配對

車主必須證明擁有車輛（證明方式取決於汽車製造商），並且可以使用從汽車製造商或車輛選單收到的電郵連結在汽車製造商 App 中啟動配對程序。在所有情況下，車主必須向 iPhone 提供保密性的一次性配對密碼，該密碼使用 SPAKE2+ 協定配搭 NIST P-256 曲線來產生安全的配對頻道。使用 App 或電郵連結時，密碼會自動傳送到 iPhone，而從車輛開始配對時必須在其中手動輸入密碼。

### 鎖匙共享

車主的配對 iPhone 可以藉由使用 iMessage 和「Apple 識別服務（IDS）」傳送特設備專屬的邀請，來與符合條件的家庭成員和朋友的 iPhone 裝置（及其配對的 Apple Watch 裝置）共享鎖匙。所有共享命令都使用點對點加密 IDS 功能進行交換。車主的已配對 iPhone 會確保 IDS 頻道在共享過程中不會更改，以防止邀請被轉發。

接受邀請後，家庭成員或朋友的 iPhone 將製作數碼鎖匙，並將鎖匙製作憑證鏈傳送回車主配對的 iPhone，以驗證鎖匙是在真正的 Apple 裝置上製作的。車主的已配對 iPhone 會在其他家庭成員或朋友 iPhone 的 ECC 公開鎖匙上簽署，然後將簽署傳送回家庭成員或朋友的 iPhone。車主裝置中的簽署操作需要用戶認證（Face ID、Touch ID 或密碼輸入）和 [Face ID 和 Touch ID 的用途](#) 中所述的安全用戶意圖。傳送邀請時會要求授權，並在朋友裝置傳回簽署要求時，將其儲存在 Secure Element 中以供使用。鎖匙權限由車輛 OEM 伺服器在網上或在車輛上首次使用共享鎖匙期間提供給車輛。

## 鎖匙刪除

鎖匙可由車主裝置從鎖匙擁有者裝置中刪除和在車內刪除。即使鎖匙持有者正在使用鎖匙，在鎖匙持有者 iPhone 上進行刪除也會立即生效。因此，刪除前會顯示強烈警告。可以隨時刪除車輛中的鎖匙，或者只有在車輛在線上時才可以刪除。

在這兩種情況下，鎖匙擁有者裝置或車輛上的刪除操作都會回報給汽車製造商的鎖匙清單伺服器 (KIS)，該伺服器為保險目的會註冊車輛所使用的已核發鎖匙。

車主可以從車主票證的背面要求刪除。此要求會首先傳送給汽車製造商，以刪除車輛中的鎖匙。從車輛刪除鎖匙的條件由汽車製造商定義。只有當車輛中的鎖匙被刪除時，汽車製造商伺服器才會將遙距終止要求傳送到鎖匙擁有者的裝置。

當鎖匙在裝置中終止時，管理數碼車匙的 Applet 將建立一份加密簽名的終止證明，該證明將被汽車製造商用作刪除證明，並用於從 KIS 移除鎖匙。

## NFC 標準異動

針對使用 NFC 鎖匙的車輛，透過在讀取器和 iPhone 端產生臨時密鑰組，可以啟動讀取器和 iPhone 之間的安全頻道。使用密鑰協商方式，可以從兩端衍生共享密鑰，並使用 Diffie-Hellman、密鑰衍生函數和來自在配對過程中所建立的長期密鑰的簽署，來產生共享對稱密鑰。

在車輛端產生的臨時公共密鑰會使用讀取器的長期專用密鑰簽署，進而可以透過 iPhone 對讀取器進行認證。從 iPhone 的角度來看，此通訊協定目的在於防止將私隱敏感資料洩露給攔截通訊的競爭對手。

最後，iPhone 使用已建立的安全頻道，以及根據讀取器的資料衍生質詢所計算出的簽署和一些額外的 App 專屬資料，來加密其公共密鑰識別碼。讀取器對 iPhone 簽署的此驗證可以讓讀取器對裝置進行認證。

## 快速作業

iPhone 會根據先前在標準作業期間共享的密鑰來產生加密碼碼。這組加密碼碼使車輛可以在要求高效能的情況下快速驗證裝置。或者，可透過從先前在標準作業期間共享的密鑰和新的臨時密鑰組中衍生出的階段作業密鑰，來建立車輛與裝置之間的安全頻道。車輛建立安全頻道的能力可將車輛認證給 iPhone。

## BLE/UWB 標準異動

對於使用 UWB 鎖匙的車輛，會在車輛和 iPhone 之間建立藍牙 LE 階段作業。與 NFC 異動類似，雙方都會衍生出一個共用密鑰，用於建立安全階段作業。該階段作業用於後續衍生和同意 UWB 測距密鑰 (URSK)。URSK 會提供給用戶裝置和車輛上的 UWB 無線電，以讓用戶的裝置能夠準確定位到車輛附近或車輛內部的特定位置。然後，車輛會使用裝置位置來決定是否允許解鎖或發動車輛。URSK 有預先定義的 TTL。為避免在 TTL 到期時中斷測距，在安全測距未啟動但已連接藍牙時，URSK 可以在裝置 SE 和車輛 HSM/SE 中預先衍生。這避免了在時間緊迫的情況下需要標準異動來衍生新的 URSK。預先衍生的 URSK 可以非常快速地傳輸到汽車和裝置的 UWB 無線電，以避免中斷 UWB 測距。

## 私隱

汽車製造商的鎖匙清單伺服器 (KIS) 不會儲存裝置 ID、SEID 或 Apple ID，只會儲存可變識別碼、即執行個體 CA 識別碼。此識別碼未綁定到裝置中或伺服器上的任何私人資料，並且在用戶完全清除其裝置 (使用「清除所有內容和設定」) 後會被刪除。

## 將交通卡和 eMoney 卡加至 Apple「銀包」

在多個全球市場中，用戶可在支援的 iPhone 和 Apple Watch 型號上將支援的交通卡和 eMoney 卡加至 Apple「銀包」中。方法因營運業者而異，可能為從實體卡將餘額或定期券（或兩者）轉移至其電子 Apple「銀包」代表票證中，或是從 Apple「銀包」或發卡機構的 App 配置新的交通卡或 eMoney 卡。將交通卡加至 Apple「銀包」後，用戶只要把 iPhone 或 Apple Watch 靠近交通卡讀卡機就可以乘搭公共交通工具。部份交通卡還能用來付款。

### 交通卡和 eMoney 卡的運作方式

已加入的交通卡和 eMoney 卡會與用戶的 iCloud 帳戶連繫。如果用戶將多張卡加至 Apple「銀包」，Apple 或交通卡發卡機構可能可以連繫卡之間的用戶個人資料和相關帳戶資料。交通卡和 eMoney 卡以及交易都受到一組階層式加密編譯密鑰保護。

從實體卡轉移餘額到 Apple「銀包」的過程中，用戶必須輸入該卡的特定資料。用戶可能也需要提供個人資料來證明卡持有人身份。將票證從 iPhone 轉移至 Apple Watch 時，兩部裝置都必須處於上線狀態。

用戶可在 Apple「銀包」中使用信用卡、扣帳卡或預付卡增值，或是透過交通卡或 eMoney 卡發卡機構的 App 增值。如要了解使用 Apple Pay 重新增值餘額時的保安，請參閱：[在 App 內使用卡付款](#)。如要了解從發卡機構的 App 內配置卡的方式，請參閱：[從發卡機構的 App 加入信用卡或扣帳卡](#)。

如果支援從實體卡配置，交通卡或 eMoney 卡發卡機構擁有認證實體卡和驗證用戶所輸入的資料所需的加密編譯密鑰。資料通過驗證後，系統可為 Secure Element 建立「裝置帳戶號碼」，並在 Apple「銀包」中啟用新加入且含有轉移餘額的票證。對於某些卡片，完成從實體卡配置後，實體卡便會停用。

無論使用哪一種配置類型，如卡餘額儲存於裝置中，都會被加密並儲存到 Secure Element 中的指定 Applet 內。營運商擁有密鑰，用於針對卡資料執行加密編譯操作以進行餘額交易。

依照預設，交通卡用戶可享有流暢的「特快交通卡」體驗，無須使用 Face ID、Touch ID 或密碼即可付款和乘搭公共交通工具。如啟用了「特快模式」，便可利用任何鄰近的非接觸式讀卡器取得最近到訪過的車站、交易記錄和其他車票等資訊。用戶如要啟用 Face ID、Touch ID 或密碼認證要求，只需在「錢包與 Apple Pay」設定中停用「特快交通卡」即可。eMoney 卡不支援「特快模式」。

與其他 Apple Pay 卡相同，用戶可透過以下方式停用或移除 eMoney 卡：

- 透過「尋找」遙距清除裝置
- 透過「尋找」啟用「遺失模式」
- 輸入流動裝置管理 (MDM) 遙距清除指令
- 從 Apple ID 帳戶頁面移除所有卡
- 從 iCloud.com 移除所有卡
- 從 Apple「銀包」中移除所有卡
- 在發卡機構的 App 中移除卡

Apple Pay 伺服器會通知卡片業者停用這些卡。如果用戶從在線上的裝置移除交通卡或 eMoney 卡，可將餘額加回以相同 Apple ID 登入的裝置上來還原餘額。如裝置離線、關閉電源或無法使用，就可能無法還原。

## 將交通卡和 eMoney 卡加至家庭成員的 Apple Watch

在 iOS 15 和 watchOS 8 中，iCloud 家庭組織者可以透過 iPhone 的 Watch App 將交通卡和 eMoney 卡加至家庭成員的 Apple Watch 裝置中。將其中一張卡配置到家庭成員的 Apple Watch 時，手錶需要在附近並使用 Wi-Fi 或藍牙連接到組織者的 iPhone。家庭成員必須為其 Apple ID 啟用雙重認證才會發生這種情況。

家庭成員可以使用 iMessage 從 Apple Watch 傳送為交通卡或 eMoney 卡增值的要求。訊息內容受點對點加密保護，如 [iMessage 保安概覽](#) 中所述。可以使用 Wi-Fi 或流動網絡連線遙距為家庭成員 Apple Watch 上的卡片增值。操作時不需要在裝置附近。

**附註：**此功能可能無法在部份國家或地區使用。

## 信用卡和扣帳卡

在某些城市，交通卡讀卡器接受以 EMV (智慧型) 卡來支付公共交通工具的費用。對這類讀卡器出示 EMV 卡或扣帳卡時，需進行用戶認證，程序與「使用信用卡和扣帳卡在商店內付款」相同。

在 iOS 12.3 或較新版本中，Apple「銀包」中的一些現有 EMV 信用卡/扣帳卡會啟用以用於「特快交通卡」。「特快交通卡」讓用戶無需 Face ID、Touch ID 或密碼，用戶為乘搭支援營運商的交通工具付款。當用戶配置 EMV 信用卡或扣帳卡，第一張配置到 Apple「銀包」的卡會啟用以用於「特快交通卡」。用戶就可以在 Apple「銀包」中點一下卡正面上的「更多」按鈕，然後透過將「特快交通設定」設定為「無」來停用該卡的「特快交通」。用戶也可透過 Apple「銀包」選擇使用其他信用卡或扣帳卡作為其「特快交通卡」。如要重新啟用或為「特快模式」選擇另一張卡，需使用 Face ID、Touch ID 或密碼。

Apple Card 和 Apple Cash 均符合「特快交通」的資格。

## Apple 錢包中的證件

在執行 iOS 15.4 或較新版本的 iPhone 8 或較新型號，及執行 watchOS 8.4 或較新版本的 Apple Watch Series 4 或較新型號上，用戶可以將他們的州證件或駕駛執照加至 Apple「銀包」，然後點一下他們的 iPhone 或 Apple Watch 以在參與地點無縫及安全地展示。

**附註：**此功能只適用於參與的美國州份。

Apple「銀包」中的證件採用用戶裝置硬件和軟件中內置的保安功能，來協助保護他們的身份並保障個人資料的安全。

## 將駕駛執照或州證件加至 Apple「銀包」

在 iPhone 上，用戶可以直接在 Apple「銀包」畫面的頂部點一下「加入」(+) 按鈕，開始加入其執照或證件。如果用戶在設定時已配對 Apple Watch，系統則會提示他們也可在 Apple Watch 上的 Apple「銀包」中加入其駕駛執照或證件。

系統首先會要求用戶用他們的 iPhone 掃描實體駕駛執照或州證件的正面和背面。iPhone 會評估影像品質和類型以協助確保提供的影像可被州發行部門所接受。這些證件影像被加密到裝置上州發行部門的密鑰，然後傳送到州發行部門。

接着，系統會要求用戶完成一連串面部和頭部動作。這些動作會由用戶的裝置和 Apple 評估，以協助降低有人使用相片、影片或面具，試圖將他人的證件加至 Apple「銀包」的風險。然後這些動作的分析結果會被傳送至州發行部門，而動作本身的影片則不會被傳送。

為協助確保將證件加入 Apple「銀包」的人與證件持有人為同一人，系統將要求你自拍。在系統將用戶的相片提交給州發行部門前，Apple 伺服器 and 用戶的裝置會將相片與執行一連串面部和頭部動作的人員肖像進行比對，並協助確保提交的相片是真人並為證件上的同一人。在比對完成後，相片將在裝置上加密並傳送到州發行部門以與部門擁有的證件影像相比較。

最後，系統會要求用戶執行 Face ID 或 Touch ID 認證。用戶的裝置會將此單一比對的 Face ID 或 Touch ID 生物特徵與州證件聯繫起來，以協助確保只有將證件加入到此 iPhone 的人才能出示有關證件；其他登記的生物特徵資料無法用於授權出示證件。這會嚴格在裝置上執行，且不會傳送給州發行部門。

州發行部門將收到設定數碼證件所需的資料。這包括用戶證件正面和背面的影像、從 PDF417 條碼讀取的資料以及用戶在身分驗證過程中拍攝的自拍。發行州還會收到一個個位值，用於協助防止詐騙，該值的依據是用戶的裝置使用模式、設定資料和有關其個人 Apple ID 的資料。然後最終會由發行州決定是否批准或拒絕將證件加至 Apple「銀包」。

在州發行部門授權將州證件或駕駛執照加至 Apple「銀包」後，iPhone 會在 Secure Element 中產生一組密鑰配對，將用戶的證件錨定到該特定裝置。如果加至 Apple Watch，Apple Watch 會在 Secure Element 中產生一組密鑰配對。

證件加至 iPhone 後，Apple「銀包」中用戶證件上所反映的資料會以受「安全隔離區」保護的加密格式來儲存。

## 在 Apple「銀包」中使用駕駛執照或州證件

如要在 Apple「銀包」中使用其證件，在 iPhone 將資料出示給證件讀卡機前，用戶需要使用已連繫至 Apple「銀包」中的證件之 Face ID 或 Touch ID 裝置進行認證。

如要在 Apple Watch 上的 Apple「銀包」中使用證件，用戶每次戴上 Apple Watch 時，都需要使用相關的 Face ID 容貌或 Touch ID 指紋來解鎖他們的 iPhone。然後，他們就可以在 Apple「銀包」中使用他們的證件而無需認證，直到他們再次除下他們的 Apple Watch。此功能運用了 [watchOS 的系統保安](#) 中的基礎「自動解鎖」功能。

當用戶將其 iPhone 或 Apple Watch 靠近證件讀卡機時，用戶會在裝置上看到提示，其顯示要求了哪些特定資料、誰要求提供，以及他們是否打算儲存資料。在以相關聯的 Face ID 或 Touch ID 授權後，系統便從裝置釋出所要求的身份資料。

**重要事項：**用戶無需解鎖、出示或移交裝置，即可出示證件。

如果用戶使用「語音控制」、「切換控制」或「輔助觸控」等輔助使用功能，而不是啟用 Face ID 或 Touch ID，則他們可以使用密碼來取用和出示他們的資料。

向證件讀卡機傳輸身份資料的過程遵循 ISO/IEC 18013-5 標準，該標準提供了多種可用的安全機制，能夠偵測、阻止和減低保安風險。這些包括身份資料完整性和防偽、裝置綁定、告知同意和無線電連結上的用戶資料機密性。

## 身份資料完整性和防偽

Apple「銀包」中的證件使用發行部門提供的簽署，以允許任何符合 ISO/IEC 18013-5 標準的讀卡機確認 Apple「銀包」中的用戶身分證。此外，「銀包」中證件上的所有資料元素均受到單獨保護以防偽造。這允許證件讀卡機要求 Apple「銀包」中證件上所顯示的資料元素的特定子集，並讓 Apple「銀包」中的證件使用相同的子集進行回應，進而僅分享要求的資料並最大限度地保護用戶的私隱。

## 裝置綁定

Apple「銀包」中的證件驗證會使用裝置簽署來防止複製證件和重複發生身份異動。透過將用於身份認證的專用密鑰儲存在 iPhone 裝置的 Secure Element 中，該證件將綁定到州發行部門為其建立證件的同一裝置。

## 知情同意

Apple「銀包」中的讀卡機認證會使用 ISO/IEC 18013-5 標準中所定義的通訊協定對證件讀卡機進行認證。在出示過程中，系統會向他們顯示一幅來自讀卡機憑證的圖像，以向用戶保證他們正在與預期的一方進行互動。

## 無線電連結上的用戶資料機密性

階段作業加密有助於確保在 Apple「銀包」中的證件和證件讀卡機之間交換的所有個人可識別資料 (PII) 均已加密。加密由應用程式層執行。因此，階段作業加密的保安不會倚賴傳輸層 (例如 NFC、藍牙和 Wi-Fi) 提供的保安。

## Apple「銀包」中的證件可協助讓用戶的資料保持私密

Apple「銀包」中的證件遵循 ISO/IEC 18013-5 中概述的「裝置檢索」程序。裝置檢索無需在出示期間進行伺服器呼叫，進而保護用戶不被 Apple 和發行部門追蹤。

# iMessage

## iMessage 保安概覽

Apple 的 iMessage 是一項適用於 iOS 裝置、iPadOS 裝置、Apple Watch 和 Mac 電腦的訊息服務。iMessage 支援文字以及相片、聯絡人、位置、連結等附件，以及直接包含在訊息中的附件，例如拇指向上圖像。訊息會顯示在用戶所有註冊的裝置上，這樣用戶就可以在其他裝置上繼續對話。iMessage 充分運用 Apple 推送通知服務 (APNs)。Apple 不會記錄訊息內容或附件，且有關內容或附件受點對點的加密服務保護，因此只有傳送者和接收者可以取用，Apple 無法解密這些資料。

當用戶開啟裝置上的 iMessage 時，裝置會產生加密和簽名密鑰組以配搭服務使用。針對加密，NIST P-256 曲線上有一個加密的 RSA 1280 位元密鑰和一個加密的 EC 256 位元密鑰。針對簽署，則使用橢圓曲線電子簽署算法 (ECDSA) 256 位元簽署密鑰。專用密鑰會儲存在裝置的鑰匙圈中，且只能在首次解鎖後存取。公用密鑰則會與裝置的 APNs 地址一起傳送至 Apple 識別服務 (IDS)，且公用密鑰會與用戶的電話號碼或電郵地址連繫。

當用戶啟用其他裝置來使用 iMessage 時，他們的加密公用密鑰和簽署公用密鑰、APNs 地址及所連繫的電話號碼都會加至目錄服務中。用戶亦可以加入更多電郵地址，系統會透過傳送確認連結來驗證這些電郵地址。電話號碼則透過電訊商網絡和 SIM 卡進行驗證。部份網絡需使用 SMS 進行驗證 (如果 SMS 不是零費率，則會向用戶顯示確認對話框)。除了 iMessage 之外，還有數項系統服務可能須進行電話號碼驗證，例如 FaceTime 和 iCloud。當有新裝置、電話號碼或電郵地址加入時，用戶所有已註冊的裝置都會顯示一則提示訊息。

## iMessage 如何安全地傳送和接收訊息

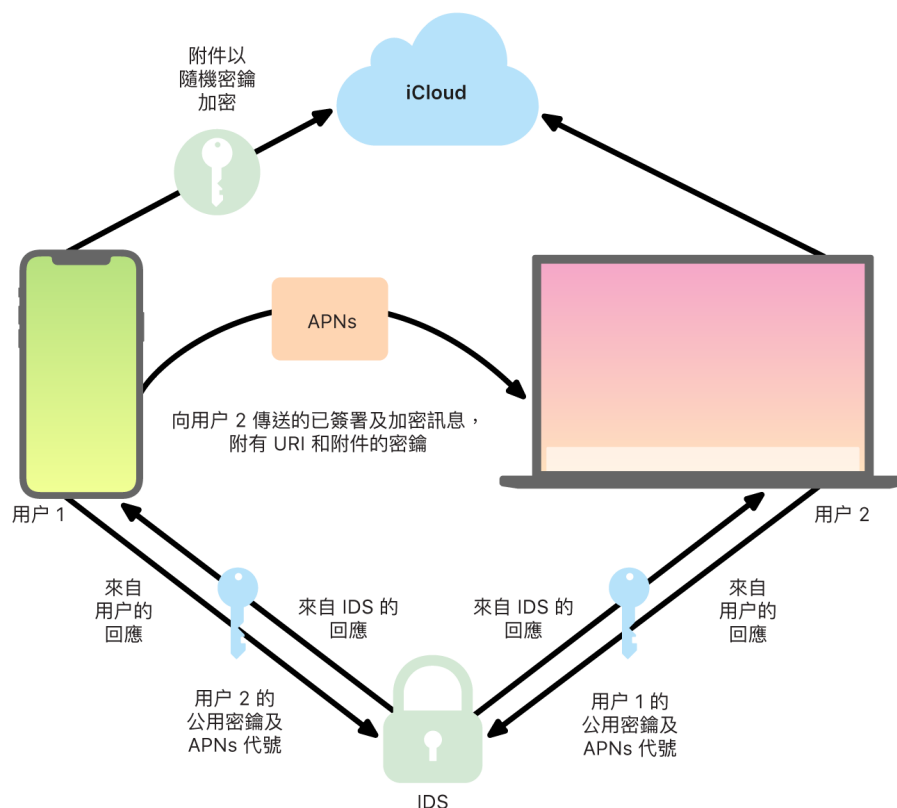
用戶藉由輸入地址或姓名來開始 iMessage 對話。如果他們輸入電話號碼或電郵地址，裝置就會聯絡「Apple 識別服務」(IDS) 以截取與該收件人綁定的所有裝置的公用密鑰和 APNs 地址。如果用戶輸入的是名字，裝置會先使用用戶的「通訊錄」App 來收集連繫至該名字的電話號碼和電郵地址，然後再從 IDS 取得公用密鑰和 APNs 地址。

用戶送出的訊息會針對接收者的每個裝置進行個別加密。接收裝置的公用加密密鑰及簽名密鑰會從 IDS 取得。針對每部接收裝置，發送裝置會產生隨機 88 位元的值並將其作為 HMAC-SHA256 密鑰，以建立從傳送者與接收者公用密鑰與純文字衍生的 40 位元值。88 位元與 40 位元值串接起來會產生 128 位元的密鑰，該密鑰會在計數器 (CTR) 模式下使用 AES 來加密訊息。接收者端會使用 40 位元的值來驗證解密純文字的完整性。系統會對接收裝置的公用密鑰使用 RSA-OAEP 以加密每則訊息的 AES 密鑰。加密訊息文字與加密訊息密鑰的組合接着會以 SHA-1 進行雜湊值運算，而雜湊值會使用發送裝置的專用簽署密鑰以橢圓曲線電子簽署算法 (ECDSA) 進行簽署。在 iOS 13 或較新版本和 iPadOS 13.1 或較新版本中，裝置可使用橢圓曲線整合加密方案 (ECIES) 加密，而非使用 RSA 加密。

產生的訊息 (每部接收裝置一則) 是由加密訊息文字、加密訊息密鑰及傳送者的電子簽署所組成。這些訊息會立即分送至 APNs 進行遞送。時間戳記和 APNs 路由資料等後設資料則不會加密。與 APNs 的通訊會使用前向安全 TLS 通道進行加密。



視 iOS 或 iPadOS 版本而定，APNs 最多只可以轉達大小為 4 或 16 KB 的訊息。如訊息文字過長或隨附了附件（如相片），附件會使用 AES 在 CTR 模式下以隨機產生的 256 位元密鑰進行加密並上載至 iCloud。附件的 AES 密鑰、其統一資源識別碼 (URI) 和其加密表單的 SHA-1 雜湊值隨後會以 iMessage 內容的形式傳送給收件者，並透過一般的 iMessage 加密保護這些內容的保密性和完整性，如下圖所示。



對於群組對話，每位接收者與其裝置之間都會重複此過程。

接收方的每部裝置都會從 APNs 接收到一份訊息，且如有需要，裝置會從 iCloud 取得附件。如傳送者的來電號碼或電郵地址與接收者的聯絡人相符，則會顯示一個名字。

與所有推送通知一樣，訊息在遞送後便會從 APNs 中刪除。然而，與其他 APNs 通知不同的是，如裝置離線，iMessage 訊息會排入佇列等待發送。訊息在 Apple 伺服器上最多可儲存 30 日。

## iMessage 名稱和相片安全分享

iMessage 的「名稱和相片分享」讓用戶可使用 iMessage 來分享名稱和相片。用戶可選取「我的卡片」資料，或自訂名稱並加入其選擇的任何影像。iMessage 的「名稱和相片分享」使用雙階段系統來分送名稱和相片。

資料分為數個欄位，每個欄位會分別加密和認證，並使用以下程序一起認證。共有三個欄位：

- 名稱
- 相片
- 相片檔案名稱

製作資料的第一個步驟之一是在裝置上隨機產生一個記錄 128 位元密鑰。接着這個記錄密鑰會透過 HKDF-HMAC-SHA256 衍生來建立三個子密鑰：Key 1:Key 2:Key 3 = HKDF(record key, "nicknames")。系統會針對每個欄位產生一個隨機 96 位元初始化向量 (IV)，並使用 AES-CTR 和密鑰 1 來加密資料。接着使用密鑰 2 透過 HMAC-SHA256 來運算訊息驗證碼 (MAC)，並覆蓋欄位名稱、欄位 IV 與欄位加密文字。最後，將各欄位 MAC 值集合串連起來，再使用密鑰 3 透過 HMAC-SHA256 運算其 MAC。256 位元的 MAC 會與加密資料一起儲存。此 MAC 的第一個 128 位元作為 RecordID 使用。

然後這個加密資料會儲存在 CloudKit 公用資料庫的 RecordID 底下。此資料永遠不會更改，且每次用戶選擇更改其名稱和相片時，都會產生新的加密記錄。當用戶 1 選擇與用戶 2 分享其名稱和相片時，會傳送記錄密鑰以及 iMessage 承載資料中的 RecordID (已加密)。

當用戶 2 的裝置收到這個 iMessage 承載資料時，會注意到承載資料中包含「暱稱和相片」RecordID 及密鑰。接下來用戶 2 的裝置會前往公共 CloudKit 資料庫，截取該記錄 ID 的加密名稱和相片，然後透過 iMessage 傳出。

訊息截取完畢後，用戶 2 的裝置會解密承載資料並使用 RecordID 本身驗證簽署。如果通過驗證，便會向用戶 2 顯示名稱和相片，然後他們可以選擇將此資料加入聯絡人中，或是用於「訊息」。

## Apple Messages for Business 保安

Apple Messages for Business 是讓用戶可使用「訊息」App 來與商戶通訊的訊息服務。有了 Apple Messages for Business，用戶的對話隨時都在控制之中。他們也能夠刪除對話，並阻止商戶之後向他們傳送訊息。有鑑於私隱性，商戶不會收到用戶的電話號碼、電郵地址或 iCloud 帳戶資料。相反地，Apple 識別服務 (IDS) 會產生一個名為 **Opaque ID** 的自訂唯一識別碼，並與商戶共享。Opaque ID 對於用戶的 Apple ID 與商戶的 Business ID 之間的關係是唯一的。對於使用 Apple Messages for Business 聯絡的每個商戶，用戶會有不同的 Opaque ID。用戶決定是否以及何時與商戶分享個人識別資料，Apple Messages for Business 服務永不儲存對話歷史記錄。

Apple Messages for Business 支援來自 Apple Business Manager 的管理式 Apple ID，並會判斷 Apple School Manager 有否為有關 Apple ID 啟用 iMessage 和 FaceTime。

傳給商戶的訊息會在用戶裝置和 Apple 的訊息伺服器之間加密，並使用像 iMessages 一樣的保安和 Apple 訊息伺服器。Apple 訊息伺服器會解密 RAM 中的這些訊息，然後使用 TLS 1.2 透過加密的連結將這些訊息轉達給企業。透過 Apple Messages for Business 服務傳遞訊息時，訊息一律會以加密的形式儲存。商戶的回覆也使用 TLS 1.2 傳送到 Apple 訊息伺服器，在其中會使用每個收件人裝置的唯一公共密鑰來加密。

如果用戶裝置在線上，則訊息將立即傳送，並且不會在 Apple 訊息伺服器上快取。如果用戶的裝置不在線上，則加密的訊息會最多快取 30 日，以便用戶在裝置回到線上狀態時，可以接收該訊息。裝置一回到線上後，訊息將被傳遞並從快取中刪除。30 日後，未傳遞的快取訊息將會過期並被永久刪除。

## FaceTime 保安

FaceTime 是 Apple 的視訊和語音通話服務。與 iMessage 相似，FaceTime 通話使用「Apple 推送通知」(APNs) 服務來與用戶已註冊的裝置建立初始連線。FaceTime 通話的語音/視訊內容受到點對點的加密保護，因此只有傳送者和接收者可以存取。Apple 無法解密這些資料。

初始 FaceTime 連線是透過 Apple 伺服器基礎架構建立，這個基礎架構負責轉送用戶已註冊的裝置之間的資料封包。透過使用 APNs 通知與「用於 NAT 的作業階段周遊公用程式」(STUN) 訊息來轉送連線，裝置會驗證其識別證書並為每個作業階段建立共享密鑰。這個共享密鑰會使用「安全即時通訊協定」(SRTP)，來為串流的媒體通道製作作業階段密鑰。系統會以計數器模式使用 AES256 來加密 SRTP 封包，並以 HMAC-SHA1 進行認證。在初始連線和保安設定後，FaceTime 便會使用 STUN 與「互聯網連接建立」(ICE) 來建立裝置間的點對點連線 (如適用)。

「群組 FaceTime」拓展了 FaceTime 的功能，可支援最多 33 位成員同時參與。如同傳統的一對一 FaceTime 一樣，群組通話會在受邀成員的裝置之間進行點對點加密。雖然「群組 FaceTime」重複使用了許多一對一 FaceTime 的基礎架構和設計，不過這些群組通話採用以「Apple 識別服務」(IDS) 所提供的確實性為基礎的密鑰建立機制。這套通訊協定提供前向保安，這表示即使用戶的裝置遭入侵，也不會洩漏過去通話的內容。作業階段密鑰使用 AES-SIV 封裝，並使用 ECIES 架構配搭臨時 P-256 ECDH 密鑰來在成員間分發。

當有新電話號碼或電郵地址加入進行中的「群組 FaceTime」通話時，使用中的裝置會建立新的媒體密鑰，且絕不會與新邀請的裝置分享先前用過的密鑰。

## 尋找

### 「尋找」保安

Apple 裝置的「尋找」App 的建置基礎為先進的公用密鑰加密編譯技術。

#### 概覽

「尋找」App 將「尋找我的 iPhone」和「尋找我的朋友」結合為 iOS、iPadOS 和 macOS 中的單一 App。「尋找」可以協助用戶定位遺失裝置，甚至是離線的 Mac。在線上的裝置只需透過 iCloud 向用戶報告位置。「尋找」可從遺失裝置送出短距離藍牙訊號，以達到離線運作的目的，而附近正在使用的其他 Apple 裝置可以偵測到該訊號。其後，附近的裝置可將偵測到的遺失裝置位置傳送到 iCloud，讓用戶可以在「尋找」App 定位裝置，以上操作皆會保障所有參與用戶的私隱和保安。「尋找」甚至適用於處於離線和睡眠狀態的 Mac。

使用藍牙和世界各地正在使用的數以億計的 iOS、iPadOS 和 macOS 裝置，即使裝置無法連接到 Wi-Fi 或流動網絡，用戶也可以找到遺失的裝置。在「尋找」設定中啟用「離線尋找」的任何 iOS、iPadOS 或 macOS 裝置都可以作為「尋找者裝置」。這代表着該裝置可以使用藍牙偵測到另一部遺失的離線裝置，然後使用其網絡連線將大約位置報告給擁有者。當裝置啟用了離線尋找功能時，這也代表了其他參與者也可以用相同的方式來找到該裝置。整個互動會點對點加密和匿名進行，且設計是要提高電池和資料效率。對電池壽命和流動數據方案使用的影響最小，並且用戶私隱得到更好的保護。

**附註：**「尋找」可能無法在部份國家或地區使用。

#### 點對點的加密

「尋找」建立在進階公用密鑰密碼學的基礎上。當「尋找」設定中的離線尋找啟用時，會直接在裝置上產生橢圓曲線 (EC) P-224 私人加密密鑰組，其標註為  $\{d, P\}$  ( $d$  表示專用密鑰， $P$  則為公用密鑰)。此外，一個 256 位元密鑰  $SK_0$  和一個計數器  $i$  被初始化為零。該專用密鑰組和密鑰將永遠不會發送給 Apple，並只使用「iCloud 鑰匙圈」以端到端的加密方式在用戶的其他裝置之間同步。密鑰和計數器用於透過以下遞迴構造得出目前對稱密鑰  $SK_i: SK_i = KDF(SK_{i-1}, \text{"update"})$ 。

基於密鑰  $SK_i$ ，使用  $(u_i, v_i) = KDF(SK_i, \text{"diversify"})$  計算兩個大整數  $u_i$  和  $v_i$ 。接下來會使用與兩個整數相關的仿射關聯，衍生出以  $d$  表示的 P-224 專用密鑰和以  $P$  代表的對應的公用密鑰，以便計算出暫時性密鑰組：衍生的專用密鑰為  $d_i$ ，其中  $d_i = u_i * d + v_i$  (以 P-224 曲線的順序為模型)，而對應的公用密鑰部份為  $P_i$  且驗證  $P_i = u_i * P + v_i * G$ 。

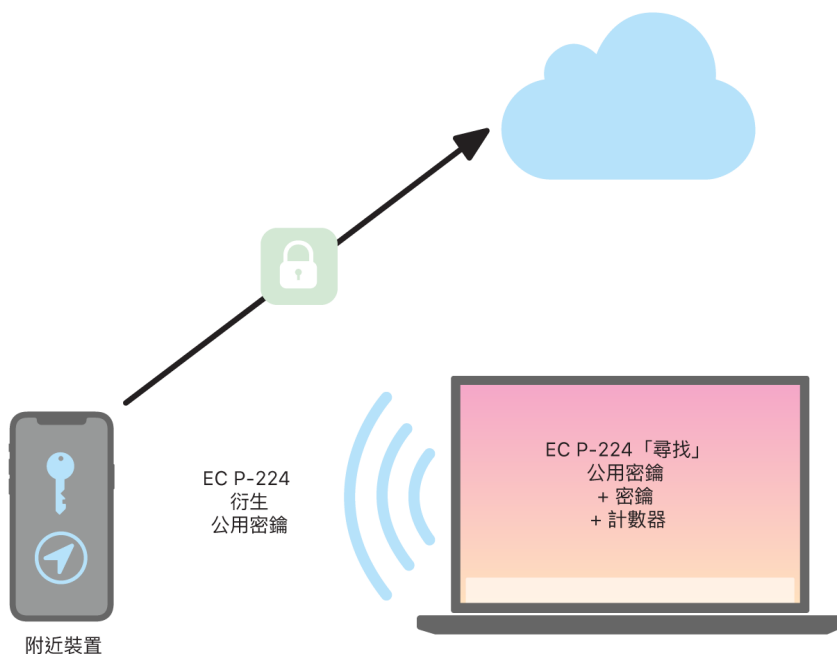
當裝置遺失且無法連接 Wi-Fi 或流動網絡時 (例如將 MacBook Pro 遺落在公園長椅上時)，裝置會於有限期間內，在藍牙承載資料中開始定時廣播衍生的公用密鑰  $P_i$ 。透過使用 P-224，公用密鑰代表可以放入單一藍牙承載資料中。周圍的裝置可以透過將其位置加密至公用密鑰來幫助找到離線裝置。大約每 15 分鐘，系統會使用遞增的計數器值和上述過程，將公用密鑰替換為新的公用密鑰，所以無法使用永久識別碼來追蹤用戶。衍生機制的設計用意是防止將不同的公用密鑰  $P_i$  連接至同一部裝置。

## 保持用戶及裝置匿名

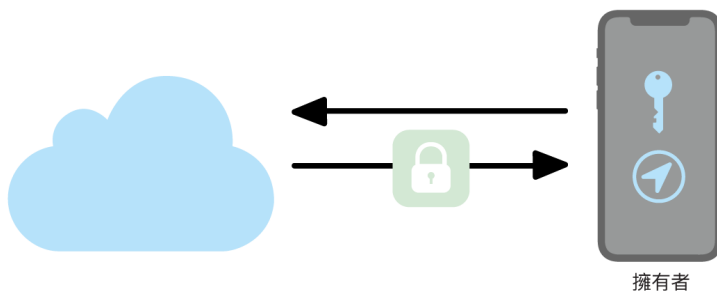
除了確保位置資料和其他資料完全加密之外，參與者的身份在彼此之間以及與 Apple 之間都保持私密。尋找者裝置傳送至 Apple 的流量中，內容或標頭均不含任何認證資料。因此 Apple 無從得知尋找者是誰，也不知道誰的裝置被找到。此外，Apple 不會記錄可能透露尋找者身份的資料，並且不會保留可讓任何人將尋找者與擁有者連繫的任何資料。裝置擁有者只會收到已解密並顯示在「尋找」App 中的加密位置資料，而資料不會指出誰是找到裝置的尋找者。

## 使用「尋找」來定位遺失的 Apple 裝置

在藍牙收訊範圍內且已啟用離線尋找的任何 Apple 裝置，都可從另一部設為允許「尋找」的 Apple 裝置偵測到此訊號並讀取目前的廣播密鑰  $P_i$ 。尋找者裝置會使用廣播中的 ECIES 架構和公用密鑰  $P_i$ ，加密其目前的位置資料並轉送至 Apple。加密的位置會與伺服器索引綁定，該索引是以藍牙承載資料中 P-224 公用密鑰  $P_i$  的 SHA256 雜湊值計算所得出。Apple 永遠不會獲得該解密密鑰，因此 Apple 無法讀取由尋找者裝置加密的位置。遺失裝置的擁有者可以重建索引並解密已加密的位置。



在嘗試尋找遺失的裝置時，將為位置搜尋時段估算計數器值的預期範圍。知道搜尋期間計數器值範圍中的原始專用 P-224 密鑰  $d$  和密鑰值  $SK_i$ ，擁有者就能重新建構整個搜尋期間的值組  $\{d_i, \text{SHA256}(P_i)\}$ 。接下來，用來定位遺失裝置的擁有者裝置，便可使用索引值組  $\text{SHA256}(P_i)$  來向伺服器進行查詢，以及從伺服器下載加密位置。然後，「尋找」App 使用配合的專用密鑰  $d_i$  在本機解密加密的位置，並在 App 中顯示遺失裝置的大概位置。來自多個尋找者裝置的位置報告由擁有者的 App 合併來產生更精確的位置。



## 定位已離線的裝置

如果用戶已在裝置上啟用「尋找我的 iPhone」，當裝置升級至 iOS 13 或較新版本、iPadOS 13.1 或較新版本和 macOS 10.15 或較新版本時，會預設啟用離線尋找功能。其設計用意是確保所有用戶都能獲得找回遺失裝置的最高可能性。但是，如果用戶不想參與，可以隨時在裝置上的「尋找」設定中停用離線尋找。停用離線尋找後，該裝置將不會再作為尋找者裝置，也無法被其他尋找者裝置偵測。但是，只要裝置可以連接到 Wi-Fi 或流動網絡，用戶仍然可以找到該裝置。

找到遺失的離線裝置時，用戶會收到通知及電郵以知會其裝置已找到。如要檢視遺失裝置的位置，用戶可開啟「尋找」App 並選擇「裝置」分頁。「尋找」不會在裝置被找到之前的空白地圖上顯示該裝置，而是顯示一個地圖位置，其中包括大致的地址以及偵測到該裝置多久的相關資料。如收到更多位置報告，目前的位置和時間戳記均會自動更新。雖然用戶無法在離線裝置上播放聲音或遙距清除，他們可以使用位置資料來回溯經過的路線，或是採取其他行動來協助找回裝置。

## 接續互通

### 「接續互通」保安概覽

「接續互通」運用 iCloud、藍牙和 Wi-Fi 等技術，可讓用戶從一部裝置到另一部裝置繼續操作、撥打和接聽電話、傳送和接收短訊，以及共享流動數據互聯網連線。

### 「接手」保安

Apple 安全地處理原生 App 和網站之間的接手，無論是從一台裝置到另一台裝置，甚至是大量資料的接手。

### 「接手」如何安全運作

當用戶的 iOS、iPadOS 和 macOS 裝置彼此接近時，用戶可以使用「接手」功能，自動將正在處理的內容從一部裝置傳送到另一部裝置。用戶可以使用「接手」功能來切換裝置並立即繼續操作。

當用戶在第二部支援「接手」功能的裝置上登入 iCloud 時，兩部裝置會透過 APNs 來建立頻外低耗電藍牙 (BLE) 4.2 配對。每則訊息的加密方式類似於 iMessage 中的訊息。裝置配對後，每部裝置都會產生對稱的 256 位元 AES 密鑰，並儲存在裝置的鑰匙圈中。此密鑰可加密和認證 BLE 廣播，其會在 GCM 模式下使用 AES256 並採用重播保護措施，將裝置目前的活動傳遞給其他已配對的 iCloud 裝置。

裝置首次接收到來自新密鑰的廣播時，會建立與起始裝置之間的 BLE 連線，並執行廣播加密密鑰的交換。此連線使用標準的 BLE 4.2 加密方式以及將個別訊息加密的方式（與 iMessage 的加密方式類似）來進行保護。在部份情況下，這些訊息會使用 APNs 而不是使用 BLE 傳送。活動的承載資料會使用與 iMessage 相同的方式進行保護和傳輸。

### 在原生 App 和網站之間使用「接手」功能

「接手」功能允許 iOS、iPadOS 或 macOS 的原生 App 繼續用戶在由 App 開發者合法控制之網域中網頁的活動。「接手」也允許原生 App 的用戶活動在網頁瀏覽器繼續進行。

為協助阻止原生 App 要求繼續取用非受開發者控制的網站，App 必須證明擁有要繼續取用的網域之合法控制權。對網站網域的控制是使用共用網頁憑證的機制來建立。如需詳細資料，請參閱：[App 對已儲存密碼的存取權限](#)。在允許 App 接受使用「接手」功能的用戶活動前，系統必須驗證 App 的網域名稱控制。

使用「接手」功能傳送的網頁來源可以是任何採用了「接手」API 的瀏覽器。當用戶檢視網頁時，系統會使用加密的「接手」廣播位元組來廣播網頁的網域名稱。只有用戶的其他裝置能夠解密該廣播位元組。

在接收裝置上，系統會偵測到已安裝的原生 App 接受了來自已廣播網域名稱的「接手」，並將該原生 App 圖像顯示為「接手」選項。啟動後，原生 App 會接收完整的 URL 和網頁標題。瀏覽器中的其他資料則不會傳送到原生 App。

相反地，如「接手」接收裝置未安裝相同的原生 App，原生 App 可指定後援 URL。在此情況下，系統會將用戶的預設瀏覽器顯示為「接手」App 選項（如該瀏覽器已採用「接手」API）。要求使用「接手」時，系統會啟動瀏覽器並接收來源 App 提供的後援 URL。後援 URL 並不一定要限制為由原生 App 開發者控制的網域名稱。

## 使用「接手」傳送較龐大的資料

除了使用「接手」的基本功能外，部份 App 可能會選擇使用支援傳送大量資料的 API（透過 Apple 建立的點對點 Wi-Fi 技術，與 AirDrop 非常類似）。例如，「郵件」App 會使用這些 API 來支援接手功能，以傳送可能包含較大附件的郵件草稿。

當 App 使用這些 API 時，兩部裝置間會開始交換，如同使用「接手」傳送一樣。不過，在使用低耗電藍牙 (BLE) 收到初始承載資料後，接收裝置會透過 Wi-Fi 來啟用新的連線。此連線是加密的（使用 TLS），其透過「iCloud 鑰匙圈」共享的身份獲得信任。證書中的識別標誌會針對每位用戶的身份進行驗證。其他承載資料會透過此加密的連線進行傳送，直到傳輸完成為止。

## 通用剪貼板

「通用剪貼板」運用「接手」安全地跨裝置傳送用戶的剪貼板內容，因此他們可以在一部裝置上複製並在另一部裝置貼上。剪貼板內容會如其他「接手」資料一樣受到保護，並依照預設與「通用剪貼板」分享，除非 App 開發者選擇不允許分享。

無論用戶是否已將剪貼板內容貼至 App 中，App 皆可取用剪貼板資料。透過「通用剪貼板」，此資料存取權限會延伸至用戶在其他裝置上執行的 App（必須以 iCloud 登入裝置來建立此存取權限）。

## iPhone 流動網絡通話轉接保安

Mac、iPad、iPod touch 或 HomePod 如連上與 iPhone 相同的 Wi-Fi 網絡，即可透過 iPhone 流動網絡連線來撥打和接聽電話。設定會要求裝置使用相同的 Apple ID 帳戶同時登入 iCloud 和 FaceTime。

收到來電時，會透過「Apple 推送通知服務」(APNs) 來通知所有已設定的裝置，每個通知都會使用與 iMessage 相同的點對點加密機制。位於相同網絡上的裝置會顯示來電通知用戶介面。用戶接聽電話時，會使用安全的點對點連線技術，在兩部裝置間無縫傳輸用戶 iPhone 的音訊。

在一部裝置上接聽來電時，會使用低耗電藍牙 (BLE) 短暫傳播來終止附近與 iCloud 配對的裝置鈴聲。傳播位元組會使用與「接手」傳播相同的方式進行加密。

撥出的通話也將透過 APNs 轉送到 iPhone，並以類似的方式透過安全的點對點連結在裝置間傳輸音訊。用戶可以在 FaceTime 設定中關閉「iPhone 流動網絡通話」來停用裝置的電話轉接功能。

## iPhone 訊息轉發保安

「訊息轉發」會自動將 iPhone 上收到的 SMS 文字短訊傳送到用戶已註冊的 iPad、iPod touch 或 Mac 上。每部裝置都必須使用相同的 Apple ID 帳戶登入 iMessage 服務。當「訊息轉發」開啟時，如啟用了雙重認證，系統會自動在用戶信任圈內的裝置上進行註冊。否則，可在每部裝置上輸入由 iPhone 產生的隨機六位數驗證碼來進行註冊。

裝置完成連結後，iPhone 便會加密傳入的 SMS 短訊並轉寄至每部裝置，其的操作方式如 [iMessage 保安概覽](#) 所述。回覆會以相同方式傳回到 iPhone，然後 iPhone 可使用電訊商的 SMS 傳輸機制以短訊來傳送回覆。「訊息轉發」功能可在「訊息」設定中開啟或關閉。

## 「即時熱點」保安

「即時熱點」會將其他 Apple 裝置連接到個人 iOS 或 iPadOS 熱點。支援「即時熱點」的 iOS 和 iPadOS 裝置使用低耗電藍牙 (BLE) 來搜尋所有裝置並與其進行通訊，前提是裝置必須使用相同的個人 iCloud 帳戶或「家人共享」所使用的帳戶 (iOS 13 和 iPadOS) 進行登入。與「即時熱點」相容且配備 OS X 10.10 或較新版本的 Mac 電腦，可使用相同的技術來搜尋支援「即時熱點」的 iOS 及 iPadOS 裝置，並與其進行通訊。

預設當用戶進入裝置上的 Wi-Fi 設定時，裝置會發出包含一個識別碼的 BLE 廣播，所有登入相同 iCloud 帳戶的裝置均接受該識別碼。該識別碼由與 iCloud 帳戶連繫的 DSID (Destination Signaling Identifier) 產生，並會定期更新。當其他登入相同 iCloud 帳戶的裝置彼此接近且支援「個人熱點」時，這些裝置會偵測訊號並加以回應，以表示可使用「個人熱點」。

當不屬於「家人共享」成員的用戶選擇將 iPhone 或 iPad 用作「個人熱點」時，會向該裝置傳送開啟「個人熱點」的要求。而該要求會透過加密的連結 (使用 BLE 加密方法) 進行傳送；要求的加密方式與 iMessage 的加密方式類似。裝置接着會透過相同的 BLE 連結，使用相同訊息專屬加密方式來回應「個人熱點」的連線資料。

屬於「家人共享」的用戶會使用類似 HomeKit 裝置同步資料的機制來安全共享「個人熱點」連線資料。具體來說，在用戶之間共享熱點資料的連線，是以用戶各自的裝置之特定 Ed25519 公用密鑰來進行身份驗證的 ECDH (Curve25519) 臨時密鑰保護。使用的公用密鑰，則是以前建立「家人共享」時使用 IDS 在「家人共享」的成員之間同步的公用密鑰。

# 網絡保安

## 網絡保安概覽

除了 Apple 用於保護 Apple 裝置上所儲存資料的內置安全保護，也有許多措施可供機構採用以確保資料在裝置間來回傳輸時安全無虞。所有這些保護機制和措施均屬於網絡安全範疇。

因為用戶必須能在全世界各處存取公司網絡，所以很重要的一點是協助確保他們獲得授權，並讓資料在傳輸過程中獲得充分保護。為了達成這些保安目標，iOS、iPadOS 及 macOS 將經過實證的技術和 Wi-Fi 及流動數據網絡連線的最新標準整合在一起。這就是我們的作業系統使用標準網絡通訊協定，並使開發者能夠存取這些通訊協定，以進行受認證、已獲授權且已加密通訊的原因。

## TLS 保安

iOS、iPadOS 和 macOS 支援傳輸層保安 (TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3) 和資料包傳輸層保安 (DTLS)。TLS 通訊協定同時支援 AES128 和 AES256，且偏好使用提供前向保密的加密套件。Safari、「日曆」和「郵件」等互聯網 App 會自動使用此通訊協定，在裝置和網絡服務之間建立一條加密的通訊通道。高階 API (如 CFNetwork) 讓開發者可以輕鬆在其 App 中採用 TLS，而低階 API (如 Network.framework) 則提供精細的控制。CFNetwork 不允許 SSL 3，而使用 WebKit 的 App (如 Safari) 也禁止進行 SSL 3 連線。

在 iOS 11 或較新版本及 macOS 10.13 或較新版本中，除非受到用戶信任，否則不再允許使用 SHA-1 證書進行 TLS 連線，也不允許使用 RSA 密鑰短於 2048 位元的證書。在 iOS 10 和 macOS 10.12 中，RC4 對稱加密套件已淘汰。依照預設，以 SecureTransport API 導入的 TLS 用戶端或伺服器並不會啟用 RC4 加密套件，且當 RC4 是唯一的加密套件時，便無法連接。為加強安全，需使用 RC4 的服務或 App 應升級，以使用安全的加密套件。在 iOS 12.1 上，2018 年 10 月 15 日以後從系統信任的根憑證核發的憑證，都必須記錄在受信任的「憑證透明度」記錄中，才允許用來進行 TLS 連線。在 iOS 12.2 中，TLS 1.3 針對 Network.framework 和 NSURLSession API 預設為啟用。使用 SecureTransport API 的 TLS 用戶端無法使用 TLS 1.3。

## App 傳輸保安

「App 傳輸保安」提供預設連線的需求，以便 App 在使用 NSURLConnection、CFURL 或 NSURLSession API 時，遵循安全連線的最佳做法。依照預設，「App 傳輸保安」會將加密選取項目限制為僅包含提供前向保密的套件，特別是：

- Galois/計數器模式 (GCM) 中的 ECDHE\_ECDSA\_AES 和 ECDHE\_RSA\_AES
- 密碼區塊鏈 (CBC) 模式



App 可針對不同網域停用前向保密要求，停用後便會將 RSA\_AES 加入可用加密集中。

伺服器必須支援 TLS 1.2 和前向保密功能，且憑證必須有效並使用 SHA256 或更高的強度（最低限度為 2048 位元 RSA 密鑰或 256 位元橢圓曲線密鑰）加以簽署。

不符合這些要求的網絡連線作業將會失敗，除非 App 凌駕「App 傳輸保安」。無效證書會造成嚴重的作業失敗和連線中斷。「App 傳輸保安」會自動套用到針對 iOS 9 或較新版本和 macOS 10.11 或較新版本編譯的 App。

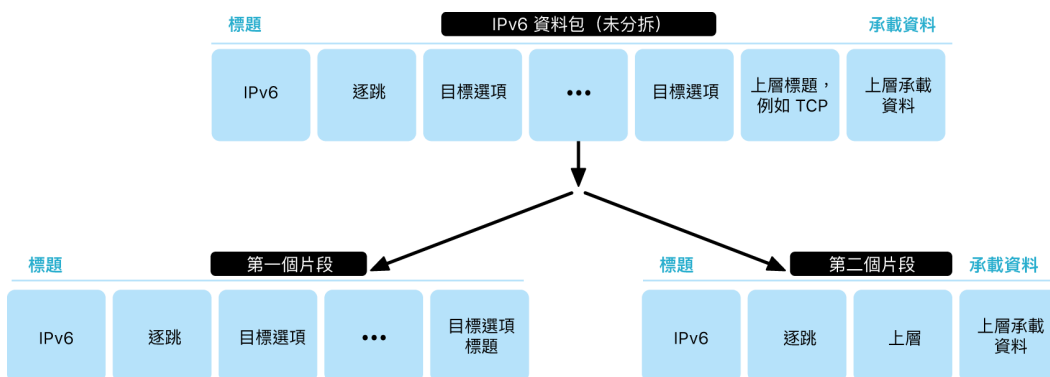
## 憑證有效性檢查

評估 TLS 證書的信任狀態是依據已建立的業界標準進行（如 RFC 5280 所列），以及整合的新興標準，例如 RFC 6962（證書透明度）。在 iOS 11 或較新版本和 macOS 10.13 或較新版本，Apple 裝置會定期更新吊銷以及受約束的證書的列表。該列表由證書吊銷列表（CRL）整合而成，而這些 CRL 為 Apple 信任的每個內置憑證授權單位及其附屬 CA 核發者所公佈。Apple 也會自行決定將其他約束包括在此列表內。當網絡 API 功能用於執行安全連接時，都會諮詢此資料。當 CA 撤銷的憑證太多而無法逐一列出時，信任評估可能會改為要求需取得線上憑證狀態回應（OCSP），而如果無法取得回應，評估便會失敗。

## IPv6 保安

所有 Apple 作業系統皆支援 IPv6 並執行數種機制，以保護用戶的私隱與網絡疊放的穩定性。使用「無狀態地址自動設定」（SLAAC）時，所有介面的 IPv6 地址會以能協助防止跨網絡追蹤裝置的方式產生，同時藉由確保網絡沒有變動時的地址穩定性來提供絕佳用戶體驗。地址產生演算法是根據 RFC 3972 的加密編譯產生地址，並藉由介面專屬的修飾元增強，以保證即使相同網絡上有不同介面，最終將具有不同的地址。此外，所建立的臨時地址其偏好存留期為 24 小時，在預設情況下，這些臨時地址會用於任何新的連線。配合 iOS 14、iPadOS 14 和 watchOS 7 推出的私人 Wi-Fi 地址功能，系統會為裝置加入的每個 Wi-Fi 網絡產生一個不重複的連結本機地址。網絡的 SSID 會合併作為產生地址的額外元素，類似 RFC 7217 的 Network\_ID 參數。此方式會用於 iOS 14、iPadOS 14 和 watchOS 7。

為了防止 IPv6 延伸標頭和分段相關的攻擊，Apple 裝置會實行 RFC 6980、RFC 7112 和 RFC 8021 中指定的保護措施。配合其他措施，此等保護措施可阻止由於上層標頭僅可在第二個片段中找到（如下所示），因而為例如無狀態封包過濾器等保安控制帶來不明確狀況的特定攻擊。



此外，為了協助確保 Apple 作業系統的 IPv6 疊放的可靠性，Apple 裝置對與 IPv6 相關的資料結構強制執行了各種限制，例如各介面的前置碼數字。

# 虛擬專用網絡 (VPN) 保安

虛擬專用網絡等安全網絡服務，通常只需要基本的設定與配置，即可配搭 iOS、iPadOS 和 macOS 裝置使用。

## 支援的通訊協定

這些裝置可配搭支援以下通訊協定和認證方式的 VPN 伺服器使用：

- IKEv2/IPsec，透過共享密鑰、RSA 憑證、橢圓曲線電子簽署算法 (ECDSA) 憑證、EAP-MSCHAPv2 或 EAP-TLS 進行認證
- SSL-VPN，使用來自 App Store 的合適用戶端 App
- L2TP/IPsec，透過 MS-CHAPv2 密碼進行用戶認證，並藉由共享密鑰 (iOS、iPadOS 和 macOS) 和 RSA SecurID 或 CRYPTOCARD (僅適用於 macOS) 進行機器認證
- Cisco IPsec，透過密碼、RSA SecurID 或 CRYPTOCARD 進行用戶認證，並藉由共享密鑰和憑證進行機器認證 (僅適用於 macOS)

## 支援的 VPN 部署

iOS、iPadOS 和 macOS 支援以下項目：

- **隨選即用 VPN**：適用於使用證書式認證的網絡。IT 規則會使用 VPN 設定描述檔來指定哪些網域需要 VPN 連線。
- **個別 App VPN**：適用於在更精確的基礎上完成建立 VPN 連線。流動裝置管理 (MDM) 可為每個受管理的 App 和 Safari 中特定的網域指定連線。這有助確保具安全考量的資料始終以安全的方式透過企業網絡進出，而用戶的個人資料則不會進出企業網絡。

iOS 和 iPadOS 支援以下項目：

- **總是開啟 VPN**：針對透過 MDM 解決方案管理，並使用 Mac 版 Apple Configurator、Apple School Manager 或 Apple Business Manager 加以監管的裝置。「總是開啟 VPN」可讓用戶在連接到流動數據與 Wi-Fi 網絡時，不需要手動開啟 VPN 即可啟用保護功能。透過將所有 IP 流量回傳至機構，讓機構對裝置流量擁有完整的控制權。IKEv2 是後續加密的預設參數和密鑰交換方式，可透過資料加密保護傳送的流量。機構可以監察並過濾傳入其裝置或自其裝置傳出的流量、保護機構網絡內的資料安全，並限制裝置的互聯網存取權限。

# Wi-Fi 保安

## 安全存取無線網絡

所有 Apple 平台支援業界水平的 Wi-Fi 驗證和加密通訊協定，以在連接以下的安全無線網絡時提供已驗證的存取和機密性：

- WPA2 個人級
- WPA2 企業級
- WPA2/WPA3 Transitional
- WPA3 個人級
- WPA3 企業級
- WPA3 企業級 192 位元保安

WPA2 及 WPA3 會驗證每次連接，並提供 128 位元 AES 加密功能，以協助確保無線傳送資料的機密性。這可為用戶提供最高等級的安全保障，在用戶透過 Wi-Fi 網絡連線傳送和接收通訊時，確保用戶的資料始終受到保護。

## WPA3 支援

以下 Apple 裝置支援 WPA3：

- iPhone 7 或較新型號
- iPad (第 5 代) 或較新型號
- Apple TV 4K 或較新型號
- Apple Watch Series 3 或較新型號
- Mac 電腦 (2013 年末或較新型號，採用 802.11ac 或較新版本)

較新型號的裝置支援「WPA3 企業級」192 位元保安的驗證，包括在連接相容無線連接點 (AP) 時支援 256 位元 AES 加密。這可為無線傳輸提供更強的機密性保護。iPhone 11、iPhone 11 Pro、iPhone 11 Pro Max，以及較新型號的 iOS 和 iPadOS 裝置支援「WPA3 企業級」192 位元保安。

## PMF 支援

除保護以無線傳輸的資料，Apple 平台擴充 WPA2 及 WPA3 層級保護，以透過 802.11w 中定義的「管理訊框保護」(PMF) 服務來單點發送與多點發送管理訊框。以下 Apple 裝置提供 PMF 支援：

- iPhone 6 或較新型號
- iPad Air 2 或較新型號
- Apple TV HD 或較新型號
- Apple Watch Series 3 或較新型號
- Mac 電腦 (2013 年末或較新型號，採用 802.11ac 或較新版本)

Apple 裝置支援 802.1X，因此可整合到各種 RADIUS 認證環境中。支援的 802.1X 無線認證方式包括 EAP-TLS、EAP-TTLS、EAP-FAST、EAP-SIM、PEAPv0 和 PEAPv1。

## 平台保護

Apple 作業系統會保護裝置，抵禦網絡處理器韌體中的漏洞。這表示使用 Wi-Fi 的網絡控制器已限制存取「應用程式處理器」記憶體。

- 使用 USB 或 SDIO (輸入輸出記憶體管理單元) 與網絡處理器連接時，網絡處理器無法啟動直接記憶體存取 (DMA) 作業至「應用程式處理器」。
- 使用 PCIe 時，每個網絡處理器位於其獨立的 PCIe 匯流排上。各 PCIe 匯流排上的輸入輸出記憶體管理單元 (IOMMU) 會進一步限制網絡處理器的 DMA 存取權限，只允許存取含有其網絡封包和控制結構的記憶體和資源。

## 已淘汰的通訊協定

Apple 裝置支援以下已淘汰的 Wi-Fi 驗證及加密通訊協定：

- 開放 WEP，使用 40 位元及 104 位元密鑰
- 共享 WEP，使用 40 位元及 104 位元密鑰
- 動態 WEP
- 臨時密鑰完整性協定 (TKIP)
- WPA
- WPA/WPA2 切換模式

這些通訊協定不再被視為安全，基於相容性、可靠性、效能及保安原因，強烈不建議使用。它們只因向後相容而支援，且可能會在將來的軟件版本中移除。

建議所有 Wi-Fi 網絡均移轉至 WPA3 個人級或 WPA3 企業級加密方式，以便盡可能提供最健全、安全及相容的 Wi-Fi 連線。

## Wi-Fi 私隱

### MAC 地址隨機化

在沒有與 Wi-Fi 網絡建立關聯的情況下執行 Wi-Fi 掃描時，Apple 平台會使用隨機「媒體存取控制地址」（MAC 地址）。系統會執行這些掃描以尋找和連接已知的 Wi-Fi 網絡，或為使用地理圍欄的 App 提供「定位服務」協助，例如基於位置的提醒事項或在 Apple「地圖」中定位。請注意，在嘗試連接偏好的 Wi-Fi 網絡時進行的 Wi-Fi 掃描未經過隨機化處理。iPhone 5 或較新型號支援 Wi-Fi MAC 地址隨機化。

當裝置沒有與 Wi-Fi 網絡產生關聯或裝置的處理器處於睡眠狀態時，Apple 平台在執行加強喜好網絡卸載（ePNO）掃描時，也會使用隨機 MAC 地址。當裝置上針對會利用地理圍欄的 App 使用「定位服務」時（例如基於位置的提醒事項在判定裝置是否接近特定位置時），便會執行 ePNO 掃描。

因為裝置中斷某個 Wi-Fi 網絡的連線時其 MAC 地址會更改，即使裝置已連接流動網絡，Wi-Fi 流量的被動觀察程式亦無法使用該地址持續追蹤裝置。Apple 已告知 Wi-Fi 製造商 iOS 和 iPadOS Wi-Fi 掃描會使用隨機 MAC 地址且 Apple 及製造商皆無法預測這些隨機 MAC 地址。

在 iOS 14 或較新版本、iPadOS 14 或較新版本，以及 watchOS 7 或較新版本中，當 iPhone、iPad、iPod touch 或 Apple Watch 連接至 Wi-Fi 網絡時，會依據個別網絡以唯一（隨機）MAC 地址自我識別。此功能可由用戶停用，或使用 Wi-Fi 承載資料中的新選項來停用。在某些情況下，裝置會改回使用實際的 MAC 地址。

如需更多資料，請參閱 Apple 支援文章：[在 iPhone、iPad、iPod touch 和 Apple Watch 上使用私人 Wi-Fi 地址](#)。

### Wi-Fi 訊框序列號碼隨機化

Wi-Fi 訊框包含序列號碼，其用於底層 802.11 通訊協定以啟用有效率及可靠的 Wi-Fi 通訊。因這些序列號碼根據傳送的訊框而遞增，其可用於在 Wi-Fi 掃描時，將傳送的資料與同一裝置傳送的其他訊框連繫。

為防止此事，Apple 裝置在 MAC 地址變更至新的隨機地址時，都會將序列號碼隨機化。這包含針對裝置解除關聯時，發出的新掃描要求隨機使用序號。以下裝置支援此隨機化：

- iPhone 7 或較新型號
- iPad (第 5 代) 或較新型號
- Apple TV 4K 或較新型號
- Apple Watch Series 3 或較新型號
- iMac Pro (Retina 5K, 27 吋, 2017 年) 或較新型號
- MacBook Pro (13 吋, 2018 年) 或較新型號
- MacBook Pro (15 吋, 2018 年) 或較新型號
- MacBook Air (Retina, 13 吋, 2018 年) 或較新型號
- Mac mini (2018 年) 或較新型號
- iMac (Retina 4K, 21.5 吋, 2019 年) 或較新型號
- iMac (Retina 5K, 27 吋, 2019 年) 或較新型號
- Mac Pro (2019 年) 或較新型號

## Wi-Fi 連線

Apple 會為 AirDrop 和 AirPlay 所使用的點對點 Wi-Fi 連線產生隨機 MAC 地址。隨機產生的地址也會用於 iOS 和 iPadOS (裝有 SIM 卡) 中的「個人熱點」和 macOS 中的「互聯網共享」。

每當這些網絡介面開始時，都會產生全新的隨機地址，且在有需要時會為每個介面獨立產生獨有的地址。

## 隱藏網絡

Wi-Fi 網絡乃是透過名為**服務組織別元 (SSID)**的網絡名稱來識別。某些 Wi-Fi 網絡設定為隱藏 SSID，這會導致無線連接點不會廣播網絡的名稱。這些網絡便稱為**隱藏的網絡**。iPhone 6s 和較新型號的裝置在網絡隱藏時會進行自動偵測。如網絡已隱藏，iOS 或 iPadOS 裝置會傳送包含 SSID 的探測要求 (如網絡並非隱藏則不會)。這可協助避免裝置廣播用戶連接過的曾隱藏網絡名稱，以進一步保障私隱。

## 藍牙保安

Apple 裝置具備兩種藍牙類型：傳統藍牙和低耗電藍牙 (BLE)。兩種版本的藍牙保安模式都包含以下不同的安全功能：

- **配對**：製作一或多個共享秘密密鑰的過程
- **綁定**：儲存在配對過程中所製作密鑰的以供之後連接之用的動作，以便建立信任的裝置配對
- **認證**：驗證兩部裝置有相同的密鑰
- **加密**：機密地傳送訊息
- **訊息完整性**：避免訊息偽造的保護措施
- **安全簡單配對**：防止被動竊聽及防禦中間人攻擊

藍牙 4.1 版將「安全連線」功能加入傳統藍牙 (BR/EDR) 實體傳輸。

以下列出各類型藍牙的安全功能。

支援	傳統藍牙	低耗電藍牙
配對	P-256 橢圓曲線	FIPS 核准演算法 (AES-CMAC 及 P-256 橢圓曲線)
綁定	配對資料儲存在 iOS、iPadOS、macOS、tvOS 和 watchOS 裝置中的安全位置	配對資料儲存在 iOS、iPadOS、macOS、tvOS 和 watchOS 裝置中的安全位置
驗證	FIPS 核准的演算法 (HMAC-SHA256 和 AES-CTR)	FIPS 核准的演算法
加密	在「控制器」中執行的 AES-CCM 加密編譯	在「控制器」中執行的 AES-CCM 加密編譯
訊息完整性	AES-CCM 用於保障訊息完整性	AES-CCM 用於保障訊息完整性
安全簡單配對：避免被動式竊聽的保護措施	橢圓曲線 Diffie-Hellman Exchange Ephemeral (ECDHE)	橢圓曲線 Diffie-Hellman 交換 (ECDHE)
安全簡單配對：防止中間人 (MITM) 攻擊的保護措施	兩種由用戶輔助的數值法：數值比較或通行密匙輸入	兩種由用戶輔助的數值法：數值比較或通行密匙輸入 配對要求用戶回應，包括所有非 MITM 配對模式

支援	傳統藍牙	低功耗藍牙
Bluetooth 4.1 或較新版本	2015 年末或較新型號的 iMac 2015 年初或較新型號的 MacBook Pro	iOS 9 或較新版本 iPadOS 13.1 或較新版本 macOS 10.12 或較新版本 tvOS 9 或較新版本 watchOS 2.0 或較新版本
Bluetooth 4.2 或較新版本	iPhone 6 或較新型號	iOS 9 或較新版本 iPadOS 13.1 或較新版本 macOS 10.12 或較新版本 tvOS 9 或較新版本 watchOS 2.0 或較新版本

## 低功耗藍牙私隱

為了協助保護用戶的私隱，BLE 包含下列兩項功能：地址隨機化和跨傳輸密鑰衍生。

**地址隨機化功能**可藉由經常更改藍牙裝置地址，來減少在一段時間內追蹤 BLE 裝置的可行性。為了讓裝置使用私隱功能來重新連接已知裝置，裝置地址（稱為**私人地址**）必須能由其他裝置解析。要產生私人地址，需使用配對程序中交換的裝置身份解析密鑰。

iOS 13 或較新版本和 iPadOS 13.1 或較新版本可跨傳輸作業衍生連結密鑰，此功能稱為**跨傳輸密鑰衍生**。例如，使用 BLE 所產生的連結密鑰可用於衍生「傳統藍牙」連結密鑰。此外，Apple 針對支援「安全連線」功能（藍牙核心規格 4.1 所推出）的裝置，將傳統藍牙加入 BLE 支援中（請參閱[藍牙核心規格 5.1](#)）。

## iOS 的超寬頻保安

Apple 新設計的 U1 晶片採用「超寬頻」技術，具備空間感知功能，讓 iPhone 11、iPhone 11 Pro 和 iPhone 11 Pro Max 或較新的 iPhone 型號可精準定位其他配備 U1 的 Apple 裝置。「超寬頻」技術用以將資料隨機化的機制，與其他支援的 Apple 裝置所採用的相同：

- MAC 地址隨機化
- Wi-Fi 訊框序列號碼隨機化

## 單一登入

### 單一登入保安

#### 單一登入

iOS 和 iPadOS 支援透過單一登入 (SSO) 驗證進入企業網絡。SSO 配搭 Kerberos 型網絡使用，針對用戶獲授權存取的服務對用戶進行認證。SSO 可用於多種網絡活動，從安全的 Safari 作業階段到第三方的 App。同時還支援證書式認證（例如 PKINIT）。

macOS 支援使用 Kerberos 驗證進入企業網絡。App 可以使用 Kerberos 來針對用戶獲授權存取的服務對用戶進行認證。Kerberos 亦可用於多種網絡活動，從安全的 Safari 作業階段和網絡檔案系統認證，到第三方的 App。支援證書式認證，但是需要 App 採用開發者 API。

iOS、iPadOS 和 macOS SSO 使用 SPNEGO 代號和 HTTP Negotiate 通訊協定，與 Kerberos 型認證管道和支援 Kerberos 票證的 Windows 整合式驗證系統配合使用。SSO 的支援以開放原始碼 Heimdal 專案為基礎。

iOS、iPadOS 和 macOS 支援以下加密類型：

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari 支援 SSO，且使用標準 iOS 和 iPadOS 網絡連線 API 的第三方 App 也可進行設定來使用。為設定 SSO，iOS 和 iPadOS 支援允許流動裝置管理 (MDM) 解決方案下推必要設定的設定描述檔承載資料。其中包括：設定用戶主要名稱 (即 Active Directory 用戶帳戶) 和 Kerberos 領域設定，以及設定應允許哪些 App 和 Safari Web URL 使用 SSO。

如要在 macOS 中設定 Kerberos，請使用「票證檢視程式」取得票證，登入 Windows Active Directory 網域，或使用 kinit 命令列工具。

## 可延伸單一登入

App 開發者可使用 SSO 延伸功能來提供他們自己的單一登入實作。當原生或 Web App 需要使用某些「身份提供者」以進行用戶認證時，系統會叫用 SSO 延伸功能。開發者可提供兩種類型的延伸功能：重新導向至 HTTPS 的延伸功能，以及使用質詢/回應機制 (例如 Kerberos) 的延伸功能。這允許可延伸單一登入支援 OpenID、OAuth、SAML2 和 Kerberos 認證計劃。

如要使用單一登入的延伸功能，App 可使用 AuthenticationServices API，或可依靠作業系統所提供的 URL 截取機制。WebKit 和 CFNetwork 提供截取層級，其可為任何原生或 WebKit App 的單一登入提供順暢的支援。如要叫用單一登入延伸功能，必須透過流動裝置管理 (MDM) 描述檔安裝由管理員提供的設定。此外，重新導向類型的延伸功能必須使用「相關的域名」承載資料，以證明其支援的識別身份伺服器知悉其存在。

作業系統隨附的唯一延伸功能為 Kerberos SSO 延伸功能。

## AirDrop 保安

支援 AirDrop 的 Apple 裝置使用低耗電藍牙 (BLE) 和 Apple 建立的點對點 Wi-Fi 技術，來向附近的裝置傳送檔案和資料，包括具有 AirDrop 功能且系統為 iOS 7 或較新版本的 iOS 裝置和 iPad 裝置，以及系統為 OS X 10.11 或較新版本的 Mac 電腦。Wi-Fi 無線電用來在裝置之間進行直接通訊，無需使用任何互聯網連線或無線連接點 (AP)。此連線經過 TLS 加密。

AirDrop 的共享設定預設為「只限聯絡人」。用戶也可以選擇使用 AirDrop 與所有人進行共享，或者完全關閉此功能。機構或部門可針對流動裝置管理 (MDM) 解決方案所控管的裝置和 App，限制其 AirDrop 的使用權。

## AirDrop 操作

AirDrop 使用 iCloud 服務以協助用戶驗證。當用戶登入 iCloud 時，一個 2048 位元 RSA 身份會儲存在裝置上，而當用戶開啟 AirDrop 時，系統會根據連繫至用戶 Apple ID 的電郵地址和電話號碼建立簡短 AirDrop 識別身份雜湊值。

當用戶選擇使用 AirDrop 共享項目時，發送裝置會透過 BLE 發出 AirDrop 訊號，其中包含用戶的簡短 AirDrop 識別身份雜湊值。附近處於喚醒狀態並已開啟 AirDrop 的 Apple 裝置，會使用點對點 Wi-Fi 來偵測訊號並回應，因此，當有任何裝置發出回應時，發送裝置即可發現其識別身份。

在「只限聯絡人」模式下，接收裝置會將收到的簡短 AirDrop 識別身份雜湊值與裝置上「通訊錄」App 中聯絡人的雜湊值進行比對。如果找到相符的聯絡人，接收裝置便會透過點對點 Wi-Fi 來以裝置的識別身份資料予以回應。如果沒有比對成功，裝置就不會回應。

在「所有人」模式中，整體會使用相同的程序，但即使沒有在「通訊錄」App 中找到比對成功的項目，接收裝置也會回應。

發送裝置接着會使用點對點 Wi-Fi 來起始 AirDrop 連線，在此連線階段送出完整的識別身份雜湊值到接收裝置。如果完整識別身份雜湊值與接收者「通訊錄」中已知聯絡人的雜湊值相符，接收者便會繼續以其完整識別身份雜湊值予以回應。

驗證雜湊值後，接收者的名稱和相片（如果「通訊錄」中有的話）便會顯示在傳送者的 AirDrop 分享頁中。在 iOS 和 iPadOS 中，其會於「人員」或「裝置」中顯示。未驗證或認證的裝置會在發送裝置的 AirDrop 的分享頁中，以剪影圖像和裝置名稱顯示，如「設定」>「一般」>「關於本機」>「名稱」所定義。在 iOS 和 iPadOS 中，這些人會被置於 AirDrop 分享頁中的「其他人」部份。

傳送方用戶之後可選擇其要分享的對象。在用戶選擇後，發送裝置會與接收裝置建立一組加密 (TLS) 連線，此連線會交換彼此的 iCloud 識別身份證書。證書中的識別身份會與用戶雙方的「通訊錄」App 進行比對驗證。

如證書成功通過驗證，系統會要求接收方用戶接受來自經識別的用戶或裝置所傳送的內容。如果選擇了多位接收者，則會針對每個目標重複此過程。

## iPhone 和 iPad 的 Wi-Fi 密碼共享保安

支援 Wi-Fi 密碼共享的 iOS 和 iPadOS 裝置所使用的機制與 AirDrop 類似，會將 Wi-Fi 密碼從一部裝置傳送至另一部。

當用戶選擇了 Wi-Fi 網絡（要求者），且系統提示要求輸入 Wi-Fi 密碼時，Apple 裝置會啟動低耗電藍牙 (BLE) 廣播，顯示需要 Wi-Fi 密碼。附近處於喚醒狀態，且擁有所選 Wi-Fi 網絡的密碼之其他 Apple 裝置，會使用 BLE 連接提出要求的裝置。

擁有 Wi-Fi 密碼的裝置（提供者）需要取得要求者的「通訊錄」資料，且要求者必須使用類似 AirDrop 的機制證明其身份。證明身份後，提供者會傳送密碼給要求者，此密碼可用來加入網絡。

組織可使用流動裝置管理 (MDM) 解決方案來限制所管理的裝置或 App 的 Wi-Fi 密碼共享使用權。

## macOS 的防火牆保安

macOS 包含內置防火牆，可防止 Mac 遭網絡存取並防禦拒絕服務攻擊。防火牆可在「系統偏好設定」的「保安與私隱」面板中加以設定，且支援下列設定：

- 封鎖任何 App 的所有傳入連線。
- 自動允許內置軟件接收傳入連線。
- 自動允許已下載及已簽署的軟件接收傳入連線。
- 根據用戶指定的 App 加入或拒絕存取。
- 阻止 Mac 回應 ICMP (互聯網控制訊息通訊協定) 探測和連接埠掃描要求。



# 開發者套件保安

## 開發者套件保安概覽

Apple 提供多種「套件」架構以支援第三方開發者擴展 Apple 服務。以下架構的設計重點為保護用戶私隱和保安：

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

## HomeKit 保安

### HomeKit 通訊保安

HomeKit 提供家居自動化的基礎架構，利用 iCloud 與 iOS、iPadOS 和 macOS 保安來保護與同步私隱資料，無須將其透露給 Apple。

HomeKit 身份與保安是以 Ed25519 公用-專用密鑰組為基礎。iOS、iPadOS 和 macOS 裝置會為 HomeKit 的每位用戶產生 Ed25519 密鑰組，這些密鑰組會變成他們的 HomeKit 身份，用於認證 iOS、iPadOS 和 macOS 裝置之間以及 iOS、iPadOS 和 macOS 裝置與配件之間的通訊。

密鑰會儲存在鑰匙圈，並只納入加密的「鑰匙圈」備份中，會在使用「iCloud 鑰匙圈」（如可用）的裝置間保持最新狀態。HomePod 和 Apple TV 會使用以下敘述的「點一下來設定」或設定模式來接收密鑰。密鑰會由 iPhone 使用 Apple 識別服務 (IDS) 分享給配對的 Apple Watch。

### HomeKit 配件之間的通訊

HomeKit 配件會產生其自己的 Ed25519 密鑰組，以用於與 iOS、iPadOS 和 macOS 裝置的通訊。如將配件還原成原廠設定，便會產生新的密鑰組。

為了在 iOS、iPadOS 和 macOS 裝置與 HomeKit 配件之間建立關係，系統會使用「安全遙距密碼」（3072 位元）通訊協定來交換密鑰，利用配件製造商所提供並由用戶於 iOS、iPadOS 裝置上輸入的八位數代碼，然後使用 ChaCha20-Poly1305 AEAD 與 HKDF-SHA512 衍生密鑰來加密。配件的 MFi 認證也會在設定期間進行驗證。沒有 MFi 晶片的配件可以在 iOS 11.3 或較新版本中建立軟件認證的支援。

當 iOS、iPadOS 和 macOS 裝置與 HomeKit 配件在使用期間進行通訊時，每個裝置會使用上述過程中交換的密鑰來認證另一部裝置。每個作業階段都會使用站對站的通訊協定來建立，並使用以作業階段專屬的 Curve25519 密鑰為基礎的 HKDF-SHA512 衍生密鑰來進行加密。這同時適用於 IP 型與低功耗藍牙 (BLE) 配件。

針對支援廣播通知的 BLE 裝置，配件會由配對的 iOS、iPadOS 和 macOS 裝置透過安全的作業階段以廣播加密密鑰配置。此密鑰會用於在配件上加密有關狀態變更的資料，這些資料會使用 BLE 廣播傳送通知。廣播加密密鑰是一種 HKDF-SHA512 衍生密鑰，資料會由 ChaCha20-Poly1305 AEAD 演算法進行加密。廣播加密密鑰會定期由 iOS、iPadOS 和 macOS 裝置變更並使用 iCloud 更新至其他裝置，如 [HomeKit 資料保安](#) 所說明。

## HomeKit 和 Siri

Siri 可用來查詢和控制配件，並可啟動場景。匿名提供給 Siri 的家居配置資料會盡量最小化，以提供房間名稱、配件和指令識別所需的場景。傳送給 Siri 的音訊可能與特定配件或指令相關，但此類 Siri 資料不會與其他 Apple 功能 (如 HomeKit) 產生關聯。

### 支援 Siri 的 HomeKit 配件

用戶可以使用「家居」App 在支援 Siri 的配件上啟用 Siri 等新功能，以及計時器、鬧鐘、對講機和門鐘等其他 HomePod 功能。啟用這些功能後，配件會與本機網絡上託管這些 Apple 功能的已配對 HomePod 進行協調。音訊會使用 HomeKit 和 AirPlay 通訊協定透過加密通道在裝置間交換。

開啟「聆聽『喂 Siri』」後，配件會使用本機執行的觸發字詞偵測引擎來聽取「喂 Siri」詞組。如果此引擎偵測到該詞組，便會使用 HomeKit 將音訊分段直接傳送到配對的 HomePod。HomePod 會對音訊進行第二次檢查，如果詞組似乎不包含觸發詞組，則可能會取消該音訊分段。

開啟「觸碰以呼叫 Siri」時，用戶可以按下配件上的專用按鈕來開始與 Siri 對話。系統會將音訊分段會直接傳送到已配對的 HomePod。

偵測到成功呼叫 Siri 後，HomePod 會將音訊傳送到 Siri 伺服器，並依據 HomePod 套用到 HomePod 本身的用戶呼叫內容，使用相同保安、私隱和加密保護措施，來滿足用戶的意圖。如果 Siri 有音訊回覆，系統會透過 AirPlay 音訊通道將 Siri 的回覆傳送到配件。部份 Siri 要求需要用戶提供其他資料 (例如，詢問用戶是否想聽到更多選項)。在這種情況下，配件會收到提示用戶的指示，並將附加音訊以串流到 HomePod。

配件需配備視覺指示器，以便在其主動聆聽時向用戶發出訊號 (例如，LED 指示燈)。除了取用音訊串流之外，配件不會知道 Siri 要求的意圖，且配件上不會儲存任何用戶資料。

## HomeKit 資料保安

可以使用 iCloud 和 iCloud 鑰匙圈，在同一名用戶的 iOS、iPadOS 和 macOS 裝置間安全地更新 HomeKit 資料。在此期間，HomeKit 資料會使用從用戶 HomeKit 身份與隨機數衍生的密鑰來進行加密，並當成不透明二進位大型物件 (或稱為 **blob**) 來處理。最近的物件會儲存在 iCloud 中，但不會用於任何其他用途。因為它是使用僅可於用戶 iOS、iPadOS 和 macOS 裝置上取得的密鑰進行加密，因此它的內容在傳輸與 iCloud 儲存期間是無法存取的。

HomeKit 資料也會在同一家居的多位用戶間進行同步。此處理會使用認證與加密，就像 iOS、iPadOS 和 macOS 裝置與 HomeKit 配件間使用的一樣。認證是以 Ed25519 公用密鑰為基礎，當用戶加入家居時，便會在裝置間交換這些密鑰。在新用戶加入家居後，所有進一步的通訊都會使用站對站的通訊協定與作業階段專屬的密鑰進行認證和加密。

一開始在 HomeKit 中建立家居的用戶或具有編輯權限的其他用戶可以新增用戶。擁有者的裝置會使用新用戶的公用密鑰來設定配件，以便讓配件可認證和接受來自新用戶的指令。當具有編輯權限的用戶新增用戶時，系統便會將此程序委派至家居控制中樞以完成操作。

## HomeKit 和 Apple TV

當用戶登入 iCloud 時，便會自動執行配置 Apple TV 的程序以配搭 HomeKit 使用。iCloud 帳戶需要啟用雙重認證。Apple TV 與擁有者的裝置會透過 iCloud 交換臨時 Ed25519 公用密鑰。當擁有者的裝置與 Apple TV 連接相同區域網絡時，臨時密鑰會使用站對站的通訊協定與作業階段專屬密鑰來保護區域網絡的連線。此處理會使用認證與加密，就像 iOS、iPadOS 和 macOS 裝置與 HomeKit 配件間使用的一樣。透過安全的區域連線，擁有者的裝置會將用戶的 Ed25519 公用-專用密鑰組傳送至 Apple TV。這些密鑰之後會用來保護 Apple TV 與 HomeKit 配件間的通訊，還有 Apple TV 和其他 iOS、iPadOS 和 macOS 裝置 (HomeKit 家居的一部份) 間的通訊。

如用戶沒有多部裝置，且並未將其家居的存取權限授予其他用戶，便不會將 HomeKit 資料傳輸至 iCloud。

## 家居資料與 App

App 對家居資料的存取權是受用戶的「私隱」設定所控制。當 App 要求提供家居資料時，系統會要求用戶授予存取權，過程類似於要求提供「通訊錄」、「相片」和其他 iOS、iPadOS 和 macOS 資料來源。如用戶許可，App 便可存取房間的名稱、配件名稱、每個配件所在的房間，以及 HomeKit 開發者文件中所載明的其他資料，網址為：<https://developer.apple.com/homekit/>。

## 本機資料儲存

HomeKit 會在用戶的 iOS、iPadOS 和 macOS 裝置上儲存家居、配件、場景和用戶的相關資料。儲存的資料會透過自用戶 HomeKit 身份密鑰所衍生的密鑰加上隨機數來進行加密。此外，系統會使用「資料保護」類別的「首次用戶認證前的保護」來儲存 HomeKit 資料。HomeKit 資料只會備份在經過加密處理的備份檔案中，因此，諸如備份至 Finder (macOS 10.15 或較新版本) 或透過 USB 備份至 iTunes (macOS 10.14 或較早版本) 的未加密備份，就不會包含 HomeKit 資料。

## 用 HomeKit 保護路由器的安全

支援 HomeKit 的路由器可讓用戶透過管理 HomeKit 配件對其區域網絡和互聯網的 Wi-Fi 存取權限，來提高其家居網絡的保安。路由器也支援私密 PSK (PPSK) 認證，因此可以使用配件特定的密鑰將配件加入 Wi-Fi 網絡，並可視需要撤銷。PPSK 認證透過避免向配件透露主 Wi-Fi 密碼，並允許路由器安全地識別配件 (即使配件更改其 MAC 地址) 來改進保安。

使用「家居」App，用戶可透過以下方式為配件群組設定取用限制：

- **沒有限制：**允許不受限制地存取互聯網和區域網絡。
- **自動：**此為預設的設定。根據配件製造商提供給 Apple 的互聯網網站和本機連接埠列表，允許存取互聯網和區域網絡。此列表包括配件可正常運作所需的所有網站和傳輸埠。(在沒有此類列表之前，設定為「沒有限制」。)
- **限制家居權限：**除了 HomeKit 用來從區域網絡 (包含從家居控制中樞到支援遙控) 搜尋和控制配件所需的連線之外，無法存取其他互聯網或區域網絡。

PPSK 是高強度、針對配件提供的 WPA2 個人密語由 HomeKit 自動產生，如果以後將配件從「家居」中移除，則會撤銷。當透過 HomeKit 路由器所設定之「家居」中的 HomeKit 將配件加到 Wi-Fi 網絡時，就會使用 PPSK；這次加入會反映為 Wi-Fi 憑證：「HomeKit 受管理」(位於「家居」App 中配件的設定畫面上)。如果配件有支援，則在加入路由器之前加入到 Wi-Fi 網絡的配件會重新設定為使用 PPSK，否則將保留其現有憑證。

作為一項額外的安全措施，用戶必須使用路由器製造商的 App 設定 HomeKit 路由器，以便該 App 驗證用戶是否有權存取路由器，並可將其加到「家居」App 中。

## HomeKit 攝影機保安

HomeKit 中具有網際網絡通訊協定位址 (IP 位址) 的攝影機可直接將影片和音訊串流直接傳送至區域網絡上存取該串流的 iOS、iPadOS、tvOS 和 macOS 裝置。系統會使用在裝置和「網際網絡通訊協定」攝影機 (或稱為網絡攝影機) 上隨機產生的密鑰來加密這些串流, 並透過安全的 HomeKit 作業階段交換至攝影機。如裝置未連接區域網絡, 則會經由家居控制中樞將加密的串流轉達至裝置。家居控制中樞不會解密串流, 且只扮演裝置和網絡攝影機之間的中繼站角色。App 向用戶顯示 HomeKit 網絡攝影機的影片畫面時, HomeKit 會透過獨立的系統程序以安全方式轉譯影片影格。因此, App 無法存取或儲存影片串流。此外, App 無權從此串流截取截圖。

### HomeKit 安全錄影

HomeKit 提供了點對點的安全和專用機制, 可記錄、分析和檢視 HomeKit 網絡攝影機的影片片段, 而無需將該影片內容洩露給 Apple 或任何第三方。當網絡攝影機偵測到動作, 影片片段會透過家居中樞和該網絡攝影機之間專用的區域網絡連線, 直接傳送到用作家居控制中樞的 Apple 裝置。區域網絡連線會以作業階段專屬 HKDF-SHA512 衍生的密鑰組加密, 該密鑰組會透過家居控制中樞與網絡攝影機之間的 HomeKit 作業階段進行交涉。HomeKit 會在家居控制中樞上解密音訊和影片串流, 並在本機分析影格, 以了解是否有任何特別事件。如偵測到特別事件, HomeKit 會使用 AES-256-GCM 和隨機產生的 AES256 密鑰來將影片片段加密。HomeKit 亦會為每個片段產生展示影格, 且使用相同的 AES256 密鑰加密這些展示影格。已加密的展示影格, 和音訊及影片資料會上載到 iCloud 伺服器。每個片段的相關後設資料 (包括加密密鑰) 會以 iCloud 點對點加密上載到 CloudKit。

對於臉部分類, HomeKit 會使用 iCloud 點對點加密在 CloudKit 中儲存用於對特定人臉進行分類的所有資料。儲存的資料包括每個人的相關資料 (例如姓名) 以及代表該人臉部的影像。這些臉部影像可以選擇從用戶的「相片」中取得, 也可以從以前分析過的網絡攝影機視訊中收集。「HomeKit 安全錄影」分析作業階段會使用此分類資料來識別其直接從網絡攝影機接收之安全視訊串流中的臉部影像, 並將該識別資料納入在前面所提到的影片片段後設資料中。

當用戶使用「家居」App 檢視攝影機的片段, 資料會從 iCloud 下載, 亦會使用 iCloud 點對點解密在本機將用於解密串流的密鑰解除封裝。已加密的影片內容會從伺服器串流, 並且於檢視程式顯示影片內容前, 在 iOS 裝置上進行本機解密。每個影片片段段落可能會被分拆為子區段, 每個子區段會使用其獨有密鑰來加密內容串流。

## Apple TV 的 HomeKit 保安

HomeKit 可安全地將一些第三方遙距配件連接到 Apple TV, 並支援為家居 Apple TV 的擁有者加入用戶個人檔案。

### 配搭 Apple TV 使用第三方的遙控器配件

部份第三方遙控器配件可為使用「家居」App 綁定的 Apple TV 提供人機介面設計 (HID) 事件和 Siri 音訊。遙控器透過安全作業階段將 HID 事件傳送到 Apple TV。當用戶以遙控器上專用的 Siri 按鈕特地啟用咪高風時, 具備 Siri 功能的電視遙控器會將音訊資料傳送到 Apple TV。遙控器會使用專用區域網絡連線, 直接將音訊分段傳送到 Apple TV。作業階段專屬 HKDF-SHA512 衍生的密鑰組會在 Apple TV 與電視遙控器之間的 HomeKit 作業階段中進行交涉, 藉此加密區域網絡連線。HomeKit 會在 Apple TV 上將各個音訊分段解密並轉送到 Siri App, 且會以與所有 Siri 音訊輸入相同的私隱保護措施處理。

### HomeKit 家居的 Apple TV 描述檔

當 HomeKit 家居的用戶將其描述檔加入家居擁有者的 Apple TV, 便可提供取用其電視節目、音樂和 Podcast 的權限給該用戶。每位用戶的設定在 Apple TV 使用的描述檔會使用 iCloud 點對點加密分享至擁有者的 iCloud 帳戶。資料由每位用戶擁有, 並會以唯讀的方式分享給擁有者。家居的每位用戶都可以在「家居」App 中更改這些值, 而擁有者的 Apple TV 會使用這些設定。

當設定開放時, 用戶的 iTunes 帳戶即可用於 Apple TV 上。當設定關閉時, 所有與該用戶有關的帳戶和資料都在 Apple TV 上刪除。初始 CloudKit 共享會由用戶裝置起始, 而用於建立安全 CloudKit 共享的代號則會透過家居用戶間同步資料所用的相同安全頻道來傳送。

## iOS、iPadOS 和 watchOS 的 SiriKit 保安

Siri 使用 App 延伸功能系統來與第三方 App 進行通訊。在裝置上，Siri 可存取用戶的聯絡人資料和裝置的目前位置。但在 Siri 向 App 提供受保護的資料前，Siri 會檢查該 App 由用戶控制的取用權限。依據有關權限，Siri 只會將原有話語片段中的相關部份傳至 App 的延伸功能。例如，如果 App 沒有通訊錄的存取權，Siri 就不會在用戶要求中解析關係（如「用『付款』App 付給媽媽 10 美元」）。在此情況下，App 可能只會看到「媽媽」這個詞。

但是如果用戶授予 App 存取通訊錄的權限，該 App 就可收到有關用戶母親的解析資料。如果在訊息的內文部份提及某個關係，例如「用『訊息』App 傳訊息跟媽媽說哥哥最好了」，無論 App 的權限為何，Siri 都不會解析「哥哥」一詞。

已啟用 SiriKit 的 App 可以向 Siri 傳送 App 專屬或用戶專屬的詞彙，例如用戶通訊錄中的聯絡人名稱。此資料允許 Siri 的語音辨認及自然語言理解功能為該 App 辨識詞彙，並連繫至隨機識別碼。自訂資料在使用身份期間皆可使用，或直至用戶在「設定」停用該 App 的 Siri 整合，或解除安裝該已啟用 SiriKit 的 App。

在話語「用『共乘』App 載我去媽媽屋企」中，此要求需要從用戶的通訊錄取用位置資料。針對該請求，Siri 會向 App 的延伸功能提供所需資料，不論用戶對該 App 的位置或聯絡資料權限設定。

## macOS 的 DriverKit 保安

DriverKit 架構讓開發者可製作供用戶安裝在 Mac 上的裝置驅動程式。透過 DriverKit 建立的驅動程式會在用戶空間中執行，而非作為核心延伸功能，因此可提升系統保安與穩定性。這可讓安裝變得更輕鬆，以及改進 macOS 的穩定性及保安。

用戶只需下載 App（當使用系統延伸功能或 DriverKit 時，安裝程式並非必須），延伸功能只會在要求時啟用。這在許多情況下會取代需要管理員特殊權限以於「/系統/資源庫」或「/資源庫」中進行安裝的 kext。

我們建議使用需核心延伸功能的裝置驅動程式、雲端儲存解決方案、網絡和保安 App 之 IT 管理員改為使用建立在系統延伸功能上的較新版本。這些較新版本可以大幅降低 Mac 發生核心錯誤的機會，並縮小受攻擊的範圍。這些新的延伸功能會在用戶空間執行，無需特殊權限以進行安裝，且會在綁架的 App 被移至「垃圾筒」時自動移除。

DriverKit 框架提供 C++ 級別予 I/O 服務、裝置配對、記憶體描述，以及分發佇列。它亦會為編號、集合、字串，以及其他常用類型定義適合 I/O 的類型。用戶會配合家居指定驅動程式框架，如 USBDriverKit 和 HIDDriverKit 使用。請使用「系統延伸功能」架構來安裝和升級驅動程式。

# iOS 和 iPadOS 的 ReplayKit 保安

ReplayKit 是允許開發者在其 App 中加入錄製與即時廣播功能的架構。此外，它允許用戶運用裝置的前鏡頭和咪高風來為其錄製的內容和廣播加上註解。

## 影片錄製

錄製影片中打造的保安層級有數層：

- **權限對話框**：在錄製開始前，ReplayKit 會向用戶提供同意提示，要求用戶確認其錄製螢幕畫面、咪高風及前置相機的意圖。系統會針對每個 App 處理程序顯示此提示一次，且如 App 停留在背景超過 8 分鐘，將會再次顯示。
- **螢幕與音訊截取**：螢幕與音訊截取是在 App 的處理程序外、於 ReplayKit 服務程式 replayd 中進行。其設計用意是確保錄製的內容從不讓 App 處理程序存取。
- **App 內螢幕與音訊截取**：這允許 App 取得於權限對話框授權的影片及樣本緩衝。
- **影片製作與儲存**：影片檔會直接寫入目錄，只有 ReplayKit 子系統可存取，且從不讓任何 App 存取。這樣有助防止錄製內容未經用戶同意而遭第三方使用。
- **終端用戶預覽與共享**：用戶可使用 ReplayKit 提供的用戶介面來預覽與共享影片。用戶介面會透過「iOS 延伸功能」基礎架構跨程序呈現，並可存取產生的影片檔。

## ReplayKit 廣播

廣播影片中打造的保安層級有數層：

- **螢幕與音訊截取**：廣播期間的螢幕與音訊截取機制與影片錄製相同，且會發生於 replayd 中。
- **廣播延伸功能**：如要讓第三方服務參與 ReplayKit 廣播，有關第三方服務需要建立兩個以 `com.apple.broadcast-services` 端點加以設定的新延伸功能：
  - 允許用戶設定其廣播的用戶介面延伸功能
  - 上載延伸功能，可處理上載影片與音訊資料至服務的後端伺服器

該架構有助確保託管 App 對廣播的影片和音訊內容沒有特殊權限。只有 ReplayKit 和第三方廣播延伸功能具有存取權限。

- **廣播選擇器**：透過廣播選擇器，用戶可直接從 App 開始發送系統廣播（使用可從「控制中心」存取的相同系統定義用戶介面）。用戶介面會使用專用 API 來導入，且為位於 ReplayKit 程式框架中、屬託管 App 的跨程序延伸功能。
- **上載延伸功能**：第三方廣播服務會執行延伸功能，以在廣播使用原始未編碼的樣本緩衝期間處理影片和音訊內容。進行此處理模式期間，系統會將影片和音訊資料序列化，並透過直接 XPC 連線來即時傳遞至第三方的上載延伸功能。影片資料完成編碼的方式是藉由從影片樣本緩衝截取 IOSurface 物件、以安全的方式編碼為 XPC 物件，再透過 XPC 傳送至第三方延伸功能，並安全地解碼回 IOSurface 物件。

## iOS 和 iPadOS 的 ARKit 保安

ARKit 架構可讓開發者在其 App 或遊戲中營造擴增實境的體驗。開發者可以使用 iOS 或 iPadOS 裝置的前置或後置相機來加入 2D 或 3D 元素。

Apple 設計的相機重視用戶的私隱，第三方 App 必須取得用戶的同意才能取用相機。在 iOS 和 iPadOS 中，當用戶授予 App 相機的取用權限時，該 App 可從前後相機取用即時影像。如 App 在使用相機時不公開狀態，則不會獲允許使用「相機」。

以相機拍攝的相片和影片可能包含其他資料，例如拍攝時間和位置、景深和 OverCapture 的內容。如用戶不想「相機」App 拍攝的相片和影片包含位置資料，用戶可以隨時前往「設定」>「私隱」>「定位服務」>「相機」中進行控制。如用戶不想在分享相片或影片時包含位置資料，用戶可以在分享頁中的「選項」選單關閉位置。

為改進用戶 AR 體驗的定位，使用 ARKit 的 App 可使用來自其他相機的世界或面孔追蹤資料。世界追蹤使用用戶裝置上的演算法處理來自感應器的資料，以決定其位置來連繫至物理空間。世界追蹤會啟用「地圖」中的「光學方位」等功能。

# 安全裝置管理

## 安全裝置管理概覽

iOS、iPadOS、macOS 和 tvOS 支援具彈性的安全政策和設定，讓用戶容易實施與管理。各機構可透過這些功能保護公司資料並協助確保員工遵守企業要求，即使員工使用自己的裝置時也一樣（例如運用在「員工自攜裝置」（BYOD）計劃時）。

公司可以使用密碼保護、設定描述檔、遙距清除和第三方流動裝置管理 (MDM) 解決方案等資源來管理大量裝置並協助確保公司的資料安全，甚至在員工使用私人裝置存取資料時，亦能保障安全。

在 iOS 13 或較新版本、iPadOS 13.1 或較新版本，以及 macOS 10.15 或較新版本中，Apple 裝置支援一項新的用戶註冊選項，此選項是專為 BYOD 計劃而設計。用戶註冊讓用戶在其裝置上享有更高的自主性，同時會將企業資料儲存於受加密方式保護的獨立 APFS (Apple 檔案系統) 卷宗上，從而提高企業資料的保安。此選項可在 BYOD 計劃的保安、私隱和用戶體驗上取得更佳平衡。

## iPhone 和 iPad 的配對模式保安

iOS 和 iPadOS 使用配對模式來從主機電腦控制裝置的存取權。配對會透過公用密鑰交換，以示在裝置與所連接的主機之間已建立信任關係。iOS 和 iPadOS 也會憑藉這種信任關係來在與所連接的主機之間啟用附加功能，例如資料同步。在 iOS 9 或較新版本中：

- 需要配對的服務會等到用戶解鎖裝置後才會啟用
- 除非裝置最近剛解鎖，否則服務不會啟動
- 某些服務 (包含相片同步) 可能會要求裝置解鎖後才會開始

配對程序需要用戶解鎖裝置並接受來自主機的配對要求。在 iOS 9 或較新版本中，用戶亦必須輸入密碼，然後主機和裝置會交換並儲存 2048 位元的 RSA 公用密鑰。然後主機會收到一個 256 位元密鑰，可解鎖儲存在裝置上的託管 Keybag。在裝置將受保護的資料傳送到主機或啟動服務 (iTunes 或 Finder 同步、檔案傳送、Xcode 開發等) 前，需要使用交換的密鑰來啟動加密 SSL 作業階段。如要將此加密作業階段用於所有通訊，裝置需透過 Wi-Fi 與主機連線，因此在這之前必須先透過 USB 配對。配對也會啟用一些診斷功能。在 iOS 9 中，如配對記錄已超過 6 個月未使用便會過期。在 iOS 11 或較新版本中，此期限縮短為 30 日。

部份診斷服務 (包含 com.apple.mobile.pcapd) 會限制為僅能透過 USB 執行。此外，需要安裝 Apple 簽署的設定描述檔才能使用 com.apple.file\_relay 服務。在 iOS 11 或較新版本中，Apple TV 可使用「安全遙距密碼」通訊協定來以無線方式建立配對關係。

用戶可以使用「重設網絡設定」或「重設定位服務與私隱」選項來清除信任的主機列表。



# 流動裝置管理

## 流動裝置管理保安概覽

Apple 作業系統支援流動裝置管理 (MDM)，此解決方案讓機構可安全地設定及管理有規模的 Apple 裝置部署。

### MDM 如何安全運作

MDM 功能建基於設定描述檔、無線註冊和「Apple 推送通知服務」(APNs) 等現有的作業系統技術。例如，APNs 可用來喚醒裝置，以便其可透過安全連線與 MDM 解決方案直接進行通訊。使用 APN 不會傳輸機密或專有資料。

使用 MDM，IT 部門便可以為企業環境中的 Apple 裝置註冊、以無線方式設定配置和更新設定、監控公司政策的遵守狀況、管理軟件更新政策，甚至可以遙距清除或鎖定受管理的裝置。

除 iOS、iPad OS、macOS 和 tvOS 支援的傳統裝置註冊外，新的註冊類型 (用戶註冊) 亦已加至 iOS 13 或較新版本、iPadOS 13.1 或較新版本，以及 macOS 10.15 或較新版本。用戶註冊是專為「員工自攜裝置」(BYOD) 部署而設的 MDM 註冊方式，意思是裝置由個人擁有，但在受管理環境下使用。用戶註冊授予 MDM 解決方案的權限比不受監管裝置註冊的權限較為有限，且會使用加密方式將用戶和公司資料分隔。

### 註冊類型

- **自動裝置註冊：**「自動裝置註冊」讓機構在裝置開箱的當下即可進行設定及管理 (以稱為「自動進行部署」的程序)。這些裝置稱為**受監管**，且用戶可選擇讓用戶無法移除 MDM 描述檔。「自動裝置註冊」是專為機構擁有的裝置而設計。
- **裝置註冊：**「裝置註冊」允許機構讓用戶手動註冊裝置，然後管理許多裝置使用層面，包含清除裝置的功能在內。「裝置註冊」也有較大範圍的承載資料和取用限制可套用至裝置。當用戶移除註冊描述檔，所有設定描述檔及其設定，以及該註冊描述檔之受管理的 App 都會一併移除。
- **用戶註冊：**「用戶註冊」專為用戶持有的裝置而設，並會與「管理式 Apple ID」結合，以在裝置上建立用戶身份。「管理式 Apple ID」是「用戶註冊」描述檔的一部份，用戶必須認證成功以完成註冊。管理式 Apple ID 可配搭用戶已登入的個人 Apple ID 使用。受管理的 App 和帳戶使用管理式 Apple ID，而個人 App 和帳戶則使用個人 Apple ID。

### 裝置功能限制

取用限制可由管理員啟用，或在部份情況下停用，以協助防止用戶在 MDM 解決方案中註冊的 iPhone、iPad、Mac 或 Apple TV 上取用特定的 App、服務或功能。取用限制會以取用限制承載資料的形式傳送至裝置，其為設定描述檔的一部份。iPhone 上的某些取用限制可能會複製到配對的 Apple Watch 上。

### 密碼設定管理

依照預設，用戶的密碼可定義為數值的 PIN。在配備 Face ID 或 Touch ID 的 iOS 和 iPadOS 裝置上，密碼長度至少需有四位數。因較長且複雜的密碼比較難以猜測或攻擊，建議使用此類密碼。

管理員可以使用 MDM 或 Microsoft Exchange ActiveSync，或是要求用戶手動安裝設定描述檔，來強制實施複雜密碼要求和其他規則。安裝 macOS 密碼規則承載資料需使用管理員密碼。有些密碼規則可能需要特定的密碼長度、組成內容或其他屬性。

## 設定描述檔的強制執行

設定描述檔是 MDM 解決方案在受管理裝置上遞送和管理規則和限制的主要方式。如果機構需要設定大量裝置或為大量裝置提供許多自訂的電郵設定、網絡設定或憑證，那麼使用設定描述檔是一種安全可靠的方式。

### 設定描述檔

**設定描述檔**是包含承載資料的 XML 檔案 (結尾為 .mobileconfig)，可將設定和授權資料載入 Apple 裝置。設定描述檔會自動處理設定、帳戶、限制和憑證的設定作業。這些檔案是由 MDM 解決方案或 Mac 版 Apple Configurator 製作，也可以手動製作。機構在將設定描述檔傳送到 Apple 裝置之前，必須使用註冊描述檔將裝置註冊到 MDM 解決方案中。

### 註冊描述檔

**註冊描述檔**是帶有 MDM 承載資料的設定描述檔，會在為該裝置指定的 MDM 解決方案中將裝置註冊。這可讓 MDM 解決方案傳送指令和設定描述檔到裝置並查詢裝置的特定層面。當用戶移除註冊描述檔，所有設定描述檔及其設定，以及該註冊描述檔之受管理的 App 都會一併移除。在裝置上一次只能存在一個註冊描述檔。

### 設定描述檔的設定

設定描述檔中包含可指定特定承載資料中的多個設定包括 (但不限於)：

- 密碼規則
- 對裝置功能的限制 (例如停用相機)
- 網絡與 VPN 設定
- Microsoft Exchange 設定
- 「郵件」設定
- 帳戶設定
- LDAP 目錄服務設定
- CalDAV 日曆服務設定
- 憑證和密鑰
- 軟件更新

### 描述檔簽署和加密

設定描述檔可以簽署來驗證其來源及進行加密，以協助確保其完整性並保護其內容。iOS 和 iPadOS 的設定描述檔是使用 [RFC 5652](#) 中指定的「加密編譯訊息語法」(CMS) 來加密 (支援 3DES 和 AES128)

### 描述檔安裝

用戶可以使用 Mac 版 Apple Configurator 直接在裝置上安裝設定描述檔，也可以使用 Safari 下載、藉由附加至電郵來傳送、使用 AirDrop 或 iOS 或 iPadOS 中的「檔案」App 來傳輸，或是使用流動裝置管理 (MDM) 解決方案以無線方式傳送。用戶在 Apple School Manager 或 Apple Business Manager 中設定裝置時，裝置會下載並安裝用於 MDM 註冊的描述檔。如需移除描述檔的相關資料，請參閱「Apple 平台部署」中的[流動裝置管理簡介](#)。

**附註：**在受監管裝置上，設定描述檔也可以鎖定到裝置上。其設計用意是徹底防範描述檔遭移除，或要求輸入密碼才能移除描述檔。由於許多機構皆持有本身的 iOS 和 iPadOS 裝置，可以移除將裝置綁定至 MDM 解決方案的設定描述檔，但這麼做也會移除所有受管理的設定資料、資料和 App。

## 自動裝置註冊

在用戶收到裝置前，公司可以在流動裝置管理 (MDM) 中自動註冊 iOS、iPadOS、macOS 和 tvOS 裝置，無需實際觸碰或準備裝置。在註冊服務後，管理員需登入服務網站，並將方案連接到其 MDM 解決方案。接着便可透過 MDM 將他們購買的裝置指定給用戶。設定裝置期間，如果確實實施適當的安全措施，將能提高敏感資料的保安。例如：

- 將用戶認證納入 Apple 裝置啟用程序中「設定輔助程式」的初始設定流程
- 提供具備有限存取權限的初步設定，及要求進行額外的裝置設定以存取敏感資料。

指定好用戶後，所有 MDM 專屬的設定、限制或控制項目便會自動安裝。裝置與 Apple 伺服器之間所有傳輸中的通訊皆會透過 HTTPS (TLS) 加密。

藉由移除裝置上「設定輔助程式」中的特定步驟，用戶的設定程序可以更加簡化，方便他們快速使用。管理員也可以控制用戶是否可從裝置上移除 MDM 描述檔，並確定裝置限制在裝置生命週期中皆會實行。裝置經開箱和啟用後，可於機構的 MDM 解決方案中註冊，所有管理設定、App 和書籍便會依照 MDM 管理員的定義安裝。

## Apple School Manager、Apple Business Manager 和 Apple Business Essentials

Apple School Manager、Apple Business Manager 和 Apple Business Essentials 是專供 IT 管理員使用的服務，用於部署機構直接向 Apple 或 Apple 授權的經銷商和電訊商購買的 Apple 裝置。

使用 MDM 解決方案時，管理員可以簡化用戶的設定程序、配置裝置設定，以及分發在這三項服務中購買的 App 和書籍。Apple School Manager 也與「學生資料系統」(SIS) 直接或使用 SFTP 整合，而这三項服務全都可與 Microsoft Azure Active Directory (Azure AD) 使用「跨網域身份識別管理系統」(SCIM) 或聯合身份驗證，以便管理員可以快速建立帳戶。

Apple 為符合 ISO/IEC 27001 和 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 資料私隱和保安實務的獨立證明。如需更多資料，請參閱「Apple 平台認證」中的 [Apple 互聯網服務保安認證](#)。

**附註：**如要了解特定國家或地區是否可使用 Apple 計劃，請參閱 Apple 支援文章：[適用於教育機構和企業的 Apple 計劃和付款方式供應情況](#)。

## 監管裝置

**監管**通常表示裝置是歸機構所有，因而讓其擁有額外的裝置設定和取用限制的控制權限。如需更多資料，請參閱「Apple 平台部署」中的[關於 Apple 裝置監管](#)。

## 啟用鎖保安

Apple 執行「啟用鎖」的方式取決於該裝置是 iPhone 或 iPad、配備 Apple 晶片的 Mac、還是配備 Apple T2 保安晶片以 Intel 為基礎的 Mac。

## 在 iPhone 和 iPad 上的行為

在 iPhone 和 iPad 裝置上，在 iOS 和 iPadOS 設定輔助程式中的 Wi-Fi 選擇螢幕之後，將透過啟用程序來強制執行「啟用鎖」。當裝置指出其正在啟用時，將會向 Apple 伺服器傳送要求以取得啟用憑證。處於「啟用鎖」鎖定狀態的裝置會要求用戶提供已啟用「啟用鎖」之用戶的 iCloud 憑證。除非取得有效的憑證，否則 iOS 和 iPadOS 設定輔助程式將不會進行。

## 在配備 Apple 晶片的 Mac 上的行為

在配備 Apple 晶片的 Mac 中，LLB 會驗證該裝置是否存在有效的 LocalPolicy，以及 LocalPolicy 規則的隨機數值是否與「安全儲存元件」中儲存的值相符。如果出現以下情況，LLB 會開機至 RecoveryOS：

- 目前的 macOS 沒有 LocalPolicy
- 該 macOS 的 LocalPolicy 無效
- LocalPolicy 隨機雜湊值與安全儲存元件中儲存的雜湊值不相符

RecoveryOS 偵測到 Mac 電腦未啟用，並與啟用伺服器聯絡以取得啟用憑證。如果裝置處於「啟用鎖」鎖定狀態，則 RecoveryOS 會要求用戶提供已啟用「啟用鎖」之用戶的 iCloud 憑證。取得有效的啟用憑證後，該啟用憑證密鑰將用來取得 RemotePolicy 憑證。Mac 電腦使用 LocalPolicy 密鑰和 RemotePolicy 憑證來產生有效的 LocalPolicy。除非具有有效的 LocalPolicy，否則 LLB 將不允許 macOS 開機。

## 以 Intel 為基礎的 Mac 電腦上的行為

在配備 Apple T2 晶片的以 Intel 為基礎的 Mac 中，T2 晶片韌體會允許電腦開機至 macOS 之前，驗證是否存在有效的啟用憑證。如果沒有有效的啟用憑證，則由 T2 晶片載入的 UEFI 韌體會負責從 T2 晶片查詢裝備的啟用狀態，並開機至 RecoveryOS 而不是開機至 macOS。RecoveryOS 偵測到 Mac 仍未啟用，並與啟用伺服器聯絡以取得啟用憑證。如果裝置處於「啟用鎖」鎖定狀態，則 RecoveryOS 會要求用戶提供已啟用「啟用鎖」之用戶的 iCloud 憑證。除非具有有效的啟用憑證，否則 UEFI 韌體將不允許 macOS 開機。

## 「受管理的遺失模式」和遙距消除

「受管理的遺失模式」會用來在受監管的裝置失竊時將其找出。找到裝置後，可透過遙距方式加以鎖定或清除。

### 受管理的遺失模式

如配備 iOS 9 或較新版本的受監管 iOS 或 iPadOS 裝置遺失或失竊，流動裝置管理 (MDM) 管理員可以在該裝置上遙距啟用「遺失模式」（稱為「受管理的遺失模式」）。當「受管理的遺失模式」啟用時，目前的用戶會被登出裝置且無法解鎖。螢幕會顯示一則可由管理員自訂的訊息，例如顯示電話號碼，以便有人尋獲裝置時可致電。管理員也可以要求裝置傳送其目前位置（即使「定位服務」已關閉），並可選擇播放聲音。當管理員關閉「受管理的遺失模式」時（這是離開此模式的唯一方式），用戶會在鎖定畫面上看見此動作的通知訊息，或在主畫面上收到提示。

### 遙距消除

管理員和用戶可以遙距清除 iOS、iPadOS 和 macOS 裝置（只在 Mac 已啟用「檔案保險箱」時才能進行即時遙距清除）。藉由從可抹除儲存空間安全地刪除媒體密鑰，讓所有資料無法讀取，即可達成立即遙距清除。如透過 Microsoft Exchange ActiveSync 執行遙距清除，裝置會在執行清除之前登入 Microsoft Exchange 伺服器。

當 MDM 或 iCloud 觸發遙距清除指令時，iPhone、iPad、iPod touch 或 Mac 裝置會傳送確認通知並執行清除作業。

遙距清除在以下的情況下無法使用：

- 透過「用戶註冊」
- 當帳戶是透過「用戶註冊」安裝時使用 Microsoft Exchange ActiveSync
- 如果裝置受監管，使用 Microsoft Exchange ActiveSync

用戶也可以使用「設定」App 來清除所持有的 iOS 和 iPadOS 裝置。如前面提到的，可以將 iOS 和 iPadOS 裝置設定為在連續多次輸入密碼失敗後，自動清除裝置。

## iPadOS 中「共用的 iPad」保安

「共用的 iPad」是在 iPad 部署中使用的一種多重用戶模式，允許用戶共用一部 iPad，同時保持每個用戶的文件和資料獨立。每位用戶可獲得專用和預留的儲存空間，這是以 APFS (Apple 檔案系統) 卷宗形式建立，且受到用戶的憑證保護。「共用的 iPad」需要使用由機構發行和擁有的管理式 Apple ID。

使用「共用的 iPad」，用戶能登入到任何由機構擁有並設定為供多位用戶使用的裝置。用戶資料會分割至個別的目錄，每個目錄都位於其專屬的資料保護網域中，且受 UNIX 權限和沙盒技術保護。在 iPadOS 13.4 或較新版本，用戶也可登入到暫時區段。當用戶登出暫時區段，其 APFS 卷宗會被刪除，且其保留的空間也會歸還到系統。

### 登入「共用的 iPad」

登入「共用的 iPad」時，原生和聯合「管理式 Apple ID」均受支援。首次使用聯合帳戶時，用戶會被導向至身份供應商 (IdP) 的登入入口網站。認證後，系統會為後備「管理式 Apple ID」核發一個短期有效的存取代號，登入程序則與原生「管理式 Apple ID」相似。登入後，「共用的 iPad」上的「設定輔助程式」會提示用戶建立密碼 (憑證)，用於保護裝置本機資料和在日後進行登入畫面的認證。就像單一用戶裝置中，用戶先使用其聯合帳戶登入「管理式 Apple ID」一次，然後使用密碼來解鎖，在「共用的 iPad」上，用戶先使用其聯合帳戶登入一次，之後便可使用已建立的密碼來解鎖。

當用戶未經聯合認證登入時，系統會使用 SRP 通訊協定透過 Apple 的識別服務 (IDS) 對「管理式 Apple ID」進行認證。如認證成功，則會授予一個該裝置專用的短期有效存取代號。如果用戶先前使用過裝置，他們便已有可使用相同憑證解鎖的本機用戶帳戶。

如果用戶之前沒有用過裝置或正在使用暫時區段功能，則「共用的 iPad」會配置一個新的 UNIX 用戶 ID、一個用於儲存用戶個人數據的 APFS 卷宗，以及一個本機鑰匙圈。由於儲存空間是在製作 APFS 卷宗時為用戶分配 (保留)，因此可能沒有足夠的空間來製作新卷宗。在這種情況下，系統會識別已完成將資料同步到雲端的現有用戶，並讓該用戶退出裝置，以便讓新用戶登入。萬一全部現有的用戶都尚未完成上載其雲端資料，新的用戶登入程序便會失敗。如要登入，新用戶將需要等待一個用戶的資料完成同步，或讓管理員強行刪除現有用戶帳戶，這樣會有遺失資料的風險。

如果裝置未連接互聯網 (例如用戶沒有 Wi-Fi 連接點時)，則可能會在有限日數內針對本機帳戶進行認證。在這種情況下，只有擁有先前已存在本機帳戶或暫時區段的用戶可以登入。這個時限過後，即使本機帳戶已存在，用戶仍需於網上進行認證。

用戶的本機帳戶解鎖或建立後，如進行遙距認證，由 Apple 伺服器核發的短期有效代號便會轉換為 iCloud 代號，以允許登入 iCloud。接着用戶的設定會還原，且其文件和資料會從 iCloud 同步。

當用戶的作業階段為使用中且裝置維持線上狀態時，文件和資料皆會在其製作或修改時儲存至 iCloud。此外，背景同步機制可協助確保變更會在用戶登出後推送至 iCloud，或其他使用 NSURLSession 背景作業階段的網絡服務。該用戶的背景同步作業完成後，系統會卸載其 APFS 卷宗，且如果用戶沒有重新登入，就無法再次裝載卷宗。

暫時區段不會與 iCloud 同步資料，且雖然暫時區段可以登入第三方同步服務 (例如 Box 或 Google 雲端硬碟)，但並沒有在暫時區段結束時繼續同步資料的功能。

### 登出「共用的 iPad」

用戶登出「共用的 iPad」時，系統會立即鎖定該用戶的 Keybag，並關閉所有 App。為了加快新用戶登入的速度，iPadOS 會暫時延遲部份的一般登出操作，並向新用戶顯示登入視窗。如果用戶在這段期間 (約 30 秒) 登入，「共用的 iPad」會執行先前延遲的清除程序，作為新用戶登入帳戶程序的一部份。但是如果「共用的 iPad」維持閒置狀態，便會觸發延遲的清除程序。執行清除期間，「登入視窗」會重新啟動，就像是發生另一項登出操作。

暫時區段結束後，「共用的 iPad」將執行完整的登出順序，並立即刪除暫時區段的 APFS 卷宗。

# Apple Configurator 保安

Mac 版 Apple Configurator 採用彈性、安全並以裝置為中心的設計，讓管理員可快速且輕鬆地設定透過 USB 連接 Mac 的一到數十部 iOS、iPadOS 和 tvOS 裝置 (或透過 Bonjour 配對的 tvOS 裝置)，再將裝置交給用戶。使用 Mac 版 Apple Configurator，管理員可以更新軟件、安裝 App 和設定描述檔、重新命名裝置與更改其背景圖片、輸出裝置資料和文件等等。

Mac 版 Apple Configurator 還可以恢復或還原配備 Apple 晶片的 Mac 電腦和配備 Apple T2 保安晶片的 Mac 電腦。以這種方式恢復或還原 Mac 時，包含作業系統 (macOS、用於 Apple 晶片的 RecoveryOS 或用於 T2 的 sepOS) 的最新次要更新項目檔案，將從 Apple 伺服器安全地下載並直接安裝在 Mac 上。成功恢復或還原後，該檔案會從執行 Apple Configurator 的 Mac 中刪除。用戶在任何時候都無法在 Apple Configurator 以外檢閱或使用此檔案。

管理員也可使用 Mac 版 Apple Configurator 或 iPhone 版 Apple Configurator，選擇將裝置加入 Apple School Manager、Apple Business Manager 或 Apple Business Essentials，即使裝置不是直接向 Apple、Apple 授權的經銷商或授權的電信業者購買的也適用。當管理員設定的裝置已手動註冊時，它會如這些服務中的任何其他裝置一般運作，包含強制性監管和流動裝置管理 (MDM) 的註冊。針對並非直接購買的裝置，用戶有 30 天的緩衝期可以將裝置從其中一項服務、監管和 MDM 中釋出。

如 iOS、iPadOS 和 tvOS 裝置完全沒有互聯網連線，且在設定時已連接具備互聯網連線的主機 Mac，機構也可以使用 Mac 版 Apple Configurator 來將其啟用。管理員可以使用其必要的設定 (包括 App、描述檔和文件) 來回復、啟用和準備裝置，而無需連接到 Wi-Fi 或流動網絡。此功能不允許管理員略過非網絡共享式啟用期間通常所需的任何現有「啟用鎖」要求。

## 「螢幕使用時間」保安

「螢幕使用時間」是一項內置功能，用於查看和管理成人及其孩子在 App、網站等上花費的時間。有兩種用戶類型：成人與 (受管理的) 孩子。

雖然「螢幕使用時間」並非新的系統安全功能，但裝置會收集許多資料，也會與其他裝置分享資料，因此了解其如何在這方面保障私隱和保安是相當重要的。「螢幕使用時間」適用於 iOS 12 或較新版本、iPadOS 13.1 或較新版本、macOS 10.15 或較新版本的功能，以及 watchOS 6 或較新版本。

以下的表格描述「螢幕使用時間」的主要功能。

功能	支援的作業系統
檢視用量資料	iOS iPadOS macOS
執行其他功能限制	iOS iPadOS macOS watchOS
設定網絡用量限制	iOS iPadOS macOS
設定 App 用量限制	iOS iPadOS macOS watchOS

功能	支援的作業系統
設定停用時間	iOS iPadOS macOS watchOS

用戶如要管理自己的裝置使用情況，可使用 CloudKit 點對點加密，在與同一個 iCloud 帳戶綁定的不同裝置上同步「螢幕使用時間」控制項目和用量資料。用戶的帳戶必須啟用雙重認證（同步功能預設為開啟）才能使用此功能。螢幕使用時間」取代了舊版 iOS 和 iPadOS 中的「功能限制」功能，以及舊版 macOS 中找到的「分級保護控制」功能。

在 iOS 13 或較新版本、iPadOS 13.1 或較新版本，和 macOS 10.15 或較新版本中，「螢幕使用時間」用戶和受管理的子女會自動在裝置間分享其使用情況（如其 iCloud 帳戶已啟用雙重認證）。用戶清除 Safari 瀏覽記錄或刪除 App 時，對應的用量資料也會從該裝置和所有同步的裝置上移除。

## 家長與「螢幕使用時間」

家長也可使用 iOS、iPadOS 或 macOS 裝置上的「螢幕使用時間」來了解和控制子女的使用情況。如果家長是家庭組織者（在 iCloud 的「家人共享」中），便可檢視子女的用量資料和管理其「螢幕使用時間」設定。當家長開啟「螢幕使用時間」時，子女會收到通知，且也可監看自己的使用情形。家長為子女開啟「螢幕使用時間」時，可設定一組密碼，以便讓子女無法進行變更。子女達到成年年齡時（年齡以所在國家或地區為準）可關閉這個監控功能。

系統會使用點對點加密的「Apple 識別服務」（IDS）通訊協定，在家長和子女的裝置間傳輸用量資料和配置設定。加密的資料會暫時存放在 IDS 伺服器上，直到接收裝置讀取這筆資料（例如當 iPhone、iPad 或 iPod touch 從關機變為開機狀態）。Apple 無法讀取這些資料。

## 「螢幕使用時間」分析

如果用戶開啟「分享 iPhone 與 Apple Watch 分析」，則系統只會收集下列匿名資料，讓 Apple 更了解「螢幕使用時間」的使用情況：

- 是在「設定輔助程式」執行期間開啟「螢幕使用時間」，還是之後才在「設定」中開啟
- 建立「類別」用量限制後的用量變更（90 日內）
- 是否已開啟「螢幕使用時間」
- 是否已開啟「停用時間」
- 使用「要求延長時間」的次數
- App 限制的數量
- 用戶在「螢幕使用時間」設定中檢視用量的次數（根據用戶類型和顯示方式類型（本機、遙距、小工具）分類）
- 用戶忽略限制的次數，依用戶類型分類
- 用戶刪除限制的次數，依用戶類型分類

Apple 不會收集特定 App 或網站用量資料。當用戶在「螢幕使用時間」用量資料中看到 App 列表時，系統會直接從 App Store 提取 App 圖像，其中不會保留來自這些要求的任何資料。

# 詞彙表

**可抹除儲存空間** NAND 儲存區中專門用於儲存加密編譯密鑰的區域，可以直接定址和安全清除。如攻擊者實際持有裝置，可抹除儲存空間便無法提供保護，但其中的密鑰可以用作密鑰階層的一部份，以執行快速清除並提高保安。

**地址空間配置隨機載入 (ASLR)** 作業系統使用的一項技術，可讓透過軟件漏洞肆虐的惡意程式成功率大幅降低。藉由確保記憶體地址和位移無法預測，入侵程式代碼便無法對這些值進行硬式編碼。

**守衛** 在 macOS 中，設計來協助確保用戶的 Mac 上只會執行受信任的軟件。

**安全儲存元件** 晶片的設計包含無法更改的 RO 程式碼、硬件亂數產生器、加密編譯引擎，以及物理篡改偵測。在受支援的裝置上，「安全隔離區」會與「安全儲存元件」配對，以用於儲存反重複隨機數。為讀取和更新隨機數，「安全隔離區」和儲存區晶片會利用安全通訊協定，以協助確保隨機數的獨佔存取權限。此技術已歷經多個世代更迭，提供不同的保安保證。

**系統協同處理器完整保護 (SCIP)** Apple 採用的機制，其設計用意是防止協同處理器韌體遭修改。

**系統軟件授權** 將內置硬件的加密編譯密鑰與網上服務合併的程序，以檢查只有來自 Apple 且合法、適用於受支援裝置的軟件才會被提供，以及在升級時安裝。

**底層啟動程式 (LLB)** 在具有雙階段開機架構的 Mac 電腦上，LLB 會包括由 Boot ROM 呼叫的代碼，接着會載入 iBoot，作為安全啟動鏈的一部份。

**直接記憶體存取 (DMA)** 可讓硬件子系統略過 CPU 直接存取主記憶體的功能。

**指紋紋路角度對應** 從指紋的一部份截取，描述紋路走向和寬度的數學表徵。

**流動裝置管理 (MDM)** 讓管理員遙距管理已註冊裝置的服務。在裝置註冊後，管理員可透過網絡使用 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。

**記憶體控制器** 單晶片系統中的子系統，負責控制 SoC 與其主記憶體之間的介面。

**配置描述檔** 一個由 Apple 簽署的屬性列表 (.plist 檔案)，其中包含一組實體和授權，允許在 iOS 或 iPadOS 裝置上安裝並測試 App。開發配置描述檔會列出開發者選擇要用來臨機操作分發的裝置；分發配置描述檔中包含企業開發 App 的 App ID。

**唯一晶片識別碼 (ECID)** 每部 iOS 及 iPadOS 裝置處理器中的一個 64 位元唯一識別碼。在一部裝置上接聽來電時，會透過低功耗藍牙 (BLE) 4.0 短暫傳播來終止附近與 iCloud 配對的裝置鈴聲。傳播位元組會使用與「接手」傳播相同的方式進行加密。用作個人化程序的一部份，此識別碼並非機密。

**唯一識別碼 (UID)** 在製造過程便直接燒入每個處理器的 256 位元 AES 密鑰。唯一識別碼無法由韌體或軟件讀取，只能由處理器的硬件「AES 引擎」使用。如要取得實際密鑰，攻擊者必須裝載極為複雜且昂貴的實體攻擊來入侵處理器的晶片。UID 與裝置上的任何其他識別碼 (包含但不限於 UDID) 均無關聯。

**密封密鑰保護 (SKP)** 「資料保護」中的一項技術，其會透過只能在硬件上取用的密鑰 (例如「安全隔離區」的 UID) 來保護 (或密封) 加密密鑰。

**密碼衍生密鑰 (PDK)** 衍生密鑰，衍生自用戶密碼與長期 SKP 密鑰和「安全隔離區」UID 的纏結。



**密鑰封裝** 使用一個密鑰來加密另一個密鑰。iOS 及 iPadOS 依照 [RFC 3394](#) 使用 NIST AES 密鑰封裝。

**軟件種子位元** 「安全隔離區 AES 引擎」中的專屬位元，從 UID 產生密鑰時會附加至 UID。每個軟件種子位元都有對應的鎖定位元。只要對應的鎖定位元尚未設定，「安全隔離區 Boot ROM」和作業系統便可獨立變更每個軟件種子位元的值。設定鎖定位元後，軟件種子位元和鎖定位元均無法修改。「安全隔離區」重新啟動時，軟件種子位元和其鎖定位元會被重設。

**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。應用程式處理器、「安全隔離區」和其他協同處理器都是 SoC 的元件。

**媒體密鑰** 加密密鑰階層的一部份，有助提供安全及即時的清除。在 iOS、iPadOS、tvOS 和 watchOS 中，媒體密鑰會將資料卷宗上的後設資料封裝 (因此不可能在沒有媒體密鑰的情況下取用所有檔案專屬密鑰，令受「資料保護」保護的檔案無法取用。) 在 macOS 中，媒體密鑰會將密鑰材料、所有後設資料，和受「檔案保險箱」保護卷宗上的資料封裝。在這兩個情況中，清除媒體密鑰會令已加密的資料無法取用。

**硬件安全模組 (HSM)** 專門用來防止竄改的電腦，可保護並管理電子密鑰。

**統一可延伸韌體介面 (UEFI) 韌體** 此技術取代 BIOS，用於將韌體連接電腦的作業系統。

**統一資源識別碼 (URI)** 一個可識別網頁式資源的字元字串。

**開機切換** 支援在受支援的 Mac 電腦上安裝 Microsoft Windows 的 Mac 工具程式。

**開機進度暫存器 (BPR)** 一組單晶片系統 (SoC) 硬件旗標，讓軟件可用來追蹤裝置進入的開機模式，例如裝置韌體升級 (DFU) 模式和「還原」模式。「開機進度暫存器」旗標設定後就無法清除。這可讓之後的軟件取得系統狀態的信任指標。

**集成電路 (IC)** 亦稱為微晶片。

**群組織別碼 (GID)** 類似 UID，但同一類別中每個處理器的 GID 皆相同。

**裝置韌體升級 (DFU) 模式** 裝置的 Boot ROM 程式碼在等待透過 USB 還原時所處的模式。處於 DFU 模式時畫面為黑色，但在連接到正在執行 iTunes 或 Finder 的電腦時，便會顯示以下提示：「iTunes (或 Finder) 偵測到一部在還原模式中的 (iPad、iPhone 或 iPod touch)。如要與 iTunes (或 Finder) 一同使用，你必須還原此 (iPad、iPhone 或 iPod touch)」。

**資料保護** 受支援的 Apple 裝置之檔案和鑰匙圈保護機制。也可以指 App 用來保護檔案和鑰匙圈項目的 API。

**增強型序列周邊介面 (eSPI)** 針對同步序列通訊設計的多合一匯流排。

**橢圓曲線 Diffie-Hellman Exchange Ephemeral (ECDHE)** 以橢圓曲線為基礎的密鑰交換機制。ECDHE 允許兩方同意一個密鑰，同時防止觀察兩方之間訊息的竊聽者發現該密鑰。

**橢圓曲線電子簽署算法 (ECDSA)** 以橢圓曲線加密技術為基礎的電子簽署算法。

**輸入/輸出記憶體管理單元 (IOMMU)** 輸入/輸出記憶體管理單元。整合式晶片中的子系統，負責控制其他輸入/輸出裝置和周邊設備的地址空間存取。

**隨機數** 用於各種保安通訊協定的唯一一次性號碼。

**檔案系統密鑰** 用於加密每個檔案後設資料的密鑰，包含其類別密鑰。檔案系統密鑰會保存在可抹除儲存空間中，以可進行快速清除而非保密為目的。

**檔案專屬密鑰** 「資料保護」用來在檔案系統加密檔案的密鑰。檔案專屬密鑰由類別密鑰封裝，且儲存在檔案的後設資料內。

**聯合測試工作群組 (JTAG)** 程式設計師和電路開發者使用的標準硬件除錯工具。

**還原模式** 如果無法識別用戶的裝置，還原模式可用於還原許多 Apple 裝置，讓用戶能重新安裝作業系統。

**鑰匙圈** Apple 作業系統和第三方 App 用來儲存和取回密碼、密鑰和其他敏感性憑證的基礎架構和 API 組。

**AES 加密編譯引擎** 實行 AES 的專屬硬件元件。

**AES-XTS** 在 IEEE 1619-2007 中定義的 AES 模式，用於加密儲存空間媒體。

**AES (進階加密標準)** 一種常見的全域加密標準，用於加密資料以確保私密性。

**APFS (Apple 檔案系統)** iOS、iPadOS、tvOS、watchOS 和使用 macOS 10.13 或較新版本的 Mac 電腦之預設檔案系統。APFS 提供高強度加密、空間共享、快照、快速調整目錄大小以及改良的檔案系統基礎。

**Apple 保安獎金** 由 Apple 提供的獎勵，向報告影響現行最新作業系統及最新硬件 (如適用) 的漏洞的研究員提供。

**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 識別服務 (IDS)** Apple 的 iMessage 公用密鑰、APNs 地址、電話號碼和電郵地址的目錄，用於查詢密鑰和裝置地址。

**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 管理員部署機構直接購自 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 管理員部署機構直接購自 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。

**Boot ROM** 裝置在第一次啟動時，由處理器所執行的第一個程式碼。作為處理器的其中一個必要部份，無論是 Apple 或攻擊者皆無法對其進行修改。

**CKRecord** 這是包含儲存於或截取自 CloudKit 的成對密鑰值的字典。

**Data Vault** 此機制由核心強制執行，可保護資料以防未經授權的存取，不論要求權限的 App 本身是否經過沙盒處理。

**HMAC** 以加密編譯雜湊函數為基礎的雜湊式訊息驗證碼。

**iBoot** 所有 Apple 裝置的第二階段開機裝載程式。用來載入 XNU 的代碼，作為安全啟動鏈的一部份。視乎單晶片系統 (SoC) 是第幾代，iBoot 可能由「底層啟動程式」載入或直接由 Boot ROM 載入。

**Keybag** 用於儲存一組類別密鑰的資料結構。每種類型 (用戶、裝置、系統、備份、託管或「iCloud 備份」) 的格式皆相同。

標頭包含以下內容：版本 (在 iOS 12 或較新版本中設定為四)、類型 (系統、備份、託管或「iCloud 備份」)、Keybag UUID、如果 Keybag 已簽署則包含 HMAC，以及用於封裝類別密鑰的方式：與 UID 或 PBKDF2，以及鹽值和反覆運算次數相配合。

類別密鑰列表：密鑰 UUID、類別 (所屬的檔案或鑰匙圈資料保護類別)、封裝類型 (僅限 UID 衍生密鑰、UID 衍生密鑰和密碼衍生密鑰)、封裝的類別密鑰，以及非對稱式類別的公用密鑰。

**NAND** 非揮發性快閃記憶體。

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

**SSD 控制器** 管理儲存媒體 (固態磁碟) 的硬件子系統。

**Tangling** 用戶的密碼轉換為加密編譯密鑰，並使用裝置 UID 強化的過程。這程序可協助確保指定裝置必須使用暴力密碼攻擊才能破解，進而降低發生率，且可避免多部裝置同時受到攻擊。Tangling 演算法為 PBKDF2，使用 AES 密鑰配搭裝置 UID，作為每次反覆運算的偽隨機函式 (PRF)。

**xART** eXtended 反重播技術的縮寫。是一組服務，運用實體儲存架構上的反重播功能，為「安全隔離區」提供經過加密和認證的持續儲存機制。請參閱：安全儲存元件。

**XNU** Apple 作業系統的中央核心。預設為受信任的狀態，且會強制執行安全措施，例如程式碼簽署、沙盒處理、授權檢查和地址空間佈局隨機化 (ASLR)。

**XProtect** 在 macOS 中，以簽署為基礎偵測和移除惡意軟件的防毒技術。

# 文件版本記錄

## 文件版本記錄

日期	摘要
2022 年 12 月	<p>已加入的主題：</p> <ul style="list-style-type: none"><li>• <a href="#">iCloud 進階資料保護</a></li></ul> <p>已更新的主題：</p> <ul style="list-style-type: none"><li>• <a href="#">iCloud 保安概覽</a></li><li>• <a href="#">iCloud 加密</a></li><li>• <a href="#">「iCloud 備份」的保安</a></li><li>• <a href="#">帳戶還原聯絡人保安</a></li><li>• <a href="#">遺產聯絡人保安</a></li></ul>

---

日期	摘要
2022 年 5 月	<p data-bbox="948 216 1065 237">已更新以適用於：</p> <ul data-bbox="948 247 1078 405" style="list-style-type: none"><li data-bbox="948 247 1040 268">• iOS 15.4</li><li data-bbox="948 279 1073 300">• iPadOS 15.4</li><li data-bbox="948 310 1073 331">• macOS 12.3</li><li data-bbox="948 342 1052 363">• tvOS 15.4</li><li data-bbox="948 373 1078 394">• watchOS 8.5</li></ul> <p data-bbox="948 415 1052 436">已加入的主題：</p> <ul data-bbox="948 447 1203 783" style="list-style-type: none"><li data-bbox="948 447 1166 468">• <a href="#">配對 RecoveryOS 的限制</a></li><li data-bbox="948 478 1149 499">• <a href="#">本機作業系統版本 (love)</a></li><li data-bbox="948 510 1036 531">• <a href="#">健康分享</a></li><li data-bbox="948 541 1117 562">• <a href="#">帳戶還原聯絡人保安</a></li><li data-bbox="948 573 1084 594">• <a href="#">遺產聯絡人保安</a></li><li data-bbox="948 604 1203 625">• <a href="#">Tap to Pay on iPhone 的保安</a></li><li data-bbox="948 636 1149 657">• <a href="#">使用 Apple「銀包」通行</a></li><li data-bbox="948 667 1068 688">• <a href="#">存取憑證類型</a></li><li data-bbox="948 699 1122 720">• <a href="#">Apple 錢包中的證件</a></li><li data-bbox="948 730 1170 751">• <a href="#">支援 Siri 的 HomeKit 配件</a></li></ul> <p data-bbox="948 772 1052 793">已更新的主題：</p> <ul data-bbox="948 804 1341 1696" style="list-style-type: none"><li data-bbox="948 804 1170 825">• <a href="#">配備 Touch ID 的精妙鍵盤</a></li><li data-bbox="948 835 1170 856">• <a href="#">Face ID、Touch ID 和密碼</a></li><li data-bbox="948 867 1068 888">• <a href="#">面孔比對保安</a></li><li data-bbox="948 898 1133 919">• <a href="#">以剩餘電量使用特快卡</a></li><li data-bbox="948 930 1235 951">• <a href="#">配備 Apple 晶片的 Mac 之開機模式</a></li><li data-bbox="948 961 1235 982">• <a href="#">配備 Apple 晶片的 Mac 之 LocalPolicy 檔案內容</a></li><li data-bbox="948 993 1312 1014">• <a href="#">iOS、iPadOS 和 macOS 的簽署系統卷宗保安</a></li><li data-bbox="948 1024 1133 1045">• <a href="#">watchOS 的系統保安</a></li><li data-bbox="948 1056 1122 1077">• <a href="#">Apple 安全研究裝置</a></li><li data-bbox="948 1087 1166 1108">• <a href="#">「Apple 檔案系統」的角色</a></li><li data-bbox="948 1119 1170 1140">• <a href="#">保護 App 對用戶資料的存取</a></li><li data-bbox="948 1150 1166 1171">• <a href="#">macOS 的 App 保安簡介</a></li><li data-bbox="948 1182 1170 1203">• <a href="#">在 macOS 中防範惡意軟件</a></li><li data-bbox="948 1213 1101 1234">• <a href="#">iCloud 保安概覽</a></li><li data-bbox="948 1245 1084 1266">• <a href="#">鑰匙圈安全同步</a></li><li data-bbox="948 1276 1166 1297">• <a href="#">「iCloud 鑰匙圈」安全還原</a></li><li data-bbox="948 1308 1166 1329">• <a href="#">使用 Apple Pay 用卡付款</a></li><li data-bbox="948 1339 1187 1360">• <a href="#">Apple Pay 中的非接觸式票證</a></li><li data-bbox="948 1371 1187 1392">• <a href="#">透過 Apple Pay 讓卡無法使用</a></li><li data-bbox="948 1402 1101 1423">• <a href="#">Apple Card 申請</a></li><li data-bbox="948 1434 1105 1455">• <a href="#">Apple Cash 保安</a></li><li data-bbox="948 1465 1284 1486">• <a href="#">將交通卡和 eMoney 卡加至 Apple「銀包」</a></li><li data-bbox="948 1497 1263 1518">• <a href="#">Apple Messages for Business 保安</a></li><li data-bbox="948 1528 1089 1549">• <a href="#">FaceTime 保安</a></li><li data-bbox="948 1560 1101 1581">• <a href="#">iOS 中的車匙保安</a></li><li data-bbox="948 1591 1170 1612">• <a href="#">Apple Configurator 保安</a></li></ul> <p data-bbox="948 1633 1052 1654">已移除主題：</p> <ul data-bbox="948 1665 1166 1686" style="list-style-type: none"><li data-bbox="948 1665 1166 1686">• <a href="#">HomeKit 配件和 iCloud</a></li></ul>

---

---

日期	摘要
2021 年 5 月	<p data-bbox="948 216 1062 237">已更新以適用於：</p> <ul data-bbox="948 247 1078 415" style="list-style-type: none"><li data-bbox="948 247 1029 268">• iOS 14.5</li><li data-bbox="948 279 1062 300">• iPadOS 14.5</li><li data-bbox="948 310 1062 331">• macOS 11.3</li><li data-bbox="948 342 1045 363">• tvOS 14.5</li><li data-bbox="948 373 1078 394">• watchOS 7.4</li></ul> <p data-bbox="948 426 1045 447">已加入的主題：</p> <ul data-bbox="948 457 1289 583" style="list-style-type: none"><li data-bbox="948 457 1175 478">• <a href="#">配備 Touch ID 的精妙鍵盤</a>。</li><li data-bbox="948 489 1240 510">• <a href="#">安全意圖以及與「安全隔離區」的連線</a>。</li><li data-bbox="948 520 1175 541">• <a href="#">自動解鎖和 Apple Watch</a>。</li><li data-bbox="948 552 1289 573">• <a href="#">CustomOS Image4 資料檔雜湊值 (coih)</a>。</li></ul> <p data-bbox="948 594 1045 615">已編輯的主題：</p> <ul data-bbox="948 625 1403 751" style="list-style-type: none"><li data-bbox="948 625 1403 646">• <a href="#">在以剩餘電量使用特快卡中</a>加入了兩個新的「特快模式」交易。</li><li data-bbox="948 657 1175 678">• 編輯了<a href="#">安全隔離區功能摘要</a>。</li><li data-bbox="948 688 1289 709">• 軟件更新內容已加至<a href="#">安全多重開機 (smb3)</a>。</li><li data-bbox="948 720 1208 741">• <a href="#">密封密鑰保護 (SKP)</a> 的其他內容。</li></ul>

---

日期	摘要
2021 年 2 月	<p>已更新以適用於：</p> <ul style="list-style-type: none"> <li>• iOS 14.3</li> <li>• iPadOS 14.3</li> <li>• macOS 11.1</li> <li>• tvOS 14.3</li> <li>• watchOS 7.2</li> </ul> <p>已加入的主題：</p> <ul style="list-style-type: none"> <li>• <a href="#">記憶體安全執行 iBoot</a></li> <li>• <a href="#">配備 Apple 晶片的 Mac 之開機程序</a></li> <li>• <a href="#">配備 Apple 晶片的 Mac 之開機模式</a></li> <li>• <a href="#">配備 Apple 晶片的 Mac 之「啟動磁碟」保安規則控制</a></li> <li>• <a href="#">LocalPolicy 簽署密鑰的建立與管理</a></li> <li>• <a href="#">配備 Apple 晶片的 Mac 之 LocalPolicy 檔案內容</a></li> <li>• <a href="#">iOS、iPadOS 和 macOS 的簽署系統卷宗保安</a></li> <li>• <a href="#">Apple 安全研究裝置</a></li> <li>• <a href="#">密碼監測</a></li> <li>• <a href="#">IPv6 保安</a></li> <li>• <a href="#">iOS 中的車匙保安</a></li> </ul> <p>已更新的主題：</p> <ul style="list-style-type: none"> <li>• <a href="#">安全隔離區</a></li> <li>• <a href="#">硬件咪高風斷線功能</a></li> <li>• <a href="#">以 Intel 為基礎的 Mac 之 RecoveryOS 和診斷環境</a></li> <li>• <a href="#">Mac 電腦的直接記憶體存取保護</a></li> <li>• <a href="#">macOS 的核心延伸功能</a></li> <li>• <a href="#">系統完整保護</a></li> <li>• <a href="#">watchOS 的系統保安</a></li> <li>• <a href="#">在 macOS 中管理檔案保險箱</a></li> <li>• <a href="#">App 對已儲存密碼的存取權限</a></li> <li>• <a href="#">密碼保安建議</a></li> <li>• <a href="#">Apple Cash 保安</a></li> <li>• <a href="#">Apple Messages for Business 保安</a></li> <li>• <a href="#">Wi-Fi 私隱</a></li> <li>• <a href="#">啟用鎖保安</a></li> <li>• <a href="#">Apple Configurator 保安</a></li> </ul>
2020 年 4 月	<p>已更新以適用於：</p> <ul style="list-style-type: none"> <li>• iOS 13.4</li> <li>• iPadOS 13.4</li> <li>• macOS 10.15.4</li> <li>• tvOS 13.4</li> <li>• watchOS 6.2</li> </ul> <p>更新項目：</p> <ul style="list-style-type: none"> <li>• <a href="#">iPad 咪高風斷線功能已加至硬件咪高風斷線功能。</a></li> <li>• <a href="#">Data Vault 已加至保護 App 對用戶資料的存取。</a></li> <li>• <a href="#">在 macOS 中管理檔案保險箱以及命令列工具更新。</a></li> <li>• <a href="#">在 macOS 中防禦惡意軟件中新增「惡意軟件移除工具」。</a></li> <li>• <a href="#">iPadOS 中「共用的 iPad」保安更新。</a></li> </ul>

日期	摘要
2019 年 12 月	<p>合併 iOS 保安指南、macOS 保安概覽和 Apple T2 保安晶片概覽。</p> <p>已更新以適用於：</p> <ul style="list-style-type: none"> <li>• iOS 13.3</li> <li>• iPadOS 13.3</li> <li>• macOS 10.15.2</li> <li>• tvOS 13.3</li> <li>• watchOS 6.1.1</li> </ul> <p>私隱控制、Siri 和 Siri 建議，以及 Safari 智慧型防追蹤已被移除。請參閱 <a href="https://www.apple.com/hk/privacy/">https://www.apple.com/hk/privacy/</a> 以取得該等功能的最新資料。</p>
2019 年 5 月	<p>已更新以適用於 iOS 12.3</p> <ul style="list-style-type: none"> <li>• 支援 TLS 1.3</li> <li>• 修訂 AirDrop 保安的說明</li> <li>• DFU 模式與還原模式</li> <li>• 配件連線的密碼需求</li> </ul>
2018 年 11 月	<p>已更新以適用於 iOS 12.1</p> <ul style="list-style-type: none"> <li>• 群組 FaceTime</li> </ul>
2018 年 9 月	<p>已更新以適用於 iOS 12 安全隔離區</p> <ul style="list-style-type: none"> <li>• OS 完整保護</li> <li>• 以剩餘電量使用特快卡</li> <li>• DFU 模式與還原模式</li> <li>• HomeKit 電視遙控器配件</li> <li>• 非接觸式票證</li> <li>• 學生證</li> <li>• Siri 建議</li> <li>• Siri 的捷徑</li> <li>• 「捷徑」App</li> <li>• 用戶密碼管理</li> <li>• 螢幕使用時間</li> <li>• 保安認證和計劃</li> </ul>
2018 年 7 月	<p>已更新以適用於 iOS 11.4</p> <ul style="list-style-type: none"> <li>• 生物識別政策</li> <li>• HomeKit</li> <li>• Apple Pay</li> <li>• 商務聊天</li> <li>• iCloud 雲端「訊息」</li> <li>• Apple Business Manager</li> </ul>
2017 年 12 月	<p>已更新以適用於 iOS 11.2</p> <ul style="list-style-type: none"> <li>• Apple Pay Cash</li> </ul>

日期	摘要
2017 年 10 月	已更新以適用於 iOS 11.1 <ul style="list-style-type: none"> <li>• 保安認證和計劃</li> <li>• Touch ID/Face ID</li> <li>• 共享的備忘錄</li> <li>• CloudKit 點對點加密</li> <li>• TLS 更新</li> <li>• Apple Pay、在網絡上使用 Apple Pay 付款</li> <li>• Siri 建議</li> <li>• 共用的 iPad</li> </ul>
2017 年 7 月	已更新以適用於 iOS 10.3 <ul style="list-style-type: none"> <li>• 安全隔離區</li> <li>• 檔案資料保護</li> <li>• Keybag</li> <li>• 保安認證和計劃</li> <li>• SiriKit</li> <li>• HealthKit</li> <li>• 網絡保安</li> <li>• 藍牙</li> <li>• 共用的 iPad</li> <li>• 遺失模式</li> <li>• 啟用鎖</li> <li>• 私隱控制</li> </ul>
2017 年 3 月	已更新以適用於 iOS 10 系統保安 <ul style="list-style-type: none"> <li>• 「資料保護」類別</li> <li>• 保安認證和計劃</li> <li>• HomeKit、ReplayKit、SiriKit</li> <li>• Apple Watch</li> <li>• Wi-Fi、VPN</li> <li>• 單一登入</li> <li>• Apple Pay、在網絡上使用 Apple Pay 付款</li> <li>• 信用卡、扣帳卡及預付卡配置</li> <li>• Safari 建議</li> </ul>
2016 年 5 月	已更新以適用於 iOS 9.3 <ul style="list-style-type: none"> <li>• 管理式 Apple ID</li> <li>• Apple ID 雙重認證</li> <li>• Keybag</li> <li>• 保安認證</li> <li>• 遺失模式、啟用鎖</li> <li>• 安全備註</li> <li>• Apple School Manager</li> <li>• 共用的 iPad</li> </ul>



---

日期	摘要
2015 年 9 月	<p data-bbox="948 218 1273 239">已更新以適用於 iOS 9 Apple Watch 啟用鎖</p> <ul data-bbox="948 252 1328 751" style="list-style-type: none"><li data-bbox="948 252 1036 273">• 密碼原則</li><li data-bbox="948 285 1110 306">• Touch ID API 支援</li><li data-bbox="948 319 1208 340">• A8 上的資料保護使用 AES-XTS</li><li data-bbox="948 352 1149 373">• 自動軟件更新的 Keybag</li><li data-bbox="948 386 1036 407">• 認證更新</li><li data-bbox="948 420 1143 441">• 企業級 App 的信任模型</li><li data-bbox="948 453 1136 474">• Safari 書籤的資料保護</li><li data-bbox="948 487 1071 508">• App 傳輸保安</li><li data-bbox="948 520 1045 541">• VPN 規格</li><li data-bbox="948 554 1192 575">• HomeKit 的 iCloud 遙距存取</li><li data-bbox="948 588 1328 609">• Apple Pay 獎勵卡 · Apple Pay 發卡機構的 App</li><li data-bbox="948 621 1166 642">• Spotlight 裝置上索引編列</li><li data-bbox="948 655 1068 676">• iOS 配對模式</li><li data-bbox="948 688 1149 709">• Apple Configurator 2</li><li data-bbox="948 722 1036 743">• 功能限制</li></ul>

---

© 2022 Apple Inc. 保留一切權利。

沒有 Apple 的書面同意，為商業用途而使用 Apple 標誌（鍵盤組合鍵為 Option + Shift + K），可能會違反美國聯邦和州法律，並構成侵犯商標權和  
不公平競爭行為。

Apple、蘋果、Apple 標誌、AirDrop、AirPlay、Apple Books、Apple Card、Apple Music、Apple Pay、Apple TV、Apple Wallet、Apple  
Watch、AppleScript、ARKit、Bonjour、Boot Camp、CarPlay、Face ID、FaceTime、FileVault、Finder、FireWire、Handoff、HealthKit、  
HomeKit、HomePod、HomePod mini、iMac、iMac Pro、iMessage、iPad、iPadOS、iPad Air、iPad Pro、iPhone、iPod touch、iTunes、  
Keychain、Lightning、Mac、Mac Catalyst、Mac mini、Mac Pro、MacBook、MacBook Air、MacBook Pro、macOS、Magic Keyboard、  
Objective-C、OS X、QuickType、Retina、Rosetta、Safari、Siri、Siri Remote、SiriKit、Swift、Spotlight、Touch ID、TrueDepth、tvOS、  
watchOS 和 Xcode 是 Apple Inc. 在美國及其他國家和地區註冊的商標。

App Clips、Find My 和 Touch Bar 是 Apple Inc. 的商標。

App Store、AppleCare、CloudKit、iCloud、iCloud Drive、iCloud Keychain 和 iTunes Store 是 Apple Inc. 在美國及其他國家和地區註冊的  
服務標誌。

Apple Messages for Business 是 Apple Inc. 的服務標誌。

Apple  
One Apple Park Way  
Cupertino, CA 95014  
[apple.com](https://apple.com)

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

Bluetooth® 字標和標誌是 Bluetooth SIG, Inc. 擁有的註冊商標，Apple 對於此類標誌的使用皆經過授權。

Java 為 Oracle 和/或其分支機構的註冊商標。

UNIX® 是 The Open Group 的註冊商標。

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。

Apple 已盡力確保本手冊的內容正確無誤。Apple 對於任何印刷或文字所造成的錯誤概不負責。

部份 App 無法在部份地區使用。App 的適用範圍可能會有所更改。

HK028-00625