



# Apple 平台安全性



2024 年 5 月

# 目錄

<b>Apple 平台安全性簡介</b>	<b>5</b>
對安全性的承諾	6
<b>硬體安全性與生物特徵辨識</b>	<b>7</b>
硬體安全性概覽	7
Apple SoC 安全性	8
安全隔離區	9
Face ID 和 Touch ID	15
硬體麥克風斷線功能	20
可使用備用電量的快速卡片	21
<b>系統安全性</b>	<b>22</b>
系統安全性概覽	22
安全開機	22
簽署系統卷宗安全性	41
安全軟體更新	42
作業系統完整性	43
安全啟動資料連線	45
驗證 iPhone 和 iPad 的配件	45
用於訊息和 IDS 的 BlastDoor	45
Apple 裝置的「封閉模式」安全性	46
其他 macOS 系統安全性功能	46
watchOS 的系統安全性	53
亂數產生	56
Apple 安全研究裝置	57

<b>加密與資料保護</b>	<b>59</b>
加密與資料保護概覽	59
密碼	59
資料保護	61
檔案保險箱	70
Apple 如何保護使用者的個人資料	72
數位簽章與加密	74
<b>App 安全性</b>	<b>76</b>
App 安全性概覽	76
iOS 和 iPadOS 的 App 安全性	77
macOS App 安全性	80
「備忘錄」App 的安全功能	83
「捷徑」App 的安全功能	84
<b>服務安全性</b>	<b>85</b>
服務安全性概覽	85
Apple ID 與管理式 Apple ID	85
iCloud	87
密碼與密碼管理	93
Apple Pay	99
使用 Apple 錢包	110
iMessage	119
Apple Messages for Business 安全性	121
FaceTime 安全性	121
尋找	122
接續互通	124
<b>網路安全性</b>	<b>127</b>
網路安全性概覽	127
TLS 安全性	127
IPv6 安全性`	128
虛擬專用網路 (VPN) 安全性	128
Wi-Fi 安全性	129
藍牙安全性	132
iOS 的超寬頻安全性	133
單一登入安全性	133
AirDrop 安全性	134
iPhone 和 iPad 的 Wi-Fi 密碼共享安全性	135
macOS 的防火牆安全性	135

<b>開發者套件安全性</b>	<b>136</b>
開發者套件安全性概覽	136
HomeKit 安全性	136
iOS、iPadOS 和 watchOS 的 SiriKit 安全性	140
WidgetKit 安全性	140
macOS 的 DriverKit 安全性	140
iOS 和 iPadOS 的 ReplayKit 安全性	141
iOS 和 iPadOS 的 ARKit 安全性	142
<b>安全裝置管理</b>	<b>143</b>
安全裝置管理概覽	143
iPhone 和 iPad 的配對模式安全性	143
行動裝置管理	143
Apple Configurator 安全性	148
「螢幕使用時間」安全性	149
<b>詞彙表</b>	<b>151</b>
<b>文件版本記錄</b>	<b>154</b>
文件版本記錄	154
<b>版權聲明</b>	<b>164</b>

# Apple 平台安全性簡介

Apple 將安全性設計融入平台的核心中。Apple 已打造出全世界最先進的行動作業系統，並以此豐富經驗製作出多種安全性架構，來因應行動裝置、手錶、桌上型電腦和家庭的獨特要求。

每一部 Apple 裝置都結合了**硬體、軟體與服務**，其設計目標是讓每一個部分相互搭配，以達到最高的安全性，並提供透明化的使用者體驗，進而達成確保個人資訊安全的最終目標。例如 Apple 設計的晶片與安全硬體讓各種重要的安全功能得以實現；軟體保護機制可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體更新，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，也保護著整個生態系統，包含使用者在本機、網路上和透過重要網際網路服務執行的任何操作。

我們的產品設計理念除了簡單、直覺和實用性，也重視安全性。重要的安全功能不會因失誤而停用，例如以硬體為基礎的裝置加密。其他功能（如 Face ID 和 Touch ID）則讓裝置安全性的操作更簡單且直覺，進而提升了使用者體驗。由於這些功能中有許多均預設為啟用，因此使用者或 IT 部門無須進行繁複的設定。

本文件將詳細介紹 Apple 平台如何運用各種安全性技術與功能，此外也協助組織在其本身的政策和程序中結合 Apple 平台安全技術與功能，以滿足特定的安全性需求。

本文件內容主要分為以下幾個主題：

- **硬體安全性與生物特徵辨識：**組成 Apple 裝置安全性基礎的晶片與硬體，包含 Apple 晶片、「安全隔離區」、加密引擎、Face ID 和 Touch ID
- **系統安全性：**專為安全開機、更新及 Apple 作業系統持續運作提供的整合硬體和軟體功能
- **加密與資料保護：**若裝置遺失或遭竊，或有未經授權的人員或程序嘗試使用或修改裝置時，對使用者資料進行保護的架構和設計
- **App 安全性：**提供安全的 App 生態系統並讓 App 可安全執行而不會犧牲平台完整性的軟體與服務
- **服務安全性：**Apple 的身分識別、密碼管理、付款、通訊和尋找遺失裝置的服務
- **網路安全性：**對傳輸中的資料提供安全認證和加密的產業標準網路通訊協定
- **開發者套件安全性：**用於以安全且隱私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 裝置進行管理、協助防止在未經授權的情況下使用裝置，並且可在裝置遺失或遭竊時啟用遠端清除的方式

## 對安全性的承諾

Apple 致力於以最先進的隱私與安全技術來幫助保障客戶個人資訊的安全；並採用全方位的方式來保護企業環境中的公司資料。Apple 也提供 Apple Security Bounty 計畫來獎勵發現漏洞的研究人員。計畫詳情和獎金類別可於 <https://security.apple.com/bounty/> 取得。

我們擁有專業的安全團隊，專門為所有的 Apple 產品提供支援。這個團隊提供產品安全稽核與測試，開發中和已發行的產品均適用。Apple 團隊亦提供安全工具和訓練，並積極監控威脅和新安全問題的報告。Apple 為「[資安事件應變小組論壇](#)」(Incident Response and Security Teams, FIRST) 的成員。

Apple 在安全及隱私保護方面持續努力突破可能的極限。它在整個產品系列 (從 Apple Watch 到 iPhone 和 iPad，再到 Mac 中的 M 系列晶片) 使用特製 Apple 晶片，不僅支援高效計算，也提供安全性。例如，Apple 晶片提供了安全開機、Face ID 和 Touch ID 以及「資料保護」的基礎。此外，由 Apple 晶片驅動提供的安全性功能 (例如「核心完整保護」、「指標認證碼」和「快速權限取用限制」)，有助於阻止常見類型的惡意利用。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 Apple 平台與生俱來的強大安全功能，我們建議組織審核其 IT 部門和安全政策，以確保可充分使用到這些平台所提供的多重安全技術。

若要深入瞭解如何向 Apple 提報問題以及訂閱安全性通知，請參閱：[回報安全性或隱私漏洞](#)。

Apple 堅信隱私權是基本人權，提供多種內建控制項目與選項，可讓使用者決定 App 如何及何時可使用其資訊及使用哪些資訊。如需深入瞭解 Apple 對於隱私權的作法、Apple 裝置上的隱私權控制以及 Apple 隱私權政策，請參閱：<https://www.apple.com/tw/privacy>。

**【注意】**除非另有說明，否則本文件適用於下列作業系統版本：iOS 17.3、iPadOS 17.3、macOS 14.3、tvOS 17.3 和 watchOS 10.3。

# 硬體安全性與生物特徵辨識

## 硬體安全性概覽

為了確保軟體的安全性，其必須位於具有內建安全性的硬體上。這正是搭載 iOS、iPadOS、macOS、tvOS 和 watchOS 的 Apple 裝置配備採用安全功能設計的矽晶片之原因。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其他矽晶片。首重安全性的硬體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。這類元件包含開機 ROM（負責組成用於安全開機的硬體信任根）、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 Apple 系統單晶片（SoC）上的元件，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 安全晶片的 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開機 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 的生物特徵辨識資料。

儲存加密必須快速而有效。同時，它無法洩漏用於建立加密密鑰關係的資料（或密鑰材料）。AES 硬體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訊。這可協助確保 Apple 的「資料保護」和「檔案保險箱」技術確實保護使用者的檔案，且不會洩漏長效加密密鑰。

Apple 已設計安全開機功能來保護最低層級的軟體避免遭竄改，且開機時只會允許載入 Apple 所信任的作業系統軟體。安全性的起點為無法更改的程式碼「開機 ROM」，這些程式碼又稱為**硬體的信任根**，在製造 Apple SoC 過程中即置入其中。在配備 T2 晶片的 Mac 電腦上，macOS 安全開機的信任根從 T2 開始。（T2 晶片和「安全隔離區」也會分別使用各自的開機 ROM 來執行自己的安全開機程序；這與 A 系列、M1 和 M2 晶片安全開機完全相同。）

「安全隔離區」也會處理來自 Apple 裝置上的 Face ID 和 Touch ID 感測器的臉部和指紋資料。這會提供安全認證，同時確保使用者生物特徵辨識資料的隱私及安全。在許多情況下，這也讓使用者可享有較複雜的長密碼帶來的安全性，以及存取或購物時享有快速認證的便利性。

# Apple SoC 安全性

如今 Apple 設計的矽晶片組成了所有 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 的世界級矽晶片設計團隊一直在建構和改良 Apple 系統單晶片 (SoC)，並因此打造出一套具有擴充性的架構，此架構的設計適用於所有裝置，而且在安全性功能方面處於業界領先地位。此安全性功能的共同基礎只為自行設計矽晶片以搭配其軟體使用的公司才可能提供。

Apple 晶片的設計和製造旨在實現多項特定的系統安全性功能，詳列如下：

功能	A10	A11、S3	A12、A13、A14 S4 至 S9	A15、A16、A17	M1、M2、M3
核心完整保護	✓	✓	✓	✓	✓
快速權限取用限制	✗	✓	✓	✓	✓
系統副處理器完整保護	✗	✗	✓	✓	✓
指標認證碼	✗	✗	✓	✓	✓
頁面保護層	✗	✓	✓	✗	✗ 請見下方附註 1。
安全頁表監視器	✗	✗	✗	✓ 請見下方附註 2。	✗

**附註 1:**「頁面保護層」(PPL) 要求平台只執行已簽署且受信任的程式碼；此安全性模式不適用 macOS。

**附註 2:**A15、A16 和 A17 支援「安全頁表監視器 (SPTM)」，並在支援的平台上取代了「頁面保護層」。

Apple 設計的矽晶片也專門啟用了下方詳述的「資料保護」功能。

功能	A10、A11 S3	A12 至 A17 S4 至 S9 M1、M2、M3
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	✗	✓

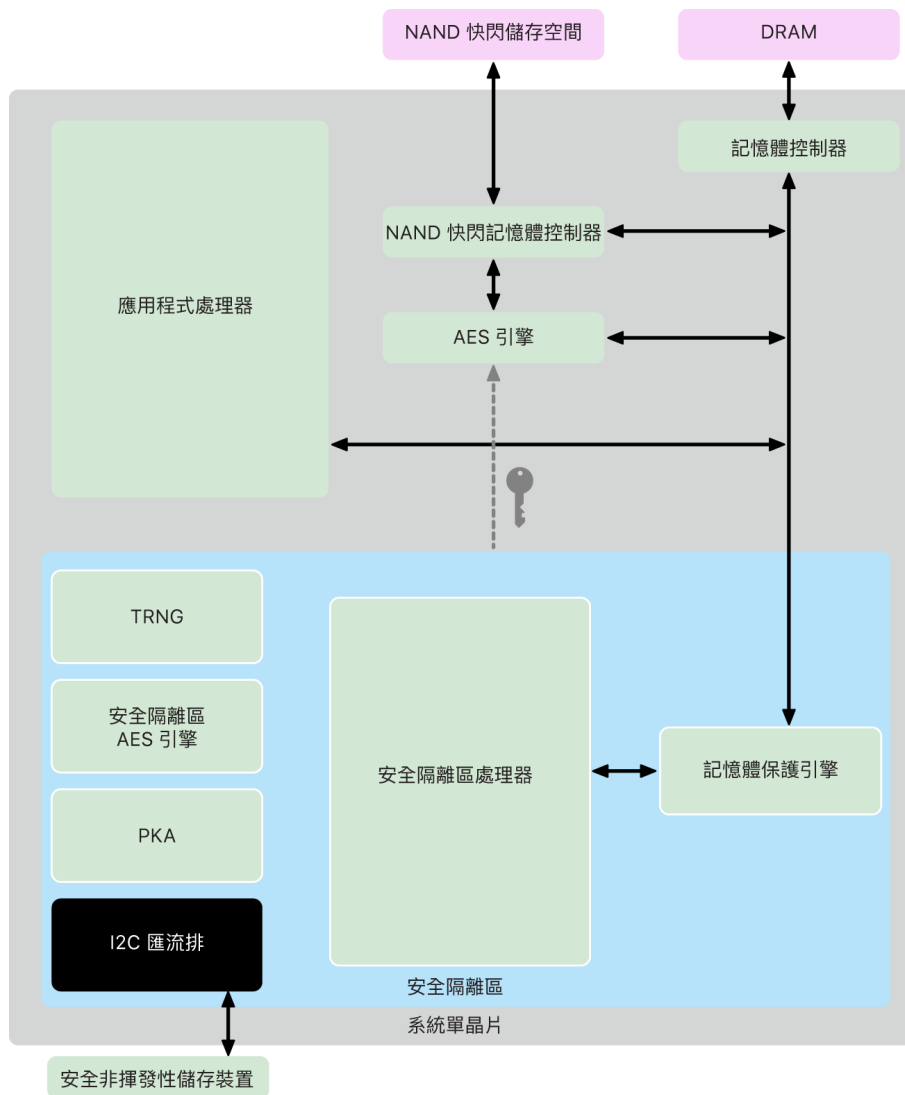


# 安全隔離區

「安全隔離區」是以下最新版本之 iPhone、iPad、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 系統單晶片 (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，以提供額外的安全性，並且即使在「應用程式處理器」核心受到威脅時，也可以確保敏感性使用者資料的安全。其遵循與 SoC 整體相同的設計原則：開機 ROM 用於建立硬體信任根、AES 引擎用於確保有效且安全的加密編譯作業，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訊安全儲存在外接的儲存裝置上 (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」是大部分 iPhone、iPad、Mac、Apple TV、Apple Watch 和 HomePod 版本的硬體功能，包含：

- iPhone 5s 或後續機型
- iPad Air 或後續機型
- 配備 Apple 晶片的 Mac 電腦
- 配備觸控列且搭載 Apple T1 晶片的 MacBook Pro 電腦 (2016 和 2017 年)
- 採用 Intel 架構並配備 Apple T2 安全晶片的 Mac 電腦
- Apple TV HD 或後續機型
- Apple Watch Series 1 或後續機型
- 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」提供主要的運算電力。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體共享同一執行核心的惡意軟體從旁進行攻擊。

「安全隔離區處理器」採用 Apple 特製的 L4 microkernel 版本。其設計宗旨為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搭配反重播功能、安全開機、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，「安全隔離區開機 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」發出錯誤訊號。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。為了協助防止安全性相關重要的資料遭到重放，「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「**反重放值**」。反重放值的作用是 CMAC 認證標記的額外調校。所有記憶體區塊的反重放值都使用根植於「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」會**更新**反重放值和完整性樹狀結構中最高至 SRAM 的每個層級。對於讀取操作，「記憶體保護引擎」會**驗證**反重放值和完整性樹狀結構中最高至 SRAM 的每個層級。反重放值不相符的處理方式與認證標記不相符的處理方式相同。

在 Apple A14、M1 或後續 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。這一切造就了強大的記憶體保護機制，同時無須犧牲效能或軟體的複雜度。

## 安全隔離區開機 ROM

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

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，「安全隔離區開機 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「安全隔離區開機 ROM」。將 sepOS 映像檔拷貝到「安全隔離區」的受保護記憶體後，「安全隔離區開機 ROM」將會檢查映像檔的加密雜湊和簽章，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「安全隔離區開機 ROM」會將控制權轉移到 sepOS。如果簽章無效，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 和較新的 SoC 上，「安全隔離區開機 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 SoC 上，「安全隔離區」包含一個「開機監視器」，其設計可確保開機 sepOS 的雜湊值具有更強的完整性。

系統啟動時，「安全隔離區處理器」的「系統副處理器完整保護」(SCIP) 設定可協助防止「安全隔離區處理器」執行「安全隔離區開機 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，「安全隔離區開機 ROM」會向「開機監視器」傳送一個要求，其中包含載入之 sepOS 的位址和大小。收到要求後，「開機監視器」將重置「安全隔離區處理器」，對已載入的 sepOS 進行雜湊處理、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。隨著系統繼續開機，只要使新程式碼可執行，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」也會執行的雜湊中包含重要的安全性參數。

開機完成後，「開機監視器」會定案執行中的雜湊，並將其發送到「公共密鑰加速器」以用於與 OS 綁定的密鑰。此處理序經設計可確保即使「安全隔離區開機 ROM」中存在漏洞，也無法略過作業系統密鑰的綁定。

## 真亂數產生器

「真亂數產生器」(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。

製造時隨機產生的 UID 會與 SoC 融合在一起。自 A9 SoC 起，製造期間，「安全隔離區」TRNG 會產生 UID，並使用完全在「安全隔離區」中執行的處理序寫入融合中。這個處理序可保護 UID 在製造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 來保護特定裝置的密鑰。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，因此若將內置 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。其他受保護裝置專用的密鑰包含 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 式儲存空間都是透過此方式加密。

「安全隔離區」也具有裝置群組 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」是一個硬體區塊，用於依據 AES 密碼執行對稱加密編譯。「AES 引擎」的設計用意在於使用定時和「靜態功率分析」(SPA) 來阻止洩漏資訊。從 A9 SoC 開始，「AES 引擎」也包括「動態功率分析」(DPA) 對策。

「AES 引擎」支援硬體和軟體密鑰。硬體密鑰衍生自「安全隔離區」的 UID 或 GID。這些密鑰位於「AES 引擎」中，即使在 sepOS 軟體中也不可見。雖然軟體可以要求使用硬體密鑰進行加密和解密作業，但其不能擷取密鑰。

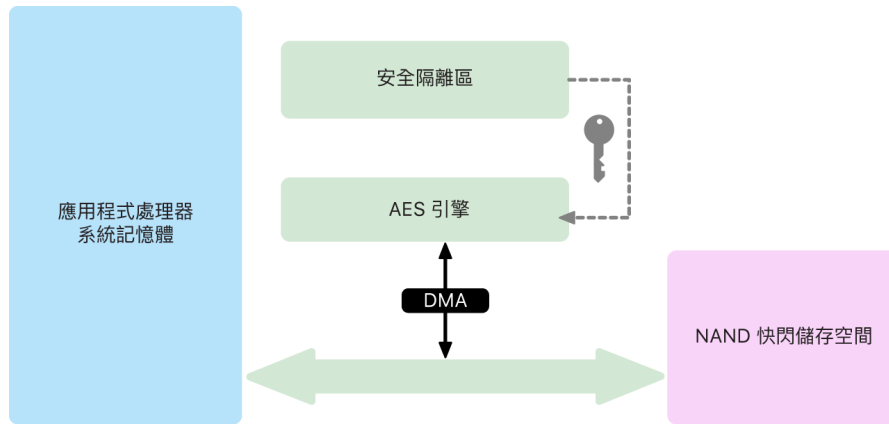
在 Apple A10 和較新的 SoC 上，「AES 引擎」包括可鎖定的種子位元，這些種子位元會讓從 UID 或 GID 衍生的密鑰更多元。這樣就可以根據裝置的操作模式來限制資料的存取。例如，當從裝置韌體升級 (DFU) 模式開機時，可鎖定的種子位元便用於拒絕存取受密碼保護的資料。如需更多資訊，請參閱：[密碼](#)。

## AES 引擎

每部具有「安全隔離區」的 Apple 裝置也配備專用的 AES256 加密引擎 (稱為「AES 引擎」)，其內建於 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 或後續晶片 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，只能存取包含使用者資料的記憶體 (透過 DMA 加密引擎)。

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」，此設計是為了防止「安全隔離區」以外的任何軟體對其進行存取。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」，藉此解封密鑰。「AES 引擎」絕對不會向軟體洩漏解封的密鑰。

**【注意】**「AES 引擎」是獨立於「安全隔離區」和「安全隔離區 AES 引擎」的元件，但是其作業與「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) 簽章和加密演算法。PKA 的用意在於透過定時阻止洩漏資訊和如 SPA 和 DPA 之類的從旁攻擊。

PKA 支援軟體和硬體密鑰。硬體密鑰衍生自「安全隔離區」的 UID 或 GID。這些密鑰位於 PKA 中，即使在 sepOS 軟體中也不可見。

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 和較新版 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。雜湊由「安全隔離區開機 ROM」或 Apple A13 和較新的 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，以及用來在沒有使用者授權的狀態下進行重要系統更動時，協助防止密鑰材料遭存取，藉此改善受密碼保護的資料安全性。

## 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。所有使用者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 和更新 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、硬體亂數產生器、依設備的唯一加密密鑰、加密引擎，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較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 salt、一個 128 位元密碼驗證器、一個 8 位元計數器和一個 8 位元嘗試次數最大值。對計數器密碼箱的存取會透過經過加密和認證的協定。

計數器密碼箱含有解鎖受密碼保護使用者資料所需的熵。若要存取這些使用者資料，配對的「安全隔離區」必須從使用者的密碼和「安全隔離區」的 UID 衍生正確的密碼熵值。嘗試解鎖的行為如果是來自配對的「安全隔離區」以外，將無法得知使用者的密碼。如果超過了密碼嘗試次數的限制（例如，在 iPhone 上嘗試 10 次），則「安全儲存元件」將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」傳送密碼熵值和嘗試次數最大值。「安全儲存元件」會使用其亂數產生器來產生 salt 值。接著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 salt 值。「安全儲存元件」會使用計數 0、所提供的嘗試次數最大值、衍生的密碼驗證器值和 salt 值來初始化計數器密碼箱。「安全儲存元件」接著會將產生的密碼箱熵值傳回「安全隔離區」。

若要從計數器密碼箱中擷取密碼箱熵值，「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嘗試次數最大值，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個演算法，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資料的密鑰，根植於儲存在計數器密碼箱中的熵裡。如需更多資訊，請參閱：[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 臉孔或 Touch ID 指紋
- Face ID 或 Touch ID 重置
- 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 中不包含專用的硬體安全性功能，也不保證對熵的獨占存取權（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 (而非 Touch ID) 的裝置上,「安全神經引擎」將 2D 影像和深度圖轉換為使用者臉度的數學表示法。

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、M1 或後續晶片開始,「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。專用的硬體安全性控制器在「應用程式處理器」和「安全隔離區」任務之間切換,在每次轉換時重置「神經引擎」狀態,以確保 Face ID 的資料安全。專用引擎適用於記憶體加密、認證和存取控制。同時,它使用單獨的加密密鑰和記憶體範圍將「安全神經引擎」限制為授權的記憶體區域。

## 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。為了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」的其餘部分大得多。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 重置才會重新啟動。

## 安全隔離區功能摘要

**【注意】**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	OS 綁定的密鑰
A11	加密、認證和重放預防	EEPROM	DPA 保護和可鎖定的種子位元	OS 綁定的密鑰
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	OS 綁定的密鑰
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	OS 綁定的密鑰
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	OS 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	OS 綁定的密鑰和開機監視器
A14 至 A17	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	OS 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	OS 綁定的密鑰
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	OS 綁定的密鑰

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	OS 綁定的密鑰
S6 至 S9	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	OS 綁定的密鑰
T2	加密和認證	EEPROM	DPA 保護和可鎖定的種子位元	OS 綁定的密鑰
M1、M2、M3	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	OS 綁定的密鑰和開機監視器

## Face ID 和 Touch ID

### Face ID 和 Touch ID 安全性

密碼對於 Apple 裝置的安全性至關重要。同時，使用者需要能夠快速取用其裝置，每天甚至會超過 100 次。生物辨識認證提供了一個方式，可以保留高強度密碼的安全性，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，但是在大部分的情況下，它們確實可以讓取用裝置的動作變得更快、更輕鬆。

Apple 的生物特徵安全架構有賴於生物特徵辨識感測器與「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。感測器會擷取生物特徵辨識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、加密和儲存相對應的 Face ID 和 Touch ID 樣板資料。在比對期間，「安全隔離區」會將來自生物特徵辨識感測器的傳入資料與儲存的樣板進行比較，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）。此架構支援內含感測器和「安全隔離區」的裝置（如 iPhone、iPad 和許多 Mac 系統），以及將感測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 安全性

只要注視螢幕，Face ID 即可安全地解鎖受支援的 Apple 裝置。Face ID 透過原深感測相機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使用者的臉部幾何結構。Face ID 會使用神經網路來判斷螢幕注視、比對和防止造假，使用者在使用支援的裝置時，便可以藉由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，並嚴密保護使用者生物特徵辨識資料的隱私與安全。

Face ID 的設計用意為確認使用者注視螢幕、提供比對錯誤率低的穩固認證方式，以及減少數位和物理性造假。

原深感測相機會在以下情況自動尋找使用者的面孔：當使用者喚醒配備 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使用者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 會辨識使用者的眼睛是否張開且直視著裝置，以確認螢幕注視並進行解鎖的意圖；針對輔助使用功能，當啟用「旁白」時會停用 Face ID 注視檢查，且可在需要時分別停用。戴口罩使用 Face ID 時，一律需要偵測注視。

在原深感測相機確認偵測到注視螢幕的面孔後，會發出並讀取超過數千個紅外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，經過數位簽章後傳送到「安全隔離區」。為了防止數位和物理性造假，原深感測相機隨機排序擷取到的一系列 2D 影像和深度圖，並發出因裝置而異的隨機圖形。「安全神經引擎」的一部分神經引擎（受「安全隔離區」保護）會將這些資料轉換為數學表示資料，並將這個表示式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使用者面孔之數學表示資料。

## Touch ID 安全性

Touch ID 是指紋感應系統，有助於更快、更輕鬆地對受支援的 Apple 裝置進行安全的存取。此技術可從任何角度來讀取指紋，隨著感測器每次使用時識別出其他重疊的節點而持續擴大指紋圖，逐漸提高對使用者指紋辨識的能力。

配備 Touch ID 感測器的 Apple 裝置可使用指紋來解鎖。Touch ID 並未取代使用裝置密碼或使用者密碼的需要，裝置開機、重新開機或登出（在 Mac 上）後仍需輸入密碼。在某些 App 中，Touch ID 也可用於代替裝置密碼或使用者密碼，例如用於在「備忘錄」App 中解鎖受密碼保護的備忘錄、解鎖受密鑰鏈保護的網站，以及解鎖支援的 App 密碼。但是某些情況下一律須使用裝置密碼或使用者密碼（例如更改現有的裝置密碼或使用者密碼，或是移除現有指紋登記或建立新指紋時）。

當指紋感測器偵測到有手指觸碰，便會觸發進階成像陣列來掃描手指，並將掃描結果傳送到「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 感測器是內置於配有「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，其為一種有損性的程序，重建使用者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」讀取為樣板，以便針對未來比對項目進行比較，但不含任何識別資訊。此資料絕對不會流出裝置，不會傳送給 Apple，也不會納入裝置備份中。

## 內置 Touch ID 頻道安全性

「安全隔離區」與內置 Touch ID 感測器之間的通訊是透過序列週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。資料會藉由區段密鑰進行加密與認證，該區段密鑰是透過每個 Touch ID 感測器出廠時佈建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 感測器安全性極高、具隨機性，且都不同。區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 的巧控鍵盤

配備 Touch ID 的巧控鍵盤（和配備 Touch ID 與數字鍵盤的巧控鍵盤）在外接鍵盤中提供了 Touch ID 感測器，可搭配配備 Apple 晶片的任何 Mac 使用。配備 Touch ID 的巧控鍵盤具備生物辨識感測器的角色；其不會儲存生物辨識樣板、執行生物辨識比對或執行安全性原則（例如，必須在 48 小時未解鎖後輸入密碼）。必須先將配備 Touch ID 的巧控鍵盤中的 Touch ID 感測器與 Mac 上的「安全隔離區」嚴密配對，然後才能使用它，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 感測器相同的方式來執行安全性原則。Apple 在出廠時對 Mac 隨附之配備 Touch ID 的巧控鍵盤進行了配對處理。如有需要，配對作業也可以由使用者執行。配備 Touch ID 的巧控鍵盤一次只能與一台 Mac 安全地配對，但是 Mac 最多可以與五個配備 Touch ID 的巧控鍵盤維持安全配對。

配備 Touch ID 的巧控鍵盤與內置 Touch ID 感測器相容。如果在配備 Touch ID 的巧控鍵盤上出現了內置 Mac Touch ID 感測器上的手指，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 的巧控鍵盤之間的通訊，該鍵盤配備了硬體「公共密鑰加速器 (PKA)」區塊，以提供證明以及搭配硬體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 的巧控鍵盤可用於 Touch ID 操作之前，需要將其安全地與 Mac 配對。配對時，Mac 上的「安全隔離區」和配備 Touch ID 的巧控鍵盤中的 PKA 區塊會交換公共密鑰（根植於受信任的 Apple CA），並且它們使用硬體持有的證明密鑰和臨時 ECDH 來安全地證明其身分。在 Mac 上，此資料受「安全隔離區」保護；在配備 Touch ID 的巧控鍵盤上，此資料則受 PKA 區塊保護。安全配對後，Mac 和配備 Touch ID 的巧控鍵盤之間的所有 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分使用 NIST P-256 曲線的臨時 ECDH 密鑰進行加密。如需更多有關使用無線模式鍵盤的資訊，請參閱：[藍牙安全性](#)。



## 確定配對意圖

若要首次執行某些 Touch ID 操作 (例如, 註冊新的指紋), 使用者必須實際確認其想要在 Mac 上使用配備 Touch ID 的巧控鍵盤的意圖。藉由在使用者介面指示時按兩次 Mac 電源按鈕或藉由成功比對先前已在 Mac 上註冊的指紋, 可以確認實際意圖。如需更多資訊, 請參閱: [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 使用者密碼並在配備 Touch ID 的巧控鍵盤上按兩次 Touch ID 按鈕。後者可讓使用者即使沒有進行 Touch ID 比對, 也可以確認實際意圖。

## 配備 Touch ID 的巧控鍵盤的頻道安全性

為了協助確保配備 Touch ID 的巧控鍵盤中的 Touch ID 感測器與配對的 Mac 上的「安全隔離區」之間的通訊頻道安全, 需要執行以下操作:

- 配備 Touch ID 的巧控鍵盤 PKA 區塊和「安全隔離區」之間的安全配對, 如上所述
- 配備 Touch ID 感測器的巧控鍵盤與其 PKA 區塊之間的安全頻道

配備 Touch ID 感測器的巧控鍵盤與其 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」及其內置感測器之間建立安全頻道, 所使用的技術相同。)

## Face ID、Touch ID 和密碼

若使用 Face ID 或 Touch ID, 使用者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, 使用者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, 因為使用者無需經常輸入密碼。Face ID 和 Touch ID 並不會取代使用者的密碼, 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, 因為安全性高的密碼是使用者的 iPhone、iPad、Mac 或 Apple Watch 以加密方式保護使用者資料的基礎。

## 需要裝置密碼或密碼的時間點

使用者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特徵辨識。以下高度要求安全性的作業一律會要求輸入密碼:

- 更新軟體
- 清除裝置
- 檢視或更改密碼設定
- 安裝設定描述檔
- 在 Mac 上的「系統設定」(macOS 13 或以上版本) 中解鎖「隱私權與安全性」面板
- 在 Mac 上的「系統偏好設定」(macOS 12 或較早版本) 中解鎖「安全性與隱私權」面板
- 在 Mac 上的「系統設定」(macOS 13 或以上版本) 中解鎖「使用者與群組」面板 (如果已開啟「檔案保險箱」)
- 在 Mac 上的「系統偏好設定」(macOS 12 或較早版本) 中解鎖「使用者與群組」面板 (如果已開啟「檔案保險箱」)

若裝置處於以下任一狀態, 也需要使用密碼:

- 裝置剛剛開機或重新開機。
- 使用者已登出其 Mac 帳號 (或尚未登入)。
- 使用者超過 48 小時未解鎖裝置。
- 使用者在 156 小時 (六天半) 內未使用密碼來解鎖裝置, 並且在 4 小時內未使用生物辨識技術來解鎖裝置。
- 裝置收到了遠端鎖定命令。

- 使用者同時按住任一個音量鍵和「睡眠/喚醒」按鈕 2 秒，然後按下「取消」，退出了關機/「SOS 緊急服務」。
- 嘗試五次生物辨識比對失敗（不過在後幾次失敗時，為了使用上的方便性，裝置應該會提供輸入密碼的選項，而非使用生物辨識功能）。

在 iPhone 上啟用戴口罩使用 Face ID 後，在以下其中一項使用者動作後的後續 6.5 個小時內可供使用：

- 嘗試比對 Face ID 成功（佩戴或不戴口罩）
- 裝置密碼驗證
- 透過 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 個小時。

當 iPhone 或 iPad 上的 Face ID 或 Touch ID 啟用時，會在按下「睡眠/喚醒」按鈕時立即鎖定裝置，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 便需要成功比對（或是選擇輸入密碼）。

人群中隨機一人可使用 Face ID 解鎖使用者的 iPhone 或 iPad 的機率為百萬分之一（包含開啟戴口罩使用 Face ID 時）。對於使用者的 iPhone、iPad、Mac 機型配備 Touch ID 和搭配巧控鍵盤的機型，此機率低於五萬分之一。此機率會隨著登記多個指紋（五個指紋的機率增加為一萬分之一）或面孔（兩個面孔的機率增加為五十萬分之一）而增加。為提供額外的保護，Face ID 和 Touch ID 皆只允許五次比對失敗，其後便需要輸入密碼才能存取使用者的裝置或帳號。使用 Face ID，錯誤比對的機率較高的情況包括：

- 長相與使用者相似的雙胞胎與兄弟姊妹
- 13 歲以下孩童（因為他們的獨特臉部特徵可能還尚未定型）

在這兩種情況下戴口罩使用 Face ID 時，機率會進一步增加。若使用者對於比對錯誤存有疑慮，Apple 建議使用密碼來認證。

## 面孔比對安全性

系統會在「安全隔離區」內利用專為此目的訓練的神經網路進行面孔比對。為了開發面孔比對神經網路，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，以便為多元使用者提供更高的準確度。Face ID 設計為可在使用者戴著帽子、圍巾、眼鏡、隱形眼鏡和各式太陽眼鏡時使用。Face ID 還支援在 iPhone 12 和 iOS 15.4 或以上版本的 iPhone 裝置上戴著口罩解鎖。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。專為偵測和抵制造假而訓練的一個額外神經網路，可防範有心人士企圖以照片或面具解鎖裝置。Face ID 資料（包含使用者面孔的數學表示資料）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，不會傳送給 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：

- 登記期間計算出的使用者面孔數學表示資料
- 某幾次解鎖時對使用者的面孔進行計算所產生的數學表示資料（如果 Face ID 認為可用於增強未來比對效果）

系統不會儲存一般操作期間捕捉的面孔影像，而是計算成數學表徵來登記 Face ID 或是比對已登記的 Face ID 資料，並且在計算完成後立即捨棄這些面孔影像。

## 改善 Face ID 比對功能

為了改善比對效能，以及跟進面孔和外貌的自然變化，Face ID 會逐漸擴充它所儲存的數學表示資料。比對成功時，Face ID 可能會使用新計算出的數學表示資料（若品質夠高）進行額外有限次數的比對，然後再捨棄這些資料。相反地，如果 Face ID 無法辨識面孔，但是比對品質高於特定標準，且使用者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示資料增強登記的 Face ID 資料。如果使用者停止用這筆新的 Face ID 資料進行比對，或是在進行有限次數的比對後，系統會捨棄這筆資料；選取重置 Face ID 選項時，新資料也會遭捨棄。這些增強程序可讓 Face ID 跟進使用者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

## 解鎖裝置或使用者帳號

若 Face ID 或 Touch ID 已關閉，在裝置或帳號鎖定時，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。除非使用者輸入密碼來解鎖裝置或帳號，否則便無法存取該類別的檔案和鑰匙圈項目。

若 Face ID 或 Touch ID 已開啟，則不會在裝置或帳號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。使用者嘗試解鎖裝置或帳號時，若裝置偵測到成功的比對，它便會提供密鑰來解除封裝「資料保護」密鑰，裝置或帳號便會解鎖。此流程藉由要求「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。

當裝置重新開機時，Face ID 或 Touch ID 解鎖裝置或帳號時所需的密鑰會遺失；「安全隔離區」在需要輸入密碼的任何條件滿足時便會捨棄密鑰。

## 透過 Apple Pay 安全進行購買

Face ID 和 Touch ID 也可以搭配 Apple Pay 使用，方便使用者在商店、App 內和網站上輕鬆且安全地進行購買：

- **在商店中使用 Face ID：**若要使用 Face ID 授權店內付款，使用者必須先按兩下側邊按鈕確認付款意圖，裝置可以透過「按兩下」這種實體手勢來確認使用者意圖，而且此手勢會直接連結到「安全隔離區」，因而可以防止惡意程序進行偽造。使用者接著用 Face ID 進行認證，然後將裝置靠近感應式付款讀卡機。通過 Face ID 認證後可選擇另一種 Apple Pay 付款方式，這需要重新進行認證，不過使用者不用再按兩下側邊按鈕。
- **在 App 內和在網站上使用 Face ID：**若要在 App 內和網站上付款，使用者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。如果使用者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：**若為 Touch ID，付款意圖是透過啟用 Touch ID 感測器的手勢並成功比對使用者指紋來完成確認。

## 使用系統提供的 API

第三方 App 可使用系統提供的 API 來要求使用者透過 Face ID、Touch ID 或密碼進行認證，且支援 Touch ID 的 App 無需任何更動就可自動支援 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 或已登記之使用者的相關資料。

## 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」比對成功或是使用裝置密碼或帳號密碼時才將它們釋出。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 確認使用者已設定密碼。App 開發者可執行以下任何操作：

- 要求「認證 API」的作業不得改回使用 App 密碼或裝置密碼來當作備用認證方式。他們可以查詢使用者是否已登記，以便允許在對安全性有高度要求的 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。

## 購買和核准購買

使用者也可設定 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辨識認證，然後核發用於簽署儲存要求的 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，即可確認使用者意圖的方式。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 或後續機型
- Apple Watch Series 1 或後續機型
- iPad Pro (所有機型)
- iPad Air (2020)
- 配備 Apple 晶片的 Mac 電腦

有了此連結，使用者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 root 特權或核心中的軟體也不會遭欺騙。

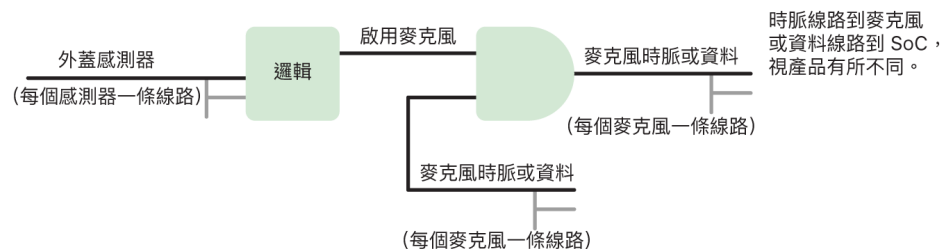
此功能用於 Apple Pay 交易過程中以及在將配備 Touch ID 的巧控鍵盤與配備 Apple 晶片的 Mac 配對完成時，確認使用者的意圖。當使用者介面提示時，按兩下相對應的按鈕 (Face ID) 或指紋掃描 (Touch ID) 可發出確認使用者意圖的訊號。如需更多資訊，請參閱：[透過 Apple Pay 安全進行購買](#)。具有 Apple T2 安全晶片且沒有觸控列的 MacBook 機型，支援以「安全隔離區」和 T2 韌體為基礎的類似機制。

## 硬體麥克風斷線功能

所有配備 Apple 晶片的 Mac 筆記型電腦和採用 Intel 架構並配備 Apple T2 安全晶片的 Mac 筆記型電腦，均具有硬體斷線功能，可在上蓋闔上時停用麥克風。在所有配備 T2 晶片的 13 吋 MacBook Pro 和 MacBook Air 筆記型電腦、所有配備 T2 晶片的 MacBook 筆記型電腦 (2019 年和後續機型) 以及所有配備 Apple 晶片的 Mac 筆記型電腦上，這個斷線功能完全是透過硬體來實現。此斷線功能的設計在於防止任何軟體 (即使具有 macOS 中的根或核心權限，以及 T2 晶片上的軟體或其他韌體) 在上蓋闔上時使用麥克風。(硬體相機不會斷線，因為其視野會完全被闔上的上蓋遮蔽。)

2020 年開始的 iPad 機型也配備硬體麥克風斷線功能。將 iPad 裝入 MFI 認證的保護殼 (包含 Apple 所販售的) 並闔上時，麥克風硬體就會中斷連線。此設計是為了防止任何軟體可使用麥克風音訊資料，即使該軟體具有 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體邏輯導入：



在具有硬體麥克風截斷功能的每項產品中，一或多個外蓋感測器會使用互動的某些物理屬性 (例如，霍爾效應感測器或鉸鏈角度感測器) 來偵測外蓋或外盒的實際閉合程度。對於需要校正的感測器，在裝置生產期間會設定參數，並且校正過程包括不可逆的硬體鎖定，以防止對感測器上敏感參數進行任何後續更動。這些感測器發出直接的硬體訊號，該訊號通過一組簡單、不可重新程式設計的硬體邏輯。這些邏輯提供去抖動、滯後作用和/或最多 500ms 的延遲，然後再停用麥克風。視產品的不同，可以藉由停用在麥克風和 SoC 之間傳輸資料的線路或藉由停用麥克風模組中使其處於作用狀態的其中一個輸入線路，例如時脈線路或類似的有效控制，來導入此訊號。

## 可使用備用電量的快速卡片

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來支援「快速卡片」交易。支援的 iPhone 裝置會自動對以下票卡提供此功能：

- 專為「快速交通卡」設計的付款卡或交通卡
- 開啟「快速模式」的識別證

按下側邊按鈕時，電池圖像會顯示電量低，並且以文字表示可使用快速卡片。此時 NFC 控制器仍會執行「快速卡片」交易，如同 iOS 仍在正常運作一般，差別在於交易只會以觸覺回饋通知表示（不會顯示視覺通知）。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。若是由使用者執行的標準關機，此功能則不會運作。

# 系統安全性

## 系統安全性概覽

系統安全性是以 Apple 硬體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。系統安全性包含開機程序、軟體更新及保護電腦系統資源，如 CPU、記憶體、磁碟、軟體程式和儲存的資料。

最新版的 Apple 作業系統安全性最佳。Apple 安全性的重要部分是**安全開機**，它可以在開機時保護系統免受惡意軟體感染。安全開機會在晶片中開始，並透過軟體建立信任鏈，交付控制權之前，每個步驟的設計都是為了確保下一個步驟可正確運作。此安全模式不僅支援 Apple 裝置的預設開機程序，也支援 Apple 裝置上的多種復原模式與即時更新。「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。更新系統的設計在於防止降級攻擊，因此無法將裝置降回舊版作業系統（攻擊者知道入侵舊版系統的方式）並藉此方式竊取使用者資料。

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、配備 Apple 晶片的 Mac、Apple Watch、Apple TV 和 HomePod 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 硬體平台支援的功能。

## 安全開機

### iPhone 和 iPad 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，如此一來，每個步驟都必須在驗證信任鏈結束後才能繼續。這些元件包含啟動程式、核心、核心延伸功能和行動網路基頻韌體。此安全開機鏈旨在確認底層的軟體未經竄改。

開啟 iPhone 和 iPad 裝置後，其「應用程式處理器」會立即執行唯讀記憶體（稱為開機 ROM）中的程式碼。此類無法更改的程式碼（稱為**硬體的信任根**）是在製造晶片時完成設定，且已間接獲得信任。開機 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 Bootloader 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。若為配備 A9 或較早 A 系列處理器的裝置，會載入額外的 Low-Level Bootloader (LLB) 階段並由開機 ROM 加以驗證，接著會載入並驗證 iBoot。

視硬體而定，載入或驗證以下階段失敗的處理方式會有所不同：

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

在兩種情況下，裝置都必須透過 USB 連接 Finder (macOS 10.15 或以上版本) 或 iTunes (macOS 10.14 或較早版本)，並回復為出廠預設值。

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

- **DFU 模式**: 在配備 Apple A12 或較新版 SoC 的裝置上透過開機 ROM 設定
- **復原模式**: 在配備 Apple A10、S2 和較新版 SoC 的裝置上透過 iBoot 設定

在具有行動數據連線功能的裝置上，行動網路基頻子系統會使用已簽署的軟體以及由基頻處理器驗證的密鑰，來執行其他安全開機作業。

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

## 為 iBoot 加入記憶體安全機制

在 iOS 14 和 iPadOS 14 或以上版本中，Apple 修改了用來建立 iBoot Bootloader 的 C 編譯器工具鏈以改善其安全性。修改後的工具鏈採用了某些程式碼，其設計是為了防止在 C 程式中常會遇到的記憶體和型別安全問題。例如，這有助於防止下列類別中大部分的弱點：

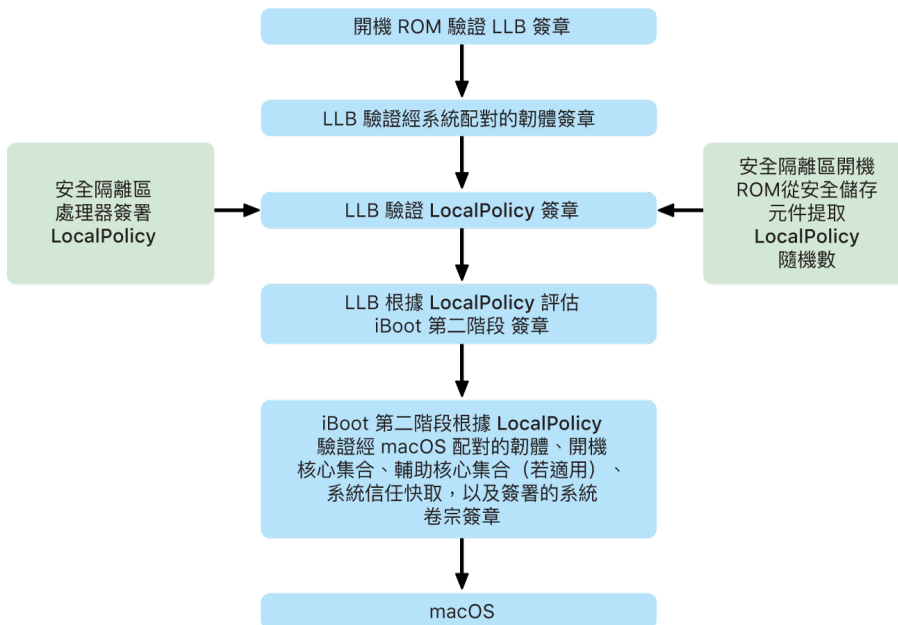
- **緩衝區溢位**: 避免方式是確保所有指標都攜帶界限資訊，這些資訊應在存取記憶體時經過驗證
- **堆積利用**: 藉由分離堆積資料與其後設資料及正確刪除雙重釋出等錯誤情況
- **型別混淆**: 避免方式是確保所有指標都攜帶執行階段型別資訊，這些資訊應在指標轉換作業期間經過驗證
- **「釋出後使用」錯誤所造成的型別混淆**: 避免方式是依靜態型別分隔所有動態記憶體配置

配備 Apple A13 仿生晶片或後續晶片的 iPhone 以及配備 A14 仿生晶片或後續晶片的 iPad 均可使用此技術。

## 配備 Apple 晶片的 Mac 電腦

### 在配備 Apple 晶片的 Mac 上進行開機程序

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開機 ROM 中的程式碼。在配備 Apple 晶片的 Mac 上，macOS 安全開機不只會驗證作業系統程式碼本身，也會驗證經授權使用者設定的安全性規則甚至是 kext (提供支援，但不建議使用)。

當 LLB (其代表「低階 Bootloader」) 啟動時, 隨即會驗證簽章並為 SoC 內部核心 (例如儲存體、顯示器、系統管理和 Thunderbolt 控制器) 載入與系統配對的韌體。LLB 也負責載入 LocalPolicy (以「安全隔離區處理器」簽署的檔案)。LocalPolicy 檔案描述使用者針對系統開機和執行階段安全性規則選擇的設定。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。

為了協助防止先前的 LocalPolicy 重放, LLB 必須從連接「安全隔離區」的「安全儲存元件」查詢反重放值。若要這麼做, 其會使用「安全隔離區 ROM」, 並確保 LocalPolicy 中的反重放值與「安全儲存元件」中的反重放值相符。這有助於防止進行安全性升級後舊版 LocalPolicy (設定的安全性可能較低) 重新套用於系統。因此, 配備 Apple 晶片的 Mac 上的安全開機不僅能防止作業系統版本回復, 也能防止安全性規則降級。

LocalPolicy 檔案會記錄作業系統是設為「完整安全性」、「較低安全性」還是「寬鬆安全性」。

- **完整安全性:** 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體。
- **較低安全性:** 系統會指示 LLB 信任與作業系統綁定的「全域」簽章。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, 此安全性模型便被稱為「較低安全性」。這也是支援開機核心延伸功能 (kext) 所必須採用的規則層級。
- **寬鬆安全性:** 系統的行為類似「較低安全性」, 也使用 iBoot 的全域簽章驗證, 不過也會告知 iBoot 應接受某些以「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。這個規則層級支援使用者建立、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「完整安全性」執行, 則 LLB 會評估 iBoot 的個人化簽章。如果它以「較低安全性」或「寬鬆安全性」執行, 則會評估全域簽章。任何簽章驗證錯誤都會導致系統開機至 RecoveryOS 以提供修復選項。

LLB 接力給 iBoot 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 傳遞給自己的 LocalPolicy 相關資訊。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詢 AuxKC, 驗證它是使用與 LocalPolicy 相同的密鑰以「安全隔離區」簽署, 並驗證其雜湊與 LocalPolicy 中儲存的雜湊相符。如果 AuxKC 通過驗證, iBoot 會透過「開機核心集合」將它放入記憶體, 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副處理器完整保護 (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, 以確認核心將掛載的檔案系統完全通過完整性驗證。

## 配備 Apple 晶片的 Mac 所具備的開機模式

配備 Apple 晶片的 Mac 具有下述的開機模式。

模式	按鍵組合	說明
macOS	在關機狀態下按下並放開電源按鈕。	<ol style="list-style-type: none"><li>1. 開機 ROM 接力給 LLB。</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) 的根簽章雜湊。</li></ol>



模式	按鍵組合	說明
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. 開機 ROM 接力給 LLB。</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，然後再接力給配對 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，會嘗試開機進入回降 RecoveryOS。</li> </ol>
回降 RecoveryOS	在開機狀態下 <b>按兩下並按住</b> 電源按鈕。	<ol style="list-style-type: none"> <li>1. 開機 ROM 接力給 LLB。</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，然後再接力給 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>
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 正常照常啟動 macOS，其也會設定 <b>nvr</b> 變數，該變數會告知 iBoot 在下次開機時不要載入 AuxKC。</li> <li>3. 系統重新啟動並開機至目標卷宗，但 iBoot 不會載入 AuxKC。</li> </ol>

## 配對 RecoveryOS 的限制

在 macOS 12.0.1 或以上版本中，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。這種設計對於採用 Intel 架構的 Mac 電腦的使用者來說很熟悉，但在配備 Apple 晶片的 Mac 上，它提供了額外的安全性和相容性保證。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 才能執行安全性降級操作。這有助於保護新版本 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 安裝作業的安全性設定，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 或以上版本的安裝作業，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 安裝項目降級安全性設定，但不能為任何其他 macOS 安裝項目降級。

若要讓任何 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，可以前往「系統設定」中的「一般」>「啟動磁碟」（macOS 13 或以上版本）或「系統偏好設定」中的「啟動磁碟」（macOS 12 或較早版本），或透過啟動任何 RecoveryOS 並在選擇卷宗時按住 Option 鍵來完成此操作。

**【注意】**回降 RecoveryOS 無法執行任何 macOS 安裝項目的降級。

## 配備 Apple 晶片的 Mac 所提供的「啟動磁碟」安全性規則控制機制

### 概覽

與採用 Intel 架構的 Mac 上的安全性規則不同，配備 Apple 晶片的 Mac 上的安全性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 執行個體和安全性規則。因此，**作業系統選擇器**已加入至「開機安全性工具程式」。



在配備 Apple 晶片的 Mac 上，「系統安全性工具程式」會指出整體使用者設定的 macOS 安全性狀態，例如啟動 kext 或「系統完整保護」(SIP) 的設定。如果更改安全性設定，會大幅降低安全性或導致系統更容易遭入侵，使用者必須按住電源按鈕來進入 RecoveryOS (讓惡意軟體無法觸發訊號，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(或支援)韌體密碼，所有重要的更動都已經藉由使用者授權來把關。如需更多 SIP 的資訊，請參閱：[系統完整保護](#)。

「完整安全性」和「較低安全性」可從 RecoveryOS 使用「開機安全性工具程式」來設定。但是「寬鬆安全性」只能由使用者從指令行工具存取，他們必須接受 Mac 安全性會大幅下降。

### 「完整安全性」規則

「完整安全性」為預設值，其行為與 iOS 和 iPadOS 類似。下載軟體準備安裝時，macOS 並非使用軟體隨附的全域簽章，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」簽章。若簽署要求的一部分包含「唯一晶片識別碼 (ECID)」(此案例中為 Apple CPU 專屬的唯一 ID)，該簽章就是個人化簽章。簽署伺服器傳回的簽章會變為唯一簽章，且只有該特定 Apple CPU 可以使用。當「完整安全」規則生效，「開機 ROM」和 LLB 會協助確認指定的簽章不僅是由 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。



比起典型的全域簽章作法，使用線上簽署伺服器也能更有效防禦回復攻擊。在全域簽署系統中，安全性 epoch 可能已更新過很多次，但從未見過最新版軟體的系統無從得知。例如，即使目前實際的安全性 epoch 為 5，目前認為屬於安全性 epoch 1 的電腦，仍可接受安全性 epoch 2 的軟體。透過 Apple 晶片線上簽署系統，簽署伺服器可拒絕為並非屬於最新安全性 epoch 的軟體建立簽章。

此外，如果攻擊者在安全性 epoch 更改後發現漏洞，便無法直接將屬於舊版 epoch 的有漏洞軟體從系統 A 中挑出，然後套用到系統 B 以進行攻擊。屬於舊版 epoch 的有漏洞軟體是針對系統 A 進行個人化以協助避免遭轉移，因此無法用於攻擊系統 B。在所有機制通力合作下，可更有效保證攻擊者無法透過刻意將有漏洞的軟體放到 Mac 上的方式，來規避最新軟體提供的防護。但是擁有 Mac 管理者使用者名稱和密碼的使用者可隨時選擇最適合其使用情況的安全性規則。

### 「較低安全性」規則

「較低安全性」類似配備 T2 晶片的 Mac (Intel 架構) 上的「中等安全性」，廠商 (此案例中為 Apple) 會為程式碼產生數位簽章來宣告其為該廠商所提供。這樣的設計有助於防止攻擊者插入未簽署的程式碼。Apple 將這類簽章稱為「全域」簽章，因為可在任何 Mac 上使用 (目前已設定「較低安全性」規則的 Mac)，且次數不限。「較低安全性」本身無法抵禦回復攻擊 (雖然未授權的作業系統更動可能導致使用者資料變為無法存取。如需更多資訊，請參閱：[配備 Apple 晶片的 Mac 上所具備的核心延伸功能](#))。

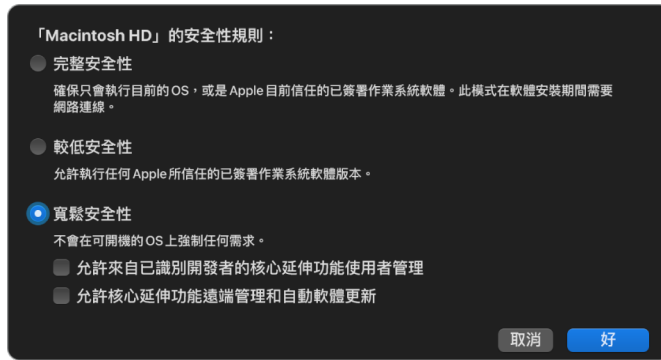


除了允許執行舊版 macOS 之外，其他作業會要求使用「較低安全性」，這會為使用者的系統安全性帶來風險，例如引入第三方核心延伸功能 (kext)。kext 的權限與核心相同，因此第三方 kext 中的任何漏洞都可能導致作業系統遭全面入侵。正因如此，強力建議開發者在未來配備 Apple 晶片的 Mac 電腦上移除 macOS 中的 kext 支援前，先採用系統延伸功能。即使第三方 kext 已啟用，仍不能將其載入隨選即用核心中，相反地，kext 會併到輔助核心集合 (AuxKC) 中，這個集合的雜湊儲存在 LocalPolicy 裡，因此它們需要重新啟動。如需更多有關產生 AuxKC 的資訊，請參閱：[在 macOS 中安全延伸核心](#)。

### 「寬鬆安全性」規則

「寬鬆安全性」適用於接受讓自己的 Mac 處於極度不安全狀態風險的使用者。此模式與配備 T2 晶片的 Mac (Intel 架構) 之「無安全性」模式不同。若使用「寬鬆安全性」，簽章驗證仍會在整個安全開機鏈中執行，但是若將規則設為「寬鬆」，就會告訴 iBoot 應接受本機「安全隔離區」簽署的開機物件，例如使用者產生的「開機核心集合」(從自訂 XNU 核心來源建立)。如此一來，「寬鬆安全性」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。這樣的設計是為了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。



「寬鬆安全性」與配備 T2 晶片的 Mac (Intel 架構) 之「無安全性」模式另一個不同之處：某些過去可獨立控制的安全性降級現在具有先決條件。最值得注意的是，若要在配備 Apple 晶片的 Mac 上停用「系統完整保護」(SIP)，使用者必須認知到自己是將系統設為「寬鬆安全性」。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，若在配備 Apple 晶片的 Mac 上停用 SIP，便會在產生 AuxKC 期間停用 kext 簽章強制執行，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，現在若要停用 SIP，必須由擁有 LocalPolicy 簽署密鑰存取權的使用者進入 RecoveryOS (按住電源按鈕) 並進行認證。這使得純軟體攻擊者、甚至是實際真實的攻擊者都很难停用 SIP。

如果無法從「開機安全性工具程式」App 降級為「寬鬆安全性」。使用者只能在 RecoveryOS 中從「終端機」執行指令來降級，例如 `csrutil` (會停用 SIP)。使用者降級後，發生的這個事件會反映在「開機安全性工具程式」中，因此使用者可輕鬆將安全性設為更安全的模式。

**【注意】** 配備 Apple 晶片的 Mac 不需要或支援特定的媒體開機規則，因為從技術面來看所有開機都是在本機執行。如果使用者選擇從外接媒體開機，必須先使用經認證的 RecoveryOS 重新啟動對該作業系統版本進行個人化。此重新啟動會在內置磁碟上製作一個 LocalPolicy 檔案，用來從儲存在外接媒體上的作業系統執行受信任的開機。這表示從外接媒體啟動的設定一律會在每個作業系統上直接啟用，且已要求使用者授權，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，或者在執行連線式清除安裝時，Mac 會從暫時回復 RAM 磁碟執行程式碼以初始化其預設狀態。在此過程中，回復環境將建立一對新的公用密鑰和專用密鑰，它們分別保存在「安全隔離區」中。專用密鑰稱為**所有者身分密鑰 (OIK)**。如果任何 OIK 已經存在，則會在此過程中銷毀它。回復環境還會初始化用於「啟用鎖定」的密鑰：**使用者身分密鑰 (UIK)**。該過程的一部分 (這對配備 Apple 晶片的 Mac 而言是專有程序) 是在為「啟用鎖定」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「啟用鎖定」取得 UIK 認證 (例如，由於該裝置目前與「尋找我的 Mac」帳號相關聯並且回報為遺失)，則該裝置將無法繼續建立 Local Policy。如果向裝置核發了**使用者身分憑證 (ucrt)**，則該 ucrt 在 X.509 v3 擴充套件中包含伺服器所施加的策略限制和使用者要求的策略限制。

成功擷取「啟用鎖定」/ucrt 後，其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，則它將驗證公用密鑰，並傳回**所有者身分憑證 (OIC)**，其由 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 根憑證具有內建信任，這讓其可信任 OIC，也可讓其信任 LocalPolicy 完整簽章。

## RemotePolicy 限制

所有 Image4 檔案 (並非只有 Local Policy) 都包含對 Image4 資訊檔評估設定的限制。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。進行簽章評估時, Image4 驗證庫會在憑證中查詢特殊憑證限制 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, 若為「個人化」簽章, 憑證限制就會包含「ECID 必須存在」, 而若是「全域」簽章, 則會包含「ECID 必須不存在」。這些限制的設計是為了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 資訊檔。

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「完整安全性」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「遠端規則」隨機數雜湊 (**rpnh**)。僅當對「尋找我的 Mac」和「啟用鎖定」採取了如註冊、取消註冊、遠端鎖定和遠端清除之類的操作時, **rpnh** 以及 RemotePolicy 才會更改。「遠端規則」限制是在使用者身分密鑰 (UIK) 認證時確定和指定的, 並已登入到已核發的「使用者身分憑證」(ucrt)。伺服器確定某些「遠端規則」限制, 例如 ECID、ChipID 和 BoardID。這樣的設計是為了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「遠端規則」限制, 以協助防止本機策略的安全性降級, 且不會同時提供取用目前 OIK 所需的本機驗證和裝置鎖定啟用之帳戶的遠端驗證。

## 配備 Apple 晶片的 Mac 上的 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 平台上安全開機鏈物件的相關資訊。在 Image4 安全開機模式中, 安裝軟體時要求藉由向 Apple 簽署伺服器傳送簽署要求來啟用安全性規則。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「開機 ROM」或 LLB 這類軟體會評估這些已簽署的 Image4 檔案和 4CC。

### 作業系統間的所有權接力

對「所有者身分密鑰」(OIK) 的取用權限稱為「所有權」。需有所有權才能允許使用者在更改規則或軟體後退出 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。這意味著它通常受使用者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使用者明確同意, 才能將所有權移交給第二個作業系統上的使用者。但是, 當安裝程式從第一個作業系統執行時, 第二個作業系統的使用者尚不存在。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使用者。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「安裝使用者」以移交所有權

當執行「安裝輔助程式」並針對第二個空白卷宗鎖定安裝時, 提示會詢問使用者是否要將目前卷宗中的使用者複製為第二個卷宗的第一個使用者。如果使用者說「好」, 則建立的「安裝使用者」實際上是從所選使用者的密碼和硬體密鑰衍生的 KEK, 其接著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, 提示輸入該使用者的密碼, 以允許其取用「安全隔離區」中針對新作業系統的 OIK。如果使用者選擇不拷貝使用者, 則仍以相同的方式建立「安裝使用者」, 但是會使用空密碼, 而非使用者密碼。對於某些系統管理方案, 則會有第二個流程。但是, 想要進行多卷宗安裝並以最安全的方式執行所有權切換的使用者, 應一律選擇將使用者從第一個作業系統拷貝到第二個作業系統。

## 配備 Apple 晶片之 Mac 上的 LocalPolicy

在配備 Apple 晶片的 Mac 上，本機安全性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。這個軟體可利用使用者的憑證和主要 CPU 的開機模式，判斷誰可以更改安全性規則，以及從哪個開機環境更改。這有助於防止惡意軟體將規則降級以取得更多權限，進而利用安全性規則控制來影響使用者。

### LocalPolicy 資訊檔屬性

LocalPolicy 檔案包含一些架構 4CC，這幾乎在所有 Image4 檔案中都會出現，例如主機板或機型 ID (BORD)、用來表示特定 Apple 晶片的資訊 (CHIP) 或唯一晶片識別碼 (ECID)。但是 4CC 只著重於使用者可設定的安全性規則。

**【注意】** Apple 使用已配對 One True RecoveryOS (1TR) 一詞來表示開機進入配對 RecoveryOS (使用按壓實體電源按鈕 (按一下並按住))。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，讓侵入 macOS 的純軟體攻擊者無法達到開機環境。

### LocalPolicy 隨機數雜湊 (lpth)

- **類型:** OctetString (48)
- **可變環境:** 1TR、RecoveryOS、macOS
- **說明:** lpth 用於 LocalPolicy 的反重播機制。這是 LocalPolicy 隨機數 (LPN) 的 SHA384 雜湊，儲存在「安全儲存元件」中，且可使用「安全隔離區開機 ROM」或「安全隔離區」存取。原始反重放值永遠不會讓「應用程式處理器」得知，僅會讓 sepOS 得知。攻擊者若想說服 LLB 他們先前擷取的 LocalPolicy 為有效，需將一個值放入「安全儲存元件」，而這個值必須雜湊為與他們想重播的 LocalPolicy 中的 lpth 值相同。通常系統上會有一個有效的 LPN，但軟體更新期間除外，同時會有兩個有效，以便在發生更新錯誤時回復以啟動舊版軟體。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 lpth 值重新簽署。當使用者更改安全設定或分別使用不同的新 LocalPolicy 來建立新的作業系統時，就會發生此更動。

### 「遠端規則」隨機數雜湊 (rpth)

- **類型:** OctetString (48)
- **可變環境:** 1TR、RecoveryOS、macOS
- **說明:** rpth 的行為與 lpth 相同，但是只會在遠端規則更新時隨之更新，例如更改「尋找」註冊狀態時。使用者在其 Mac 上更改「尋找」狀態時，便會發生此更動。

### RecoveryOS 隨機數雜湊 (ronh)

- **類型:** OctetString (48)
- **可變環境:** 1TR、RecoveryOS、macOS
- **說明:** 此 ronh 的行為與 lpth 相同，但是只存在於 RecoveryOS 的 LocalPolicy 中。當系統 RecoveryOS 更新時會隨之更新，例如軟體更新時。使用獨立於 lpth 和 rpth 的反重放值，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 (藉由移除其「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」帳號的 iCloud 密碼) 時，可重新啟用作業系統。當使用者更新系統 RecoveryOS 或建立新的作業系統時，便會發生此更動。

### 下一階段 Image4 資訊檔雜湊 (nsih)

- **類型:** OctetString (48)
- **可變環境:** 1TR、RecoveryOS、macOS
- **說明:** 此 **nsih** 欄位代表 Image4 資訊檔資料結構的 SHA384 雜湊，描述已啟動的 macOS。macOS Image4 資訊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) 的測量。當系統指示 LLB 啟動指定的 macOS 時，其設計會確保 macOS Image4 資訊檔的雜湊附加至在 LocalPolicy 的 **nsih** 欄位中擷取到的 iBoot 相符項目。如此一來，**nsih** 便能知道使用者是為了哪個作業系統製作 LocalPolicy。因此使用者可在執行軟體更新時，間接更改 **nsih** 值。

### Cryptex1 Image4 資訊檔雜湊 (spih)

- **類型:** OctetString (48)
- **可變環境:** 1TR、RecoveryOS、macOS
- **說明:** **spih** 欄位代表 Cryptex1 Image4 資訊檔資料結構的 SHA384 雜湊。Cryptex1 Image4 資訊檔包含其 Cryptex 的測量值、檔案系統密封以及相關的信任快取。macOS 啟動時，XNU 核心和「頁面保護層」會確保 Cryptex1 Image4 資訊檔的雜湊與 iBoot 從 LocalPolicy 的 **spih** 欄位發佈的相符。使用者可在安裝「快速安全回應」或執行軟體更新時，間接更改 **spih** 值。Cryptex1 Image4 資訊檔雜湊可獨立於下一階段 Image4 資訊檔雜湊進行更新。

### Cryptex1 世代 (stng)

- **類型:** 64 位元未簽署整數
- **可變環境:** 1TR、RecoveryOS、macOS
- **說明:** **stng** 欄位是計數值，代表上次在 LocalPolicy 中更新 Cryptex1 Image4 資訊檔雜湊的時間。在「頁面保護層」評估本機政策以套用傳入的 Cryptex 期間，會提供反重放值以取代 **lpmh**。使用者可在安裝「快速安全回應」(RSR) 或軟體更新時，間接提高 **stng** 值。

### 輔助核心集 (AuxKC) 規則雜湊 (auxp)

- **類型:** OctetString (48)
- **可變環境:** macOS
- **說明:** **auxp** 是一種 SHA384 雜湊，是來自「使用者授權 kext 列表」(UAKL) 的規則。這用於產生 AuxKC 時，以協助確保只有使用者授權的 kext 包含在 AuxKC 中。**smb2** 是設定此欄位的先決條件。使用者從「系統設定」中的「隱私權與安全性」(macOS 13 或以上版本) 或「系統偏好設定」中的「安全性與隱私權」面板 (macOS 12 或較早版本) 核准 kext 來更改 UAKL 時，會間接更改 **auxp** 值。

### 輔助核心集 (AuxKC) Image4 資訊檔雜湊 (auxi)

- **類型:** OctetString (48)
- **可變環境:** macOS
- **說明:** 在系統檢查 UAKL 雜湊與 LocalPolicy 中的 **auxp** 欄位並確認兩者相符後，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 資訊檔簽章的 SHA384 雜湊會放入 LocalPolicy 中，以避免在開機時將先前簽署的 AuxKC 與作業系統混合搭配。如果 iBoot 在 LocalPolicy 中發現 **auxi** 欄位，它會嘗試從儲存空間載入 AuxKC 並驗證簽章。它也會驗證附加至 AuxKC 的 Image4 資訊檔雜湊與 **auxi** 欄位是否相符。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。使用者從「系統設定」中的「隱私權與安全性」(macOS 13 或以上版本) 或「系統偏好設定」中的「安全性與隱私權」面板 (macOS 12 或較早版本) 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 (auxr)

- 類型: OctetString (48)
- 可變環境: macOS
- 說明: **auxr** 是 AuxKC 收據的 SHA384 雜湊, 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, 可將其排除在 AuxKC 之外, 就算使用者已授權也一樣。此外, 某些可用來破壞使用者核心邊界的 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。使用者若想要這些功能, 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。使用者從「系統設定」中的「隱私權與安全性」(macOS 13 或以上版本) 或「系統偏好設定」中的「安全性與隱私權」面板 (macOS 12 或較早版本) 建立新的 AuxKC 時, 會間接更改 **auxr** 值。

#### CustomOS Image4 資訊檔雜湊 (coih)

- 類型: OctetString (48)
- 可變環境: 1TR
- 說明: **coih** 是 CustomOS Image4 資訊檔的 SHA384 雜湊。該資訊檔的承載資料是由 iBoot (而非 XNU 核心) 用來移轉控制權。當使用者在 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** 表示一個卷宗群組, 該群組應由核心當作根群組來使用。此欄位主要作用是提供資訊, 並不會用於安全性限制。此 **vuid** 是在使用者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** 表示開機的卷宗。密鑰加密密鑰通常用於「資料保護」。對於每個 LocalPolicy, 其是用來保護 LocalPolicy 簽署密鑰。在使用者安裝一份新的作業系統時, **kuid** 會被間接設定。

#### 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 雜湊計算, 排除反重放值, 藉此得出不隨時間變動的一致測量 (因為 **lpmh** 這類反重放值會經常更新)。**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。

#### 有安全隔離區簽署 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。若否, 那麼 RecoveryOS LocalPolicy 是由負責簽署 macOS Image4 檔案這類項目的 Apple 線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 OS 版本。此版本是在 LocalPolicy 建立期間從下一個階段資訊檔取得的，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:**若 smb0 存在且為 true，LLB 會允許全域簽署下一階段 Image4 資訊檔，而非要求個人化簽章。使用者可透過「開機安全性工具程式」或 `bputil` 來更改此欄位以降級為「較低安全性」。

#### 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 相同的密鑰以「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。使用者可以使用指令行工具（例如 `csrutil` 或 `bputil`）來更改此欄位以降級為「較低安全性」。

#### 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 相同的密鑰以「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。使用者可使用「開機安全性工具程式」或 `bputil` 來更改此欄位以降級為「較低安全性」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，表示操作裝置的使用者已選擇加入其系統的行動裝置管理 (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，而非要求本機使用者認證。使用者可使用「開機安全性工具程式」或 `bputil` 來更改此欄位以啟用第三方 kext 和軟體更新的管理式控制。（在 macOS 11.2 或以上版本中，如果目前安全性模式為「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 校務管理」、「Apple 商務管理」或「Apple 商務必備」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，而非要求本機使用者認證。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，便會在這裡加入 (而非使用如下所示的幾個 LocalPolicy 欄位)。使用者可以從 1TR 使用 `csrutil` 來更改此欄位以停用 SIP 和降級為「寬鬆安全性」。

### 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。使用者可以從 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) 硬體暫存器。使用者可以從 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 將不會強制執行其 boot-args NVRAM 變數的內建允許列表 (強制執行時會過濾傳送至核心的選項)。使用者可以從 1TR 使用 `csrutil` 或 `bputil` 來更改此欄位。

### 憑證和 RemotePolicy

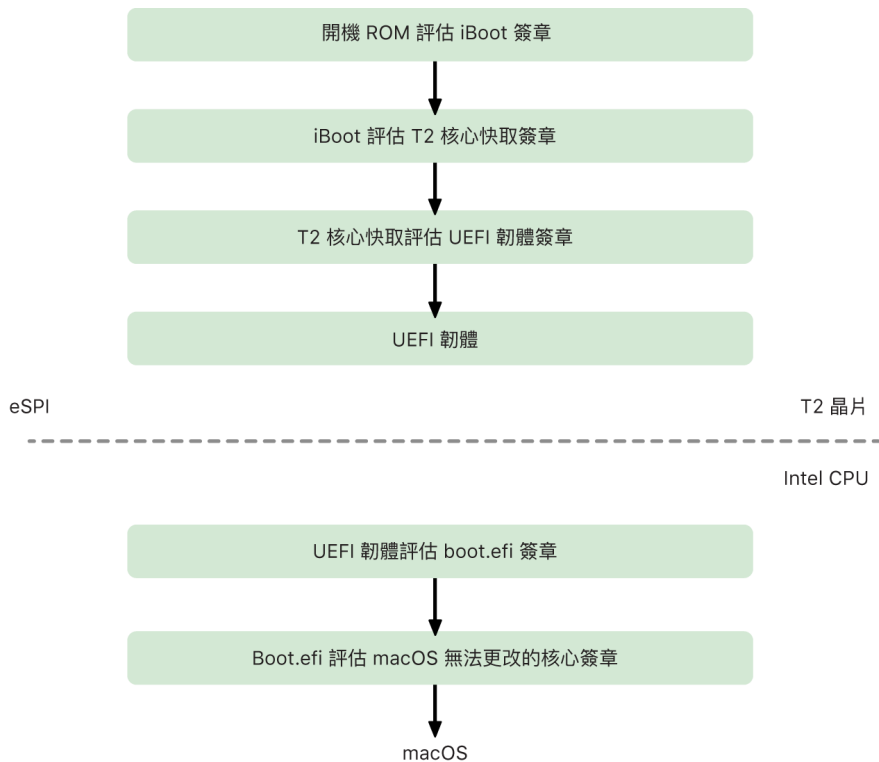
如 [LocalPolicy 簽署密鑰的建立與管理](#) 中所述，LocalPolicy Image4 也包含「所有人身分憑證」(OIC) 和內嵌 RemotePolicy。

# Intel 架構式 Mac 電腦

## 採用 Intel 架構的 Mac 如何進行開機程序

### 採用 Intel 架構並配備 Apple T2 安全晶片的 Mac

當採用 Intel 架構並配備 Apple T2 安全晶片的 Mac 電腦開啟時，晶片會從其開機 ROM 執行安全開機，執行方式與 iPhone、iPad 和配備 Apple 晶片的 Mac 相同。這會驗證 iBoot Bootloader，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，接著 T2 晶片會檢查 Intel UEFI 韌體。UEFI 韌體和關聯的簽章最初僅可供 T2 晶片取用。



通過驗證後，UEFI 韌體映像檔會對應到 T2 晶片記憶體上的一部分。這個記憶體透過「增強型序列週邊介面」(eSPI) 提供給 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、記憶體對應的韌體拷貝擷取 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 Bootloader) 的簽章。採用 Intel 技術的 macOS 安全開機簽章，儲存於與用於 iOS、iPadOS 和 T2 晶片安全開機相同的 Image4 格式，且剖析 Image4 檔案的程式碼同於最新 iOS 和 iPadOS 安全開機實作的強化程式碼。接著 boot.efi 會驗證新檔案 immutablekernel 的簽章。當安全開機啟用時，immutablekernel 檔案代表著啟動 macOS 所需的整組 Apple 核心延伸功能。安全開機規則會在接力給 immutablekernel 時終止，在這之後，macOS 安全性規則 (例如「系統完整保護」和已簽署的核心延伸功能) 便會生效。

此過程中若發生任何錯誤或失敗，都會導致 Mac 進入復原模式、Apple T2 安全晶片復原模式或 Apple T2 安全晶片裝置韌體升級 (DFU) 模式。

## 採用 Intel 架構並配備 T2 晶片的 Mac 上的 Microsoft Windows

依照預設，支援安全開機且採用 Intel 架構的 Mac 只信任 Apple 簽署的內容。但是為了提高「啟動切換」安裝項目的安全性，Apple 也支援 Windows 的安全開機功能。統一可延伸韌體介面 (UEFI) 韌體包含一份 Microsoft Windows Production CA 2011 憑證 (用於認證 Microsoft Bootloader)。

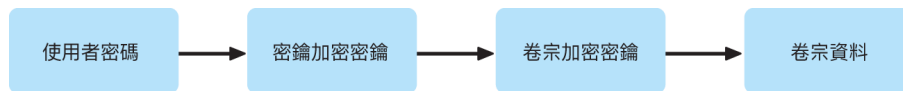
**【注意】**目前沒有針對 Microsoft Corporation UEFI CA 2011 (這會允許驗證 Microsoft 合作夥伴所簽署的程式碼) 提供信任。此 UEFI CA 常用於針對其他作業系統 (例如 Linux 的各種衍生版本) 驗證 Bootloader 的真實性。

Windows 安全開機的支援並非預設為啟用，而是需使用「啟動切換輔助程式」(BCA) 來啟用。當使用者執行 BCA 時，開機期間會將 macOS 設定為信任 Microsoft 第一方簽署的程式碼。BCA 完成後，如果 macOS 無法在安全開機期間傳送 Apple 第一方信任評估，UEFI 韌體會嘗試根據 UEFI 安全開機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，並通知使用者信任評估失敗。

## 採用 Intel 架構而未配備 T2 晶片的 Mac 電腦

未配備 T2 晶片的 Intel 架構 Mac 不支援安全開機。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。為了保護開機鏈的完整性，使用者應啟用下列所有安全機制：

- **系統完整保護 (SIP)**：預設為啟用，此機制可保護開機程式和核心，從執行中的 macOS 內部抵禦惡意寫入。
- **檔案保險箱**：啟用方式有兩種：由使用者或行動裝置管理 (MDM) 管理者啟用。此機制可抵禦實體存在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：由使用者或 MDM 管理者啟用。這有助於防止實體存在的攻擊者啟動替用開機模式，例如 RecoveryOS、單一使用者模式或目標磁碟模式，這些模式可覆寫開機程式。也有助於防止從替用媒體開機，若以此方式開機，攻擊者便可執行程式碼來覆寫開機程式。



## 採用 Intel 架構並配備 Apple T2 安全晶片的 Mac 所具備的開機模式

採用 Intel 架構並配備 Apple 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「開機安全性工具程式」中將安全性規則更改為「無安全性」，否則部分開機模式如「單一使用者」模式會無法運作。

模式	按鍵組合	說明
macOS 開機	無	UEFI 韌體會接力給 macOS 開機程式 (UEFI 應用程式)，然後再接力給 macOS 核心。在啟用「檔案保險箱」的標準 Mac 開機程序中，macOS 開機程式會呈現「登入視窗」介面，其回接收密碼以將儲存空間解密。
開機管理程式	Option (⌥)	UEFI 韌體會啟動內建的 UEFI 應用程式，而這個應用程式會向使用者顯示開機裝置選取介面。
目標磁碟模式 (TDM)	T	UEFI 韌體會啟動內建的 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 機型而定) 連接的區塊式原始儲存裝置。
單一使用者模式	Command (⌘) + S	macOS 核心傳送 launchd 裡引數向量中的 <code>-s</code> 旗標，然後 launchd 在「系統監視程式」App 的 tty 中建立單一使用者 Shell。 <b>【注意】</b> 如果使用者退出 Shell，macOS 會繼續開機程序，進入「登入視窗」。
RecoveryOS	Command (⌘) + R	UEFI 韌體從內置儲存裝置上的已簽署磁碟映像檔 (.dmg) 載入精簡版 macOS。
網際網路 RecoveryOS	Option (⌥) + Command (⌘) + R	使用 HTTP 從網際網路下載已簽署的磁碟映像檔。
診斷	D	UEFI 韌體從內置儲存裝置上的已簽署磁碟映像檔載入精簡版 UEFI 診斷環境。
網際網路診斷	Option (⌥) + D	使用 HTTP 從網際網路下載已簽署的磁碟映像檔。
Windows 開機	無	如果已使用「啟動切換」安裝 Windows，UEFI 韌體會接力給 Windows 開機程式，然後再接力給 Windows 核心。

## 配備 Apple T2 安全晶片的 Mac 所採用的開機安全性工具程式

### 概覽

在採用 Intel 架構並配備 Apple T2 安全晶片的 Mac 上，「開機安全性工具程式」會處理許多安全性規則設定。開機進入 RecoveryOS 並從「工具程式」選單中選取「開機安全性工具程式」，即可取用此工具程式，並保護受支援的安全性設定，避免遭攻擊者輕鬆操控。



即使處於復原模式也需要認證才能才能重要規則。初次打開「開機安全性工具程式」時，會提示使用者輸入管理者密碼，此密碼必須來自已安裝的主要 macOS，而且此份 macOS 必須與目前啟動的 RecoveryOS 相關聯。如果不存在管理者，必須先建立管理者才能更改規則。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。安全性規則更動有兩個隱式需求，RecoveryOS 必須：

- 從直接連接 T2 晶片的儲存裝置啟動，因為其他裝置上的磁碟分割區沒有以「安全隔離區」支援的憑證綁定內部儲存裝置。
- 位於 APFS 型卷宗上，由於僅支援儲存傳送至磁碟中「開機前」APFS 卷宗的「安全隔離區」之「復原中認證」憑證，因此 HFS plus 格式的卷宗無法使用安全開機。

此規則只會顯示於採用 Intel 架構並配備 T2 晶片的 Mac 上的「開機安全性工具程式」中。雖然大多數使用情況應該都不需要更改安全開機規則，不過使用者最終可控制其裝置設定，且可根據需要選擇停用或降級 Mac 上的安全開機功能。

從此 App 中進行的安全開機規則更動，只會套用到 Intel 處理器上進行驗證的信任鏈。「安全啟動 T2 晶片」選項永遠有效。

安全開機規則可設為以下三個設定中的其中一個：「完整安全性」、「中等安全性」和「無安全性」。「無安全性」會完全停用 Intel 處理器上的安全開機評估，並允許使用者隨時開機。

### 完整安全性開機規則

「完整安全性」是預設的開機規則，其行為類似 iOS 和 iPadOS 或配備 Apple 晶片的 Mac 上的「完整安全性」。下載軟體並準備安裝時，簽章要求的一部分會在簽章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)，透過這個簽章進行個人化。簽署伺服器傳回的簽章會變為唯一簽章，且只有該特定 T2 晶片可以使用。當「完整安全性」規則生效，統一可延伸韌體介面 (UEFI) 韌體的設計會確保指定的簽章不僅是由 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。這有助於防止回復攻擊，如同針對配備 Apple 晶片的 Mac 上的「完整安全性」說明的情況。

## 中等安全性開機規則

「中等安全性」開機規則某種程度上類似於傳統 UEFI 安全開機，廠商（此例中為 Apple）會為程式碼產生數位簽章來宣告其為該廠商所提供。如此一來，便能防止攻擊者插入未簽署的程式碼。我們將這類簽章稱為「全域」簽章，因為可在任何 Mac 上使用（目前已設定「中等安全性」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章。此設定不會嘗試防止回復攻擊。

## 媒體開機規則

媒體開機規則只存在於配備 T2 晶片的 Intel 架構 Mac 上，且獨立於安全開機規則。因此即便使用者停用安全開機，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。如需更多資訊，請參閱：[「啟動磁碟」安全性規則控制](#)。）

## 採用 Intel 架構的 Mac 所具備的韌體密碼保護機制

採用 Intel 架構並配備 Apple T2 安全晶片的 Mac 電腦之 macOS，支援使用「韌體密碼」，以協助防止在特定 Mac 上對韌體設定進行非預期的修改。「韌體密碼」的設計是為了防止選取替用開機模式，例如開機進入 RecoveryOS 或「單一使用者模式」、從未授權的卷宗開機，或是開機進入目標磁碟模式。

**【注意】** 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 要求使用者進行認證才能取其重要功能。

最基本的韌體密碼模式，在**未配備** T2 晶片的 Intel 架構 Mac 上，可從 RecoveryOS「韌體密碼工具程式」取用；在採用 Intel 架構並**配備** T2 晶片的 Mac 上，則需透過「開機安全性工具程式」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 晶片的 Intel 架構 Mac 電腦上，從實體存在的攻擊者受到攻擊的風險。韌體密碼有助於防止攻擊者開機進入 RecoveryOS（若進入便可停用「系統完整保護」（SIP））。藉由限制替用媒體啟動，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週邊韌體。

提供韌體密碼重設機制，可協助忘記密碼的使用者。使用者在開機時按下按鍵組合，就會顯示一組機型專屬的字串，此字串需提供給 AppleCare。AppleCare 會以數位方式簽署通過「統一資源識別碼」（URI）簽章檢查的資源。如果簽章通過驗證，且內容為特定 Mac 專用，UEFI 韌體便會移除韌體密碼。

使用者若不希望本人以外的任何人透過軟體移除其韌體密碼，可使用已加入 macOS 10.15 中 `firmwarepasswd` 命令列工具裡的 `-disable-reset-capability` 選項。設定此選項前，使用者必須瞭解當忘記密碼且需移除時，使用者需自行承擔達成此目的所需的主機板更換費用。組織若想保護其 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：

- 在佈建期間手動使用 `firmwarepasswd` 命令列工具
- 透過使用 `firmwarepasswd` 命令列工具的第三方管理工具
- 使用行動裝置管理 (MDM)

## 採用 Intel 架構的 Mac 所適用的 RecoveryOS 和診斷環境

### RecoveryOS

RecoveryOS 與主要 macOS 完全隔離，且完整內容均儲存在 BaseSystem.dmg 磁碟映像檔中。此外還有一個關聯的 BaseSystem.chunklist，用於驗證 BaseSystem.dmg 的完整性。chunklist 是一連串 10 MB BaseSystem.dmg 區塊的雜湊。統一可延伸韌體介面 (UEFI) 韌體會評估 chunklist 檔案的簽章，然後一次評估 BaseSystem.dmg 的一個區塊。這有助於確保其與 chunklist 中已簽署的內容相符。如果這些雜湊中有任一個不相符，便會中止從本機 RecoveryOS 開機，然後 UEFI 韌體會改為嘗試從網際網路 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分與啟動 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) 裡的 diags.efi 檔案，然後這個檔案會負責调用其他各種 UEFI 驅動程式，這些驅動程式可以連接並檢查硬體中的錯誤。

### 網際網路 RecoveryOS 和診斷環境

如果啟動本機復原或診斷環境時發生錯誤，UEFI 韌體會嘗試改從網際網路下載映像檔。(使用者也可具體要求使用啟動時保留的特殊密鑰序列來從網際網路擷取映像檔)。從 OS 復原伺服器下載的磁碟映像檔和 chunklist 之完整性驗證方式，與從儲存裝置所下載的項目相同。

雖然連線至 OS 復原伺服器時是使用 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路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 復原伺服器重新要求該區塊 11 次，然後再放棄並顯示錯誤。

Mac 電腦的網際網路復原和診斷模式是於 2011 年加入，當時決定最好使用較簡單的 HTTP 傳輸，以及使用 chunklist 機制來處理內容認證，而非在 UEFI 韌體中實作較複雜的 HTTPS 功能，因此增加了韌體的攻擊面。



## 簽署系統卷宗安全性

Apple 在 macOS 10.15 中首次採用唯讀系統卷宗，這是供系統內容專用的隔離卷宗。macOS 11 或更新版本則為**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 有效加密編譯簽章的任何資料（程式碼與非程式碼）。從 iOS 15 和 iPadOS 15 開始，iPhone 或 iPad 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分的任何 Apple 軟體，也可讓 macOS 軟體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 加入加密編譯雜湊並加以延伸，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（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處理，而雜湊之後會與檔案系統後設資料中的預期值做比較。若發生不一致，系統會假設資料已遭到竄改，且不會傳回給提出要求的軟體。

每個 SSV SHA256 雜湊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，驗證其子項目雜湊的完整性，類似二位元雜湊 (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，這表示加密編譯簽章涵蓋整個系統卷宗。

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 簽署的測量驗證其測量。在配備 Apple 晶片的 Mac 上，將控制權傳送給核心之前，Bootloader 會驗證印章。在採用 Intel 架構並配備 Apple T2 安全晶片的 Mac 上，Bootloader 會將測量值和簽章轉送至核心，然後核心會直接在掛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，且系統會提示使用者重新安裝 macOS。此程序會在每次開機時重複執行，除非使用者選擇進入較低的安全性模式，且已分別選擇停用簽署系統卷宗。

在 iOS 和 iPadOS 軟體更新期間，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 會驗證封存是否完好無損並且符合 Apple 簽署值。開機時若不相符，則會提示使用者更新裝置上的系統軟體。使用者無法在 iOS 和 iPadOS 上停用已簽署之系統卷宗的保護機制。

## SSV 和程式碼簽章

程式碼簽章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 物件記憶體對應到可執行檔時，程式碼簽章可提供保護。SSV 和程式碼簽章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 或以上版本中，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。如果使用者已開啟「檔案保險箱」，資料卷宗上的使用者內容仍會以使用者提供的密碼加密。

如果使用者選擇停用 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擷取加密的使用者資料。因此，如果已開啟「檔案保險箱」，系統將不會允許使用者停用 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（受到使用者提供的密碼保護）加密使用者和系統內容，藉此保護靜態作業系統軟體。此功能會保護裝置，以防可實際取用裝置的攻擊者存取或有效地修改包含系統軟體的檔案系統。

## SSV 和配備 Apple T2 安全晶片的 Mac

在配備 Apple T2 安全晶片的 Mac 上，只有 macOS 本身受到 SSV 保護。在 T2 晶片上執行和驗證 macOS 的軟體受到安全開機保護。

## 安全軟體更新

安全性是一個過程；以可靠的方式啟動出廠時安裝的作業系統版本，仍不足以保障安全，系統還必須具備另一套機制，以便快速且安全地取得最新的安全性更新項目。Apple 會定期釋出軟體更新以解決浮現的安全性顧慮。iPhone 和 iPad 裝置的使用者會透過裝置接收更新通知。Mac 使用者可在「系統設定」（macOS 13 或以上版本）或「系統偏好設定」（macOS 12 或較早版本）中找到可用的更新項目。更新項目會以無線方式傳送，以利快速採用最新安全性修正。

## 更新程序安全性

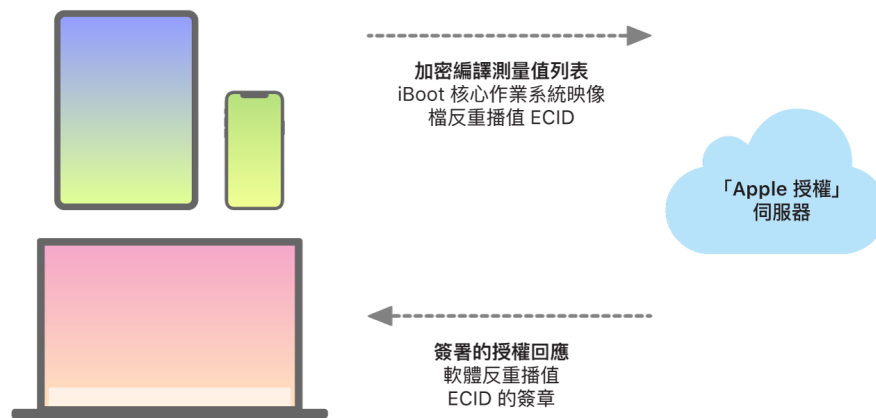
更新程序會使用與安全開機所用之相同的硬體式信任根，其設計僅會安裝 Apple 簽署的編碼。此外，更新程序也會使用系統軟體授權，以確保只有經 Apple 主動簽署的作業系統版本才可複製並安裝在 iPhone 和 iPad 裝置，或是「開機安全性工具程式」中「完整安全性」設定為安全開機規則的 Mac 電腦上。有了這些到位的安全程序，Apple 便可停止簽署包含已知漏洞的較舊作業系統版本，並可協助防止降級的攻擊。

為了達到更高的軟體更新安全性，當要升級的裝置實際連接到 Mac 時，便會下載一份完整的 iOS 或 iPadOS 並加以安裝。但是無線傳輸 (OTA) 的軟體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，藉此改進網路效率。再者，軟體更新可在執行 macOS 10.13 或以上版本並已開啟「內容快取」的 Mac 上進行快取，如此 iPhone 和 iPad 裝置便無須透過網際網路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，會提供特定資訊給 Apple 安裝授權伺服器：要安裝之安裝套件中各部分的加密編譯測量值列表（如 iBoot、核心及作業系統映像檔）、隨機反重複值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，若找到相符項目，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，這是升級程序的一部分。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。



啟動時的信任鏈結評估程序會驗證該次簽署是否來自 Apple，並確認從磁碟載入的項目測量值在結合裝置 ECID 後，是否與該簽章所涵蓋的內容相符。這些步驟的設計是為了確保在支援個人化的裝置上，授權是針對特定裝置進行，且舊版作業系統或韌體版本無法從一部裝置拷貝到另一部裝置。反重複值有助於阻止攻擊者儲存伺服器的回應，並阻止使用該回應來破壞裝置或以其他方式竄改系統軟體。

由於需進行個人化程序，因此只要裝置採用了 Apple 設計的晶片，一律需要網路連線至 Apple 以進行更新，這類裝置也包含採用 Intel 架構並配備 Apple T2 安全晶片的 Mac。

在配備「安全隔離區」的裝置上，硬體會以類似方式使用系統軟體授權來檢查軟體的完整性，以協助防止降級安裝作業。

## 作業系統完整性

Apple 設計的作業系統以安全性為核心。這樣的設計包硬體信任根 (用來啟用安全開機) 以及快速且安全的安全軟體更新程序。Apple 作業系統也採用其特製的晶片式硬體功能, 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 的作業系統軟體可協助緩解攻擊和利用技巧, 無論源自於惡意 App、網路或經由任何其他管道都能應付。這裡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、A13、A14 S4 至 S9	A15、A16、A17	M1、M2、M3
核心完整保護	✓	✓	✓	✓	✓
快速權限取用限制	✗	✓	✓	✓	✓
系統副處理器完整保護	✗	✗	✓	✓	✓
指標認證碼	✗	✗	✓	✓	✓
頁面保護層	✗	✓	✓	✓	✗ 請見下方附註 1。
安全頁表監視器	✗	✗	✗	✓ 請見下方附註 2。	✗

附註 1: 「頁面保護層」(PPL) 要求平台只執行已簽署且受信任的程式碼; 此安全性模式不適用 macOS。

附註 2: A15、A16 和 A17 支援「安全頁表監視器 (SPTM)」, 並在支援的平台上取代了「頁面保護層」。

## 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應特權碼, 以及協助防止核心記憶體區域內的實體記憶體可寫入對應。

為了防止重新設定, 用於啟用 KIP 的硬體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, 引入了全新的硬體原型。這個原型 (「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, 可應付來自網路的攻擊, 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。

## 系統副處理器完整保護

副處理器韌體處理許多重要系統任務，例如「安全隔離區」、影像感測器處理器以及動作副處理器。因此其安全性是整套系統安全性的關鍵所在。為避免副處理器韌體遭修改，Apple 採用系統副處理器完整保護 (SCIP) 機制。

SCIP 的運作方式很類似「核心完整保護」(KIP)：在開機時，iBoot 會將每個副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 會設定每個副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分外的可執行對應
- 受保護的記憶體區域部分內的可寫入對應

同樣在開機時，為了針對「安全隔離區」設定 SCIP，會使用「安全隔離區」作業系統。開機程序完成後，用於啟用 SCIP 的硬體會遭鎖定。這樣的設計是為了防止重新設定。

## 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。系統軟體和內建 App 會使用 PAC 來協助防止修改函式指標和傳回位址 (程式碼指標)。PAC 使用五個機密 128 位元值來簽署核心指示與資料，且所有使用者空間處理序都有各自專屬的 B 鍵。系統會對項目進行 Salt 處理和簽署，如下所示。

項目	索引鍵	Salt
函式傳回位址	IB	儲存位址
函式指標	IA	0
區塊叫用函式	IA	儲存位址
Objective-C 方法快取	IB	儲存位址 + 類別 + 選取器
C++ 虛擬表格項目	IA	儲存位址 + 雜湊 (混合方法名稱)
運算 Goto 標籤	IA	雜湊 (函式名稱)
核心執行緒狀態	GA	•
使用者執行緒狀態暫存器	IA	儲存位址
C++ 虛擬表格指標	DA	0

簽章值儲存在 64 位元指標頂端未使用的填補位元中。使用前會先驗證簽章，且會儲存填補以協助確保函式指標位址運作中。驗證失敗會導致中止。這個驗證機制提高了許多攻擊的難度 (例如返回導向程式設計 (ROP) 攻擊)，這些攻擊會試圖操縱儲存在堆疊上的函式傳回位址，藉此惡意誘使裝置執行現有的程式碼。

## 頁面保護層

程式碼簽章驗證完成後，iOS、iPadOS 和 watchOS 的「頁面保護層」(PPL) 的設計會防止使用者空間程式碼遭修改。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 可變更包含使用者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積，即使是遭入侵的核心面積也適用。這個防護機制並未在 macOS 上提供，因為 PPL 僅適用於要求所有執行的程式碼都必須經過簽署的系統。

## 安全頁表監視器和受信任執行監視器

安全頁表監視器 (SPTM) 和受信任執行監視器 (TXM) 經過精心設計，可以彼此搭配運作，即使攻擊者可寫入核心和繞過控制流程防護機制，也能為使用者和核心程序保護頁表，避免遭到修改。SPTM 落實此機制的方式，是使用比核心還高的權限層級，並採用權限較低的 TXM，以實際強制執行管程式碼執行的規則。根據這套系統的設計，由於如此區隔權限及管控兩者間的信任，TXM 入侵不會自動轉譯為 SPTM 略過。在 A15、A16 和 A17 SOC 中，SPTM (搭配 TXM) 取代了 PPL，其縮小了攻擊面，且不仰賴核心的信任，即使在開機程序的早期階段也一樣。SPTM 也仰賴新的晶片基本元件，是 PPL 所採用「快速權限取用限制」的革新技術。

## 安全啟動資料連線

在 iPhone、iPad 裝置和 Mac 電腦上，如果最近沒有建立任何資料連線，使用者必須使用 Face ID、Touch ID 或密碼，透過 Thunderbolt、USB、Lightning 或聰穎接點介面來啟用資料連線；在 macOS 13.3 或以上版本中，則是經過 SD Extended Capacity「SDXC」卡介面來啟用。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允許其他配件的用途。如果 iPhone 或 iPad 已鎖定超過一小時，或是配件的資料連線已終止超過一小時，裝置就不會允許建立任何新資料連線，直到裝置解鎖為止。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。系統會在上次連接過這些配件後，記住它們 30 天。若此期間有未知配件嘗試開啟資料連線，將會停用所有透過那些連線進行的配件資料連線，直到再次解鎖裝置。這一小時期間：

- 協助經常連接 Mac 或 PC、配件或有線 CarPlay 的使用者，確保他們不需要在每次連接裝置時都輸入密碼
- 是必要的，因為配件生態系統在建立資料連線前，並不會提供可靠的加密方式來識別配件

此外，如果配件的資料連線在建立後維持超過三天，裝置會在鎖定後立即拒絕新的資料連線。這是為了進一步保護不常使用此類配件的使用者。當裝置處於需要密碼以重新啟用生物辨識認證的狀態時，這些資料連線也會被停用。

使用者可以在「設定」中選擇重新啟用永久資料連線 (設定某些輔助裝置會自動執行此操作)。

## 驗證 iPhone 和 iPad 的配件

Made for iPhone and iPad (MFi) 授權計畫可為經過審查的配件製造商，提供 iPod 配件通訊協定 (iAP) 和必要支援硬體元件的存取權限。

MFi 配件與 iPhone 或 iPad 通訊時，配件必須向 Apple 證明自己已通過審查。(配件是透過 Thunderbolt、Lightning、藍牙與裝置連線，特定裝置則使用 USB-C。) 為證明授權，配件會傳送 Apple 提供的憑證給裝置，裝置接著會加以驗證。然後，裝置會傳送一個質詢，配件必須使用已簽署的回應來答覆。這個過程完全由 Apple 提供給經核准配件製造商的特製積體電路 (IC) 處理，而且配件本身亦可獲得所有相關資訊。

經過驗證的 MFi 配件可以要求存取不同的傳輸方式和功能；例如透過 Thunderbolt 連接線存取數位音訊串流，或透過藍牙存取所提供的位置資訊。認證 IC 的設計可協助確保只有經過核准的 MFi 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分的序列 (UART) 音訊播放控制。

AirPlay 也會利用認證 IC 來驗證接收器已通過 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 以計數器 (CTR) 模式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 IC 的 1024 位元 RSA 密鑰來簽署，以作為端到端 (STS) 通訊協定的一部分。

## 用於訊息和 IDS 的 BlastDoor

iOS、iPadOS、macOS 和 watchOS 包含名為 **BlastDoor** 的安全功能，此功能是在 iOS 14 和相關發行版本中首度推出。BlastDoor 的目標是透過圍定攻擊者來協助保護系統，增加他們利用「訊息」和 Apple 識別服務 (IDS) 進行攻擊的難度。BlastDoor 透過隔離、剖析、轉碼以及驗證進入「訊息」、IDS 和其他向量的未受信任資料，以協助防止攻擊。

BlastDoor 利用沙盒限制以及對輸出的記憶體安全驗證來做到這一點，這對攻擊者構成重大的障礙，使其難以抵達作業系統的其他部分。BlastDoor 的設計目標是要大幅改善使用者對抗攻擊的防禦能力，特別是針對「零點擊」攻擊，這類攻擊不需要使用者互動。

最後，「訊息」將來自「已知寄件人」的流量與來自「未知的寄件人」的流量區分處理，為每個群體提供不同的功能集，並將「已知」與「未知」資料分隔到不同的 BlastDoor 實例中。

## Apple 裝置的「封閉模式」安全性

「封閉模式」為極少數使用者提供了選用的最高等級保護，有鑑於其身分或從事的工作，他們可能成為一些最複雜的數位威脅（例如目標鎖定式傭兵間諜軟體）的個人目標。大多數人從未成為此類攻擊的目標。

「封閉模式」開啟時，裝置的運作方式與平常不同。為了縮小可能遭惡意利用的攻擊面，特定 App、網站和功能受到嚴格安全限制，且部分體驗可能完全無法使用。

iOS 16、iPadOS 16、macOS 13 和 watchOS 10 或以上版本提供「封閉模式」。iOS 17、iPadOS 17、macOS 14 提供額外保護，而 watchOS 10.1 或以上版本提供更新項目。若要使用「封閉模式」的其他功能，裝置須更新為最新版作業系統。如需更多資訊，請參閱 Apple 支援文章：[關於「封閉模式」](#)。

「封閉模式」以功能、效能或兩者為代價，來換取更高的安全性。這些取舍會影響：

- 背景服務
- 連線
- 裝置管理
- FaceTime
- GameCenter
- 郵件
- 訊息
- 照片
- Safari
- 系統設定
- WebKit

## 其他 macOS 系統安全性功能

### 其他 macOS 系統安全性功能

macOS 可在更廣泛的硬體上執行（例如採用 Intel CPU、採用 Intel CPU 並搭配 Apple T2 安全晶片，以及配備 Apple 晶片 SoC 的硬體），且支援一般用途下的各種運算情況。有些使用者僅使用基本的預先安裝 App 或可從 App Store 取得的 App，而其他使用者則是核心駭客，他們需要停用所有平台保護機制，以便可以最高信任層級來執行和測試其執行程式碼。大部分的使用者則介於兩者之間，其中有許多人擁有要求不同取用層級的週邊設備和軟體。Apple 設計的 macOS 平台透過採用硬體、軟體與服務的整合作法，此平台在設計時即內建安全性，且簡化了設定、部署和管理的操作，不過也保留了使用者期望的可設定性。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路環境內進行整合。

下列功能支援和協助保護 macOS 使用者的不同需求。包括：

- 簽署系統卷宗安全性

- 系統完整保護
- 信任快取
- 週邊設備保護
- Rosetta 2 (自動轉譯) 支援和配備 Apple 晶片的 Mac 安全性
- DMA 支援與保護
- 核心延伸功能 (kext) 支援與安全性
- Option ROM 支援與安全性
- UEFI 韌體安全性 (採用 Intel 架構的 Mac 電腦)

## 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, 這是獨立於硬體式「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。

### 強制存取權限控制

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)。此作法與任意存取權限控制不同, 任意存取權限控制會根據使用者的偏好設定來允許覆蓋安全政策。

強制存取權限控制不會向使用者顯示, 但是其為協助啟用多種重要功能的基礎技術, 包含沙盒、分級控制、受管理的偏好設定、延伸功能和系統完整保護。

### 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」是電腦專用的設定, 當使用者升級至 OS X 10.11 或以上版本時預設為啟用。在採用 Intel 架構的 Mac 上, 若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 將此安全性規則套用到系統上執行的所有處理序, 無論是否以沙盒執行或具有管理權限。

## 信任快取

安全開機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代表。為進行有效率地搜尋, 這些雜湊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。若要在配備 Apple 晶片的 Mac 上停用信任快取強制執行, 安全開機必須設為「寬鬆安全性」。

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應至現有程序的過程), 系統都會擷取其程式碼目錄並進行雜湊處理。如果產生的雜湊出現在信任快取中, 為該二進位檔建立的可執行對應就會獲得平台權限, 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章的真實性就能執行。採用 Intel 架構的 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鏈才能執行, 而且其可擁有的授權受限於 Apple Developer Program 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, 其程式碼目錄雜湊仍必須存在信任快取中才能執行。在採用 Intel 架構的 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，進而防止攻擊者取得優勢。

## 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 和開發工具堆疊。即使如此，在配備 Apple 晶片的 Mac 和配備 T2 晶片的 Mac 上，系統仍允許它們以平台權限執行。由於這個平台軟體是獨立於 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**遞送某些軟體套件。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 信任的簽署服務的個人化）或全域簽署物件（其簽章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，會隨著配備 Apple 晶片的 Mac 上用於執行診斷的磁碟映像一起提供。這個信任快取經過個人化處理並隨著磁碟映像提供，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體以平台權限執行。

全域簽署信任快取會隨著 macOS 軟體更新一起提供。這個信任快取允許軟體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體更新所需的所有工作。

## Mac 電腦的週邊設備處理器安全性

所有現代運算系統均配備多個內建週邊設備處理器，專門處理網路、繪圖、電力管理等作業。這些週邊設備處理器通常為單一用途，且功能遠不如主要 CPU 強大。內建的週邊設備若沒有實作充分的安全機制，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。若有週邊設備處理器韌體感染，攻擊者便能鎖定主要 CPU 上的軟體為目標，或是直接擷取敏感資料（例如乙太網路裝置可查看未加密封包的內容）。

Apple 盡可能地致力減少必要週邊設備處理器的數量，或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，其會在啟動時從主要 CPU 下載經驗證的韌體
- 讓週邊設備處理器實作專屬的安全開機鍵，以在每次 Mac 開機時都會驗證週邊設備處理器韌體

Apple 與廠商共同合作來稽核其實作情況，並增強其設計以納入所需的屬性，例如：

- 確保最低加密編譯強度
- 確保強制撤銷已知惡意的韌體
- 停用除錯介面
- 使用受 Apple 控制的硬體安全模組 (HSM) 中所儲存的加密編譯密鑰來簽署韌體

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。

當免儲存裝置作業和外加儲存裝置安全開機都不是適用選項時，設計會強制要求韌體更新必須進行加密編譯簽署和驗證，才能更新永續性儲存體。

## 配備 Apple 晶片之 Mac 上的 Rosetta 2

配備 Apple 晶片的 Mac 可使用一套稱為 **Rosetta 2** 的轉譯機制來執行以 x86\_64 指令集編譯的程式碼。此機制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的早期階段識別 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 `dyld(1)`。接著這個轉譯虛設常式會在映像執行期間轉譯 x86\_64 頁面。這個轉譯作業完全在處理序中進行。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章，驗證每個 x86\_64 頁面的程式碼雜湊。若雜湊不相符，核心就會強制執行適用於該處理序的修復規則。

## 提前轉譯

若採用提前 (AOT) 轉譯路徑，當系統認為這種方式可以使程式碼達到最佳的回應效率時，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訊。為了強制這個綁定關係，有特殊權限的使用者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使用者空間實體，而系統會利用受限制的權限來識別這個實體。為了轉譯成品而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。轉譯成品本身上的簽章也稱為**補充簽章**。

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)`。但是接著 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，再將它對應到處理序中並執行。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章進行認證) 的程式碼目錄雜湊。這個處理序與原始 x86\_64 映像的程式碼目錄雜湊無關。

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該 Data Vault。Rosetta 服務會藉由分發唯讀檔案描述元給個別轉譯成品來管理快取的存取，這樣可限制存取 AOT 成品快取。這個服務的程序間通訊和獨立的磁碟使用量會刻意維持在極小的範圍內，藉此限縮其攻擊面。

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

如果遠端處理序向核心查詢 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 或以上版本隨附 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，使用者可選擇透過 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：

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

Rosetta AOT 轉譯程序具確定性，因為其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 macOS 版本相關聯的 Rosetta AOT 轉譯流程，藉此將程式碼目錄雜湊記錄在信任快取中。為求效率，實際的轉譯產品不會隨作業系統提供，且會在使用者提出要求時隨需重新建構。

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位於靜態信任快取中，所產生 AOT 成品的程式碼目錄雜湊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 安全開機鏈中。

## 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章的情況下執行。這個簽章可以像「臨機操作」程式碼簽章 (cf. [codesign\(1\)](#)) 一樣簡單，不包含來自非對稱式密鑰組秘密部分的任何實際的識別資料 (只是二進位檔的未認證測量)。

為了讓二進位檔具有相容性，系統允許轉譯的 x86\_64 程式碼在沒有簽章的情況下透過 Rosetta 執行。不會有任何識別資料透過裝置專用的「安全隔離區」簽署程序傳達到這個程式碼中，且其執行限制與在採用 Intel 架構的 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，電腦必須支援週邊設備的直接記憶體存取 (DMA)。也就是說，週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 電腦已實作多種技術以保護 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 都有專屬的一組位址轉譯表，用於轉譯 DMA 要求，因此透過 PCIe 或 Thunderbolt 連接的週邊設備，只能存取已明確對應供其使用的記憶體。週邊設備無法存取屬於系統其他部分的記憶體 (例如核心或韌體)，或指派給其他週邊設備的記憶體。如果 IOMMU 偵測到有週邊設備嘗試存取並非對應供該週邊設備使用的記憶體，則會觸發核心異常。

### 採用 Intel 架構的 Mac 上的直接記憶體存取保護

採用 Intel 架構並配備 Intel 虛擬化技術的 Mac 會初始化 IOMMU，在開機程序的極早期啟用 DMA 重新對應並中斷重新對應，藉此減輕各種安全性漏洞類別的威脅。Apple IOMMU 硬體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週邊設備的 DMA 要求。軟體初始化 IOMMU 後，IOMMU 會開始允許來自週邊設備的 DMA 要求傳至已明確對應供其使用的記憶體區域。

**【注意】**在配備 Apple 晶片的 Mac 上，中斷 PCIe 的重新對應並非必要程序，因為每個 IOMMU 都會針對其自己的週邊設備處理 MSI。

從 macOS 11 開始，所有配備 Apple T2 安全晶片的 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，它降低了在處理 DMA 緩衝區的驅動程式中發生漏洞的影響。

## 在 macOS 中安全延伸核心

從 macOS 11 開始，如果第三方核心延伸功能 (kext) 已啟用，就不能載入隨選即用核心。相反地，它們會合併到一個**輔助核心集合 (AuxKC)**中，其會在開機程序期間載入。對於配備 Apple 晶片的 Mac，AuxKC 的測量值已簽署到 LocalPolicy 中 (而對於先前的硬體，AuxKC 則會留在資料卷宗上)。若要重建 AuxKC，需要使用者核准並重新啟動 macOS，以將更動載入核心中，且需要將安全開機設為「較低安全性」。

**【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 建議使用者應選擇不需要延伸核心的解決方案。

### 配備 Apple 晶片的 Mac 上所具備的核心延伸功能

在配備 Apple 晶片的 Mac 上，kext 必須以明確的方式啟用，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「較低安全性」，並勾選該註記框來啟用核心延伸功能。此動作還需要輸入管理者密碼以授權降級。1TR 和密碼需求的結合讓純軟體攻擊者很難從 macOS 內部開始將 kext 注入 macOS (他們隨後可藉此取得核心權限)。

在使用者授權 kext 載入後，上述「使用者核准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 中擷取使用者授權 kext 列表 (UAKL) 的 SHA384 雜湊。之後核心管理精靈 (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 的簽章納入 AuxKC 中前，對其進行驗證。
- 如果 SIP 已停用，則不會強制執行 kext 簽章。

這個作法允許「寬鬆安全性」為沒有參與 Apple Developer Program 的開發者或使用者執行流程，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 結構的一部分，也會產生一個 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 雜湊和 kext 收據。LLB 在開機時會使用 AuxKC Image4 雜湊進行額外的驗證，以協助確保無法透過較新的 LocalPolicy 來啟動由「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，它們可能會干擾 macOS 的可信度。如果有 kext 已載入，那麼 Apple Pay 功能可能會遭停用。

## 系統延伸功能

macOS 10.15 可讓開發者能藉由安裝和管理在使用者空間中 (而非核心層級) 執行的系統延伸功能來延伸 macOS 的功能。藉由在使用者空間中執行，系統延伸功能可提高 macOS 的可靠性和安全性。即使 kext 本質上具有整個作業系統的完全存取權，在使用者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 (例如防資料遺失或其他端點代理程式) 及 VPN 和網路工具，而不需要寫入 kext。只有當第三方安全性代理程式採用這些 API，或具有移入第三方安全性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。

## 使用者核准的核心延伸功能載入

為了提高安全性，若要載入安裝 macOS 10.13 時或安裝後提供的核心延伸功能，必須取得使用者同意。這個程序稱為**使用者核准的核心延伸功能載入**。需要管理者授權才能核准核心延伸功能。若核心延伸功能具備以下條件，則不需要授權：

- 在執行 macOS 10.12 或較早版本時已安裝在 Mac 上
- 將取代先前核准的延伸功能
- 若使用 Mac 從 RecoveryOS 開機時可用的 `spctl` 命令列工具，無需取得使用者同意便可載入
- 獲得允許，可使用行動裝置管理 (MDM) 設定來載入

從 macOS 10.13.2 開始，使用者可使用 MDM 來指定不需要使用者同意即可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，且已透過「Apple 校務管理」、「Apple 商務管理」，或使用使用者完成的 MDM 註冊，來在 MDM 中註冊的 Mac。

## macOS 的 Option ROM 安全性

**【注意】** 配備 Apple 晶片的 Mac 目前不支援 Option ROM。

### 配備 Apple T2 安全晶片的 Mac 之 Option ROM 安全性

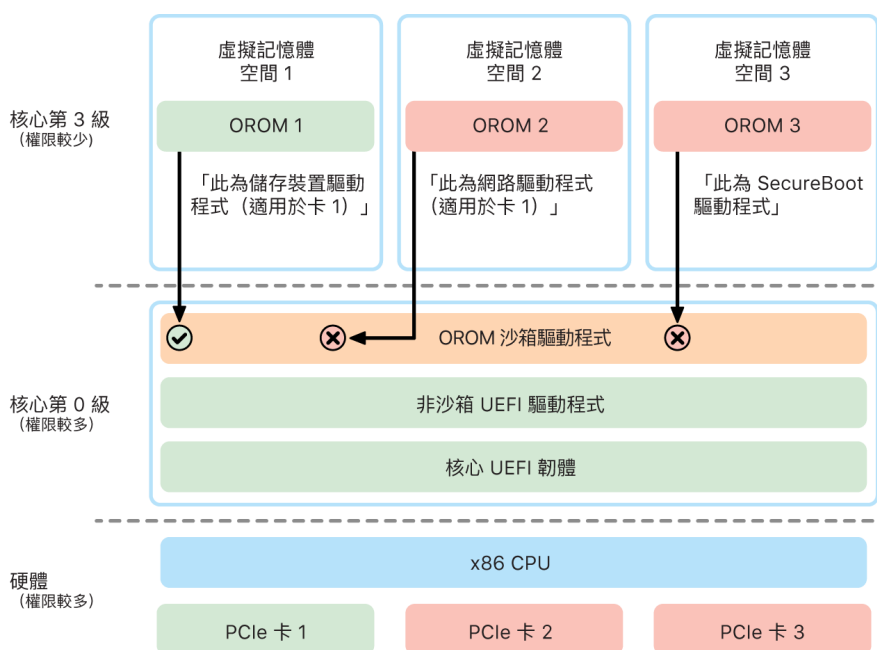
Thunderbolt 和 PCIe 裝置都具有與裝置實體連接的「Option ROM」(OROM)。(這通常不是真正的 ROM，而是儲存著韌體的可寫入晶片。) 在 UEFI 系統上，該韌體通常為 UEFI 驅動程式，會由 UEFI 韌體讀取然後執行。執行的程式碼應會初始化和設定其擷取來源硬體，以便讓該硬體可供韌體的其餘部分使用。此功能需要專門的第三方硬體可在早期開機階段載入和運作，例如從外部 RAID 陣列開機。

然而，由於 OROM 通常可重複寫入，如果攻擊者覆寫合法週邊設備的 OROM，攻擊者的程式碼便可在開機程序的早期階段執行，且可透過執行環境竄改，以及破壞後續載入的軟體完整性。同樣地，如果攻擊者將自己的惡意裝置引入系統中，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，當使用者設定韌體密碼時，即使按下按鍵組合也無法執行 OROM。這可防止實體存在的攻擊者刻意引入惡意的 OROM。已設定韌體密碼的使用者如果仍需執行 OROM，可以使用 macOS 中的 `firmwarepasswd` 命令列工具來設定非預設選項。

## OROM 沙盒安全性

在 macOS 10.15 中，UEFI 韌體已更新為包含對 OROM 執行沙盒和解除權限的機制。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 記憶體中的任一位置，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積，並強迫攻擊者先逃離沙盒再提高權限。

## 採用 Intel 架構的 Mac 所具備的 UEFI 韌體安全性

採用 Intel 架構並配備 Apple T2 安全晶片的 Mac 使用 UEFI (Intel) 韌體來提供安全性。

### 概覽

自 2006 開始，配備 Intel CPU 的 Mac 電腦，是根據「可延伸韌體介面」（EFI）開發套件（EDK）第 1 或 2 版來使用 Intel 韌體。以 EDK2 為基礎的程式碼遵循「統一可延伸韌體介面」（UEFI）規格。本節以 **UEFI 韌體** 來稱呼 Intel 韌體。UEFI 韌體是 Intel 晶片上執行的第一個程式碼。

若 Mac 未配備 Apple T2 安全晶片並採用 Intel 架構，UEFI 韌體的信任根則為儲存著韌體的晶片。UEFI 韌體更新是由 Apple 數位簽章，且須由韌體進行驗證後才會更新儲存體。為了協助防止回復攻擊，更新項目的版本必須一律比現有版本新。但是，攻擊者若能實體取用 Mac，便可能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 韌體的舊開機程序中（在其限制寫入儲存晶片之前）發現弱點，也可能導致 UEFI 韌體持續感染。這個硬體架構限制在大部分採用 Intel 架構的 PC 上很常見，且所有未配備 T2 晶片並採用 Intel 架構的 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 晶片中的 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：[採用 Intel 架構的 Mac 如何進行開機程序](#)。

## 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，採用 Intel 架構的 Mac 會執行自訂的 ME 韌體，其中大部分元件都已移除。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。其名稱為「系統管理模式」(SMM)，最初引入的目的是處理對時間準確度要求高的作業，例如電力管理。但是為了執行這類作業，Mac 電腦長久以來均使用稱為「系統管理控制器」(SMC) 的離散微控制器。SMC 不再是獨立的微控制器，而是已整合到 T2 晶片內。

# watchOS 的系統安全性

Apple Watch 使用許多 iOS 所用的相同硬體式平台安全性功能。例如，Apple Watch：

- 執行安全開機和安全軟體更新
- 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 和網際網路通訊時保護資料

支援的技術包含「系統安全性」中列出的項目（例如 KIP、SKP 和 SCIP）以及資料保護、鑰匙圈和網路技術。

## 更新 watchOS

watchOS 可以設定為隔夜更新。如需深入瞭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

如果啟用手腕偵測功能，裝置從使用者手腕取下不久後即會自動鎖定。如果手腕偵測已停用，「控制中心」會提供鎖定 Apple Watch 的選項。Apple Watch 鎖定時，只有在 Apple Watch 上輸入密碼才能使用 Apple Pay。使用者可以在 iPhone 上的 Apple Watch App 中關閉手腕偵測。此設定也可使用行動裝置管理 (MDM) 解決方案來強制執行。

## 啟用鎖定

在 iPhone 上開啟「尋找」後，其配對的 Apple Watch 也會使用「啟用鎖定」。「啟用鎖定」可讓 Apple Watch 在遺失或遭竊時無法由其他人輕易使用或銷售。「啟用鎖定」需要使用者的 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，並透過藍牙低功耗 (BLE) 連結共享密鑰。Apple Watch 會顯示動畫圖形，而使用者必須用 iPhone 上的相機來掃描它。圖形包含已編碼的密鑰，用於 BLE 4.1 頻外配對。若有需要，「標準 BLE 通行密鑰項目」(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 會使用以下任一項來交換密鑰：

- 改寫自 Apple 識別服務 (IDS) 的程序，如 [iMessage 安全性概覽](#) 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 256 位元 Ed25519 公用密鑰與專用密鑰組，且在初始密鑰交換過程中會交換公用密鑰。當執行 watchOS 10 或以上版本的 Apple Watch 初次配對時，專用密鑰會以其「安全隔離區」為根。

在執行 iOS 17 或以上版本的 iPhone 上，專用密鑰不會以「安全隔離區」為根，因為使用者會將「iCloud 備份」回復到保留現有 Apple Watch 配對的相同 iPhone 上，不需要進行移轉。

**【注意】**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 或以上版本的 Apple Watch 配對時，執行 iOS 13 或以上版本的 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行動數據連結。
- (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 或以上版本，並與執行 watchOS 8 或以上版本的 Apple Watch Series 4 或後續機型配對的 iPhone 裝置上，這些裝置之間的進一步通訊使用 AES-256-GCM 進行加密和完整性保護。(ChaCha20-Poly1305 搭配 256 位元密鑰用於舊型裝置或是執行舊版作業系統的裝置。)

藍牙低功耗裝置位址每 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。

為了支援需要連續傳輸資料的 App，會利用 [FaceTime 安全性](#) 中提到的方式來提供加密，如使用由已配對 iPhone 所提供的 Apple 識別服務 (IDS) 或直接網際網路連線。

Apple Watch 採用硬體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安全性。如需更多資訊，請參閱：[資料保護的 Keybag](#)。

## 自動解鎖與 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。
- 偵測到使用者的鼻子和嘴巴遭遮蔽時，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：相互認證的端到端 (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，被解鎖的裝置 (「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」)。接著，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 連線相互連接。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。在下一生物辨識或密碼解鎖期間，目標裝置將其密碼衍生密鑰 (PDK) 與解鎖密鑰包裝在一起，並從其記憶體中丟棄該解鎖密鑰。

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，並且滿足所需的安全性原則，則發起方會透過 STS 通道將其解鎖密鑰傳送給目標。接著，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鎖，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 會從目標記憶體中丟棄。

### Apple Watch 自動解鎖安全性原則

為了增加便利性，首次啟動後，iPhone 可以直接將 Apple Watch 解鎖，使用者無需先在 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 自動解鎖安全性原則

其他安全性原則適用於使用 Apple Watch 的 iPhone 自動解鎖。Apple Watch 無法用來代替 iPhone 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聯的觸覺通知。如果使用者點一下通知中的「鎖定 iPhone」按鈕，則手錶會透過 BLE 向 iPhone 傳送鎖定命令。當 iPhone 收到鎖定命令時，它會鎖定並將 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。

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

- 將相關聯的 Apple Watch 放在手腕上並解鎖後，必須至少使用另一種方法對 iPhone 進行一次解鎖。
- 感測器必須能夠偵測到鼻子和嘴巴被遮蔽了。
- 測量距離必須是 2–3 公尺或更短
- Apple Watch 不得處於就寢模式。
- Apple Watch 或 iPhone 最近必須已解鎖，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 在過去 6.5 個小時內必須至少解鎖一次。
- iPhone 必須處於允許 Face ID 執行裝置解鎖的狀態。(如需更多資訊，請參閱：[Face ID](#)、[Touch ID](#) 和 [密碼](#)。)

## 使用 Apple Watch 在 macOS 中進行核准

「使用 Apple Watch 自動解鎖」啟用時，Apple Watch 可用於適當位置或搭配 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
- 要求授權的第三方 App
- 已儲存的 Safari 密碼
- 安全備忘錄

## 安全使用 Wi-Fi、行動網路、iCloud 和 Gmail

當 Apple Watch 不在藍牙範圍內時，可改為使用 Wi-Fi 或行動數據。Apple Watch 會自動加入其配對 iPhone 已加入過的 Wi-Fi 網路 (網路的憑證必須在兩部裝置都位於連線範圍內時同步至 Apple Watch)。接著在 Apple Watch 上，便可於「設定」App 的 Wi-Fi 部分中設定個別網路的「自動加入」動作。若為先前未於任何裝置上加入過的 Wi-Fi 網路，可在 Apple Watch 上於「設定」App 的 Wi-Fi 部分手動加入。

當 Apple Watch 和 iPhone 在範圍外時，Apple Watch 會直接連接到 iCloud 和 Gmail 伺服器以擷取郵件，而不是透過網際網路與配對的 iPhone 同步「郵件」資料。針對 Gmail 帳號，使用者必須在 iPhone 上 Watch App 的「郵件」部分中向 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，以便其用來擷取郵件。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) 是安全軟體的重要構成要素。有鑑於此，Apple 提供受信任的軟體 CPRNG，在 iOS、iPadOS、macOS、tvOS 及 watchOS 核心中執行。此軟體負責彙總來自系統的原始熵，並提供安全亂數給核心和使用者空間中的取用者。



## 熵來源

核心 CPRNG 源自於開機期間和裝置生命週期中的多個熵來源。其中包含 (取決於可用性)：

- 「安全隔離區」硬體 TRNG
- 開機期間收集的時基誤差
- 從硬體中斷收集的熵
- 讓每次開機皆能維持熵的種子檔案
- Intel 隨機指令，例如 RDSEED 和 RDRAND (僅適用於採用 Intel 架構的 Mac)

## 核心 CPRNG

核心 CPRNG 是針對 256 位元安全性層級由 Fortuna 衍生的設計。它使用下列 API，為使用者空間取用者提供高品質的亂數：

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

核心 CPRNG 可透過寫入隨機裝置接受使用者提供的熵。

## Apple 安全研究裝置

「Apple 安全研究裝置」是以特殊方式配置電路的 iPhone，讓安全研究人員用於對 iOS 進行研究，而不會損失或停用 iPhone 的平台安全性功能。透過此裝置，研究人員可側載以等同於平台的權限執行的內容，進而在更接近生產裝置模型的平台上進行研究。

為協助確保使用者裝置不會受到安全研究裝置執行規則影響，在 LLB 變體和開機核心集中導入了規則更動。這些無法在使用者硬體上啟動。研究用的 LLB 會檢查是否有新的電路配置狀態，若在並非為研究而配置的硬體上執行。

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，其設計用意是為了確保這個子系統不會在使用者裝置上允許執行：

- 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，它將會中止。
- `AppleImage4` 不會提供用於在正常客戶裝置上驗證研究 Cryptex 的反重放值。
- 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隱私，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) 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使用者裝置，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，便會進入復原模式。如果使用者開始充電並將裝置重新開機，裝置就會正常開機。當 XNU 啟動，無需為裝置充電即可繼續操作。
- LLB 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.”

以下是在軟體中導入的其他測量，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) 字樣會顯示在鎖定螢幕上和「設定」App 中。

安全研究裝置為研究人員提供下列功能 (使用者裝置不提供), 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
- 重新開機後保留內容
- 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; 在簽名驗證期間, 任何具有此授權的程序都會在客戶裝置上終止。

- 個人化和回復自訂核心快取

# 加密與資料保護

## 加密與資料保護概覽

安全開機鍊、系統安全性和 App 安全性功能皆有助於確認只有可信的編碼和 App 才能在裝置上執行。即使安全基礎架構的其他部分遭入侵 (例如若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使用者資料。這些功能都對於使用者與 IT 管理者都大有助益，可保護個人與企業的資訊，並提供裝置遭竊或遺失時，於遠端立即完全清除的方式。

iPhone 和 iPad 裝置採用「**資料保護**」檔案加密方法，而採用 Intel 架構的 Mac 電腦上的資料受到「**檔案保險箱**」卷宗加密技術的保護。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 Intel 架構式 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」的專用矽晶片上，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 Intel 架構式 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 使用**作業系統核心**來強制執行保護和安全性。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

為了保護使用者資料免受惡意攻擊，Apple 在 iOS 和 iPadOS 中使用密碼並在 macOS 中使用密碼。密碼越長，就越強大，並且更容易阻止暴力攻擊。為了進一步阻止攻擊，Apple 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，使用者會自動啟用資料保護。其他配備 Apple 系統單晶片 (SoC) 的裝置也啟用了資料保護，例如配備 Apple 晶片的 Mac、Apple TV 和 Apple Watch。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提高安全性

iOS 和 iPadOS 支援六位數、四位數和任意長度的英數密碼。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 纏結，因此要攻擊該裝置只能以暴力破解法來進行。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，這需要 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。

使用者密碼的強度越高，加密密鑰就越難破解。且藉由使用 Face ID 和 Touch ID，使用者可製作一個比實用密碼安全性更高的密碼。更強的密碼增加了加密密鑰 (用於「資料保護」) 進行保護的密碼強度，而且不會對一天中多次解鎖裝置的使用者體驗產生負面影響。

若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，而且可提供類似的安全性。

使用者可在「設定」>「Touch ID 與密碼」或「Face ID 與密碼」選項中選取「自訂英數字密碼」，來指定較長的英數字元密碼。

## 增加延遲時間如何阻止暴力攻擊

在 iOS、iPadOS 和 macOS 中，為了進一步阻止暴力密碼的破解攻擊，系統會增加輸入無效密碼或 PIN 後的延遲時間（視裝置和其所處的狀態而定），如下表所示。

嘗試次數	3	4	5	6	7	8	9	10 次以上
iOS 和 iPadOS 鎖定畫面	無	1 分鐘	5 分鐘	15 分鐘	1 小時	3 小時	8 小時	裝置會被停用，且必須連接 Mac 或 PC
watchOS 鎖定畫面	無	1 分鐘	5 分鐘	15 分鐘	1 小時	3 小時	8 小時	裝置會被停用，且必須連接 iPhone
macOS 登入視窗和鎖定畫面	無	1 分鐘	5 分鐘	15 分鐘	1 小時	3 小時	8 小時	8 小時
macOS 復原模式	無	1 分鐘	5 分鐘	15 分鐘	1 小時	3 小時	8 小時	請參閱下方的「在 macOS 中增加延遲時間如何阻止暴力攻擊」
檔案保險箱搭配復原密鑰（個人、機構或 iCloud）	無	1 分鐘	5 分鐘	15 分鐘	1 小時	3 小時	8 小時	請參閱下方的「在 macOS 中增加延遲時間如何阻止暴力攻擊」
macOS 遠端鎖定 PIN 碼	1 分鐘	5 分鐘	15 分鐘	30 分鐘	1 小時	1 小時	1 小時	1 小時

如果開啟了 iPhone 或 iPad 的「清除資料」選項（在「設定」>「[Face ID] 與密碼」或「[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行動裝置管理 (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。若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。

## 在 macOS 中增加延遲時間如何阻止暴力攻擊

為了協助防止暴力密碼破解攻擊，當 Mac 啟動時，不能在「登入視窗」中嘗試輸入密碼 10 次以上，且密碼輸入錯誤特定次數後會增加延遲時間。延遲是由「安全隔離區」強制執行。若 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。

為了協助防止惡意軟體藉由嘗試攻擊使用者的密碼造成永久性資料遺失，在使用者成功登入 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。若輸入錯誤密碼已達 10 次，重新開機進入 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」復原機制 (iCloud 復原、「檔案保險箱」復原密鑰和其他機構密鑰) 都會有 10 次機會，最多可嘗試 30 次。在用盡這些額外的嘗試機會後，「安全隔離區」就不會再處理任何解密卷宗或驗證密碼的要求，且磁碟上的資料會變為無法復原。

若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」設定規則。組織有多個選項可用來管理加密的卷宗，包含機構復原密鑰、個人復原密鑰 (可選擇透過 MDM 儲存以進行託管) 或兩者的組合。也可在 MDM 中將密鑰轉換為規則。

在配備 Apple T2 安全晶片的 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 也提供額外的密碼復原選項：

- iCloud 復原
- 「檔案保險箱」復原
- 「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，同時對使用者資料啟用較高層次的加密。特定系統 App (如「訊息」、「郵件」、「行事曆」、「聯絡人」、「照片」) 和「健康」的資料值都預設使用「資料保護」。第三方 App 會自動獲得此項保護措施。

### 實施方式

「資料保護」是透過建構和管理密鑰階層來完成導入，並建立在每部 Apple 裝置的硬體加密技術上。「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；可存取性則取決於該類密鑰是否已解鎖。隨著 APFS (Apple 檔案系統) 的誕生，檔案系統可以依據範圍進一步細分密鑰 (一個檔案的不同部分可擁有不同密鑰)。

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**)，並提供給硬體 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 到 A17，以及 M1 到 M3 裝置上，加密作業會使用 XTS 模式的 AES-256，其中 256 位元檔案專屬密鑰會通過「密鑰衍生函數」(NIST 特別出版物 800-108) 衍生 256 位元 Tweak 密鑰和 256 位元加密密鑰。在 A9 到 A13，以及 S5 到 S9 裝置上，加密機制使用 XTS 模式的 AES-128，其中 256 位元檔案專屬密鑰經過分割，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——這可有效地為使用者資料重建「檔案保險箱」的安全模型。使用者仍必須選擇使用「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的更高層級保護類別。

## Apple 裝置上的「資料保護」

在具備「資料保護」的 Apple 裝置上，每個檔案都是使用檔案 (或範圍) 專屬密鑰來加以保護。依據檔案的可存取性情況，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接著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 (使用寫入時拷貝技術的零成本拷貝)。檔案複製後，複本的每一半會各自獲得一個用於接受寫入的新密鑰，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應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。

當打開檔案時，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 (或範圍) 專屬密鑰會使用類別密鑰來解除封裝，然後提供給硬體 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。所有封裝檔案密鑰的處理作業會在「安全隔離區」中進行；系統永遠不會直接向「應用程式處理器」洩漏檔案密鑰。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，它們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，或使用者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。使用者每次清除裝置時密鑰封裝密鑰都會更改。在 A9 (和較新版本) 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。如需更多資訊，請參閱：[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。此密鑰的功能並非提供額外的資料保密性，而是可以視需求快速清除 (由使用者使用「清除所有內容和設定」選項來清除，或者由使用者或管理者從行動裝置管理 (MDM) 解決方案、Microsoft Exchange ActiveSync 或 iCloud 發出遠端清除指令來清除)。以此方式清除密鑰將會透過加密編譯的方式讓裝置上的所有檔案無法存取。

系統可能會使用一或數個檔案 (或範圍) 專屬密鑰來加密檔案的內容，該密鑰使用類別密鑰封裝並儲存在檔案的後設資料中，檔案後設資料接著又使用檔案系統密鑰進行加密。類別密鑰使用硬體 UID 取得保護，而某些類別則透過使用者密碼取得保護。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。配備 Apple 晶片的 Mac 電腦不支援類別 D：「無保護」，安全界限是針對登入與登出而建立 (而不是如 iPhone 和 iPad 般針對裝置鎖定或解鎖而建立)。

類別	保護類型
類別 A: 完整保護	NSFileProtectionComplete
類別 B: 未打開檔案的保護	NSFileProtectionCompleteUnlessOpen
類別 C: 首次使用者認證前的保護	NSFileProtectionCompleteUntilFirstUserAuthentication
<b>【注意】</b> macOS 使用卷宗密鑰來重建「檔案保險箱」保護特性。	
類別 D: 無保護	NSFileProtectionNone
<b>【注意】</b> macOS 不支援。	

### 完整保護

**NSFileProtectionComplete:** 類別密鑰會使用從使用者密碼和裝置 UID 所衍生的密鑰加以保護。使用者鎖定裝置後不久 (若「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，如此一來只有在使用者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，上一個使用者登出後不久，系統會捨棄已解密的類別密鑰，如此一來，只有當同一個使用者再次輸入密碼或使用 Touch ID 或 Face ID 登入裝置時，才可以存取此類別中的所有資料。

## 未打開檔案的保護

**NSFileProtectionCompleteUnlessOpen**：裝置鎖定或使用者登出時可能需要寫入某些檔案。在背景中下載的電子郵件附件就是一個典型的例子。此行為是藉由使用非對稱橢圓曲線加密 (ECDH over Curve25519) 技術來達成。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 是鏈結密鑰衍生函數 (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 則用於雜湊函式。檔案一旦關閉，檔案專屬密鑰便會從記憶體中清除。若要再次打開檔案，系統會使用「未打開檔案的保護」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，系統上的任何使用者只要登入或經過認證，就能取用 NSFileProtectionCompleteUnlessOpen 的私密部分。

## 首次使用者認證前的保護

**NSFileProtectionCompleteUntilFirstUserAuthentication**：此類別與「完整保護」類別的行為方式相同，只是在鎖定裝置或使用者登出時，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上型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，只要掛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。因為解密該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遠端清除時才具有效益。即使未對檔案指定「資料保護」類別，此檔案仍會以加密形式儲存 (就像 iOS 和 iPadOS 裝置上的所有資料一樣)。

macOS 不支援此功能。

**【注意】**在 macOS 中，針對沒有與啟動的作業系統對應的卷宗，只要掛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

在 iOS、iPadOS、tvOS 和 watchOS 中，系統會收集檔案和鑰匙圈「資料保護」類別的密鑰，並在 Keybag 中進行管理。這些作業系統使用下列 Keybag：使用者、裝置、備份、託管和「iCloud 備份」。

### 使用者 Keybag

使用者 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，會從使用者 Keybag 中載入 NSFileProtectionComplete 並解除封裝。這是二進位屬性列表 (.plist) 檔案，儲存在「無保護」類別中。

在配備 A9 以前 SoC 的裝置上，.plist 檔案內容以密鑰 (保存在可抹除儲存空間中) 加密。為了對 Keybag 提供更高的安全性，使用者每次更改密碼時，系統都會清除並重新產生此密鑰。

在配備 A9 或後續晶片 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」所控制的反重複值保護。

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

## 裝置 Keybag

裝置 Keybag 是用來儲存封裝類別密鑰 (用於與裝置專屬有關的作業)。設為共用的 iPadOS 裝置有時需要先存取憑證, 才能讓任何和使用者登入, 因此需使用不受使用者密碼保護的 Keybag。

iOS 和 iPadOS 不支援使用者專屬檔案系統內容的加密編譯分隔, 這表示系統會使用來自裝置 Keybag 的類別密鑰來封裝檔案專屬密鑰。不過, 鑰匙圈會使用來自使用者 Keybag 的類別密鑰來保護使用者鑰匙圈裡的項目。在針對單一使用者 (預設設定) 設定的 iPhone 和 iPad 裝置上, 裝置 Keybag 和使用者 Keybag 是同一個, 且受使用者的密碼保護。

## 備份 Keybag

備份 Keybag 是在 Finder (macOS 10.15 或以上版本) 或 iTunes (macOS 10.14 或較早版本) 進行加密備份時製作, 其儲存在裝置進行備份的電腦上。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備份它們的裝置, 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。而安全性夠高的密碼可以降低此威脅。

若使用者選擇不加密備份, 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 用於透過 USB 和 行動裝置管理 (MDM) 來與 Finder (macOS 10.15 或以上版本) 或 iTunes (macOS 10.14 或以上版本) 同步。此 Keybag 可讓 Finder 或 iTunes 在不要求使用者輸入密碼的情況下執行備份和同步, 還能讓 MDM 解決方案從遠端清除使用者密碼。它儲存在用來與 Finder 或 iTunes 進行同步的電腦, 或者遠端管理裝置的 MDM 解決方案上。

託管 Keybag 改善了裝置同步期間的使用者體驗, 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, 系統會提示使用者輸入密碼。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割到裝置和主機或伺服器上, 其資料則以「首次使用者認證前的保護」類別儲存在裝置上。這就是使用者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) 軟體更新, 在一開始進行更新時, 系統會提示使用者輸入密碼。這會用來安全地建立一次性解鎖代號, 其會在更新後解鎖使用者 Keybag。若未輸入使用者的密碼, 便無法產生此代號, 且若使用者密碼有所更改, 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體更新安裝情形。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 (或後續晶片) SoC 上, 即時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」控制的反重放值保護。

手動軟體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 或以上版本中, 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。若裝置在 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, 軟體更新將會自動執行:

- 已在 iOS 12 或以上版本中設定自動更新。
- 使用者在收到更新通知時選擇「稍後安裝」。

使用者輸入密碼後, 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, 並在每一次的後續解鎖時重新建立。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 中的所有類別密鑰都是非對稱式的 (與「未打開檔案的保護」資料保護類別一樣, 使用 Curve25519)。非對稱式 Keybag 也用來保護復原「iCloud 鑰匙圈」所需的備份鑰匙圈。

## 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提供使用者資料存取權給經授權的使用者。「資料保護」類別的設計目的是支援各種使用情況, 例如即使裝置遭鎖定 (但須在首次解鎖後) 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使用者資料的存取, 例如用於裝置韌體升級 (DFU) 模式、復原模式、Apple 診斷或軟體更新期間使用的模式。這些功能的基礎是硬體和軟體功能的組合, 並隨著 Apple 設計的晶片發展而擴展。

功能	A10	A11 至 A17 S3 至 S9 M1、M2、M3
復原: 所有資料保護類別均受到保護	✓	✓
DFU 模式、復原和軟體更新的替用開機: 類別 A、B 和 C 資料受到保護	✗	✓

「安全隔離區」AES 引擎配備可鎖定的軟體種子位元。從 UID 建立密鑰時, 這些種子位元會包含在密鑰衍生函式中以建立其他密鑰階層。種子位元的使用方式因系統單晶片而異:

- 自 Apple A10 和 S3 SoC 起, 種子位元專門用於區分受使用者密碼保護的密鑰。種子位元是為了需要使用者密碼的密鑰而設 (包含「資料保護類別 A」、「類別 B」和「類別 C」密鑰), 而無需使用者密碼的密鑰 (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。
- 在系統為 iOS 13 或以上版本和 iPadOS 13.1 或以上版本且配備 A10 或較新版本裝置上, 當裝置開機進入「診斷模式」時, 所有使用者資料都經過加密編譯而變得無法存取。方法為引入額外的種子位元, 其設定管控著媒體密鑰的存取權, 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 (以及所有檔案的內容)。這個保護機制適用於受到所有類別 (A、B、C 和 D) 保護的檔案, 不只是需要使用者密碼的檔案。
- 在 A12 SoC 上, 如果「應用程式處理器」已進入裝置韌體升級 (DFU) 模式或復原模式, 「安全隔離區」開機 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。此設計是為了防止存取受使用者密碼保護的資料。

在裝置進入 DFU 模式後加以回復, 可讓裝置回到已知的正常狀態, 該狀態可確保只會使用未經修改且由 Apple 簽署的程式碼。可透過手動方式進入 DFU 模式。

請參閱以下 Apple 支援文章以瞭解如何讓裝置進入 DFU 模式:

裝置	Apple 支援文章
iPhone、iPad	<a href="#">如果忘記 iPhone 密碼</a>
Apple TV	<a href="#">如果你在 Apple TV 上看到警告符號</a>
配備 Apple 晶片的 Mac	<a href="#">如何喚醒或回復 Mac 的韌體</a>

## 遭遇攻擊時保護使用者資料

企圖擷取使用者資料的攻擊者，通常會嘗試多種手法：將加密的資料擷取到另一個媒介上，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安全性規則以便發動攻擊。若要攻擊裝置上的資料，通常需要使用實體介面（例如 Thunderbolt、Lightning 或 USB-C）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，其設計用意在於確保加密編譯材料經過轉譯，一旦離開裝置，或是如果在無適當使用者授權的情況下操縱作業系統版本或安全性設定，便無法存取這些材料。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體暫存器予以支援，以便為解密非「安全隔離區」相關之使用者資料所需的密鑰，提供額外一層保護。

**【注意】**裝置必須配備 Apple 設計的 SoC，才能使用 SKP。

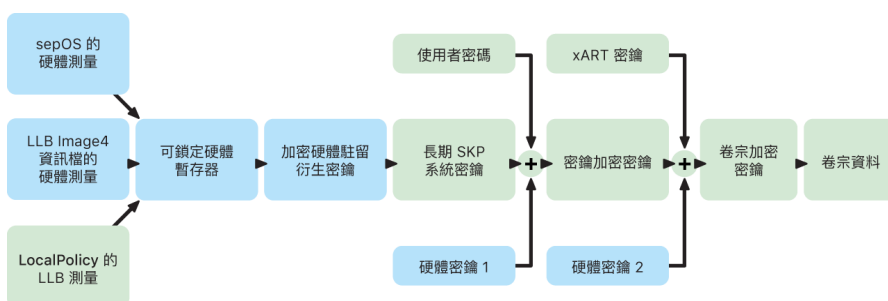
功能	A11 至 A17 S3 至 S9 M1、M2、M3
密封密鑰保護	✓

iPhone 和 iPad 裝置也可以設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) 受到系統上軟體的測量值保護 (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，整合了有關系統安全性規則的資訊，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安全性規則更改 (例如，停用安全開機或 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) 來導入。

衍生自使用者密碼、長期 SKP 密鑰和硬體密鑰 1 (「安全隔離區」的 UID) 的密鑰稱為**密碼衍生密鑰**。此密鑰用於保護使用者 Keybag (在所有受支援的平台上) 和 KEK (僅在 macOS 上)，然後啟用生物特徵辨識解鎖或使用其他裝置 (如 Apple Watch) 自動解鎖。



「安全隔離區」的「開機監視器」會擷取所載入「安全隔離區」OS 的測量值。當「應用程式處理器」的「開機 ROM」測量附加至 LLB 的 Image4 資訊檔時，該資訊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 的核心安全性設定。LocalPolicy 也包含 **nsih** 欄位，這是 macOS Image4 資訊檔的雜湊。macOS Image4 資訊檔包含所有 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) 的測量值。

如果攻擊者能未預期地更改任何上述任何受到測量的韌體、軟體或安全性設定元件，便會修改儲存在硬體暫存器中的測量。修改測量值會造成從**系統測量根密鑰 (SMRK)** 衍生的加密硬體衍生為其他值，會直接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)**，進而造成無法存取 KEK 和資料。

然而，當系統未受攻擊時，必須根據合法軟體更新進行調適，這些更新會更改韌體測量及 LocalPolicy 中的 `nsih` 欄位以指向新的 macOS 測量。在其他企圖整合韌體測量但沒有已知真實來源的系統中，使用者必須停用安全性、更新韌體，然後再重新啟用，這樣才能擷取新的測量基準。這大幅提高了攻擊者在軟體更新期間可能竄改韌體的風險。Image4 資訊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 的硬體，也可以將 SMDK 加密為建議的未來 SMRK。藉由指定軟體更新後預期的測量，硬體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 中的安全性設定時，必須根據 LLB 下次重新啟動時會運算的 LocalPolicy 測量值，將 SMDK 加密為未來 SMRK。

## 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、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「寫入時拷貝」機制、空間共享、檔案與目錄複製、快照、快速目錄大小調整、自動安全儲存基本型別，以及改良的檔案系統基礎，而且獨特的寫入時拷貝設計採用 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 可隨需分配儲存空間。當單一 APFS 容器包含多個卷宗時，可共享容器的可用空間，並在需要時分配至任何個別卷宗。每個卷宗只會使用整個容器的一部分，因此可用空間是容器的總計大小，減去容器內所有卷宗中已用空間的大小。

### 多個卷宗

在 macOS 10.15 或以上版本中，用來啟動 Mac 的 APFS 容器必須包含至少五個卷宗，而使用者無法看見前三個卷宗：

- **開機前卷宗**：此卷宗未加密，並包含啟動容器中每個系統卷宗所需的資料。
  - **VM 卷宗**：此卷宗未加密，macOS 使用其來儲存加密的交換檔案。
  - **復原卷宗**：此卷宗未加密，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**：包含下列各項：
    - 啟動 Mac 所需的所有檔案
    - macOS 原生安裝的所有 App (原來位於「/應用程式」檔案夾的這些 App 現在位於「系統/應用程式」)
- 【注意】**在預設情況下，沒有任何程序可以寫入「系統」卷宗，即使是 Apple 系統程序也是如此。
- **資料卷宗**：包含可更改的資料，例如：
    - 使用者檔案夾中的所有資料，包括照片、音樂、影片和文件
    - 使用者安裝的 App，包括 AppleScript、Automator 應用程式
    - 使用者、組織或第三方 App 安裝的自訂框架和服務程式
    - 使用者擁有且可寫入的其他位置，如 /應用程式、/資源庫、/使用者、/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 和復原卷宗都是共享卷宗，不能複製。

在 macOS 11 或以上版本中，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掛載啟動。

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。鑰匙圈能以安全的方式儲存這些項目。不同的 Apple 作業系統使用不同機制來強制執行與不同鑰匙圈保護類別相關聯的保證。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」會產生對服務程式發出的呼叫，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 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、佈建描述檔和 [Apple Developer Program](#) 強制執行。

系統用來保護鑰匙圈項目的類別結構，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	NSFileProtectionComplete UnlessOpen	✘
首次解鎖後	NSFileProtectionComplete UntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
總是	NSFileProtectionNone	kSecAttrAccessibleAlways
密碼已啟用	✘	kSecAttrAccessibleWhen PasscodeSetThisDeviceOnly

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

若密碼遭移除或重置，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拷貝時一律受到 UID 保護，因此若回復到其他裝置，將會無法使用。Apple 依據所保護資訊的類型和 iOS 和 iPadOS 需要這些資訊的時間來選擇不同的鑰匙圈類別，妥善地在安全性與可用性之間取得平衡。

## 鑰匙圈資料類別保護

系統會為鑰匙圈項目強制執行以下所列的類別保護。

項目	可存取
Wi-Fi 密碼	首次解鎖後
郵件帳號	首次解鎖後
Microsoft Exchange ActiveSync 帳號	首次解鎖後
VPN 密碼	首次解鎖後
LDAP、CalDAV、CardDAV	首次解鎖後
社群網路帳號代號	首次解鎖後
接力功能的廣播加密密鑰	首次解鎖後
iCloud 代號	首次解鎖後
iMessage 密鑰	首次解鎖後
家人共享密碼	未鎖定時
Safari 密碼	未鎖定時
Safari 書籤	未鎖定時
Finder/iTunes 備份	未鎖定時, 不可遷移
VPN 憑證	首次解鎖後, 不可遷移
藍牙密鑰	永遠, 不可遷移
Apple 推播通知服務 (APNs) 代號	永遠, 不可遷移
iCloud 憑證和專用密鑰	永遠, 不可遷移
SIM PIN	永遠, 不可遷移
尋找功能的代號	總是
語音信箱	總是

在 macOS 上, 透過設定描述檔安裝的所有鑰匙圈項目**永遠**可供取用。在 iOS 和 iPadOS 上, 透過設定描述檔安裝的鑰匙圈項目根據其類型、參考方式和安裝時間, 提供取用的情況會有所不同。依照預設, 使用設定描述檔安裝的鑰匙圈項目在**首次解鎖後可供取用且不可遷移**。但是如果發生以下情況, 透過設定描述檔安裝的鑰匙圈項目**永遠**可供取用:

- 升級至 iOS 15、iPadOS 15 或以上版本之前就安裝
- 本身為憑證 (而非身分)
- 為 IdentityCertificateUUID 在 com.apple.mdm 承載資料中參考的身分

## 鑰匙圈存取控制

「鑰匙圈」可使用連線權限控制列表 (ACL) 來設定可存取性和認證需求的規則。項目可以設定在哪些條件下必須由使用者進行認證, 方法是指定需使用 Face ID、Touch ID 或輸入裝置密碼進行認證, 否則無法存取。若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是否未經過更改。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。

## macOS 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使用者名稱和密碼、數位識別身分、加密密鑰和安全註釋。在「/應用程式/工具程式/」中打開「鑰匙圈存取」App 便可存取。使用鑰匙圈便無需輸入（甚至不需要記住）每個資源的憑證。系統會為每位 Mac 使用者製作一個初始預設鑰匙圈，而使用者可針對特定目的製作其他鑰匙圈。

除了仰賴使用者鑰匙圈外，macOS 還需要許多系統層級的鑰匙圈，以維護不屬於特定使用者的認證資產，如網路憑證和公用密鑰基礎架構 (PKI) 識別身分。其中一種鑰匙圈為無法變更的「系統根」，且它儲存了網際網路 PKI 根憑證授權管理中心 (CA) 的憑證，可讓網路銀行業務和電子商務等常見作業更加順利。使用者能以類似方式將內部佈建的 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 電腦提供「檔案保險箱」（保護所有靜態資料的內建加密功能）。「檔案保險箱」使用 AES-XTS 資料加密演算法來保護內置和可卸除式儲存裝置上的所有卷宗。

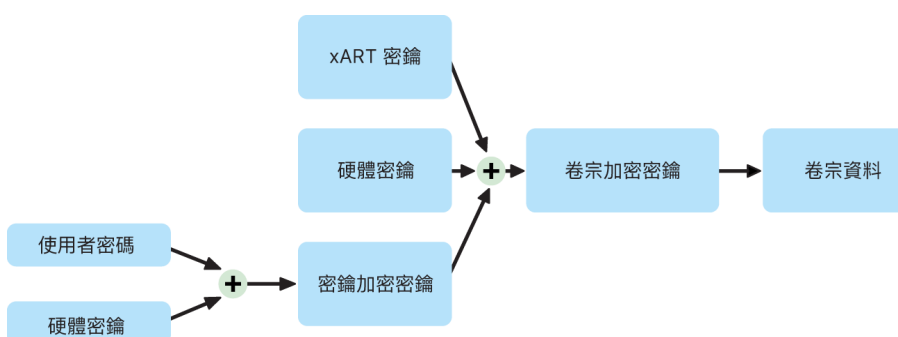
在配備 Apple 晶片的 Mac 上，「檔案保險箱」是使用「資料保護」的「類別 C」（採用卷宗密鑰）所導入。在配備 Apple 晶片的 Mac 和配備 Apple T2 安全晶片的 Mac 上，直接連接「安全隔離區」的加密內部儲存裝置會使用自身和 AES 引擎的硬體安全功能。使用者在 Mac 上開啟「檔案保險箱」後，需在開機程序進行期間提供其憑證。

**【注意】**如果 Mac 電腦，(1) 是配備 T2 晶片機型之前的舊款機型，或者 (2) 內部儲存空間並非 Mac 出廠原裝，或者 (3) 連接了外接儲存裝置：在開啟「檔案保險箱」後，所有現有檔案和後續寫入的任何資料都將被加密。在開啟「檔案保險箱」之前加入後刪除的資料不會加密，且也許可以使用合法資料復原工具復原。

### 開啟「檔案保險箱」的內部儲存裝置

即使實體儲存裝置已卸除並連接其他電腦，若沒有提供有效的登入憑證資料或加密復原密鑰，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 晶片的 Mac 以及配備 T2 晶片的 Mac 上，內部卷宗加密的實作方式為建構和管理密鑰階層結構，並以晶片上內建的硬體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：

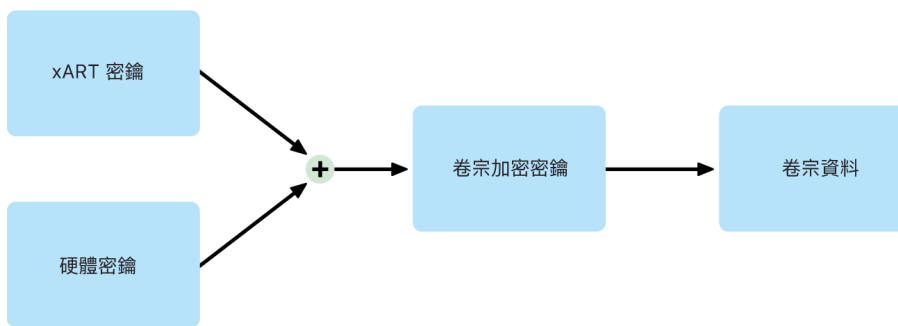
- 要求提供使用者的密碼以進行解密
- 幫助系統抵禦暴力密碼破解攻擊，以防止從 Mac 卸下的儲存媒體遭到直接攻擊
- 透過刪除必要加密編譯材料來提供迅速且安全的清除內容方式
- 讓使用者可更改其密碼（因此也可更改用來保護其檔案的加密編譯密鑰），而不需要重新加密整個卷宗



在配備 Apple 晶片的 Mac 以及配備 T2 晶片的 Mac 上，所有「檔案保險箱」密鑰處理都在「安全隔離區」中發生，絕對不會向 Intel CPU 洩漏加密密鑰。根據預設，所有 APFS 卷宗都是透過卷宗加密密鑰製作。卷宗和後設資料內容是以這個卷宗加密密鑰進行加密，而這個卷宗密鑰會和密鑰加密密鑰 (KEK) 一起封裝。當「檔案保險箱」開啟時，KEK 受到使用者密碼和硬體 UID 組合的保護。

### 關閉「檔案保險箱」的內部儲存裝置

在配備 Apple 晶片的 Mac 或配備 T2 晶片的 Mac 上，如果初始「設定輔助程式」程序執行期間沒有開啟「檔案保險箱」，卷宗仍會加密，但是卷宗加密密鑰只會受到「安全隔離區」中的硬體 UID 保護。



如果之後開啟「檔案保險箱」（因為資料已加密，此程序會立即生效），反重播機制會協助防止舊的密鑰（僅根據硬體 UID）用來將卷宗解密。卷宗便會如先前所述受到使用者密碼與硬體 UID 組合保護。

### 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。這有助於防止未來「安全隔離區」透過此密鑰進行存取。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保密性，相反地，而是設計為提供快速且安全的資料刪除方式，因為若沒有這個密鑰，就不可能解密。

在配備 Apple 晶片的 Mac 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（例如遠端 MDM 指令）來清除媒體密鑰。以此方式清除媒體密鑰，會透過加密編譯的方式讓卷宗無法存取。

### 可卸除式儲存裝置

可卸除式儲存裝置的加密不會使用「安全隔離區」的安全功能，且其加密的執行方式與採用 Intel 架構且未配備 T2 晶片的 Mac 相同。

## 在 macOS 中管理檔案保險箱

在 macOS 中，組織可以使用 SecureToken 或 Bootstrap Token 來管理「檔案保險箱」。

### 使用 Secure Token

macOS 10.13 或以上版本中的「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，是在使用者或組織於 Mac 上開啟「檔案保險箱」時所製作。在 APFS 卷宗上的 macOS 中，密鑰則是在建立使用者期間、設定第一位使用者的密碼或 Mac 使用者的首次登入期間產生的。這種加密密鑰實行方式、產生時間，以及儲存方式皆屬 **Secure Token** 功能的一部分。具體來說，Secure Token 是封裝版本的密鑰加密密鑰 (KEK)，受使用者的密碼保護。

在 APFS 上部署「檔案保險箱」時，使用者可繼續：

- 使用現有工具和程序，例如個人復原密鑰 (PRK)，其可由行動裝置管理 (MDM) 解決方案儲存以進行託管
- 延遲啟用「檔案保險箱」，直到使用者登入或登出 Mac

- 建立和使用機構復原密鑰 (IRK)

在 macOS 11 中，為 Mac 上的第一位使用者設定初始密碼會讓該使用者取得 Secure Token。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 Secure Token 將需要登入使用者帳號。為了避免此情況發生，請在設定使用者的密碼前，先將 `;DisabledTags;SecureToken` 加入程式所建立的使用者 `AuthenticationAuthority` 屬性中，如下所示：

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

## 使用 Bootstrap 代號

macOS 10.15 引入了 **Bootstrap 代號** 的新功能，以協助將安全代號授予行動帳號和透過註冊建立的選擇性裝置管理者帳號（「受管理的管理者」）。在 macOS 11 中，Bootstrap 代號可以向登入到 Mac 電腦的任何使用者（包括本機使用者帳號）授予安全代號。使用 macOS 10.15 或較新版本的 Bootstrap Token 功能有以下要求：

- 使用「Apple 校務管理」或「Apple 商務管理」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 或以上版本中，任何已啟用安全代號的使用者初次登入時，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 Token 並交由 MDM 託管。

在 macOS 11 中，Bootstrap 代號還可以用於將安全代號授予使用者帳號。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體更新項目。

## 機構與個人復原密鑰

CoreStorage 和 APFS 卷宗上的「檔案保險箱」都支援使用機構復原密鑰 (IRK，舊稱「**檔案保險箱**」主身分) 來解鎖卷宗。雖然 IRK 對於使用命令列作業來解鎖卷宗或關閉「檔案保險箱」而言很有用，但其工具程式對組織而言卻很有限，尤其是最近的 macOS 版本。而在配備 Apple 晶片的 Mac 上，IRK 沒有提供任何功能價值，主要有兩個原因：其一是 IRK 無法用來取用 recoveryOS，其次則是因為已停止支援目標磁碟模式，無法藉由連接到另一部 Mac 來解鎖卷宗。基於上述和其他原因，我們已不再建議使用 IRK 來在 Mac 電腦上管理機構的「檔案保險箱」。請改為使用個人復原密鑰 (PRK)。

# Apple 如何保護使用者的個人資料

## 保護 App 對使用者資料的存取

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 在未經授權下存取使用者的個人資料。使用者可以在 iOS 和 iPadOS 的「設定」中，以及在 macOS 的「系統設定」（macOS 13 或以上版本）或「系統偏好設定」（macOS 12 或較早版本）中，查看使用者已允許哪些 App 存取特定資訊，亦可授予或撤銷往後的任何存取權。以下情況會強制提供存取權：

- iOS、iPadOS 和 macOS：行事曆、相機、聯絡人、麥克風、照片、提醒事項和語音辨識
- iOS 和 iPadOS：藍牙、家庭、媒體、媒體 App 和 Apple Music、運動和健身
- iOS 和 watchOS：健康
- macOS：輸入監控（例如鍵盤筆劃）、提示、螢幕錄影（例如靜態擷圖和錄影），以及系統設定（macOS 13 或以上版本）或系統偏好設定（macOS 12 或較早版本）

在 iOS 13.4 或以上版本和 iPadOS 13.4 或以上版本中，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 或以上版本中的其他類別包括「區域網路」、「鄰近互動」、「研究感測器與使用狀況資料」以及「專注模式」。



如果使用者登入 iCloud，在 iOS 和 iPadOS 中預設便會授予 App 存取「iCloud 雲碟」的權限。使用者可以在「設定」中的 iCloud 底下控制每個 App 的存取權。iOS 和 iPadOS 也提供取用限制，其設計的用意是防止資料於行動裝置管理 (MDM) 解決方案和使用者所安裝的 App 和帳號之間移動。

## 保護使用者健康資料的存取

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，如相容的低功耗藍牙 (BLE) 心率監視器以及許多 iOS 裝置內建的動作副處理器。HealthKit 和健康與健身 App、醫療機構及健康與健身裝置之間的所有互動，都需要使用者的權限。此資料會儲存在「未打開檔案的保護」這個「資料保護」類別中。裝置鎖定後 10 分鐘便會捨棄資料存取權，當使用者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訊 (用來在新資料可用時啟動 App)。此資料會儲存在「資料保護」類別的「首次使用者認證前的保護」中。臨時日誌檔會儲存裝置鎖定時產生的健康記錄 (例如當使用者從事運動時)。這些臨時日誌檔會儲存在「未打開檔案的保護」這個「資料保護」類別中。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」資料的端對端加密需要 iOS 12 或以上版本及雙重認證。否則，使用者的資料仍會在儲存與傳輸期間加密，但不會以端對端加密。使用者開啟雙重認證並更新至 iOS 12 或以上版本後，其健康資料會移轉到端對端加密。

若使用者以 Finder (macOS 10.15 或以上版本) 或 iTunes (macOS 10.14 或較早版本) 備份裝置，只有在備份經過加密的情況下才會儲存健康資料。

### 臨床健康記錄

使用者可以在「健康」App 內登入支援的健康系統，以取得一份臨床健康記錄。將使用者連接到健康系統時，使用者需使用 OAuth 2 用戶端憑證進行驗證。連線成功後，便會使用受到 TLS 1.3 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。

### 健康資料真實性

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數位簽章副本。其用意是為記錄 (由受信任之裝置所產生) 提供資料真實性。用於數位簽章的格式為 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「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 也必須提供隱私政策給使用者，並詳述其對健康資料的使用方式。

App 對健康資料的存取權是受使用者的「隱私權」設定所控制。當 App 要求存取健康資料時 (類似於「聯絡人」、「照片」和其他 iOS 資料來源)，系統會要求使用者授予存取權。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。使用者可以在「設定」>「健康」>「資料權限與裝置」底下檢視和撤銷他們授予存取健康資料的權限。

若 App 取得寫入資料的權限，便也可讀取其寫入的資料。若 App 取得讀取資料的權限，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。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。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。此設計用意可避免 App 藉由得知使用者正在追蹤的資料類型，來推測使用者的健康狀態。

## 使用者的「醫療卡」

「健康」App 可讓使用者選擇填寫「醫療卡」表單和發生緊急醫療事故時所需的重要資料。此資訊是手動輸入或更新，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「醫療卡」資訊。此資訊會使用「無保護」這個「資料保護」類型來儲存於裝置上，如此一來無須輸入裝置密碼即可存取。「醫療卡」是選擇性的功能，可讓使用者決定如何同時在安全性和隱私考量上取得平衡點。此資料在 iOS 13 或更早版本上會備份在「iCloud 備份」中。在 iOS 14 中，「醫療卡」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 為使用者提供了與其他使用者分享「健康」資料的選項。「健康」資料會使用端對端 iCloud 加密在兩位使用者之間分享，而 Apple 無法取用透過「健康」分享所傳送的資料。若要使用此功能，傳送的使用者和接收的使用者都必須執行 iOS 15 或以上版本並啟用雙重認證。

使用者也可以選擇使用「健康」App 中的「與提供者分享」功能，與他們的醫療服務提供者分享他們的「健康」資料。使用此功能分享的資料僅供使用者使用端對端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。若要進一步瞭解此服務設計如何保護使用者的「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[「安全性與隱私」](#)章節。

# 數位簽章與加密

## 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分的 App 存取，除非使用者明確核准那些 App。此保護措施便能針對組織在 Apple 裝置中使用的各種應用程式與服務提供保護認證身分的機制。

## 郵件

在「郵件」App 中，使用者可以傳送經過數位簽章及加密的訊息。「郵件」會在相容智慧卡中所附加的「個人識別驗證」(PIV) 代號上，於數位簽章和加密憑證上自動搜索適用的 RFC 5322 (區分大小寫) 電子郵件地址主旨或主旨替代名稱。如果設定的電子郵件帳號符合附加 PIV 代號上數位簽章和加密憑證中的電子郵件地址，「郵件」就會自動在新訊息視窗的工具列中顯示簽章按鈕。如果「郵件」具有收件人的電子郵件加密憑證或可在 Microsoft Exchange 全域通訊清單 (GAL) 找到它，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。

## 個別郵件 S/MIME

iOS、iPadOS 和 macOS 支援個別郵件 S/MIME 技術。這代表 S/MIME 使用者依照預設可選擇一律簽署和加密訊息，或者選擇性地簽署和加密個別訊息。

搭配 S/MIME 使用的認證可使用設定描述檔、行動裝置管理 (MDM) 解決方案、「簡單憑證註冊通訊協定」(SCEP) 或 Microsoft Active Directory 憑證授權單位來傳遞至 Apple 裝置。

## 智慧卡

macOS 10.12 或以上版本原生支援 PIV 卡。這些卡片廣泛用於商業和政府機構的雙重認證、數位簽章和加密用途。

智慧卡包含一或多個數位身分識別，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) 的憑證驗證 (簽署)。

智慧卡可用於雙重認證。解鎖卡片所需的兩個要素為「使用者擁有的東西」(卡片) 和「使用者知道的內容」(PIN)。macOS 10.12 或以上版本也原生支援智慧卡「登入視窗」認證，及 Safari 上的網站用戶端憑證認證。此外也支援使用密鑰組 (PKINIT) 的 Kerberos 認證，用於使用 Kerberos 技術支援的單一登入服務。若要瞭解有關智慧卡和 macOS 的更多資訊，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，加密磁碟映像檔的功用為安全容器，使用者可以在其中儲存或傳送敏感文件和其他檔案。加密磁碟映像檔是使用「磁碟工具程式」所製作，位於「/應用程式/工具程式/」。可使用 128 位元或 256 位元 AES 加密方式來加密磁碟映像檔。由於裝載的磁碟映像檔會視為連接 Mac 的本機卷宗，因此使用者可以拷貝、搬移和打開其中儲存的檔案和檔案夾。如同「檔案保險箱」，磁碟映像檔的內容可以即時加密和解密。使用加密磁碟映像檔，使用者可以將加密磁碟映像檔儲存到可卸除式媒體上、以郵件附件形式傳送，或是儲存在遠端伺服器上，以安全地交換文件、檔案和檔案夾。如需加密磁碟映像檔的詳細資訊，請參閱 [磁碟工具程式使用手冊](#)。

# App 安全性

## App 安全性概覽

App 是現在安全架構最關鍵的要素之一。雖然 App 可顯著提高使用者的生產力，但若處理不當，也可能對系統安全性、穩定性和使用者資料產生負面影響。

因此 Apple 提供多層保護，有助於確保 App 沒有包含已知的惡意軟體且未遭竄改。其他保護機制強制要求謹慎協調 App 對使用者資料的存取。這些安全控制提供了穩定且安全的平台，讓成千上萬的開發者能夠提供數十萬款的 iOS、iPadOS 和 macOS App，而不會影響系統的完整性。使用者可以在其 Apple 裝置上存取這些 App，無須過度擔心病毒、惡意軟體或未經授權的攻擊。

在 iPhone 和 iPad 上，所有 App 都需從 App Store 取得，且所有 App 都以沙盒技術限制，以提供最嚴格的控制。

在 Mac 上，許多 App 是從 App Store 取得，但是 Mac 使用者也可以從網際網路下載並使用 App。為了安全支援網際網路下載，macOS 提供多層額外控制。首先，在 macOS 10.15 或以上版本的預設狀態下，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體，同時讓這些 App 可以不必透過 App Store 來提供。其次，macOS 包含最先進的防毒保護機制，可封鎖惡意軟體並在必要時予以移除。

作為額外的控制存取平台，沙盒可協助保護使用者資料，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，因此有助於確保使用者保有「桌面」、「文件」、「下載項目」中檔案和所有 App 的其他區域的存取控制權，無論嘗試存取其 App 本身是否以沙盒技術限制。

原生能力	第三方等效機制
外掛模組未核准列表、Safari 延伸功能未核准列表	病毒/惡意軟體定義
檔案隔離	病毒/惡意軟體定義
XProtect/YARA 簽章	病毒/惡意軟體定義；端點防護
門禁	端點防護；在 App 上強制執行程式碼簽章，以協助確保僅執行受信任的軟體
eficheck (未配備 Apple T2 安全晶片的 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	內建於 macOS
強制存取權限控制	內建於 macOS
Kext 排除列表	內建於 macOS
強制 App 程式碼簽署	內建於 macOS

## iOS 和 iPadOS 的 App 安全性

### iOS 和 iPadOS 的 App 安全性簡介

與其他行動平台不同，iOS 和 iPadOS 不允許使用者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。相反地，（歐盟以外地區）所有 App 都需從 App Store 下載，確保所有 App 皆來自已識別的開發者，且需通過自動與人工審核。在執行階段，會在載入所有可執行記憶體頁面後對其進行程式碼簽章檢查，以協助確保 App 自安裝或上次更新後未曾遭到修改。

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 或系統的其他部分。

### 關於 App Store 安全性

App Store 是受信任的資源，使用者可以在此安全地發掘及下載 App。App Store 上的 App 都來自同意遵循 Apple 準則的已識別開發者，且皆透過無法修改的加密保證以安全地發佈給使用者。每款 App 及每項 App 更新都會經過審核，評估是否達到隱私權、安全性與安全防護的要求。這個過程持續不斷改進，旨在保護使用者，將惡意軟體、網路犯罪和詐騙擋在 App Store 外。此外，專為兒童設計的 App 需遵循嚴格的資料收集與安全準則以確保兒童安全，且需與 iOS 和 iPadOS 的分級保護控制功能緊密整合。

App Store 的安全性保護功能包括：

- **自動掃描已知的惡意軟體：**協助防止它們入侵 App Store 而影響或妨害到使用者。
- **由專業團隊進行人工審核：**審核行銷文字、截圖等 App 描述內容的準確性。這項審核大舉防範了用以散佈惡意軟體的最常見詐騙方式：將惡意軟體偽裝成熱門 App，或聲稱提供不存在的誘人功能。
- **人工檢查：**檢查 App 是否未要求存取不必要的敏感性資料，並對專為兒童所設計的 App 進行額外評估，以協助確保其遵守嚴格的資料收集與安全規則。
- **可信度高且匯集一處的使用者評論：**協助浮現問題，並大幅降低攻擊者誤導廣大使用者的可能性。即使惡意 App 能在審核程序中完全隱藏其行為，遇到並回報問題的 App 使用者也能警示其他使用者及 Apple，進而提供另一種偵測途徑。App Store 積極打擊詐騙評論，以提高此訊號的價值。
- **修正與移除流程：**以防發生問題。在 App 上架 App Store 後才被發現違反準則的情況下，Apple 會與開發者一起快速解決此問題。在涉及詐騙和惡意活動的危險情況下，App 會立即從 App Store 下架，而已下載此 App 的使用者也能收到 App 惡意行為的通知。

iOS 和 iPadOS 上的 App 安全性仰賴於每個層面的緊密配合：透過完善的 App 審核來防止惡意 App 的安裝，以及藉由強大的平台保護來限制惡意 App 可能造成的損害。iOS 和 iPadOS 在設計中深植的安全性為使用者提供了所有消費性裝置中最強大的保護，但這些保護措施的設計沒有防止使用者可能因遭誘騙而做出的選擇。App 審核會強制執行 App Store 安全性原則，這些原則是設計來避免 App 企圖損害使用者或誘騙他們授予敏感性資料的取用權限。而且，在惡意 App 試圖略過裝置防護的極度嚴重情況下，App 審核首先就會讓其難以侵入使用者的裝置。

雖然僅靠 App Store 安全性措施無法滴水不漏地完全防範，但作為平台安全性防禦深度策略的一部分，它們仍有助於讓針對 iOS 和 iPadOS 使用者的廣泛攻擊變為徒勞一場，並使金融相關的攻擊者得不償失。透過在 App Store 上架前就先審核每個 App，就可以協助確保其不含惡意軟體，且能為使用者帶來正確的體驗。審核過程中如果發現了有害 App，Apple 還會迅速移除以停止發佈，並限制未來不同版本的傳播。藉此保護生態系統的安全性，也讓客戶能全然安心。

## iOS 和 iPadOS 的 App 程式碼簽署程序

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

### 強制程式碼簽署

iOS 或 iPadOS 核心啟動後，會控制哪些使用者程序和 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 和 iPadOS 會要求所有可執行的程式碼均使用 Apple 核發的憑證進行簽署。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 核發的憑證進行驗證和簽署。強制性程式碼簽署將信任鏈的概念從作業系統延伸至 App，可協助防止第三方 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）對他們的 App 進行簽署。他們還可以在 App 中嵌入框架，並使用 Apple 核發的憑證（透過團隊識別碼）對程式碼進行驗證。

- **憑證的驗證：**若要在 iPhone 或 iPad 裝置上開發並安裝 App，開發者必須向 Apple 註冊並加入 Apple Developer Program。Apple 會先驗證每位開發者（無論是個人或企業）的真實身分，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 都是由身分可識別的個人或組織提交的，藉此阻止製作惡意 App。這些 App 都經過 Apple 嚴格審核，以協助確保它們可以如所述方式正常執行，且沒有明顯的程式錯誤或其他重大問題。除了已討論過的技術外，此挑選過程還會讓使用者對所購買的 App 的品質更加放心。
- **程式碼簽章驗證：**iOS 和 iPadOS 允許開發者將框架嵌入 App 中，以便供 App 本身或嵌入 App 中的延伸功能使用。為了保護系統並防止其他 App 在其位址空間中載入第三方的程式碼，系統將為啟動時程序所連結的所有動態資源庫執行程式碼簽章驗證。此驗證過程透過團隊識別碼（Team ID）來達成，該識別碼擷取自 Apple 核發的憑證。團隊識別碼是 10 個字元的英數字元字串，例如 1A2B3C4D5F。程式可透過連結到隨系統發佈的任何資源庫平台，或其程式碼簽章中具有相同團隊識別碼的資源庫平台來成為主要執行檔。作為系統一部分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源庫。

### 驗證內部專用 App

合格的企業可以編寫供組織內部使用的內部專用 App，並分發給員工。企業和組織可以申請加入 Apple Developer Enterprise Program (ADEP, Apple 開發者企業計畫)。如需更多資訊並檢閱資格要求，請參閱：[Apple Developer Enterprise Program 網站](#)。組織成為 ADEP 的成員後，便可註冊以取得一個佈建描述檔，該描述檔允許內部專用 App 在其授權的裝置上執行。

使用者必須安裝佈建描述檔才能執行這些 App。這可以協助確保只有組織要求的使用者能夠將 App 載入到其 iPhone 或 iPad 上。透過行動裝置管理 (MDM) 安裝的 App 會間接獲得信任，因為組織與裝置間的關係已建立。在其他情況下，使用者必須在「設定」中核准 App 的佈建描述檔。組織也可以限制使用者，不允許其核准來自未知開發者的 App。第一次啟動任一內部專用 App 時，裝置必須收到來自 Apple 允許執行 App 的確認。

## iOS 和 iPadOS 的執行階段程序安全性

iOS 和 iPadOS 藉由使用沙盒、宣告授權及位址空間配置隨機載入 (ASLR) 來協助確保執行階段的安全性。

## 沙盒

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更動時會受到限制。沙盒的設計可防止 App 收集或修改其他 App 儲存的資訊。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訊以外的其他資訊，只能透過 iOS 和 iPadOS 明確提供的服務來執行。

系統檔案和資源也會與使用者的 App 加以區隔。大部分的 iOS 和 iPadOS 系統檔案和資源會執行為非特權使用者「行動裝置」，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（如遠端登入服務）並未包含在系統軟體中，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 對使用者資訊，以及功能（如 iCloud）和延伸功能的存取權。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 使用者 ID）進行認證。授權已經過數位簽章，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，則需要以根使用者身分執行程序。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續航力。

## 位址空間配置隨機載入

位址空間配置隨機載入（ASLR）可協助防止利用記憶體損壞錯誤發動的攻擊。內建 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、系統資源庫和相關程式設計結構的記憶體位址，進一步降低遭到許多攻擊的可能性。例如，「return-to-libc」攻擊試圖藉由操縱堆疊和系統資源庫的記憶體位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大幅增加執行攻擊的難度，尤其是對多部裝置的攻擊。Xcode 和 iOS 或 iPadOS 開發環境，可在開啟 ASLR 支援的狀態下自動編譯第三方程式。

## 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 若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位址）。Safari 就是將此功能用於 JavaScript just-in-time (JIT) 編譯器。

## 在 iOS、iPadOS 和 macOS 中支援延伸功能

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，並提供給使用相符系統的其他 App 使用。

## 擴充點

支援延伸功能的系統區域稱為**擴充點**。每個擴充點都提供 API，並為該區域強制執行規則。系統依據擴充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，「今天顯示方式」小工具只會顯示在「通知中心」內，而共享的延伸功能則只能從「共享」面板中使用。舉例來說，「今天」小工具、「分享」、「動作」、「照片編輯」、「檔案提供程式」和「自訂鍵盤」都是擴充點。

## 延伸功能的通訊方式

延伸功能會在自己的位址空間中執行。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 對隱私權控制具有相同的存取權限。因此，若使用者對 App 授予「聯絡人」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，是由使用者啟用且適用於整個系統。鍵盤延伸功能啟用後，會用於所有文字欄位，但密碼輸入和任何安全文字的顯示方式除外。為了限制使用者資料的傳送，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路、阻止代表程序執行網路操作的服務，並阻止可允許延伸功能暗中輸入資料的 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，讓系統在得到使用者的同意後在預設的沙盒中執行延伸功能。

## MDM 與延伸功能

對於在行動裝置管理 (MDM) 解決方案中註冊的裝置，文件和鍵盤延伸功能將遵循「受管理的打開方式」原則。例如，MDM 解決方案可協助防止使用者將受管理 App 中的文件輸出到未受管理的「文件提供程式」，或協助防止他們在受管理的 App 中使用未受管理的鍵盤。此外，App 開發者可避免在其 App 中使用第三方的鍵盤延伸功能。

## iOS 和 iPadOS 中的 App 保護和 App 群組

在 iOS 和 iPadOS 中，組織可以使用 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 軟體開發套件 (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，而加密密鑰會以使用者裝置上的密碼進行保護。「行事曆」(不包括附件)、「聯絡人」、「提醒事項」、「備忘錄」、「訊息」和「照片」會導入 Data Protection 授權的「首次使用者認證前的保護」。

沒有選擇加入某個特定「資料保護」類別且由使用者安裝的 App 預設會接受「首次使用者認證前的保護」。

### 加入 App 群組

指定開發者帳號所擁有的 App 和延伸功能在設定為「App 群組」的一部分後，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」的一部分後，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) 可協助確保 App 群組 ID (GID) 在整個 App 生態系統中均不重複。

## macOS App 安全性

### macOS 的 App 安全性簡介

macOS 的 App 安全性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，可協助確保從網際網路下載的 App 不含已知的惡意軟體。macOS 也提供偵測和移除惡意軟體的技術，以及專為防止不受信任的 App 存取使用者資料而設計的額外保護。Apple 服務 (例如「公證」和 XProtect) 設計用於協助阻止惡意軟體安裝。在必要時，這些服務會找到一開始躲過偵測的惡意軟體，再快速且有效地移除之。最後，macOS 確保使用者可在易操作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 皆已經過 Apple 簽署。此簽署的設計可確保這些 App 未曾遭竄改或更動。Apple 會簽署 Apple 裝置隨附的所有 App。

在 macOS 10.15 中，所有在 App Store 外部發佈的所有 App，都必須由開發者使用 Apple 核發的開發者 ID 憑證（結合專用密鑰）來簽署，且需由 Apple 公證，才能在預設「門禁」設定下執行。企業內部開發的 App 也必須使用 Apple 核發的開發者 ID 簽署，以便讓使用者驗證其完整性。

在 macOS 中，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。開發者需使用自己的開發者 ID 憑證（Apple 所核發）來執行程式碼簽署。驗證此簽章可向使用者證明開發者的軟體未經竄改，因為是由開發者建置並簽署。公證可由軟體分銷鏈中的任何人執行，證明已提供檢查惡意軟體的程式碼拷貝給 Apple，且沒有發現任何已知惡意軟體。公證的輸出為票證，會儲存在 Apple 伺服器上，且可選擇附加至 App（任何人均可執行此操作），此過程並不會使開發者的簽署失效。

「強制存取權限控制」（MAC）需要程式碼簽署才能啟用受到系統保護的授權。例如，要求穿越防火牆權限的 App，必須以適當的 MAC 授權簽署程式碼。

## macOS 的門禁與執行階段保護

macOS 提供「門禁」技術和執行階段保護，可協助確保使用者的 Mac 上只會執行受信任的軟體。

### 門禁

macOS 包含名為「門禁」的安全性技術，此設計可協助確保使用者的 Mac 上只會執行受信任的軟體。當使用者下載並打開來自 App Store 外部 App、外掛模組或安裝程式套件時，「門禁」會驗證該軟體來自已識別的開發者，經過 Apple 公證不含已知惡意內容，且未曾遭更動。第一次打開軟體時，「門禁」也會要求使用者核准，以確認使用者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。「門禁」也會追蹤下載軟體所寫入檔案的來源。

依照預設，「門禁」可協助確保所有下載的軟體均已由 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都能確保 App 不含任何已知惡意軟體。因此依照預設，無論軟體透過何種方式安裝在 Mac 上，**macOS 中的所有軟體第一次打開時，系統都會檢查是否包含已知的惡意內容。**

使用者和組織可選擇只允許安裝來自 App Store 的軟體。或者，使用者可以覆蓋「門禁」規則以打開任何軟體，除非受到行動裝置管理（MDM）解決方案限制。組織可以使用 MDM 來配置「門禁」設定，包含允許以替身身分簽署的軟體。如有需要，也可完全停用「門禁」。

「門禁」也可防止透過安全 App 散佈的惡意外掛模組。在此情況下，當使用者使用該 App 時，會在不知情的狀況下觸發載入惡意的外掛模組。必要時，「門禁」會從隨機的唯讀位置打開 App。此設計可防止自動載入隨著 App 散佈的外掛模組。

### 執行階段保護

系統檔案、資源與核心會與使用者的 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 中防禦惡意軟體

Apple 進行一套威脅情報程序，可快速識別和阻擋惡意軟體。

### 三層防護

惡意軟體防禦具有三層結構：

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

第一層防禦機制設計用於遏制惡意軟體傳播，以及讓惡意軟體一次也無法啟動；這是 App Store 和結合「門禁」與「公證」的目標。

下一層防禦機制用於協助確保倘若惡意軟體出現在 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體染指的 Mac。XProtect 搭配「門禁」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體。

這些在下方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體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體造成的可能損害。請參閱[保護 App 對使用者資料的存取](#)，瞭解 macOS 如何協助保護使用者資料不受惡意軟體侵害，並參閱[作業系統完整性](#)，瞭解 macOS 如何限制惡意軟體可在系統上執行的動作。

## 公證

「公證」為 Apple 提供的惡意軟體掃描服務。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 會掃描這個軟體是否包含已知的惡意軟體，如果沒有發現任何惡意軟體，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「門禁」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「門禁」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，因為相較於推播新 XProtect 簽章的背景更新，在背景執行的更新頻率高出許多。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 的內建防毒技術 XProtect 可根據簽章偵測和移除惡意軟體。系統使用 YARA 簽章，此工具用於執行惡意軟體的簽章式偵測，Apple 會定期對其進行更新。Apple 會監視新的惡意軟體感染與病種，並自動更新簽章（獨立於系統更新），以協助 Mac 防止惡意軟體感染。XProtect 會自動偵測和封鎖已知惡意軟體的執行。在 macOS 10.15 或以上版本中，每當發生以下情況，XProtect 都會檢查是否包含已知的惡意內容：

- App 初次啟動
- App 經過更動（在檔案系統中）
- XProtect 簽章更新

當 XProtect 偵測到已知的惡意軟體，就會封鎖該軟體並通知使用者，提供選項讓使用者將該軟體移至「垃圾桶」。

**【注意】**「公證」對於已知檔案（或檔案雜湊）來說很有效，且可在先前已啟動的 App 上使用。XProtect 的簽章式規則比特定檔案雜湊更通用，因此可找出 Apple 未曾見過的變體。XProtect 只會掃描有變動或初次啟動的 App。

如果惡意軟體成功進入 Mac，XProtect 所包含的技術也可修復感染。例如，其包含一個引擎，可根據 Apple 自動遞送的更新（屬於系統資料檔案自動更新與安全性更新的一部分）修復感染。此系統在收到更新的資訊後會移除惡意軟體，並會定期檢查是否有感染；不過，XProtect 不會自動重新啟動 Mac。此外，XProtect 包含一個進階引擎，可以基於行為分析來偵測未知的惡意軟體。此引擎所偵測到的惡意軟體相關資訊，包含最終負責下載它的軟體，會被用來改進 XProtect 簽章和 macOS 安全性。

## 自動化 XProtect 安全性更新

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 每天都會檢查這些更新。「公證」更新是使用 CloudKit 同步來發佈，頻率高出許多。

## 發現新的惡意軟體時, Apple 如何回應

發現新的惡意軟體時, 系統會執行幾個步驟:

- 任何關聯的開發者 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 簽章。

這些簽章也可以追溯方式套用至先前通過公證的軟體, 且任何新的偵測都會產生一或多項先前發生的動作。

最後, 惡意軟體偵測機制會在接下來數秒、數小時和數天內啟動一系列步驟, 將可能的最佳防護措施傳播給 Mac 使用者。

## 在 macOS 中控制 App 對檔案的存取權

Apple 認為使用者對於哪些 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 都必須取得使用者的同意, 才能取用「文件」、「下載項目」、「桌面」、「iCloud 雲端」和網路卷宗內的檔案。在 macOS 10.13 或以上版本中, 要求完整儲存裝置存取權的 App, 必須在「系統設定」(macOS 13 或以上版本) 或「系統偏好設定」(macOS 12 或較早版本) 中明確加入。此外, 輔助使用和自動化功能需要使用者的許可, 以協助確保不會規避其他保護機制。視存取規則而定, 系統可能會要求或強制使用者前往以下位置更改設定:

- macOS 13 或以上版本: 「系統設定」> 「隱私權與安全性」> 「隱私權」
- macOS 12 或較早版本: 「系統偏好設定」> 「安全性與隱私權」> 「隱私權」

項目	App 提示使用者	使用者必須編輯系統隱私權設定
輔助使用	✗	✓
內部儲存空間完整	✗	✓
檔案和檔案夾 <b>【注意】</b> 包含「桌面」、「文件」、「下載項目」、網路卷宗和可卸除式卷宗	✓	✗
自動化 (Apple Event)	✓	✗

使用者若在 Mac 上開啟「檔案保險箱」, 系統會要求提供有效的憑證資料, 才能繼續開機程序和取得專用開機模式的取用權。即使實體儲存裝置已卸除並連接其他電腦, 若沒有提供有效的登入憑證資料或復原密鑰, 整個卷宗會維持加密狀態並禁止未經授權的存取。

若要保護企業設定的資料, IT 人員應使用行動裝置管理 (MDM) 來定義和強制執行「檔案保險箱」設定規則。組織有多個選項可用來管理加密的卷宗, 包含機構復原密鑰、個人復原密鑰 (可選擇透過 MDM 儲存以進行託管) 或兩者的組合。也可在 MDM 中將密鑰輪換設為規則。

## 「備忘錄」App 的安全功能

「備忘錄」App 包含安全備忘錄功能, 在 iPhone、iPad、Mac 和 iCloud 網站上, 都可讓使用者保護特定備忘錄的內容。使用者也可以安全地與其他人共享備忘錄。

### 安全備忘錄

安全備忘錄是以使用者提供的密語進行端對端加密, 為檢視 iOS、iPadOS、macOS 裝置和 iCloud 網站上的備忘錄所需。每個 iCloud 帳號 (包含「在我的」裝置帳號) 都能使用獨立的密語。

當使用者加密備忘錄時，會從使用者透過 PBKDF2 和 SHA256 製作的密語衍生 16 位元組密鑰。備忘錄和其所有附件都使用 AES 搭配 Galois/計數器模式 (AES-GCM) 進行加密。新的記錄會在「核心資料」和 CloudKit 中製作，以儲存加密的備忘錄、附件、標籤和初始化向量。製作新的記錄後，便會刪除原始的未加密資料。支援加密的附件包含影像、塗鴉、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忘錄。

若要檢視安全備忘錄，使用者必須輸入其密語，或是使用 Face ID 或 Touch ID 來認證。使用者成功通過認證後，無論要檢視或製作安全備忘錄，「備忘錄」都會打開安全作業階段。安全作業階段打開時，使用者可以檢視或保護其他備忘錄，不需要進行其他認證。但是安全作業階段僅適用於受到所提供密語保護的備忘錄。備忘錄若受到其他密語的保護，使用者仍需認證。安全作業階段會在以下情況關閉：

- 使用者點一下「備忘錄」中的「立即鎖定」按鈕時
- 「備忘錄」切換至背景超過 3 分鐘 (macOS 為 8 分鐘) 時
- iOS 或 iPadOS 裝置鎖定時

若要更改安全備忘錄的密語，使用者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 會重新將所有現有的備忘錄 (以先前的密語加密的備忘錄) 封裝到同一個帳號中。

如果使用者連續打錯密語三次，「備忘錄」就會顯示使用者提供的提示 (若使用者在設定時有提供)。若使用者仍無法想起密語，可以在「備忘錄」的設定中重設。此功能可讓使用者以新的密語製作新的安全備忘錄，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。重置密語需要使用者的 iCloud 帳號密語。

## 共享的備忘錄

沒有用密語進行端對端加密的備忘錄可以與其他人共享。在共享的備忘錄中，使用者加入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 可管理參與者可加密和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 與其他使用者分享捷徑。捷徑會以加密格式儲存在本機上。

自訂捷徑包羅萬象，類似於指令碼或程式。從網際網路下載捷徑時，系統會警告使用者該捷徑尚未經過 Apple 審核，且有機會檢驗該捷徑。為了抵禦惡意捷徑，系統會在執行時下載更新版惡意軟體定義，以便辨識惡意捷徑。

若從共享工作表啟動，自訂捷徑也可在 Safari 中對網站執行使用者指定的 JavaScript。為了抵禦惡意 JavaScript (例如誘騙使用者在社群媒體上執行會收集其資料的指令碼)，系統會根據上述版惡意軟體定義來驗證 JavaScript。使用者第一次在網域上執行 JavaScript 時，系統會提示使用者允許包含 JavaScript 的捷徑在該網域的目前網頁上執行。

# 服務安全性

## 服務安全性概覽

Apple 開發了一套完善的服務，可協助使用者從裝置上獲得更多實用性和生產力。這些服務提供雲端儲存、同步、密碼儲存、認證、付款、傳訊、通訊等強大的功能，同時保護著使用者的隱私及其資料的安全。

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」中使用的安全技術。

**【注意】** Apple 服務與內容不適用於部分國家或地區。

## Apple ID 與管理式 Apple ID

### Apple ID 安全性概覽

Apple ID 是用來登入 Apple 服務的帳號。對使用者而言，安全保護其 Apple ID 以協助防止帳號遭未經授權的存取十分重要。為協助保護帳號，Apple ID 需搭配高強度的密碼，其條件如下：

- 長度必須至少八個字元
- 必須包含字母和數字
- 不得包含三個或以上的連續相同字元
- 不能為常見密碼

使用者更可以超越此規則，加入更多的字元和標點符號，來讓密碼變得更為安全。

在對帳號進行重要更動（例如變更密碼或帳單資訊），或使用 Apple ID 來在新裝置上登入時，Apple 也會透過電子郵件或推播通知，或者同時透過此兩者來通知使用者。若有任何異常情事，Apple 會提示使用者立即更改其 Apple ID 的密碼。

此外，Apple 運用多種規則和程序，旨在保護使用者的帳號。這些包含限制重試登入和密碼重置的次數、積極的詐騙監視以協助識別發生的攻擊，以及定期規則檢查，可讓 Apple 因應任何可能影響使用者安全的新資訊。

**【注意】** 管理式 Apple ID 密碼規則需由管理者在「Apple 校務管理」或「Apple 商務管理」中設定。

### 雙重認證

為協助使用者進一步保護其帳號，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，仍只有帳號的持有人可以存取帳號。若使用雙重認證，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，使用者的帳號就只能在受信任的裝置上使用，例如使用者的 iPhone、iPad、Mac 或其他裝置。若要在任何新裝置上首次登入，則需要兩項資訊：Apple ID 密碼，以及顯示在使用者信任裝置上或傳送到信任電話號碼的六位數驗證碼。輸入驗證碼後，使用者確認他們信任新的裝置且可安全登入。由於只靠密碼已不足以存取使用者帳號，因此雙重認證能提升使用者 Apple ID 的安全性，以及他們透過 Apple 儲存的所有個人資訊的安全性。其直接整合至 iOS、iPadOS、macOS、tvOS、watchOS 和 Apple 網站使用的認證系統。

當使用者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使用者 iCloud 帳號關聯的所有信任裝置，要求核准網頁作業階段。如果使用者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。當使用者在裝置上輸入驗證碼時，便會核准網頁作業階段。

### 密碼重置和帳號復原

如果忘記 Apple ID 帳號的密碼，使用者可以在受信任的裝置上重置密碼。如果無法使用受信任的裝置但密碼已知，使用者可以使用受信任的電話號碼，透過 SMS 驗證的方式進行認證。此外，為了立即復原 Apple ID，先前使用的密碼可以和 SMS 驗證一起用來重置。如果沒有這些選項，則必須遵循帳號復原的處理程序。如需更多資訊，請參閱 Apple 支援文章：[無法重置 Apple ID 密碼時如何使用帳號復原](#)。

## 管理式 Apple ID 安全性

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。這些組織可以重置密碼和關閉通訊（如 FaceTime 和 iMessage），以及替員工、職員、教師和學生設定以角色為基礎的權限。

若使用管理式 Apple ID，某些服務會停用（例如 Apple Store、HomeKit 和「尋找」）。

### 管理式 Apple ID 的取用管理

組織可以使用「Apple 商務管理」、「Apple 校務管理」和「Apple 商務必備」中的取用管理功能，以定義管理式 Apple ID 的使用範圍和可使用的服務。

透過取用管理功能，你可以定義使用者是否能在任何裝置上、僅限在受管理裝置上，或是僅限在受管理和受監管裝置上，使用管理式 Apple ID 登入。此外，管理者也可以設定使用者是否可以登入網頁版 iCloud。這讓組織可將裝置的管理狀態當成判斷因素，決定是否應授予組織資料的取用權限。

此外，管理者可以定義使用者可使用哪些 iCloud 服務。這包含定義 Apple Developer Program 和 AppleSeed for IT Beta 版計畫的取用權限，以及決定是否允許使用者取用 Apple 隱私權入口網站 ([privacy.apple.com](http://privacy.apple.com))。

管理式 Apple ID 也支援使用 Keynote、Numbers、Pages、「提醒事項」和「備忘錄」來合作編輯文件，以及使用 FaceTime 和 iMessage 進行通訊。針對這些服務，組織可以定義使用者是否能與任何人合作，還是只能與在相同「Apple 校務管理」、「Apple 商務管理」或「Apple 商務必備」組織內建立的帳號合作。

如果取用管理規則改變，會同步反映在使用者以管理式 Apple ID 登入的裝置上。如果對裝置管理狀態的要求改變，當裝置不符合新的要求時，管理式 Apple ID 就會自動登出裝置。

### 檢閱管理式 Apple ID

在「Apple 校務管理」中建立的管理式 Apple ID 也支援**檢查**，可讓組織遵守法律和隱私法規。具有「管理員」、「機構經理」、「成員經理」或「教師」角色的使用者，可以檢查特定的管理式 Apple ID 帳號。

檢查者只能監視組織階層中層級低於自己的帳號。例如，教師可以監視學生；經理可以檢閱教師和學生；管理員可以檢查經理、教師和學生。

在使用「Apple 校務管理」要求憑證時，系統會核發一個特殊帳號，其僅能存取要求檢閱的管理式 Apple ID。接著檢查者可以讀取和修改使用者儲存在 iCloud 或具備 CloudKit 功能的 App 中的內容。稽核存取的每個要求都會記錄在「Apple 校務管理」中。記錄會顯示誰是檢查者、檢查者要求存取的管理式 Apple ID、要求的時間，以及是否有執行檢查。

# iCloud

## iCloud 安全性概覽

iCloud 會儲存使用者的聯絡人、行事曆、照片、文件和更多項目，並在其所有裝置間自動保持最新的資訊。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。使用者透過使用 Apple ID 登入並選擇他們想要使用的服務來設定 iCloud。IT 管理者可以使用 [行動裝置管理 \(MDM\)](#) 設定描述檔來停用某些 iCloud 功能，例如「iCloud 雲碟」和「iCloud 備份」。

iCloud 使用強大的安全性方式並使用嚴格的原則來保護使用者資料。大部分 iCloud 資料會先在使用者的裝置上使用裝置產生的 iCloud 密鑰進行加密，再上傳到 iCloud 伺服器。針對非端對端加密的資料，使用者的裝置會以安全的方式將這些 iCloud 密鑰上傳到 Apple 資料中心的「iCloud 硬體安全性模組」。這可讓 Apple 協助使用者進行資料復原，並在使用者需要時為解密資料（例如當他們在新裝置登入、從備份回復，或在網路上取用其 iCloud 資料時）。在使用者裝置和 iCloud 伺服器之間移動的資料會在傳輸過程中透過 TLS 單獨加密，而 iCloud 伺服器在儲存使用者資料時會使用額外的靜態加密層。

Apple 可用的加密密鑰會在 Apple 資料中心受到保護。在處理儲存在第三方資料中心的資料時，這些加密密鑰只能由安全伺服器上執行的 Apple 軟體取用，並且只能在進行必要的處理時取用。為了增加隱私和安全性，許多 Apple 服務使用端對端加密，這意味著只有使用者自己才能取用他們的 iCloud 資料，並且只能在使用者以其 Apple ID 登入的受信任裝置上取用。

Apple 提供使用者兩個選項來加密和保護他們儲存在 iCloud 的資料：

- **標準資料保護 (預設設定)**：使用者的 iCloud 資料會經過加密，加密密鑰在 Apple 資料中心受到保護，而 Apple 可以協助處理資料和帳號復原。只有部分 iCloud 資料 (14 種資料類別，包含「健康」資料和「iCloud 鑰匙圈」中的密碼) 是端對端加密。
- **iCloud 的進階資料保護**：有一項選擇性設定可提供 Apple 最高層級的雲端資料安全性。如果使用者選擇開啟「進階資料保護」，他們信任的裝置將保留對其大部分 iCloud 資料的加密密鑰唯一取用權，從而使用端對端加密來保護這些資料。當使用者開啟「進階資料保護」時，使用端對端加密的資料類別數會增加至 23 種，並包含使用者的「iCloud 備份」、「照片」、「備忘錄」等。

使用端對端加密保護的特定 iCloud 資料類別列於 [Apple 支援文章：iCloud 資料安全性概覽](#)。

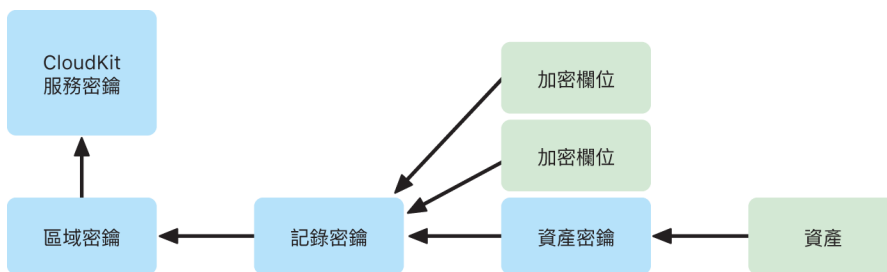
## iCloud 加密

iCloud 中的資料加密與資料儲存模型密切相關，從 CloudKit 架構和 API 開始，允許 App 和系統軟體代表使用者將資料儲存在 iCloud 中，並使所有裝置和網路上的所有內容保持最新狀態。

### CloudKit 加密

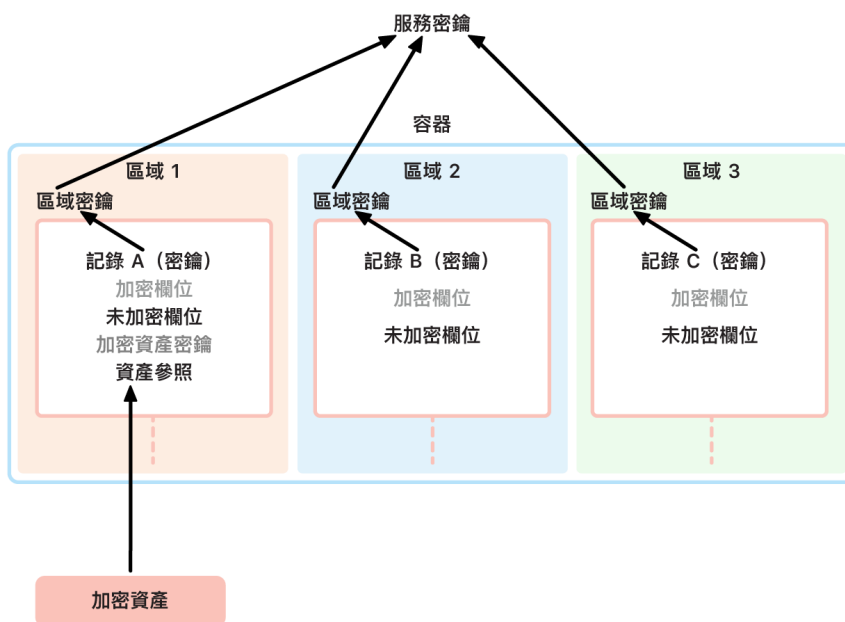
[CloudKit](#) 是一種架構，可讓 App 開發者在 iCloud 中儲存鍵值資料、結構資料和資產 (大型資料會與資料庫分開儲存，例如影像或影片)。CloudKit 同時支援公用和專用資料庫，以容器分類。公用資料庫為公開共享，通常用於一般資產，而不會經過加密。專用資料庫則會儲存每個使用者的 iCloud 資料。

CloudKit 會使用與資料結構相符的密鑰階層。每個容器的專用資料庫受到密鑰階層保護，該密鑰階層根植於稱為「CloudKit 服務密鑰」的非對稱式密鑰。這些密鑰對於每個 iCloud 使用者都是唯一的，並於他們信任的裝置上產生。當資料寫入 CloudKit 時，所有記錄密鑰皆會在使用者信任的裝置上產生，並在上傳任何資料前封裝至適當的密鑰階層。



許多 Apple 服務 (Apple 支援文章 [iCloud 資料安全性概覽](#) 中詳盡列出) 都使用端對端加密，並搭配受到與「iCloud 鑰匙圈」同步功能相同方式保護的 CloudKit 服務密鑰。對這些 CloudKit 容器而言，服務密鑰只能在使用者信任的裝置上使用，Apple 或任何第三方均無法取用。就算使用者選擇不使用「iCloud 鑰匙圈」來同步密碼、通行密鑰和其他使用者資料，這些密鑰還是會在使用者的裝置間同步。當裝置遺失時，使用者可以利用 [保護「iCloud 鑰匙圈」復原](#)、「[帳號復原聯絡人](#)」或「[帳號復原密鑰](#)」來復原其「iCloud 鑰匙圈」資料。

### 加密密鑰管理



CloudKit 中加密資料的安全性是依靠相應加密密鑰的安全性。CloudKit 服務密鑰分為兩類：端對端加密和認證後可用。

- **端對端加密服務密鑰**：對於端對端加密的 iCloud 服務，Apple 伺服器永遠無法取得相關的 CloudKit 服務專用密鑰。服務密鑰組 (包含專用密鑰) 會在使用者信任的裝置端上建立，並使用「[iCloud 鑰匙圈](#)」[安全性](#)傳輸到使用者的其他裝置。雖然「iCloud 鑰匙圈」復原和同步流程是由 Apple 伺服器所協調，但加密方式可防止這些伺服器取用使用者的任何鑰匙圈資料。在失去「iCloud 鑰匙圈」取用權和所有復原機制的最壞情況下，CloudKit 中的端對端加密資料會遺失。Apple 無法協助復原這些資料。



- **認證後可用服務密鑰**：對於其他服務，例如「照片」和「iCloud 雲碟」，服務密鑰會儲存在 Apple 資料中心的「iCloud 硬體安全性模組」中，而且可由部分 Apple 服務取用。使用者在新裝置上登入 iCloud 並認證其 Apple ID 時，這些密鑰無需進一步的使用者互動或輸入便可由 Apple 伺服器取用。例如，在登入 iCloud.com 後，使用者可以立即在線上檢視其照片。這些服務密鑰即為**認證後可用密鑰**。

## iCloud 的進階資料保護

iCloud 的「進階資料保護」為一項選擇性設定，提供 Apple 最高層級的雲端資料安全性。使用者開啟「進階資料保護」時，他們信任的裝置將保留對其大部分 iCloud 資料的加密密鑰唯一取用權，從而使用**端到端加密**來保護這些資料。對於開啟「進階資料保護」的使用者，使用端到端加密保護的資料類別總數會從 14 增加至 23 種，並包含「iCloud 備份」、「照片」、「備忘錄」等。

**【注意】**此功能可能未在所有國家或地區提供。

「進階資料保護」在概念上相當簡單：在裝置上產生並稍後上傳到 Apple 資料中心內**認證後可用**「iCloud 硬體安全性模組」(HSM)的所有「CloudKit 服務密鑰」，會從這些 HSM 中刪除，並改為完全保存在帳號的「iCloud 鑰匙圈」保護網域內。「CloudKit 服務密鑰」的處理會如同現有的**端到端加密**服務密鑰，即表示 Apple 無法再讀取或取用這些密鑰。

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

### 啟用「進階資料保護」

使用者開啟「進階資料保護」時，其受信任的裝置會執行兩個動作：第一，裝置會確認使用者要對自己加入端對端加密的其他裝置開啟「進階資料保護」的意圖。裝置會將裝置本機密鑰所簽署的新的值寫入其「iCloud 鑰匙圈」裝置後設資料來執行此操作。此證明與使用者的其他裝置同步時，Apple 伺服器無法對其進行移除或修改。

第二，裝置會將**認證後可用**服務密鑰從 Apple 資料中心移除。由於這些密鑰受 iCloud HSM 保護，此刪除操作會立即執行、永久生效且無法取消。刪除密鑰後，Apple 便無法再取用由使用者的服務密鑰所保護的**任何**資料。此時，裝置會開始進行非同步密鑰輪換操作，這會替每個先前提供密鑰給 Apple 伺服器取用的服務，製作新的服務密鑰。若密鑰輪換因網路中斷或任何其他錯誤而失敗，裝置會重新嘗試密鑰輪換直到輪換成功。

在服務密鑰輪換成功後，就無法使用舊的服務密鑰來解密新寫入服務的資料。新資料會以新密鑰保護，而新密鑰由使用者的受信任裝置單獨控制，Apple 永遠無法取得此密鑰。

### 進階資料保護和 iCloud.com 網頁取用權限

在使用者初次開啟「進階資料保護」時會自動關閉其 iCloud.com 資料的網頁取用權限。這是因為 iCloud 網頁伺服器無法再取用要解密和顯示使用者資料所需的密鑰。使用者可以選擇再次開啟網頁取用權限，並使用其參與的受信任裝置來取用他們在網頁上的加密 iCloud 資料。

開啟網頁取用權限後，每次使用者參訪 iCloud.com 時，都必須在自己其中一部受信任裝置上授權網頁登入。此授權會針對網頁取用權限，「強化」裝置的安全性。接下來一小時，此裝置會接受來自特定 Apple 伺服器上傳個別服務密鑰的要求，但對應的密鑰僅限一般可在 iCloud.com 上取用的允許列表內服務。換句話說，即使使用者授權網頁登入，伺服器要求也無法誘導使用者的裝置上傳服務密鑰以取得非預期在 iCloud.com 上檢視的資料（例如「健康」資料或「iCloud 鑰匙圈」中的密碼）。Apple 伺服器只會針對使用者在網頁上要求取用特定資料，要求解密所需的服務密鑰。每次上傳服務密鑰時，服務密鑰會使用綁定使用者所授權之網頁作業階段的臨時密鑰加密，而且使用者的裝置上會出現通知，顯示其資料暫時可供 Apple 伺服器使用的 iCloud 服務。

### 保留使用者的選擇

「進階資料保護」和 iCloud.com 網頁取用權限設定只能由使用者修改。這些值會儲存在使用者的「iCloud 鑰匙圈」裝置後設資料中，且只能從其中一部使用者的受信任裝置更改。Apple 伺服器無法替使用者修改這些設定，也無法將其回復成之前的設定。

## 共享和合作的安全性影響

在多數情況下，當使用者共享內容以彼此合作，例如共享的「備忘錄」、共享的「提醒事項」、「iCloud 雲碟」中的共享檔案夾，或「iCloud 共享的照片圖庫」，而且所有使用者皆開啟「進階資料保護」時，Apple 伺服器只會用來建立共享而不會取用共享資料的加密密鑰。共享內容會維持端對端加密且只能在參與者的受信任裝置上取用。對於每個共享操作，標題和代表的縮覽圖可能會由 Apple 使用標準資料保護儲存以對接收的使用者顯示預覽。

啟用合作時選取「任何擁有連結的使用者」選項會在標準資料保護下讓該內容可供 Apple 伺服器使用，因為伺服器需要能夠提供權限給可打開 URL 的任何人。

iWork 合作和「照片」中的「共享的相簿」功能不支援「進階資料保護」。使用者在 iWork 文件上合作，或從「iCloud 雲碟」的共享檔案夾中打開 iWork 文件時，文件的加密密鑰會安全地上傳到 Apple 資料中心中的 iWork 伺服器。這是因為 iWork 中的即時合作需要伺服器端中繼才能在參與者之間協調文件更動。加入「共享的相簿」的照片會以標準資料保護儲存，因為此功能才會允許相簿公開在網頁上共享。

## 停用「進階資料保護」

使用者可以隨時關閉「進階資料保護」。若使用者決定執行此操作：

1. 使用者的裝置會在「iCloud 鑰匙圈」參與後設資料中先記錄其新選擇，而且此設定會安全地同步到他們所有的裝置。
2. 使用者的裝置會安全地將所有**認證後可用**服務的服務密鑰上傳到 Apple 資料中心中的 iCloud HSM。這絕對不會包含在標準資料保護下以端對端加密的服務密鑰，例如「iCloud 鑰匙圈」和「健康」。

裝置會上傳「進階資料保護」開啟前產生的原始服務密鑰，以及使用者開啟該功能後產生的新服務密鑰。這會讓這些服務中的所有資料在認證後可供取用並使帳號回復為標準資料保護，即 Apple 可在使用者失去帳號取用權限時再次協助使用者復原其大部分資料。

## 未由「進階資料保護」涵蓋的 iCloud 資料

由於全域電子郵件、聯絡人和行事曆系統互相操作的需要，「iCloud 郵件」、「聯絡人」和「行事曆」不會受到端對端加密。

即使「進階資料保護」已開啟，iCloud 仍會在沒有使用者特定 CloudKit 服務密鑰的保護下儲存部分資料。「CloudKit 記錄」欄位必須在容器的架構中明確宣告為「已加密」才能受到保護，而且讀取和寫入加密的欄位會要求使用專用的 API。檔案或物件經過修改的日期和時間會用來排序使用者的資訊，而檔案和照片資料的核對碼會用來協助 Apple 刪除重複並最佳化使用者的 iCloud 和裝置儲存空間，一切皆無須取用檔案和照片本身。關於加密如何用於特定資料類別的詳細資訊，可於 Apple 支援文章 [iCloud 資料安全性概覽](#) 中取得。

這些決定，例如使用刪除重複資料的核對碼，即知名的**收斂加密**技術，是 iCloud 服務啟動時原始設計的一部分。後設資料會一律加密，但加密密鑰會由 Apple 使用標準資料保護儲存。為了繼續加強所有使用者的安全性保護，Apple 致力於確保更多資料，包含此類後設資料，在「進階資料保護」開啟時獲得端對端加密。

## 「進階資料保護」需求

開啟 iCloud 的「進階資料保護」的需求包含下列項目：

- 使用者的帳號必須支援端對端加密。端對端加密會要求其 Apple ID 使用雙重認證，並且在其受信任裝置上設定密碼。如需更多資訊，請參閱 Apple 支援文章 [Apple ID 雙重認證](#)。
- 使用者以其 Apple ID 登入的裝置必須更新到 iOS 16.2、iPadOS 16.2、macOS 13.1、tvOS 16.2、watchOS 9.2 或以上版本，以及最新版本的 Windows 版 iCloud。此需求可在之前版本的 iOS、iPadOS、macOS、tvOS 或 watchOS 受誤導而嘗試修復帳號狀態時，防止它們將新製作的服務密鑰重新上傳到**認證後可用** HSM 的不當處理。
- 使用者必須設定至少一種替代復原方式：一個或多個復原聯絡人或復原密鑰，即使用者可用來在失去自己帳號取用權限時復原其 iCloud 資料。

若復原方式失敗，例如復原聯絡人的資訊過時，或使用者忘記該資訊，Apple 便無法協助復原使用者的端對端加密 iCloud 資料。

iCloud 的「進階資料保護」只能針對 Apple ID 開啟。不支援管理式 Apple ID 和兒童帳號（因國家或地區而異）。

## 「iCloud 備份」的安全性

iCloud 會每天透過 Wi-Fi 備份資訊，包含裝置設定、App 資料、「相機膠卷」中的照片和影片，以及「訊息」App 中的對話。「iCloud 備份」只有在裝置鎖定時、已連接電源並透過 Wi-Fi 連接網際網路時才會執行。考量到 iOS 和 iPadOS 中所使用的儲存加密技術，「iCloud 備份」經過精心設計，既可保護資料安全，又能兼顧增量、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到 Apple 資料中心中的「iCloud 硬體安全性模組」，且為認證後可用資料類別的一部分。對於開啟 iCloud 的「進階資料保護」的使用者，「iCloud 備份」服務密鑰會使用端對端加密保護，而且僅供使用者在其受信任裝置上使用。

如果檔案製作時採用「資料保護」類別，且該類別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檔案備份至 iCloud。如 [CloudKit 加密](#) 中所說明，所有檔案都會在傳送期間加密，且會在儲存時使用基於帳號的密鑰來加密。

「iCloud 備份」Keybag 包含用於資料保護類別的非對稱 (Curve25519) 密鑰，當裝置鎖定時無法存取。備份集是儲存於使用者的 iCloud 帳號中，由使用者的檔案拷貝和「iCloud 備份」Keybag 組成。「iCloud 備份」Keybag 受到隨機密鑰的保護，其也會與備份集一起儲存。使用者的 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。

回復後，備份的檔案、「iCloud 備份」Keybag 和 Keybag 的密鑰將會從使用者的 iCloud 帳號取回。「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中的檔案，這些檔案會作為新檔案寫入到檔案系統中，再根據其「資料保護」類別加以重新加密。

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。使用者的「iCloud 備份」包含使用者裝置上現有已購買內容的相關資訊，但不包括已購買的內容本身。當使用者從「iCloud 備份」回復時，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分國家或地區不會自動下載，且在內容已退款或其個別商店不再提供內容時，可能無法取得先前的購買項目。完整購買記錄會與使用者的 Apple ID 綁定。
- 使用者裝置上的照片與影片。請注意，若使用者在 iOS 8.1、iPadOS 13.1 或是 OS X 10.10.3 或以上版本中開啟「iCloud 照片」，其照片與影片便已儲存在 iCloud 中，因此不會包含在使用者的「iCloud 備份」裡。
- 聯絡人、行事曆行程、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
- 「醫療卡」資料
- 「語音備忘錄」密碼 (如有需要，必須裝有備份期間所使用的實體 SIM 卡)
- 「訊息」、Apple Messages for Business、簡訊 (SMS) 與 MMS 訊息 (如有需要，必須裝有備份期間所使用的實體 SIM 卡)

「iCloud 備份」也會用來備份本機裝置鑰匙圈，以裝置衍生的「安全隔離區」UID 根加密編譯密鑰進行加密。此密鑰為裝置獨有而且無法由 Apple 得知。這樣可讓資料庫只能回復至原先產生它的同一台裝置，這意味著任何人 (包括 Apple) 都無法讀取。如需更多資訊，請參閱：[安全隔離區](#)。

## iCloud 雲端「訊息」

iCloud 雲端「訊息」可讓使用者的完整訊息記錄保持更新並在所有裝置上可用。

使用標準資料保護時，iCloud 雲端「訊息」在「iCloud 備份」關閉時會進行端對端加密。「iCloud 備份」開啟時，備份會包含 iCloud 雲端「訊息」加密密鑰的副本，因此即使使用者失去「iCloud 鑰匙圈」和其受信任裝置的取用權限，Apple 仍可協助使用者復原其訊息。若使用者關閉「iCloud 備份」，則會在其裝置上產生新的密鑰來保護未來的 iCloud 雲端「訊息」。新密鑰只會儲存在「iCloud 鑰匙圈」中，僅供使用者在其受信任裝置上使用，而且寫入容器的新資料無法以舊容器密鑰解密。

使用「進階資料保護」時，iCloud 雲端「訊息」會一律進行端對端加密。「iCloud 備份」開啟時，「iCloud 備份」中的所有內容都會進行端對端加密，包含 iCloud 雲端「訊息」加密密鑰。「iCloud 備份」服務密鑰以及 iCloud 雲端「訊息」容器密鑰都會在使用者開啟「進階資料保護」時輪換。如需更多資訊，請參閱 Apple 支援文章：[iCloud 資料安全性概覽](#)。

## iCloud 私密轉送安全性

「iCloud 私密轉送」主要會在使用 Safari 瀏覽網頁時協助保護使用者，但其也包括所有 DNS 名稱解析要求。這有助於確保任何一方（甚至 Apple）都無法將使用者的 IP 位址與其瀏覽活動產生關聯。其藉由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。若要使用「iCloud 私密轉送」，使用者必須執行 iOS 15、iPadOS 15 或 macOS 12.0.1 或以上版本，並使用其 Apple ID 登入 iCloud+ 帳號。之後便可在「設定」>「iCloud」或「系統設定」>「iCloud」中開啟「iCloud 私密轉送」。

如需更多資訊，請參閱：[iCloud 私密轉送概覽](#)。

## 帳號復原聯絡人安全性

無論使用者是否已開啟「進階資料保護」，使用者最多可以加入五位他們信任的人員作為帳號復原聯絡人，以協助他們復原其 iCloud 帳號和資料，包括其所有端對端加密資料。Apple 和復原聯絡人都沒有個別的必要資訊來復原使用者的端對端加密 iCloud 資料。

「復原聯絡人」的設計將使用者隱私納入考量。使用者所選的復原聯絡人無法由 Apple 識別。Apple 伺服器只會在使用者要求聯絡人協助且其聯絡人實際開始協助復原後的復原嘗試末期得知復原聯絡人的相關資訊。該資訊在復原完成後不會保留。

### 復原聯絡人安全程序

使用者設定「帳號復原聯絡人」時，系統會產生與該聯絡人綁定的密鑰。此密鑰可保護使用者 iCloud 資料（包含端對端加密的 CloudKit 資料）的存取權限。接下來，系統會產生一組隨機 256 位元 AES 密鑰，用於加密「復原聯絡人」密鑰以建立「復原聯絡人封包」。加密的封包會傳送給「復原聯絡人」保管，而隨機 AES 密鑰會由 Apple 儲存。AES 密鑰和封包都不會提供有關基礎密鑰本身的任何資訊。進行復原時，使用者裝置成功向其「復原聯絡人」取得「復原聯絡人封包」，並向 Apple 取得 AES 密鑰後，就能組合這兩者來復原原始密鑰，並取用使用者的 iCloud 資料。

為設定「帳號復原聯絡人」，使用者的裝置會與 Apple 伺服器通訊以上傳 Apple 持有的密鑰資訊部分（上述的 AES 密鑰）。裝置接著會與復原聯絡人建立端對端加密 CloudKit 容器，以分享復原聯絡人所需的資料（使用 AES 密鑰加密的「復原聯絡人封包」）。Apple 建立的授權機密也會與復原聯絡人分享。此機密將用於復原帳號及協助帳號進行密碼重置。邀請和接受復原聯絡人的通訊是透過相互認證的 IDS 通道進行。復原聯絡人會自動在「iCloud 鑰匙圈」中儲存接收到的資訊。Apple 無法取用 CloudKit 容器的內容，也無法取用儲存此資訊的「iCloud 鑰匙圈」。執行分享時，Apple 伺服器只會檢視復原聯絡人的匿名 ID。

之後，當使用者需要復原他們的帳號和 iCloud 資料時，可以向他們的復原聯絡人要求協助。屆時，復原聯絡人的裝置會產生一個代碼，復原聯絡人便可透過不同的方法（例如親自或透過電話）將其提供給使用者。然後，使用者在他們的裝置上輸入代碼，以使用 SPAKE2+ 通訊協定在裝置間建立安全連線，Apple 並無法取用此內容。此互動由 Apple 伺服器協調，但 Apple 無法啟動復原程序。

建立安全連線並完成所有必要的安全檢查後，復原聯絡人的裝置會將密鑰資訊的部分和先前建立的授權密鑰傳回給要求復原的使用者。使用者向 Apple 伺服器出示此授權密鑰，此授權密鑰會授予權限來存取 Apple 保管的密鑰資訊。提供授權密鑰也會授權重置帳號密碼以復原帳號取用權限。

最後，使用者的裝置會合併從 Apple 及「帳號復原聯絡人」接收的密鑰資訊，然後用來解密和復原其 iCloud 資料。

有保護措施可以防止復原聯絡人在未經使用者同意的情況下啟動復原，其中包括對使用者帳號的活動性檢查。如果帳號處於使用中狀態，使用「復原聯絡人」進行復原也需要知道最近裝置密碼或 iCloud 安全碼。

## 遺產聯絡人安全性

如果使用者想要指定受益人在他們死後可以取用其資料，他們可以在其帳號上設定「遺產聯絡人」。「遺產聯絡人」的建立方式與「復原聯絡人」很類似，不同之處是受益人使用的密鑰資訊，不包含解密去世者的「iCloud 鑰匙圈」所需的資訊。使用的密鑰結構與帳號復原聯絡人相同，不同之處在於此情況下是由 Apple 儲存加密的封包，並由受益人保管 AES 密鑰。這會讓受益人收到的部分較短，因此必要時可以更容易列印出來，同時仍提供相同的屬性，亦即這兩個部分都不會提供有關基礎密鑰本身的任何資訊。

受益人收到的密鑰資訊在終端使用者的文件中被稱為取用密鑰。取用密鑰會自動儲存在支援的裝置上，但也可以列印和離線儲存以供使用。如需更多資訊，請參閱 Apple 支援文章：[如何為 Apple ID 加入遺產聯絡人](#)。

使用者去世後，「遺產聯絡人」登入 Apple 聲明網站以啟動取用權限。這需要死亡證明，並且部分使用上一節中提到的授權密鑰進行授權。完成所有安全性檢查後，Apple 會為新帳號核發使用者名稱和密碼，並將密鑰資訊釋出給「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行動條碼的英數代碼。輸入後，對去世者 iCloud 資料的取用權限則會復原。這可以在裝置上執行，也可以線上建立取用權限。如需更多資訊，請參閱 Apple 支援文章：[以遺產聯絡人身分要求存取 Apple 帳號](#)。

## 密碼與密碼管理

### 密碼安全性概覽

iOS、iPadOS 及 macOS 讓使用者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」讓使用者不需要建立和管理額外的帳號或密碼，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」功能可讓使用者的裝置於網站和 App 中自動建立、同步和輸入不重複的高強度密碼。密碼會儲存至特別的「密碼自動填寫」鑰匙圈中，這個鑰匙圈由使用者控制，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使用者手動建立的密碼。

### 「使用 Apple 登入」安全性

對其他單一登入系統而言，「使用 Apple 登入」是可保護隱私的替用方式。此功能提供點按即登入的便利性與效率，讓使用者能一目瞭然地控制自己的個人資訊。

「使用 Apple 登入」讓使用者可設定一個帳號，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。設定帳號時 App 只能詢問使用者的名稱和電子郵件地址，而使用者隨時可選擇：可以與 App 分享自己的個人電子郵件地址，或是選擇保留個人郵件地址隱私，改用 Apple 新推出的隱私電子郵件轉送服務。此電子郵件轉送服務會分享一個不重複的匿名電子郵件地址，而這個地址會轉送至使用者的個人地址，因此仍可收到來自開發者的通訊內容，同時保留一定程度的隱私和個人資料控制權。

「使用 Apple 登入」為內建的安全功能。使用「使用 Apple 登入」的所有使用者都必須為其 Apple ID 啟用雙重認證。雙重認證不僅有助於保護使用者的 Apple ID，還可保護其使用 App 建立的帳號。此外，Apple 還開發出可保護隱私的防詐騙訊號，並整合到「使用 Apple 登入」中。這讓開發者具有信心，能確保獲得的新使用者皆為真人，而非機器人或執行指令的帳號。

## 自動使用高強度密碼

當「iCloud 鑰匙圈」已啟用，iOS、iPadOS 及 macOS 會在使用者於 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。使用者必須選擇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」的裝置間保持最新狀態。

根據預設，iOS 和 iPadOS 產生的密碼長度為 20 個字元。其中包含一個數字、一個大寫字元、兩個連字號和 16 個小寫字元。產生的密碼具有高強度，且包含 71 位元的熵。

系統會根據啟發法產生密碼，啟發法可判斷密碼欄位使用體驗是否適用於製作密碼。如果啟發法無法辨識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"`。

為了協助確保產生的密碼相容於相關服務，App 和網站可以提供規則。開發者使用 `UITextInputPasswordRules` 或 `input` 元素中的 `passwordrules` 屬性來提供規則。接著裝置會產生可滿足這些規則的最高強度密碼。

## 「密碼自動填寫」安全性

「密碼自動填寫」會自動填寫儲存在「鑰匙圈」中的憑證。「iCloud 鑰匙圈」密碼管理程式和「密碼自動填寫」提供以下功能：

- 在 App 和網站中填入憑證
- 產生高強度密碼
- 在 App 和 Safari 中的網站上儲存密碼
- 以安全方式將密碼傳送給使用者的聯絡人
- 提供密碼給附近要求憑證的 Apple TV

在 App 內產生和儲存密碼，以及提供密碼給 Apple TV 這兩項功能，只能在 iOS 和 iPadOS 中使用。

## App 內的「密碼自動填寫」

iOS 和 iPadOS 允許使用者在 App 裡的憑證相關欄位中，輸入已儲存的使用者名稱和密碼，類似 Safari 中的「密碼自動填寫」功能。在 iOS 和 iPadOS 中，使用者需點一下軟體鍵盤「快速輸入」列中的直觀功能按鍵。在 macOS 中，若使用以 Mac Catalyst 建置的 App，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 網站關聯機制（透過同一個 `apple-App-site-association` 檔案驅動）來與網站建立高強度關聯時，如果有任何憑證已儲存至「密碼自動填寫」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。如此一來使用者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。

「密碼自動填寫」不會向 App 提供任何憑證資訊，除非使用者同意釋出憑證給 App。系統會從 App 的程序中提取或呈現憑證列表。

當 App 和網站具有受信任關係，且使用者在 App 中提交了憑證，iOS 和 iPadOS 可能會提示使用者將這些憑證儲存至「密碼自動填寫」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「密碼自動填寫」鑰匙圈協助使用

`ASAuthorizationPasswordProvider` 和 `SecAddSharedWebCredential` 讓使用者登入。密碼提供者及其要求可搭配「使用 Apple 登入」使用，因此相同 API 會呼叫以協助使用者登入 App，無論使用者的帳號採用密碼，還是透過「使用 Apple 登入」所建立。

只有 App 開發者和網站管理者核准且使用者同意後，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

若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 標記為具有信任關係。只有在具有信任關係的情況下，才會呼叫這兩個 API 並向使用者發出提示，使用者同意後，才會將密碼核發給 App、更新或刪除。

## 密碼安全性建議

iOS、iPadOS 和 macOS 中「密碼自動填寫」的密碼列表，會指出使用者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號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，藉此入侵其他帳號。

- 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**。
- 攻擊者可輕易猜到的密碼會被標記為**強度弱**。iOS、iPadOS 和 macOS 會偵測用來建立好記密碼的常見模式，例如使用字典中可找到的單字、常用替代字元（例如使用「p4ssw0rd」而非「password」）、鍵盤上可找出的模式（例如 QWERTY 鍵盤上的「q12we34r」，或是重複序列（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。

由於許多服務指定使用四或六位數的 PIN 碼，系統會以不同的規則評估這些短密碼。PIN 碼若為最常見的 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「密碼監視」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**。如需更多資訊，請參閱：[密碼監視](#)。

強度偏弱、重複使用和洩漏的密碼會在密碼列表 (macOS) 中指出，或顯示於專用的「安全建議介面」(iOS 和 iPadOS) 中。如果使用者在 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，強烈建議其升級為自動使用高強度密碼。

## 升級 iOS 和 iPadOS 中的帳號認證安全性

導入了「帳號認證修改擴充」（位於「認證服務」架構中）的 App 可為採用密碼的帳號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。這個擴充點可用於 iOS 和 iPadOS。

如果 App 已導入擴充點並安裝在裝置上，則使用者在「設定」的「iCloud 鑰匙圈」密碼管理程式中檢視與該 App 關聯的憑證「安全建議」時，便會看到擴充升級的選項。當使用者使用有風險的憑證登入到 App 時，也會提供升級。App 能告訴系統在登入後不要提示使用者升級選項。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 中的帳號設定或帳號管理畫面進行。

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，系統將會為使用者產生自動使用高強度密碼。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。當使用者將帳號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，以將該帳號與其相關聯。使用者的 Apple ID 電子郵件不會作為憑證的一部分提供。成功進行「使用 Apple 登入」升級後，系統將從使用者的鑰匙圈中刪除以前使用的密碼憑證（如果已儲存在其中）。

「帳號認證修改擴充」有機會在執行升級之前執行其他使用者認證。對於在密碼管理程式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號提供使用者名稱和密碼。若為 App 內升級，則只會提供使用者名稱。如果擴充程序需要進一步的使用者認證，則可在繼續升級之前要求顯示自訂使用者介面。顯示此使用者介面的預期用途是讓使用者輸入第二個認證因子來授權升級。

## 密碼監視

「密碼監視」是一項功能，可將儲存在使用者其「密碼自動填寫」鑰匙圈中的密碼與不斷更新和整理的密碼列表（已知已暴露於不同線上組織的洩漏資料中）進行比對。如果啟用了此功能，則監控通訊協定會持續將使用者的「密碼自動填寫」鑰匙圈密碼與整理的列表相比對。

### 監視功能如何運作

使用者裝置連續對使用者密碼進行循環檢查，並以不受使用者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。這有助於確保驗證狀態與洩漏密碼的目前最新整理列表保持最新。為了協助防止洩漏使用者擁有多少個專屬密碼的相關資訊，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，並且如果使用者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

密碼的比對過程分為兩部分。最常洩露的密碼包含在使用者裝置的本機列表中。如果使用者的密碼出現在此列表中，則會立即通知使用者，而無需進行任何外部互動。這樣的設計可以確保不會洩露因密碼洩露而讓使用者產生最大風險的相關密碼資訊。

如果該密碼未包含在最頻繁洩漏的列表中，則將其與洩漏頻率較低的密碼比對。

### 將使用者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 伺服器的一些互動作業。為了協助確保不會將合法使用者的密碼傳送給 Apple，我們部署了一種加密的**私密集交叉**作業，將使用者的密碼與大量洩露的密碼進行比較。這樣的設計可以確保，對於侵害風險較低的密碼，與 Apple 共享更少的資訊。對使用者的密碼而言，此資訊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 Web 服務儲存貯體中密碼的相對頻率變化，從這些查詢中推測使用者密碼是徒勞的。

此底層協定將整理的密碼列表劃分為  $2^{15}$  個不同的儲存貯體，其中的密碼在撰寫本文時包含大約 15 億個密碼。密碼所屬的儲存貯體是依據密碼的 SHA256 雜湊值的前 15 位元。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。此轉換的設計用意在於透過計算隱藏密碼的值，並透過「密碼監視」來協助防止揭露新洩漏的密碼。

為了計算私密集的交集，使用者裝置會使用  $\lambda$  (SHA256(upw) 的 15 位元前置碼) 來決定使用者密碼所屬的儲存貯體，其中 upw 是其中一個使用者密碼。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  $\lambda$  對應的儲存貯體要求傳送到伺服器。 $\beta$  在此處隱藏了有關使用者密碼的資訊，並且限制為  $\lambda$  (從密碼到 Apple 所揭露的資訊)。最後，伺服器取得使用者裝置所傳送的點，計算出  $\alpha P_c = \alpha \beta \cdot H_{SWU}(upw)$ ，並將其連同相關的點— $B_\lambda = \{ P_{pw} \mid \text{SHA256}(pw) \text{ 以前置碼 } \lambda \}$ —傳回至裝置。

傳回的資訊讓裝置可以計算  $B'_\lambda = \{ \beta \cdot P_{pw} \mid P_{pw} \in B_\lambda \}$ ，如果  $\alpha P_c \in B'_\lambda$ ，則確定使用者密碼已遭洩漏。

## 傳送密碼給其他使用者或 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使用者或 Apple 裝置。



## 使用 AirDrop 將憑證儲存到另一台裝置

啟用 iCloud 後，使用者可以使用 AirDrop 將儲存的憑證傳送到另一部裝置。憑證包括使用者名稱和密碼以及為其儲存的網站。無論使用者的設定為何，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，使用者同意後便會將憑證儲存在使用者的「密碼自動填寫」鑰匙圈中。

## 在 Apple TV 上的 App 中填入憑證

「密碼自動填寫」可用於在 Apple TV 上的 App 中填寫憑證。當使用者專注填寫 tvOS 上的使用者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「密碼自動填寫」要求。

附近的任何 iPhone 或 iPad 會顯示提示，邀請使用者與 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 帳號，兩部裝置間的加密會自動進行。
- 如果裝置登入的 iCloud 帳號與 Apple TV 所使用的不同，則系統會提示使用者使用 PIN 碼來建立加密連線。若要收到這則提示，iPhone 必須解鎖並靠近與該 Apple TV 配對的 Siri 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 上的相關文字欄位中。

## 憑證提供者延伸功能

在 iOS、iPadOS 和 macOS 中，使用者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「密碼自動填寫」或在「系統設定」(macOS 13 或以上版本) 或「系統偏好設定」(macOS 12 或較早版本) 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。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使用者名稱，但不包含其密碼。使用者選擇將憑證填入 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」安全性概覽

「iCloud 鑰匙圈」可讓使用者在 iPhone 與 iPad 裝置和 Mac 電腦之間安全同步密碼，不會將密碼提供給 Apple。除了強大的隱私保護和安全性，「iCloud 鑰匙圈」的設計和架構還有其他目標，就是提供易用性，以及即使使用者的所有裝置都無法取用，仍可回復鑰匙圈內容的能力。「iCloud 鑰匙圈」由兩項服務組成：鑰匙圈同步和鑰匙圈復原。

「iCloud 鑰匙圈」和鑰匙圈復原功能設計成在下列情況下，仍可確保使用者的密碼和通行密鑰受到保護：

- 使用者的 iCloud 帳號被盜。
- 外部攻擊者或員工入侵了 iCloud。
- 第三方存取使用者帳號。

### iCloud 鑰匙圈與密碼管理程式的整合

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 中的帳號密碼。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，但會使用端對端加密，Apple 和其他裝置均無法讀取其內容。

## 保護鑰匙圈同步

當使用者第一次為雙重認證帳號開啟「iCloud 鑰匙圈」時，裝置會為自己製作同步身分。同步身分包括非對稱橢圓密鑰（使用 P-384），會儲存在裝置的鑰匙圈中。每部裝置都會各自維護該使用者其他裝置的同步身分列表，並使用其中一個身分密鑰簽署該列表。這些列表會儲存在 CloudKit 中，讓使用者的裝置對於如何在彼此間安全地同步鑰匙圈資料達成共識。

為了與舊版 iCloud 裝置相容，系統會建立類似的同步信任圈，並形成另一個同步身分。同步身分的公用密鑰會置於信任圈中，該信任圈已經過兩次簽署：第一次由同步身分的專用密鑰簽署，第二次由使用者 iCloud 帳號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（隨機密鑰和反覆運算次數），用於製作以使用者 iCloud 密碼為基礎的密鑰。

## 同步信任圈的 iCloud 儲存

對於雙重認證帳號，每部裝置的信任裝置列表會儲存在 CloudKit 中。如果不知道使用者的 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。

同樣地，已簽署的同步信任圈會存放於使用者的 iCloud 鍵值儲存區域，如果不知道使用者的 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分的專用密鑰，就無法對其進行有效修改。

## 使用者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」復原。

在配對流程中，申請裝置為同步信任圈和同步列表（用於雙重認證帳號）建立新的同步身分，並將其提供給贊助者。贊助者會將新成員的公用密鑰加入到同步信任圈，並使用其同步身分和來自使用者 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章。在雙重認證帳號中，贊助者裝置也會向加入的裝置提供由其身分密鑰簽署的憑證，表示應信任申請裝置。然後，其會更新其受信任同步身分的個別列表以納入申請者。

假設簽章信任圈有兩個成員，並且每個成員擁有與其配對的公用密鑰。這時會開始透過 CloudKit 或 iCloud 鍵值儲存空間來交換個別的鑰匙圈項目（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，則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，因此只能由使用者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，當第三個裝置加入時，它可以與現有裝置中的任何一個配對。每當有新的同級裝置加入，每部同級裝置都會與新裝置進行同步。這樣的設計是為了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

部分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。若要防止非預期的資料傳輸，每個要同步的項目都必須用 `kSecAttrSynchronizable` 屬性明確標示。

Apple 已經為 Safari 使用者資料（包括使用者名稱、密碼和信用卡卡號），以及 Wi-Fi 網路密碼、HomeKit 加密密鑰和其他支援端對端 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。

## 保護「iCloud 鑰匙圈」復原

「iCloud 鑰匙圈」會與 Apple 託管使用者的鑰匙圈資料而不讓 Apple 讀取密碼和其他所包含的資料。即便使用者只有一部裝置，鑰匙圈復原也可以提供安全網來防止資料遺失。如果使用了 Safari 來為網頁帳號隨機產生強式密碼或通行密鑰，鑰匙圈復原就顯得格外重要，因為只有鑰匙圈會記錄這些密碼。

鑰匙圈復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。使用者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拷貝。

### 使用第二個認證

建立高強度密碼的方式有以下幾種：

- 若使用者的帳號已啟用雙重認證，便會使用裝置密碼來復原託管的鑰匙圈。
- 若未設定雙重認證，則會要求使用者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，使用者可自行指定較長的安全碼，或是可讓裝置以加密編譯方式製作隨機安全碼，方便使用者自行記錄和保存。

### 鑰匙圈託管程序

建立密碼後，鑰匙圈便會隨 Apple 託管。iOS、iPadOS 或 macOS 裝置會先匯出使用者的鑰匙圈拷貝，然後加密封裝至非對稱式 Keybag 的密鑰中，並將其放置在使用者的 iCloud 鍵值儲存區域中。Keybag 會以使用者的 iCloud 安全碼和儲存託管記錄的硬體安全模組 (HSM) 叢集公用密鑰進行封裝。這會變成使用者的 **iCloud 託管記錄**。若為雙重認證帳號，鑰匙圈也儲存在 CloudKit 中，包裝為僅可使用 iCloud 託管記錄內容來復原的中間鑰匙，進而提供相同等級的保護。

託管記錄的內容還允許復原裝置重新加入「iCloud 鑰匙圈」，向任何現有裝置證明復原裝置已順利執行託管過程，並因此得到帳號持有人的授權。

**【注意】**除了建立安全碼，使用者也須為其 iCloud 帳號註冊一個電話號碼。這提供了進行鑰匙圈復原期間的第二層認證機制。使用者會收到一則 SMS 簡訊，必須予以回覆才能繼續進行復原。

### 「iCloud 鑰匙圈」的託管安全性

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使用者和裝置能執行復原作業。iCloud 背後部署的是硬體安全性模組 (HSM) 叢集，可保護託管記錄。如本文件前文所述，叢集的每個成員都有一個密鑰，用來對其監管的託管記錄進行加密。

若要復原鑰匙圈，使用者必須使用其 iCloud 帳號和密碼進行身分認證，當訊息傳送至所註冊的電話號碼時，使用者必須進行回覆。回覆完成後，使用者必須輸入其 iCloud 安全碼。HSM 叢集會使用「安全遠端密碼」(SRP) 通訊協定來驗證使用者是否知道其 iCloud 安全碼；安全碼本身不會傳送給 Apple。叢集的每個成員會單獨驗證使用者是否未超過擷取記錄所允許的最大嘗試次數，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使用者的裝置。

接著，裝置會使用託管資料來將用於加密使用者鑰匙圈的隨機密鑰解除封裝。透過這個密鑰，系統會將鑰匙圈從 CloudKit 和 iCloud 鍵值儲存擷取出，然後解密並復原到裝置上。託管服務只允許嘗試認證和擷取託管記錄 10 次。多次嘗試失敗後，將會鎖定記錄，使用者必須聯絡「Apple 支援」才能進行更多嘗試。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擷取記錄。

這些規則已寫入 HSM 韌體程式碼中。允許更改韌體的管理存取卡已銷毀。任何嘗試更改韌體或存取專用密鑰的操作，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 安全性概覽

使用 Apple Pay，使用者可以使用受支援的 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。使用者也可將支援 Apple Pay 功能的交通卡、學生證和識別證加入「Apple 錢包」。Apple Pay 對於使用者來說相當簡單易用，且在硬體和軟體方面皆具備整合性的安全措施。

Apple Pay 的設計目標也在於保護使用者的個人資訊。Apple Pay 不會收集任何可追蹤使用者的交易資訊。付款交易僅於使用者、商家和發卡機構之間流通。

## Apple Pay 元件安全性

Apple Pay 使用多種硬體和軟體功能來提供安全可靠的購買體驗。

### Secure Element

Secure Element 是符合業者標準且經過認證的晶片，於 Java Card 平台上運作，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 已通過「共同準則」標準的認證。

### NFC 控制器

NFC 控制器會處理近場通訊的通訊協定，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 錢包

「Apple 錢包」App 可用來加入和管理信用卡、簽帳金融卡和商店卡，以及使用 Apple Pay 付款。使用者可以檢視其卡片，且能同時檢視發卡機構提供的其他資訊，例如發卡機構的隱私政策、近期交易，以及「Apple 錢包」中的其他內容。使用者也可在以下位置將卡片加入 Apple Pay：

- iOS 和 iPadOS 的「設定輔助程式」和「設定」
- 用來設定 Apple Watch 的 Watch App
- 在配備 Touch ID 的 Mac 電腦上，「系統設定」(macOS 13 或以上版本)或「系統偏好設定」(macOS 12 或較早版本)中的「錢包與 Apple Pay」

此外，使用者也可用「Apple 錢包」來加入和管理交通卡、酬賓卡、登機證、票券、禮品卡、學生證、識別證等票卡。

### 安全隔離區

在 iPhone、iPad、Apple Watch、配備 Touch ID 的 Mac 電腦和配備 Apple 晶片且使用配備 Touch ID 之巧控鍵盤的 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，而使用者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 錢包」中信用卡、簽帳金融卡、交通卡、學生證和識別證的設定與佈建。伺服器也會管理儲存在 Secure Element 中的「裝置帳號號碼」。它們會與裝置和付款網路或發卡機構伺服器進行通訊。Apple Pay 伺服器也負責為 App 內和網路上的付款重新加密付款憑證。

# Apple Pay 如何保護使用者的購買項目

## Secure Element

Secure Element 備有一種特殊設計的 Applet 來管理 Apple Pay，其中也包含經過付款網路或發卡機構認證的 Applet。加密這些 Applet 的付款網路或發卡機構會使用密鑰來傳送信用卡、簽帳金融卡或預付卡資料，且只有付款網路或發卡機構和 Applet 的安全網域擁有密鑰的相關資訊。此資料會儲存在這些 Applet 中，並受到 Secure Element 的安全功能保護。在交易期間，終端機會經由專用硬體匯流排，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。只有感應範圍內的終端機所傳送的付款要求才會由 NFC 控制器標記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、簽帳金融卡或預付卡 (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便會由控制器專門傳送至 NFC 感應場。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 感應場內，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 將資訊加密至 Apple Pay 伺服器。

## 信用卡、簽帳金融卡及預付卡

### 卡片佈建的安全性概覽

當使用者加入信用卡、簽帳金融卡或預付卡 (包含商店卡) 到「Apple 錢包」時，Apple 會以安全的方式將卡片資訊及使用者帳號和裝置的其他資訊，傳送到發卡機構或發卡機構授權維修中心 (通常為付款網路)。發卡機構 (或其服務供應商) 會使用此資訊來判定是否要核准將該卡片加入「Apple 錢包」。作為卡片佈建程序的一部分，Apple Pay 使用三種伺服器端呼叫來傳送和接收與發卡機構或付款網路之間的通訊：

- 需要的欄位
- 檢查卡片
- 連結和佈建

發卡機構或付款網路會使用這些呼叫來讓發卡機構驗證、核准卡片以及將卡片加入「Apple 錢包」。這些用戶端伺服器階段作業使用 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，系統會建立一個唯一的「裝置帳號號碼」，並對其加密，然後儲存在 Secure Element 中。這個唯一的「裝置帳號號碼」會以此方式進行加密，讓 Apple 無法存取。「裝置帳號號碼」是唯一的號碼，且與大部分的信用卡或簽帳金融卡號不同，發卡機構或付款網路可以防止將此號碼用於磁條卡、電話或網站。Secure Element 中的「裝置帳號號碼」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、配備 Touch ID 的 Mac 電腦，以及使用配備 Touch ID 的巧控鍵盤並配備 Apple 晶片的 Mac 電腦隔離。

搭配 Apple Watch 使用的卡片，是使用 iPhone 上的 Apple Watch App 或在發卡機構的 iPhone App 中提供給 Apple Pay。將卡片加入 Apple Watch 會要求手錶必須位於藍牙通訊範圍內。卡片會特別註冊為搭配 Apple Watch 使用且具有專屬的「裝置帳號號碼」，此資訊會儲存在 Apple Watch 上的 Secure Element 內。

在使用相同 iCloud 帳號登入的裝置上執行「設定輔助程式」期間，已加入的信用卡、簽帳金融卡或預付卡 (包含商店卡) 會顯示在卡片列表中。只要至少在一部裝置上為啟用狀態，這些卡片就會保留在這份列表上。從所有裝置上移除卡片 7 天後，該卡片就會從此列表中移除。此功能需要對個別 iCloud 帳號啟用雙重認證。

## 將信用卡或簽帳金融卡加入 Apple Pay

可手動將信用卡加入 Apple 裝置中的 Apple Pay。

### 手動加入信用卡或簽帳金融卡

若要手動加入卡片，需要提供姓名、卡號、到期日和 CVV 以執行佈建程序。從「設定」、「Apple 錢包」或 Apple Watch App 中，使用者可以使用裝置上的相機拍攝來輸入該資訊。當相機擷取到卡片資訊時，Apple 會嘗試填入姓名、卡號和到期日。照片並不會儲存在裝置上或照片圖庫中。所有欄位均填妥後，「卡片檢查」程序會驗證 CVV 以外的欄位。接著所有資訊會經過加密並傳送到 Apple Pay 伺服器。

若「卡片檢查」程序傳回條款與約定 ID，則 Apple 會下載發卡機構的使用條款與約定，並顯示給使用者閱覽。如果使用者接受發卡機構的條款與約定，Apple 便會將所接受條款的 ID 連同 CVV 傳送至「連結」和「佈建」程序。此外，作為「連結」和「佈建」程序的一部分，Apple 會與發卡機構或網路分享裝置的資訊。這包括像是 (a) 使用者 iTunes 和 App Store 帳戶活動的相關資訊 (例如使用者是否在 iTunes 內有長期的交易記錄)、(b) 使用者裝置 (例如電話號碼、裝置名稱及裝置機型，以及任何設定 Apple Pay 所需的輔助 Apple 裝置) 以及 (c) 加入卡片時的大略位置 (若使用者已啟用「定位服務」)。發卡機構會使用此資訊來判定是否要核准將該卡片加入 Apple Pay。

「連結」和「佈建」程序會產生兩個結果：

- 裝置會開始下載代表信用卡或簽帳金融卡的「Apple 錢包」票卡檔案。
- 裝置會開始將卡片綁定至 Secure Element。

票卡檔案包含 URL，可供下載卡片封面、與卡片相關的後設資料 (例如聯絡資訊)、相關發卡機構 App 和支援的功能。它也包含票卡狀態，其中的資訊包含 Secure Element 的個人化是否已完成、卡片目前是否已遭發卡銀行停用，或是在卡片可以搭配 Apple Pay 進行付款前，還需要進行哪些額外驗證。

### 從 iTunes Store 帳號加入信用卡或簽帳金融卡

若要使用向 iTunes 登記的信用卡或簽帳金融卡，使用者可能需要重新輸入其 Apple ID 密碼。系統會從 iTunes 擷取卡號，並隨之啟動「卡片檢查」程序。如果卡片符合使用 Apple Pay 的資格，裝置會下載並顯示發卡機構的條款與約定，並連同條款 ID 和卡片安全碼傳送至「連結」和「佈建」程序。iTunes 帳號存檔的卡片資料可能需要額外驗證。

### 從發卡機構的 App 加入信用卡或簽帳金融卡

App 註冊使用 Apple Pay 時，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片資訊。這樣有助於避免資訊遭 Apple 裝置讀取。此佈建流程類似於上述手動加入卡片所使用的流程，但替代 CVV 所用的一次性密碼除外。

### 從發卡機構的網站加入信用卡或簽帳金融卡

某些發卡機構提供了直接從其網站啟動「Apple 錢包」卡片佈建流程的功能。在這種情況下，使用者透過在發卡機構的網站上選取要佈建的卡片來啟動任務。然後，系統會將使用者重新導向至獨立的 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，使用者接著選擇一個或多個裝置來佈建卡片，並需要在每個個別的目標裝置上確認佈建結果。

### 加入其他驗證

發卡機構有權決定信用卡或簽帳金融卡是否需要其他驗證。視發卡機構提供的選項而定，使用者可能有多種額外驗證選項，例如簡訊、電子郵件、客服電話，或是經核准第三方 App 所提供的方法來完成驗證。若使用簡訊或電子郵件，使用者會看到選項，可從發卡機構既存檔案的聯絡資訊中選擇。接著會傳送一組代碼，使用者必須將其輸入「Apple 錢包」、「設定」或 Apple Watch App 中。若使用客服或 App 驗證，發卡機構會實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，系統才會進行付款。在 iPhone、iPad 或配備 Touch ID (或與配備 Touch ID 的巧控鍵盤配對) 的 Mac 上，需確認使用者已透過生物辨識認證機制或裝置密碼進行認證。生物辨識認證 (如果可用) 是預設方式，但是隨時都能使用密碼，且在嘗試比對指紋三次或比對面孔兩次 (適用於 iPhone 和 iPad) 失敗後，系統會自動建議改用密碼；嘗試失敗五次後，就必須使用密碼。未設定生物辨識認證或沒有為 Apple Pay 開啟此功能時，也須輸入密碼。若要在 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。

### 使用共享密鑰組

「安全隔離區」和 Secure Element 之間的通訊會在序列介面上進行，過程使用以 AES 為基礎的加密和認證機制，並運用加密編譯反重放值來抵禦重放攻擊。雖然兩端沒有直接相連，但它們使用製造期間佈建的共享密鑰組以安全的方式通訊。在此過程中，「安全隔離區」會從其 UID 密鑰和 Secure Element 的獨有識別碼產生密鑰組。接著會在出廠時安全地將密鑰組傳輸至硬體安全模組 (HSM)。然後 HSM 會將密鑰組插入 Secure Element 中。

### 授權安全交易

當使用者授權交易時 (其中包括直接傳達給 Secure Enclave 的實際手勢)，「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。當使用者首次佈建信用卡並於 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」的加密和反復原機制保護。它會藉由運用密鑰組安全地傳送到 Secure Element。在接收到新的 AR 值時，Secure Element 會將任何先前加入過的卡片標記為已終止。

### 使用付款密碼來達成動態安全性

來自付款 Applet 的付款交易包含付款密碼及「裝置帳號號碼」。這組密碼為一次性代碼，是系統使用交易計數器和密鑰運算而出。交易計數器會隨著每筆新交易而遞增。密鑰是在進行個人化期間於付款 Applet 中佈建，且付款網路或發卡機構或此二者皆知道。視付款方案而定，也可能會使用其他資料來進行計算，包含：

- Terminal Unpredictable Number (適用於近場通訊 (NFC) 交易)
- Apple Pay 伺服器反重放值 (適用於 App 內交易)
- 使用者驗證結果，例如持卡人驗證方式 (CVM) 資訊

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

## 以卡片進行 Apple Pay 付款

Apple Pay 可用來在商店、App 內和網站上購買商品。

### 在商店使用卡片付款

如果 iPhone 或 Apple Watch 已開機且偵測到 NFC 感應場，便會向使用者顯示要求的卡片 (若該卡已開啟自動選取功能)，或顯示「設定」中管理的預設卡片。使用者也可前往「Apple 錢包」並選擇卡片，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
- 使用允許從鎖定螢幕支付 Apple Pay 的輔助使用功能

接下來，在發送付款資訊前，使用者必須使用 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片。所有付款資訊皆需經過使用者認證始得發送。

使用者認證完成後，在處理付款時便會使用「裝置帳號號碼」和因交易而異的動態安全碼。無論是 Apple 還是使用者的裝置，皆不會將完整的信用卡或簽帳金融卡號碼傳送給商家。Apple 可能會接收到匿名的交易資訊，如交易的約略時間和地點，這可協助改進 Apple Pay 及其他的 Apple 產品和服務。

## 在 App 內使用卡片付款

Apple Pay 也可以用來在 iOS、iPadOS、macOS 和 watchOS App 內進行付款。當使用者在 App 內使用 Apple Pay 付款時，Apple 會收到加密的交易資訊以傳給開發者或商家。發送出該資訊給開發者或商家前，Apple 會使用開發者專用的密鑰來重新加密交易。Apple Pay 會保留匿名的交易資訊，例如約略購買金額。此資訊無法用來追蹤使用者，且絕不包含使用者購買的商品資訊。

當 App 起始 Apple Pay 付款交易時，Apple Pay 伺服器會比商家先收到來自裝置的加密資訊。Apple Pay 伺服器接著會以商家專用的密鑰重新加密，然後再傳遞給商家。

當 App 要求付款時，會呼叫 API 以判別裝置是否支援 Apple Pay，以及使用者所使用的信用卡或簽帳金融卡是否可在商家認可的付款網路上進行付款。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，以及聯絡資訊。App 接著會要求 iOS、iPadOS、macOS 或 watchOS 出示 Apple Pay 表單，其會要求 App 的資訊以及其他必要資訊，例如要使用的卡片。

需在此時提供城市、行政區和郵遞區號等資訊給 App 以計算最終運費。直到使用者以 Face ID、Touch ID 或裝置密碼授權付款，所要求的全部資訊才會提供給 App。付款一經授權，Apple Pay 表單內出示的資訊便會傳送給商家。

## 在輕巧 App 內使用卡片付款

輕巧 App 是 App 的一小部分，可讓使用者快速執行作業（如租借自行車、支付停車費等），不需要下載完整 App。在支援付款功能的輕巧 App 中，使用者可以「使用 Apple 登入」，然後使用 Apple Pay 進行付款。當使用者在輕巧 App 內進行付款，所有安全和隱私保護措施都與在一般 App 中付款相同。

## 使用者授權、商家驗證、App 付款的方式

使用者和商家可藉由將資訊傳遞至 Apple 伺服器、Secure Element、裝置和 App 的 API，確保 App 付款安全無虞。首先，當使用者授權 App 付款，App 會呼叫 Apple Pay 伺服器以取得加密編譯反重放值。伺服器會將此值和其他交易資料傳送到 Secure Element 以計算付款憑證，此付款憑證會以 Apple 密鑰進行加密。Secure Element 接著會將付款憑證傳回給 Apple Pay 伺服器以進行解密，根據 Apple Pay 伺服器最初傳送的反重放值驗證其反重放值，然後透過「商家 ID」關聯的商家密鑰重新加密。然後 Apple 伺服器會將付款傳回至裝置，再由裝置回傳給 App API，讓 API 傳遞至商家系統進行處理。商家會解密付款憑證以驗證其為正確的交易接收者。

API 會要求一個授權，此授權用來指定支援的「商家 ID」。App 也可以包含其他資料（例如訂單編號或客戶身分）來傳送至待簽署的「安全隔離區」，確保交易無法轉移至其他客戶。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。商家接著會負責驗證 applicationData 雜湊值是否與付款資料內包含的雜湊值相符。

## 在網站上使用卡片付款

你可在 iPhone、iPad、Apple Watch 以及配備 Touch ID 的 Mac 電腦上，使用 Apple Pay 來在網站中付款。Apple Pay 交易也可在 Mac 上進行，並在使用相同 iCloud 帳號且啟用 Apple Pay 的 iPhone 或 Apple Watch 上完成。

網路上的 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 來提供它們的內容服務。針對每次付款交易，網站需要使用 Apple 發出的 TLS 用戶端憑證來向 Apple 伺服器取得安全且唯一的商家作業階段。商家作業階段資料則會由 Apple 加以簽署。商家作業階段簽章經過驗證後，網站便可查詢使用者是否具有支援 Apple Pay 的裝置，以及這些裝置上是否已啟用信用卡、簽帳金融卡或預付卡。任何其他細節皆不會共享。如果使用者不想要共享此資訊，他們可以在 iPhone、iPad 和 Mac 裝置上的 Safari 隱私權設定中停用 Apple Pay 查詢。



商家作業階段經過驗證後，所有隱私權與安全性措施皆與使用者在 App 內付款時相同。

如果使用者將付款相關資訊從 Mac 傳輸至 iPhone 或 Apple Watch，Apple Pay「接力」會使用端對端的加密「Apple 識別服務」(IDS) 通訊協定，在使用者的 Mac 與授權裝置間傳輸付款的相關資訊。Mac 上的 IDS 用戶端會利用使用者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訊，而這些密鑰無法供 Apple 使用。為 Apple Pay「接力」進行的裝置搜尋包含使用者信用卡的類型與唯一識別碼，以及部分後設資料。使用者卡片的「裝置帳號號碼」不會共享，且會安全地繼續保留在使用者的 iPhone 或 Apple Watch 上。Apple 也會透過「iCloud 鑰匙圈」安全地傳送使用者最近使用過的聯絡人、送貨及帳單地址。

使用者使用 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，針對每個網站商家憑證進行專屬加密的付款代號就會安全地從使用者的 iPhone 或 Apple Watch 傳輸到他們的 Mac，然後傳遞到商家的網站。

只有鄰近的裝置可要求和完成付款。鄰近位置是透過低功耗藍牙 (BLE) 廣播來加以判定。

## 自動付款與商家代號

在 iOS 16 或以上版本中，提供 Apple Pay 功能的 App 和網站可使用 Apple Pay 商家代號，確保在使用者的所有裝置上都能安全付款。iOS 16 的更新版 Apple Pay 付款表單也將預先授權付款體驗最佳化。Apple Pay API 的新交易類型讓 App 和網站開發者能設定訂閱項目、定期帳單、分期付款和自動重新載入卡片餘額等項目，藉此微調付款表單體驗。

商家代號不會綁定裝置，因此如果使用者從裝置移除特定付款卡，還是可進行持續性定期付款。

## 付款給多個商家

在 iOS 16 或以上版本中，Apple Pay 提供新功能，可在單一 Apple Pay 付款表單中指定多個商家的購買金額。這為客戶帶來彈性，可一次購買搭售商品，例如包含航班、租車和旅館的旅遊套裝行程，然後再分別付款給不同商家。

## Apple Pay 中的感應式票卡

為了將資料從支援的票卡傳輸到相容的 NFC 終端機，Apple 使用「Apple 增值服務」(Apple VAS) 通訊協定。VAS 通訊協定可在感應式終端機上或在 iPhone App 中導入，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，且可用來單獨出示感應式票卡，或做為 Apple Pay 交易的一部分。

將裝置拿近 NFC 終端機時，終端機會藉由發送票卡要求來起始接收票卡資訊的程序。若使用者擁有帶有票卡提供者識別碼的票卡，系統會要求使用者透過 Face ID、Touch ID 或密碼授權使用。票卡資訊、時間戳記及一次性隨機 ECDH P-256 密鑰會與票卡提供者的公用密鑰一起使用，以便為卡片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，使用者可手動選擇票卡再向商家的 NFC 終端機出示。在 iOS 13.1 或以上版本中，票卡提供者可設定手動選取的票卡需要使用者認證，或是不經認證就可使用。

## 停用卡片的 Apple Pay 功能

只有在 Secure Element 使用與加入卡片時相同的密鑰組和「授權隨機」(AR) 值出示授權時，才能使用加入到 Secure Element 的信用卡、簽帳金融卡和預付卡。在接收到新的 AR 值時，Secure Element 會將任何先前加入過的卡片標記為已終止。這會使作業系統在下列情況發出指令，讓「安全隔離區」將 AR 拷貝標記為無效，讓卡片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

方式	裝置
使用者登出 iCloud。	iPhone、iPad、Mac、Apple Watch
使用者選擇「清除所有內容和設定」。	iPhone、iPad、Mac、Apple Watch
裝置從「復原模式」回復。	iPhone、iPad、Mac、Apple Watch
取消配對	Apple Watch

## 停用、移除和清除卡片

使用者可以使用「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。使用者也可以使用「尋找」、iCloud.com 或直接在裝置上使用「Apple 錢包」來清除 Apple Pay 中的卡片。在 Apple Watch 上，可以使用 iCloud 設定或 iPhone 上的 Apple Watch App 移除卡片，或是直接在手錶上移除。在裝置上使用卡片來進行付款的功能將會由發卡機構或個別付款網路在 Apple Pay 中停用或移除，即使裝置處於離線狀態且未連線至行動數據或 Wi-Fi 網路也能進行。使用者也可撥打電話給其發卡機構來從 Apple Pay 停用或移除卡片。

當使用者透過「清除所有內容和設定」、使用「尋找」或將裝置回復來清除整部裝置時，iPhone、iPad、Mac 和 Apple Watch 會指示 Secure Element 將所有卡片標記為已終止。這會立即將卡片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 完全清除卡片為止。除此之外，「安全隔離區」會將 AR 標記為無效，使先前登記的卡片無法進行進一步的付款授權。當裝置為線上狀態時，會嘗試聯絡 Apple Pay 伺服器，以協助確保 Secure Element 中的所有卡片皆已清除。

## Apple Card 安全性

在支援的 iPhone 和 Mac 機型上，使用者可以安全地申請 Apple Card。

### Apple Card 申請

在 iOS 12.4 或以上版本、macOS 10.14.6 或以上版本以及 watchOS 5.3 或以上版本中，可搭配 Apple Pay 使用 Apple Card 來在商店、App 內和網站上進行付款。

如需申請 Apple Card，使用者必須在相容於 Apple Pay 的 iPhone 或 iPad 上登入其 iCloud 帳號，且須為 iCloud 帳號設定雙重認證，或者可以在登入 Apple ID 後至 [apply.applecard.apple](https://apply.applecard.apple) 申請。申請經過核准後，就可在使用者已登入 Apple ID 的任何合格裝置上，於「Apple 錢包」或「設定」>「錢包與 Apple Pay」中取用 Apple Card。

當使用者申請 Apple Card 時，Apple 的身分提供者合作夥伴會以安全方式驗證使用者的身分資訊，然後基於身分與信用卡評估目的與 Goldman Sachs Bank USA 共享這些資訊。

申請期間提供的社會安全碼或身分證件影像等資訊，都會以安全方式傳輸給 Apple 的身分提供者合作夥伴和/或 Goldman Sachs Bank USA，且會用其各自的密鑰進行加密。Apple 無法解密這些資料。

申請期間提供的收入資訊，以及用於扣款的銀行帳戶資訊，都會以安全方式傳輸給 Goldman Sachs Bank USA 且會用其密鑰進行加密。銀行帳戶資訊會儲存在鑰匙圈中。Apple 無法解密這些資料。

將 Apple Card 加入「Apple 錢包」時，某些資訊可能會與 Apple 合作銀行 Goldman Sachs Bank USA 和 Apple Payments Inc. 共享，這些資訊與使用者加入信用卡或簽帳金融卡時所提供的相同。這些資訊只會用於疑難解答、防詐騙和法規目的。

在 iOS 14.6 或以上版本、iPadOS 14.6 或以上版本以及 watchOS 7.5 或以上版本中，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片。使用者需要認證才能確認邀請。「Apple 錢包」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名。該簽名會在 Apple 伺服器上驗證。

組織者可以選擇為參與者設定交易上限。參與者卡也可以透過「Apple 錢包」隨時加以鎖定以暫停消費。當 18 歲以上的共同持有人或參與者接受邀請並提出申請時，他們將按照「Apple 錢包」中 Apple Card 申請部分中定義的相同申請流程進行申請。

## Apple Card 使用

使用可透過「Apple 錢包」中的 Apple Card 訂購實體卡片。使用者收到實體卡片後，需使用裝著實體卡片的對折信封內的 NFC 標籤來啟用卡片。此標籤為該卡片專用，無法用於啟用其他使用者的卡片。或者，也可在「Apple 錢包」設定中手動啟用卡片。此外，使用者也可隨時至「Apple 錢包」選擇鎖定或解鎖實體卡片。

## Apple Card 付款與「Apple 錢包」票卡詳細資訊

Apple Card 帳號應付的款項，可從網頁瀏覽器或 iOS 的「Apple 錢包」，透過 Apple Cash 和銀行帳戶付款。可將帳單付款排程為定期付款，或是在指定日期一次付款（使用 Apple Cash 和銀行帳戶）。使用者進行付款時，系統會呼叫 Apple Pay 伺服器以取得加密編譯反重放值（類似 Apple Cash）。反重放值和付款設定詳細資訊會傳遞到 Secure Element 以計算簽章。簽名則會傳回到 Apple Pay 伺服器。Apple Pay 伺服器會透過簽章和反重放值驗證付款的認證、完整性和正確性，而訂單會傳送至 Goldman Sachs Bank USA 進行處理。

「Apple 錢包」藉由提供憑證來擷取 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，它使用此密鑰對 Apple Card 卡號進行加密，接著將其傳回到「Apple 錢包」，這樣只有請求 Apple Card 卡號的 iPhone 才能解密它。解密後，Apple Card 卡號會儲存在「iCloud 鑰匙圈」中。

若要使用「Apple 錢包」在票卡中顯示 Apple Card 卡號詳細資訊，需透過 Face ID、Touch ID 或密碼進行使用者認證。使用者可在卡片資訊區域取代及停用先前的上述詳細資訊。

## 進階詐騙防範

在 iOS 15 或以上版本以及 iPadOS 15 或以上版本中，Apple Card 使用者可以在「Apple 錢包」中啟用「進階詐騙防範」。啟用後，「卡片安全碼」每隔幾天會重新整理一次。

## Apple Cash 安全性

在 iOS 11.2 或以上版本、iPadOS 13.1 或以上版本及 watchOS 4.2 或以上版本上，使用者可在 iPhone、iPad 或 Apple Watch 上使用 Apple Cash 向其他使用者付款、收款和請款。使用者收款時，款項會加入 Apple Cash 帳號中，且可在使用者已用 Apple ID 登入的合格裝置上，前往「Apple 錢包」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 驗證身分的 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使用者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 帳號復原，則家庭的組織者必須手動為該使用者重新啟用 Apple Cash 卡片。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號中。

使用者設定 Apple Cash 時，某些資訊可能會與我們的合作銀行 Green Dot Bank 和 Apple Payments Inc. 共享，這些資訊與使用者在加入信用卡或簽帳金融卡時所提供的相同。Apple Payments Inc. 是我們專為保護使用者的隱私而成立的全資子公司，其儲存和處理資訊的過程獨立於 Apple 與其餘子公司，且方法完全保密。此資訊僅用於排解疑難問題、防範詐騙和法規用途。

## 在 iMessage 中使用 Apple Cash

若要使用個人對個人付款和 Apple Cash，使用者必須在與 Apple Cash 相容的裝置上登入自己的 iCloud 帳號，並為 iCloud 帳號設定雙重認證。使用者間的請款和轉帳程序可從「訊息」App 內啟動或要求 Siri 執行。使用者嘗試付款時，iMessage 會顯示 Apple Pay 表單。系統會一律先使用 Apple Cash 餘額。如有必要，會從使用者加入「Apple 錢包」中的第二信用卡或簽帳金融卡提取額外款項。

## 在商店、App 內和在網站上使用 Apple Cash

「Apple 錢包」中的 Apple Cash 卡片可搭配 Apple Pay 使用，以便在商店、App 內和網站上進行付款。Apple Cash 帳號中的錢也可以轉帳到銀行帳戶中。除了收取其他使用者所付的款項，也可使用「Apple 錢包」中的簽帳金融卡或預付卡為 Apple Cash 帳號加值。

一旦交易完成，基於疑難問題排解、防範詐騙或法規目的，Apple Payments Inc. 會儲存且可能運用使用者的交易資料。Apple 與其餘子公司均無從得知使用者的付款、收款對象或是使用 Apple Cash 卡片進行購買的地點。

當使用者透過 Apple Pay 付款、將款項加入 Apple Cash 帳號中，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反重放值，這個反重放值與 App 中針對 Apple Pay 傳回的數值類似。反重放值和其他交易資料會傳遞到 Secure Element 以計算付款簽章。簽名會傳回到 Apple Pay 伺服器。Apple Pay 伺服器會透過付款簽章和反重放值驗證交易的認證、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使用者。

如果交易牽涉以下項目：

- 對 Apple Cash 儲值的簽帳金融卡
- 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 帳號的餘額超過一定金額後，或是當偵測到異常活動時，系統就會提示使用者驗證其身分。社會安全碼或問題的回答（例如確認使用者先前居住地址的街道名稱）等提供用於驗證使用者身分的資訊，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 無法解密這些資料。如果使用者執行了 Apple ID 帳號復原作業，則系統將提示使用者再次驗證其身分，然後才能重新取用其 Apple Cash 餘額。

## 「iPhone 卡緊收」的安全性

iOS 15.4 或以上版本提供的「iPhone 卡緊收」，允許商家使用 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 iPhone 裝置的使用者可以安全地接受非接觸式支付和支援 Apple Pay NFC 的票卡。透過「iPhone 卡緊收」，商家無需額外的硬體即可接受非接觸式支付。

「iPhone 卡緊收」的設計目標也在於保護付款人的個人資訊。此服務不會收集可追蹤付款人的交易資訊。信用卡/簽帳金融卡號 (PAN) 等付款卡資訊受到 Secure Element 保護，不會顯示在商家裝置上。付款卡資訊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。

「iPhone 卡緊收」經過受認可安全性實驗室的外部評估，已通過核准，可供開放此功能的地區內所有支援的支付網路使用。

### 非接觸式支付元件的安全性

- **Secure Element**：Secure Element 主控著付款核心，用於讀取和保護非接觸式付款卡的資料。
- **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。
- **「iPhone 卡緊收」伺服器**：「iPhone 卡緊收」伺服器會管理裝置中付款核心的設定和佈建。這些伺服器監控 iPhone 裝置上的「iPhone 卡緊收」安全性的方式，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，且符合 PCI DSS。

### 「iPhone 卡緊收」如何讀取信用卡、簽帳金融卡和預付卡

「iPhone 卡緊收」如何佈建安全性

首次使用足夠授權的 App 來使用「iPhone 卡緊收」時，「iPhone 卡緊收」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。驗證完成後，付款接受 applet 會從「iPhone 卡緊收」伺服器下載並安裝在 Secure Element 上，也會一併安裝相關的付款核心設定。此操作會在「iPhone 卡緊收」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。

#### 「iPhone 卡緊收」如何安全讀取卡片

「iPhone 卡緊收」App 要求從 ProximityReader 架構讀取卡片時，會顯示一個由 iOS 控制的表單，並提示使用者感應付款卡。沒有任何 App 可以讀取使用感應交易畫面期間可能洩漏機密卡片資料任何部分的感應器。iOS 會初始化付款卡讀卡機，然後要求 Secure Element 中的付款核心啟動讀卡。

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 之間交換卡片資料。只有在此模式下才能讀取付款卡。

Secure Element 上的付款接受 applet 完成讀取付款卡後，會對卡片資料進行加密和簽署。付款卡資料在到達支付服務供應商之前會一直保持加密和認證。只有 App 用來要求讀卡的支付服務供應商才能解密付款卡資料。支付服務供應商必須從「iPhone 卡緊收」伺服器要求付款卡資料解密的密鑰。驗證資料的完整性和真實性，並驗證讀卡是在索取付款卡資料解密密鑰後 60 秒內執行之後，「iPhone 卡緊收」伺服器會向支付服務供應商發出解密密鑰。

此模型有助於確保付款卡資料不會遭 PSP 以外的任何人解密，PSP 會為商家處理此交易。

## 透過輸入 PIN 碼來授權交易

iOS 16.0 或以上版本提供的 PIN 碼輸入功能，可讓付款者在商家的裝置上輸入自己的 PIN 碼以授權交易。根據與付款卡交換的資訊，感應後可能會立即觸發 PIN 碼輸入畫面。或者，支付服務供應商可提供簽署代號（僅對一次交易有效）來觸發 PIN 碼畫面。

PIN 碼輸入機制經過受認可安全性實驗室的外部評估，已通過核准，可供開放此功能的地區內所有支援的支付網路使用。PIN 碼輸入畫面受到保護，可防止截圖和螢幕鏡像輸出，且沒有任何 App 可以讀取使用 PIN 碼輸入畫面期間可能洩漏 PIN 碼值任何部分的感應器。

Secure Element 會安全擷取輸入的 PIN 碼。Secure Element 會利用這些 PIN 碼建立符合支付業界標準的加密 PIN 區塊。Apple 會以安全方式從符合 PCI PIN 的後端提供加密 PIN 區塊給 PSP 進一步處理。

PIN 碼值：

- 商家絕對無法在其裝置上取用
- Apple 絕對不會解密
- Apple 絕對不會留存

# 使用 Apple 錢包

## 使用 Apple 錢包存取

在支援的 iPhone 和 Apple Watch 裝置上的「Apple 錢包」中，使用者可以儲存多種類型的鑰匙。當使用者抵達門口時，甚至能自動顯示正確的鑰匙（如果鑰匙支援且開啟「快速模式」），讓他們使用近場通訊 (NFC) 功能輕觸一下即可進入。

### 使用者便利性

#### 快速模式

若將鑰匙加入「Apple 錢包」，系統就會預設開啟「快速模式」。處於「快速模式」的鑰匙能與接受該鑰匙的終端機互動，不需要使用 Face ID、Touch ID、密碼認證或按兩下 Apple Watch 的側邊按鈕。若要停用此功能，在「Apple 錢包」中，使用者可以在代表鑰匙的卡片正面上，點一下「更多」按鈕來關閉「快速模式」。若要重新開啟「快速模式」，他們必須使用 Face ID、Touch ID 或密碼。

#### 鑰匙共享

在 iOS 16 或以上版本中，特定鑰匙類型支援鑰匙共享功能。

透過將鑰匙擁有者 iPhone 上的安全性和隱私設定，套用到受邀鑰匙接收者的 iPhone 上，使用者可以共享鑰匙（例如家門或汽車鑰匙）的取用權限。點一下「Apple 錢包」中鑰匙的共享圖像，就能共享鑰匙，也可以使用「分享表單」中顯示的方式來共享。鑰匙擁有者也可以選擇每個共享鑰匙的使用權限層級和有效時段。鑰匙擁有者可以看到自己共享的所有鑰匙，也可以撤銷任何共享鑰匙的使用權限，包含初始鑰匙接收者再次將鑰匙與另一位使用者共享的情況。

鑰匙共享邀請會由信箱內的專用伺服器以匿名且安全的方式儲存，並以 AES 128 或 256 加密密鑰保護。加密密鑰永遠不會與伺服器或目標鑰匙接收者以外的任何人共享，且只有鑰匙接收者可以解密邀請。建立信箱時，鑰匙擁有者的 iPhone 會提供一個裝置宣告，只會由伺服器與該信箱綁定。鑰匙接收者的 iPhone 最初取用這個信箱時，需出示鑰匙接收者裝置宣告。只有出示有效裝置宣告的鑰匙擁有者和鑰匙接收者 iPhone 裝置可以存取該信箱。每部 iPhone 裝置宣告都有唯一的 RFC4122 UUID 值。

為提供額外安全措施，鑰匙擁有者可以開啟 6 位數隨機產生的啟用碼，要求在鑰匙接收者的 iPhone 上輸入。鑰匙擁有者或合作夥伴伺服器會強制執行與驗證代碼的重試次數。鑰匙擁有者必須將這組啟用碼傳達給鑰匙接收者，而鑰匙接收者必須在鑰匙擁有者或合作夥伴伺服器要求進行驗證時出示該代碼。

鑰匙接收者兌換邀請後，接收 iPhone 就會立即將該邀請從伺服器上清除。含有鑰匙共享邀請的信箱亦具有時效性，這會在建立信箱時設定，並由伺服器強制執行。伺服器會自動清除所有已過期的邀請。

視原始製造商而定，鑰匙也可以與非 Apple 裝置共享，不過安全共享鑰匙的方式可能與 Apple 不同。

## 隱私權與安全性

「Apple 錢包」中的申領密鑰充分利用了 iPhone 和 Apple Watch 內建的隱私權和安全性。使用者使用「Apple 錢包」中的密鑰的時機和地點，永遠不會與 Apple 共享或儲存在 Apple 伺服器上，且憑證會安全儲存在受支援裝置的 Secure Element 中。Secure Element 會託管專門設計的 applet 來安全管理密鑰，確保密鑰無法遭截取或洩漏。

在佈建任何密鑰之前，使用者必須在相容的 iPhone 上登入其 iCloud 帳號，並為其 iCloud 帳號開啟雙重認證，但學生證除外，它不需要雙重認證即可開啟。

當使用者啟動佈建程序時，會發生與信用卡和簽帳金融卡佈建中所涉及的類似步驟，例如**連結和佈建**。在交易期間，讀卡機會使用建立的安全通道，透過近場通訊 (NFC) 控制器直接與 Secure Element 進行通訊。

可以佈建密鑰的裝置數量 (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的佈建密鑰的最大數量，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。有鑑於隱私權與安全性的緣故，每個合作夥伴的識別碼都不一樣。

合作夥伴也會收到使用者識別碼 (識別碼經過匿名處理，而且每個合作夥伴的識別碼都是唯一的)，因此可在初始佈建期間將密鑰安全綁定至使用者 iCloud 帳號。在透過合作夥伴建立的使用者帳號遭入侵 (例如發生帳號接管攻擊) 的情況下，這個措施可防止其他使用者佈建此密鑰。

可藉由以下方式停用或移除鑰匙：

- 透過「尋找」從遠端清除裝置
- 透過「尋找」啟用「遺失模式」
- 接收行動裝置管理 (MDM) 遠端清除指令
- 從 Apple ID 帳號頁面移除所有卡片
- 從 iCloud.com 移除所有卡片
- 從「Apple 錢包」中移除所有卡片
- 在發卡機構的 App 中移除卡片

在 iOS 15.4 或以上版本中，當使用者按兩下配備 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，不會顯示他們的票卡和申領密鑰詳細資訊。在票卡特定資訊 (包括旅館預訂詳細資訊) 在「Apple 錢包」中顯示之前，需要進行 Face ID、Touch ID 或密碼認證。

## 申領密鑰類型

「Apple 錢包」提供不同類型的取用權限，例如旅館、公司識別證、學生證、住家鑰匙和汽車鑰匙。

### 旅館

「Apple 錢包」中的旅館房間鑰匙有助於提供從入住到退房的輕鬆、非接觸式體驗，有別於傳統塑料旅館鑰匙卡，為客人提供額外的隱私權與安全性優勢。受支援地點的旅館客人可以在相容的 iPhones 和 Apple Watch Series 4 或後續機型上，使用「Apple 錢包」中的房間鑰匙點一下解鎖。

「Apple 錢包」中的功能專為減少客戶的不便而設計：

- 從旅館的 App 進行抵達前佈建，以便在入住前將票卡加入到「Apple 錢包」中
- 入住票卡，用於從「Apple 錢包」啟動登記入住和房間分配

- 佈建後鑰匙更新，以支援延長或修改目前的住宿天數
- 「Apple 錢包」中單次票卡的多房間鑰匙支援
- 「Apple 錢包」中過期鑰匙的自動封存

## Disney MagicMobile 票卡

使用者可以將 Disney MagicMobile 票卡加入 iPhone 或 Apple Watch 上的「Apple 錢包」，方便進入適用票卡方案的 Disney 主題樂園。MagicMobile 票卡可用來進入樂園，也可在園內的其他適用讀卡機使用。

若要加入 Disney MagicMobile 票卡，除了須為 iCloud 帳號啟用雙重認證外，使用者也必須擁有與有效 My Disney Experience 帳號綁定的適用樂園門票或預約。使用者可在 iPhone 上的 My Disney Experience App 中，選取一張或多張票卡來加入「Apple 錢包」。如果使用者已有配對的 Apple Watch，選取的票卡會自動佈建到使用者的 iPhone 和配對的 Apple Watch 上。加入 iPhone 和 Apple Watch 裝置的票卡都會預設開啟「快速模式」。為了方便使用，開啟「快速模式」時，也會同時為目前在裝置上的所有 MagicMobile 票卡開啟。

一次可將多張票卡加入單一裝置，方便使用者管理所有同行成員的票卡。使用者也可以選擇使用 My Disney Experience App 來與其他使用者共享票卡。如此一來，接收者就能將共享的票卡加入自己裝置上的「Apple 錢包」。

## 公司識別證

受支援合作夥伴的員工識別證可以加入到 iPhone 和 Apple Watch 上的「Apple 錢包」，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。若要加入識別證，員工必須為其用於登入其雇主所提供之 App 的帳號啟用多重認證。

員工識別證使用 Apple 的取用功能，允許使用者：

- 透過推播佈建自動將員工識別證加入到配對的 Apple Watch，無需安裝合作夥伴的 App
- 使用「快速模式」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 或以上版本中，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 機型上加入「Apple 錢包」，以便進出校園設施及在接受其證件的地方付款。

使用者需透過學生證發卡機構或參與學校提供的 App，將其學生證加入「Apple 錢包」中。此操作的技術程序，與從發卡機構的 App 加入信用卡或簽帳金融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號使用雙重認證。一張卡片可同時在使用者的 iPhone 和配對 Apple Watch 上設定。

## 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 錢包」中的住家鑰匙進入他們的建築物、住所和公共區域。你可以從合作夥伴提供的 App 中佈建住家鑰匙。對於支援便利佈建的合作夥伴，物業經理可以向租戶傳送連結以使用他們偏好的傳訊管道（例如電子郵件或 SMS）來啟動佈建，租戶只需按一下該連結即可兌換鑰匙。「輕巧 App」也提供安全無縫的體驗，無需安裝合作夥伴的 App 即可佈建鑰匙。如需更多資訊，請參閱 Apple 支援文章：[在 iPhone 上使用輕巧 App](#)。

多人家庭住家鑰匙也可在「快速模式」中使用，且可與朋友和家庭成員安全共享。如需更多資訊，請參閱：[鑰匙共享](#)。

## 住家鑰匙

只需輕點一下 iPhone 或 Apple Watch，即可將「Apple 錢包」中的住家鑰匙與支援 NFC 的門鎖搭配使用。有關使用者如何設定和使用住家鑰匙的更多資訊，請參閱 Apple 支援文章：[在 iPhone 上使用住家鑰匙解除你的門鎖](#)。



當使用者設定住家鑰匙時，他們家中的所有居民也會自動收到住家鑰匙。若要進一步共享住家鑰匙或刪除共享家庭的成員，家庭擁有者可以使用「家庭」App 來管理邀請函和成員。當使用者選擇接受邀請函以使用住家鑰匙加入家庭時，這會啟動將住家鑰匙佈建到其裝置上的「Apple 錢包」中的作業。如果使用者選擇離開住家或家庭擁有者撤回他們的取用權限，這些動作也會從「Apple 錢包」中移除住家鑰匙。

## 汽車鑰匙

受支援的 iPhone 裝置和配對的 Apple Watch 裝置上，提供在「Apple 錢包」中儲存數位汽車鑰匙的原生功能。汽車鑰匙在「Apple 錢包」中會顯示為票卡（由 Apple 代表汽車製造商製作），並支持完整的 Apple Pay 卡片生命週期（iCloud「遺失模式」、「遠端清除」、本機票卡刪除以及「清除所有內容和設定」）。如同標準 Apple Pay 卡片，還可以從車主的 iPhone、Apple Watch 和車輛人機介面（HMI）中刪除共享的汽車鑰匙。

汽車鑰匙可用於解鎖和鎖定車輛、打開和關上後車箱、開啟和關閉警報器、發動引擎或將車輛設為行駛模式等等。「標準作業」提供相互認證，且對於發動引擎來說是強制性的。在講求效率表現時，解鎖和鎖定操作可能會使用「快速作業」。

如果車輛為車主自有且在支援之列，車主可將 iPhone 與該車輛連接或配對以製作鑰匙。所有鑰匙都是根據橢圓曲線（NIST P-256）車上鑰匙生成（ECC-OBKG）機制在 Secure Element 內製作的，專用鑰匙永遠不會離開 Secure Element。裝置和車輛之間的通訊是使用 NFC 或混用藍牙低功耗與超寬頻（UWB）技術進行。鑰匙管理機制則是使用具有相互認證 TLS 的 Apple 對汽車製造商伺服器 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佈建鑰匙則需要重新配對或共享。

汽車鑰匙也可在「快速模式」中使用，且可與朋友和家庭成員安全共享。如需更多資訊，請參閱：[鑰匙共享](#)。如需數位汽車鑰匙安全性和隱私保護的更多資訊，請參閱：[iOS 中的汽車鑰匙安全性](#)。

## 機車鑰匙

在 iOS 17 或以上版本和在特定國家或地區的支援合作夥伴，使用者可以從合作夥伴 App 直接將機車鑰匙佈建到受支援 iPhone 和配對 Apple Watch 上的「Apple 錢包」中，用途如下：

- 感應以上鎖或解鎖機車
- 感應以上鎖或解鎖機車的車廂（若有）

Secure Element 中的專用 applet 會安全處理與機車鑰匙相關聯的加密編譯憑證，進而與機車安全進行資料交換。

使用者可在票卡背面取得有關機車的其他資訊，例如車輛識別號碼（VIN）的後四碼以及行照或車牌號碼。這些可能被視為私密資訊，只能在使用生物特徵認證或裝置密碼時取用。

機車鑰匙也可在「快速模式」中使用，且可與朋友和家庭成員安全共享。如需更多資訊，請參閱：[鑰匙共享](#)。

## iOS 中的汽車鑰匙安全性

在受支援的 iPhone 和已配對的 Apple Watch 上，開發者能支援無須鑰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子郵件連結在汽車製造商 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+ 協定搭配 NIST P-256 曲線來產生安全的配對頻道。使用 App 或電子郵件連結時，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。

## 鑰匙共享

車主的配對 iPhone 可以藉由使用 iMessage 和「Apple 識別服務 (IDS)」傳送特定設備的邀請，來與符合條件的家庭成員和朋友 iPhone 裝置 (及其配對的 Apple Watch 裝置) 共享鑰匙。所有共享命令都使用端對端加密 IDS 功能進行交換。車主配對的 iPhone 會確保 IDS 頻道在共享過程中不會更改，以防止邀請函轉發。

接受邀請後，家庭成員或朋友的 iPhone 將製作數位鑰匙，並將鑰匙製作憑證傳送回車主配對的 iPhone，以驗證鑰匙是在真正的 Apple 裝置上製作的。車主的配對 iPhone 會在其他家庭成員或朋友 iPhone 的 ECC 公開鑰匙上簽署，然後將簽章傳送回家成員或朋友的 iPhone。車主裝置中的簽章操作需要使用者認證 (Face ID、Touch ID 或密碼輸入) 和 [Face ID 和 Touch ID 的用途](#) 中所述的安全使用者意圖。傳送邀請時會要求授權，並在朋友裝置傳回簽章要求時，將其儲存在 Secure Element 中以供使用。鑰匙權限由車輛 OEM 伺服器在線上或在車輛上首次使用共享鑰匙期間提供給車輛。

## 鑰匙刪除

鑰匙可由車主裝置從鑰匙持有者裝置中刪除和在車內刪除。即使鑰匙持有者正在使用鑰匙，在鑰匙持有者 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鑰匙，或者只有在車輛在線上時才可以刪除。

在這兩種情況下，鑰匙持有者裝置或車輛上的刪除作業都會回報給汽車製造商的鑰匙清單伺服器 (KIS)，該伺服器為保險目的會註冊車輛所使用的已核發鑰匙。

車主可以從車主票卡的背面要求刪除。此要求首先傳送給汽車製造商，以取下車輛中的鑰匙。從車輛刪除鑰匙的條件由汽車製造商定義。只有當將鑰匙移出車輛時，汽車製造商伺服器才會將遠端終止要求傳送到鑰匙持有者的裝置。

當鑰匙在裝置中終止時，管理數位汽車鑰匙的 Applet 將建立一個加密簽章的終止證明，該證明將被汽車製造商用作刪除證明，並用於從 KIS 移除鑰匙。

## NFC 標準異動

針對使用 NFC 鑰匙的車輛，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章，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密鑰簽章，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隱私敏感性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來加密其公共密鑰識別碼，以及根據讀取器的資料衍生質詢所計算出的簽章以及一些其他特定 App 的資料。讀取器對 iPhone 簽章的此驗證作業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密碼。這組加密密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向 iPhone 認證車輛。

## BLE/UWB 標準異動

對於使用 UWB 鑰匙的車輛，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 會提供給使用者裝置和車輛上的 UWB 無線電，以讓使用者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。

## 隱私權

汽車製造商的鑰匙清單伺服器 (KIS) 不會儲存裝置 ID、SEID 或 Apple ID。它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，並且在使用者完全清除其裝置 (使用「清除所有內容和設定」) 後會被刪除。

## 將交通卡和 eMoney 卡加入到 Apple 錢包

在許多個全球市場中，使用者可在支援的 iPhone 和 Apple Watch 機型上將支援的交通卡和 eMoney 卡加入「Apple 錢包」中。方法因營運業者而異，可能為從實體卡片將餘額或定期券 (或兩者) 轉移至其數位「Apple 錢包」代表票卡中，或是從「Apple 錢包」或發卡機構的 App 佈建新交通卡或 eMoney 卡。將交通卡加入「Apple 錢包」後，使用者只要把 iPhone 或 Apple Watch 靠近交通卡讀卡機就可以搭乘大眾運輸工具。部分交通卡還能用來付款。

### 交通卡和 eMoney 卡如何運作

加入的交通卡和 eMoney 卡會與使用者的 iCloud 帳號綁定。如果使用者將多張卡片加入至「Apple 錢包」，Apple 或發卡機構可能可以連結卡片間的使用者個人資料和相關帳號資訊。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。

從實體卡片轉移餘額到「Apple 錢包」的過程中，使用者必須輸入該卡片專屬的資訊。使用者也需要提供個人資料來證明卡片持有人身分。將票卡從 iPhone 轉移至 Apple Watch 時，兩部裝置都必須處於上線狀態。

使用者可在「Apple 錢包」中使用信用卡、簽帳金融卡或預付卡進行加值，或是透過交通卡或 eMoney 卡發卡機構的 App 進行加值。若要瞭解使用 Apple Pay 時重新載入餘額的安全性，請參閱：[在 App 內使用卡片付款](#)。若要瞭解從發卡機構的 App 內佈建卡片的方式，請參閱：[從發卡機構的 App 加入信用卡或簽帳金融卡](#)。

如果支援從實體卡片佈建，交通卡或 eMoney 卡發卡機構擁有認證實體卡片和驗證使用者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「裝置帳號號碼」，並在「Apple 錢包」中啟用新加入且含有轉移餘額的票卡。對於某些卡片，完成從實體卡片佈建後，實體卡片便會停用。

如果卡片餘額儲存在裝置上，無論使用哪一種佈建類型，結束時系統都會加密交通卡餘額，並儲存到 Secure Element 中的指定 Applet 內。營運業者擁有密鑰，用於針對卡片資料執行加密編譯作業以進行餘額交易。

依照預設，交通卡使用者可享有流暢的「快速交通卡」體驗，無須使用 Face ID、Touch ID 或密碼即可付款和搭乘大眾運輸工具。若啟用了「快速模式」，便可利用鄰近的任何感應式讀卡機取得最近造訪過的車站、交易記錄和其他票券等資訊。使用者若要開啟 Face ID、Touch ID 或密碼認證要求，只需在「錢包與 Apple Pay」設定中停用「快速交通卡」即可。eMoney 卡不支援「快速模式」。

與其他 Apple Pay 卡片相同，使用者可藉由以下方式停用或移除 eMoney 卡：

- 透過「尋找」從遠端清除裝置
- 透過「尋找」啟用「遺失模式」
- 輸入行動裝置管理 (MDM) 遠端清除指令
- 從 Apple ID 帳號頁面移除所有卡片
- 從 iCloud.com 移除所有卡片
- 從「Apple 錢包」中移除所有卡片
- 在發卡機構的 App 中移除卡片

Apple Pay 伺服器會通知卡片業者停用這些卡片。如果使用者從在線上的裝置移除了交通卡或 eMoney 卡，可將餘額加回以相同 Apple ID 登入的裝置上來復原餘額。如果裝置離線、關機或無法使用，則不能復原餘額。

## 將交通卡和 eMoney 卡加入到家庭成員的 Apple Watch

在 iOS 15 或以上版本和 watchOS 8 或以上版本中，iCloud 家庭組織者可以透過 iPhone 的 Watch App 將交通卡和 eMoney 卡加入到家庭成員的 Apple Watch 裝置中。將其中一張卡佈建到家庭成員的 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 卡加值的要求。訊息內容受端對端加密保護，如 [iMessage 安全性概覽](#) 中所述。可以使用 Wi-Fi 或行動網路連線遠端為家庭成員 Apple Watch 上的卡片加值。操作時不需要鄰近裝置。

**【注意】** 此功能可能未在所有國家或地區提供。

## 信用卡和簽帳金融卡

在某些城市，交通卡讀卡機接受以 EMV (智慧型) 卡片來支付大眾運輸工具的費用。對這類讀卡機出示 EMV 卡或簽帳金融卡時，需進行使用者認證，程序與「使用信用卡和簽帳金融卡在商店內付款」相同。

在 iOS 12.3 或以上版本中，「Apple 錢包」中的一些現有 EMV 信用卡/簽帳金融卡會啟用以用於「快速交通卡」。「快速交通卡」讓使用者無需 Face ID、Touch ID 或密碼，即可在支援的大眾運輸營運商支付路程費用。當使用者佈建 EMV 信用卡或簽帳金融卡，第一張佈建至「Apple 錢包」的卡片會啟用以用於「快速交通卡」。然後使用者就可以在「Apple 錢包」中點一下卡片正面的「更多」按鈕，也可停用將該卡用於「快速交通卡」，方法為將「快速交通卡設定」設定為「無」。使用者也可透過「Apple 錢包」選擇使用其他信用卡或簽帳金融卡作為其「快速交通卡」。若要重新啟用或選擇其他卡片以用於「快速交通卡」，需使用 Face ID、Touch ID 或密碼。

Apple Card 和 Apple Cash 可用於「快速交通卡」。

## Apple 錢包中的身分證

### Apple 錢包中的身分證

在執行 iOS 15.4 或以上版本的 iPhone 8 或後續機型以及執行 watchOS 8.4 或以上版本的 Apple Watch Series 4 或後續機型上，使用者可以將他們的州身分證或駕駛執照加入到「Apple 錢包」，然後點一下他們的 iPhone 或 Apple Watch 以在參與地點無縫安全地展示。

**【注意】** 此功能僅適用於參與的美國各州。

「Apple 錢包」中的 ID 採用使用者裝置硬體和軟體中內建的安全性功能，來協助保護他們的身分並保護個人資訊的安全。

### 將駕駛執照或州身分證加入到「Apple 錢包」

在 iPhone 上，使用者可以直接在「Apple 錢包」畫面的頂部點一下「加入」(+) 按鈕，開始加入其執照或身分證。如果使用者在設定時有配對 Apple Watch，則會提示他們也在 Apple Watch 上的「Apple 錢包」中加入其駕駛執照或身分證。

首先會要求使用者用他們的 iPhone 掃描他們的實體駕駛執照或州身分證的正面和背面。iPhone 會評估影像品質和類型以協助確定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，然後傳送給州發行部門。

接下來，會要求使用者完成一連串面部和頭部動作。這些動作由使用者的裝置和 Apple 進行評估，以協助降低有人使用照片、影片或面具試圖將他人的身分證加入到「Apple 錢包」的風險。然後將這些動作的分析結果傳送給州發行部門，而不是傳送動作本身的影片。

為協助確保將證件加入「Apple 錢包」的人與證件持有人為同一人，系統將要求你拍攝自拍照。在將使用者的照片提交給州發行部門前，Apple 伺服器和使用者的裝置會將照片與執行一連串面部和頭部動作的人員肖像進行比對，並協助確保提交的照片是真人並為身分證上的同一人。在比對完成後，照片將在裝置上加密並傳送到州發行部門以與部門有的證件影像相比較。

最後，會要求使用者執行 Face ID 或 Touch ID 認證。使用者的裝置會將此單一相符的 Face ID 或 Touch ID 生物特徵與州身分證聯繫起來，以協助確保只有將身分證加入此 iPhone 的人才能出示它；其他登記的生物特徵資訊無法用於授權出示身分證。這會嚴格在裝置上執行，且不會傳送到州發行部門。

州發行部門將收到設定數位身分證所需的資訊。這包括使用者身分證正面和背面的影像、從 PDF417 條碼讀取的資料以及使用者在身分證確認過程中拍攝的自拍照。發行州還會收到一個單位數值，用於協助防止詐欺，該值的依據是使用者的裝置使用模式、設定資料和有關其個人 Apple ID 的資訊。然後最終由發行州決定是否批准或拒絕將身分證加入到「Apple 錢包」。

在州發行部門授權將州身分證或駕駛執照加入到「Apple 錢包」後，iPhone 會在 Secure Element 中產生一組密鑰配對，將使用者的身分證錨定到該特定裝置。如果加入到 Apple Watch，Apple Watch 會在 Secure Element 中產生一組密鑰配對。

身分證位於 iPhone 上後，「Apple 錢包」中使用者身分證上所反映的資訊會以受「安全隔離區」保護的加密格式來儲存。

### 透過證件讀卡機使用「Apple 錢包」中的駕駛執照或州身分證

若要在「Apple 錢包」中使用其身分證，在 iPhone 將資訊呈現給證件讀卡機之前，使用者需要使用與「Apple 錢包」中的身分證相關聯的 Face ID 或 Touch ID 裝置進行認證。

若要在 Apple Watch 上的「Apple 錢包」中使用他們的身分證，每次戴上 Apple Watch 上時，使用者都需要使用相關的 Face ID 外觀或 Touch ID 指紋來解鎖他們的 iPhone。然後，他們可以在「Apple 錢包」中使用他們的身分證，而不會認證，直到他們再次卸下他們的 Apple Watch。此功能運用了 [watchOS 的系統安全性](#) 中的基礎「自動解鎖」功能。

當使用者在證件讀卡機附近持有 iPhone 或 Apple Watch，或是在 App 內分享自己的身分證件時，使用者會在裝置上看到提示，顯示要求了哪些特定資訊、誰要求提供，以及對方是否打算儲存這些資訊。在相關聯的 Face ID 或 Touch ID 作出授權後，便從裝置釋出所要求的身分資訊。

**【重要事項】** 使用者無需解鎖、顯示或移交裝置，即可出示身分證。

如果使用者擁有「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訊。

向證件讀卡機傳輸身分資料的過程遵循 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、阻止和減輕安全性風險。這些包括身分資料完整性和防偽、裝置綁定、告知同意和無線電連結上的使用者資料機密性。

### 透過 iOS App 使用「Apple 錢包」中的駕駛執照或州身分證

使用者也可以透過 iOS App 分享「Apple 錢包」中的駕駛執照或州身分證資訊。使用者與 App 分享自己的證件資料後，「Apple 錢包」會擷取並驗證向 App 開發者註冊的加密憑證。

此憑證會用於加密使用者同意分享的資訊。「Apple 錢包」會使用 HPKE 加密資訊，且絕對不會提供給 Apple。「錢包」會定期查詢 Apple 伺服器以驗證該證件資料仍有效。如果最近沒有執行任何檢查，可能會在使用者與 App 分享證件資料時進行檢查。

## 「Apple 錢包」中的身分證安全性

使用「Apple 錢包」中的身分證時，以下功能可幫助增強其安全性。

## 身分資料完整性和防偽

「Apple 錢包」中的身分證使用發行部門提供的簽名，以允許任何符合 ISO/IEC 18013-5 標準的讀卡機確認「Apple 錢包」中的使用者身分證。此外，「錢包」中身分證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 錢包」中身分證上所顯示的資料元素的特定子集，並讓「Apple 錢包」中的身分證使用相同的子集進行回應，進而僅共享要求的資料並最大限度地保護使用者的隱私。

## 裝置綁定

「Apple 錢包」中的身分證驗證會使用裝置簽名來防止證件遭複製和出示身分重複發生。「Apple 錢包」會將用於身分認證的專用密鑰儲存在 iPhone 裝置的 Secure Element 中，該身分證會綁定到州發行部門為其建立身分證的同一裝置。

## 告知同意

「Apple 錢包」中的身分證會使用認證來識別使用 ISO/IEC 18013-5 標準中所定義通訊協定的讀卡機。出示證件期間，如果讀卡機有「Apple 錢包」信任的憑證，便會顯示一個圖像，向使用者保證，他們正在與指定的交易方互動。

## 無線電連結上的使用者資料機密性

階段作業加密有助於確保在「Apple 錢包」中的身分證和證件讀卡機之間交換的所有個人可識別資訊 (PII) 均已加密。加密由應用程式層執行。因此，階段作業加密的安全性不倚賴傳輸層 (例如 NFC、藍牙和 Wi-Fi) 提供的安全性。

## 「Apple 錢包」中的身分證可協助讓使用者的資訊保持私密

「Apple 錢包」中的身分證遵循 ISO/IEC 18013-5 中概述的「裝置擷取」程序。裝置擷取無需在出示期間進行伺服器呼叫，進而保護使用者不被 Apple 和發行部門追蹤。

## 證件驗證安全性

在 iOS 17 或以上版本中，美國企業和組織可以使用 iPhone 流暢安全讀取本人出示的 ISO 18013-5 相容行動版證件，不需使用外接硬體。「證件驗證」的使用方式有兩種，取決於驗證使用案例：

- **僅顯示證件驗證：**可在只要求視覺確認的使用案例中，透過 iOS 使用者介面顯示姓名、年齡、證件照片和年齡已滿 N 的資料。這項服務不允許收集可追蹤出示者身分的個人可識別資訊 (PII)。
- **ID Verifier Data Transfer：**可讓 App 請求出生日期和地址等其他資料元素，以符合法律驗證要求。ID Verifier Data Transfer 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要求。例如，App 必須出示法律要求才能請求身分資料。App 也必須提供隱私權政策，詳細說明所請求身分資料的處理、儲存或其他使用方式。

## 讀取行動版證件

「證件驗證」遵循 ISO/IEC 18013-5 標準定義的通訊協定。App 使用 ID Verifier API 請求來讀取行動版證件時，會顯示一個由 iOS 控制的表單，並提示行動版證件持有人拿著裝置靠近證件感應器。此時會使用 NFC 功能 (如 ISO/IEC 18013-5 標準所定義，QR 碼可用來啟動藍牙切換程序而非 NFC)，在兩部裝置之間建立安全藍牙低功耗 (BLE) 連線。此時行動版證件持有人可以在裝置上查看對方請求的資訊。行動版證件持有人同意後，請求的身分資料就會傳輸到讀取裝置。使用 ID Verifier Data Transfer API 的 App 會收到回應資料並進行處理，而使用僅顯示證件驗證 API 的 App 會直接看到 iOS 顯示的資料。

ISO/IEC 18013-5 標準提供多種安全防護機制，可偵測、阻擋和緩解安全風險。「證件驗證」會同時執行核發者簽名和裝置簽名驗證。此外，「證件驗證」支援使用 ISO/IEC 18013-5 標準中所定義的通訊協定，對讀卡機進行認證。App 可以選擇顯示圖像和名稱，在證件持有人與使用讀卡機憑證的目標對象互動時，為證件持有人提供保證。

## 核發者和裝置驗證

為防止偽造，「證件驗證」會驗證受信任行動版證件核發者的「行動安全物件」簽名。ID Verifier Data Transfer 也會提供 API 來讓 App 自行執行簽名驗證 (如果想要的話)，而非由 iOS 執行。為了向企業或組織保證行動版證件並非從另一部裝置複製而來，「證件驗證」會透過作業階段資料驗證簽名。

## 讀卡機認證

出示證件時，與 Apple 根憑證授權管理中心 (CA) 鏈結的讀卡機認證憑證相關聯的專用密鑰，會簽署「證件驗證」讀卡機請求，其中包含相關 x509 自訂延伸模組，可向持有人指出企業是否意圖儲存資料。如果應用程式想向證件持有人顯示名稱和圖像，App 管理者必須使用 Apple Business Register 註冊，並提供正確的品牌資訊。提交的資訊成功通過驗證後，進行交易時，讀卡機認證憑證就會透過讀卡機認證憑證向證件持有人提供來自 Apple Register 與該實體相關的資訊。

# iMessage

## iMessage 安全性概覽

Apple 的 iMessage 是一項適用於 iPhone 和 iPad 裝置、Apple Watch 和 Mac 電腦的傳訊服務。iMessage 支援文字以及照片、聯絡人、位置、連結等附件，以及直接包含在訊息中的附件，例如比讚圖像。訊息會顯示在使用者所有註冊的裝置上，這樣使用者就可以在其他裝置上繼續對話。iMessage 充分運用 Apple 推播通知服務 (APNs)。Apple 不會記錄訊息內容或附件，且其受端對端的加密服務保護，因此只有傳送者和接收者可以存取。Apple 無法解密這些資料。

當使用者在裝置上開啟 iMessage 時，裝置會產生加密和簽署密鑰對以供服務使用。針對加密，提供加密 RSA 1280 位元密鑰，以及 NIST P-256 曲線上的加密 EC 256 位元密鑰。針對簽章，則使用橢圓曲線數位簽章算法 (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。公用密鑰會與裝置的 APNs 位址一起傳送至 Apple 識別服務 (IDS)，而公用密鑰會與使用者的電話號碼或電子郵件地址綁定。

當使用者啟用其他裝置來使用 iMessage 時，他們的加密方式和用來簽署的公用密鑰、APNs 位址及所綁定的電話號碼都會加入到目錄服務中。使用者還可以加入更多電子郵件地址，系統會藉由傳送確認連結來驗證這些電子郵件地址。電話號碼則透過電信業者網路和 SIM 卡進行驗證。部分網路需使用 SMS 進行驗證 (如果 SMS 不是零費率，則會向使用者顯示確認對話框)。除了 iMessage 之外，還有多个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、電話號碼或電子郵件地址加入時，使用者所有已註冊的裝置都會顯示一則提示訊息。

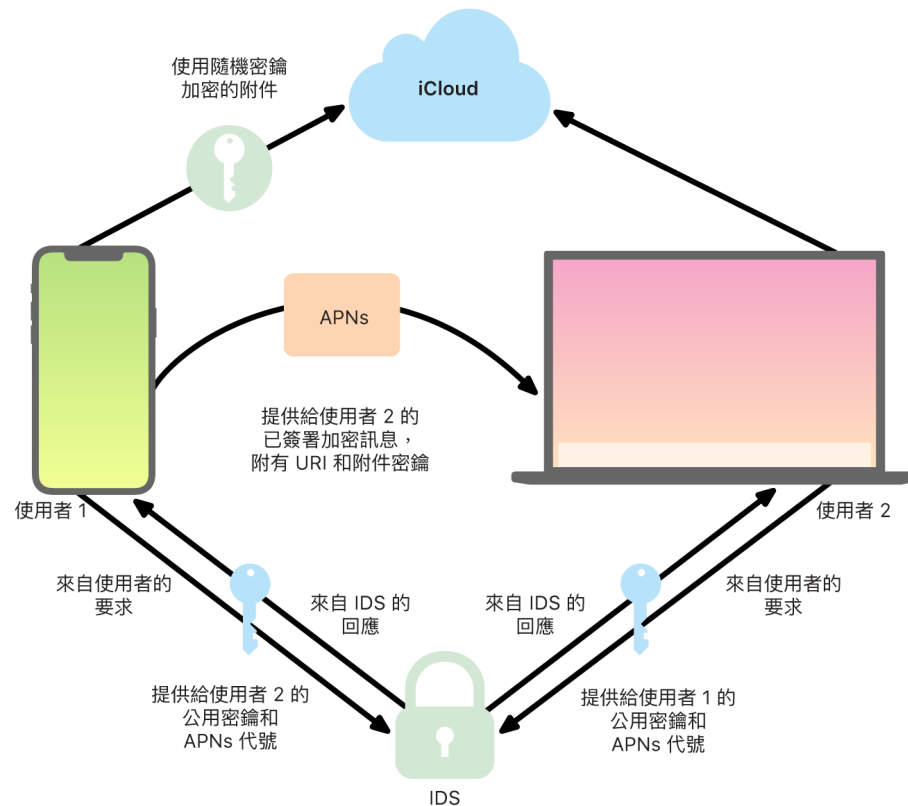
## iMessage 如何安全地傳送和接收訊息

使用者藉由輸入位址或姓名來開始 iMessage 對話。如果他們輸入電話號碼或電子郵件地址，裝置就會聯絡「Apple 識別服務」(IDS) 以擷取與該位址綁定的所有裝置的公用密鑰和 APNs 位址。如果使用者輸入的是名字，裝置會先使用使用者的「聯絡人」App 來收集與該名字綁定的電話號碼和電子郵件地址，然後再從 IDS 取得公用密鑰和 APNs 位址。

使用者的外送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和簽署密鑰會從 IDS 擷取。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 位元值的鏈結會產生 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著會以 SHA-1 進行雜湊運算，而雜湊值會使用發送裝置的專用簽署密鑰以橢圓曲線數位簽章算法 (ECDSA) 進行簽署。在 iOS 13 或以上版本和 iPadOS 13.1 或以上版本中，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數位簽章所組成。這些訊息隨即會分送至 APNs 進行遞送。時間戳記和 APNs 路由資訊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 最多只可以中繼大小為 4 或 16 KB 的訊息。若訊息文字過長或隨附了附件（如照片），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傳至 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，並透過正規的 iMessage 加密保有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 擷取附件。若傳送者的來電號碼或電子郵件地址與接收者的聯絡人相符，則會顯示一個名字。

與所有推播通知一樣，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，若裝置離線，iMessage 訊息會排入佇列等待發送。訊息最多可在 Apple 伺服器上儲存 30 天。

## 安全的 iMessage 名稱與照片分享

iMessage 的「名稱與照片分享」讓使用者可使用 iMessage 來分享名稱和照片。使用者可選取其「我的名片」資訊，或自訂名稱並加入其選擇的任何影像。iMessage 的「名稱與照片分享」使用雙階段系統來分送名稱和照片。

資料會再細分到欄位中，並分別進行加密和認證，也會透過以下程序一起認證。共有三個欄位：

- 名稱
- 照片
- 照片檔名



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。接著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。接著使用密鑰 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 MAC 會連同加密的資料一起儲存。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，且每次使用者選擇更改其名稱和照片時，都會產生新的加密記錄。當使用者 1 選擇與使用者 2 分享其名稱和照片時，會傳送密鑰以及 iMessage 承載資料中的 RecordID (已加密)。

當使用者 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「暱稱和照片」RecordID 及密鑰。接下來使用者 2 的裝置會前往公共 CloudKit 資料庫，擷取該記錄 ID 的加密名稱和照片，然後透過 iMessage 傳出。

訊息擷取完畢後，使用者 2 的裝置會解密承載資料並使用 RecordID 本身驗證簽章。如果通過驗證，便會向使用者 2 顯示名稱和照片，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 安全性

Apple Messages for Business 是讓使用者可使用「訊息」App 來與商家通訊的傳訊服務。有了 Apple Messages for Business，使用者的對話隨時都在控制之中。他們也能夠刪除對話，並阻止商家之後向他們傳送訊息。有鑑於隱私性，商家不會收到使用者的電話號碼、電子郵件地址或 iCloud 帳號資訊。相反地，而是 Apple 識別服務 (IDS) 會產生一個名為 **Opaque ID** 的自訂唯一識別碼，並與商家共享。Opaque ID 對於使用者的 Apple ID 與商家的 Business ID 之間的關係是唯一的。對於使用 Apple Messages for Business 聯絡的每個商家，使用者會有不同的 Opaque ID。使用者決定是否以及何時與商家分享個人識別資訊，Apple Messages for Business 服務從不儲存對話歷史記錄。

Apple Messages for Business 支援來自「Apple 商務管理」的管理式 Apple ID，並會決定是否在「Apple 校務管理」中為 iMessage 和 FaceTime 加以啟用。

傳給商家的訊息會在使用者裝置和 Apple 的傳訊伺服器之間加密，並使用像 iMessages 一樣的安全性和 Apple 傳訊伺服器。Apple 傳訊伺服器會解密 RAM 中的這些訊息，然後使用 TLS 1.2 透過加密的連結將它們中繼給企業。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。商家的回覆也使用 TLS 1.2 傳送到 Apple 傳訊伺服器，在其中會使用每個收件人裝置的唯一公共密鑰來加密。

如果使用者裝置在線上，則訊息將立即傳送，並且不會在 Apple 傳訊伺服器上快取。如果使用者的裝置不在線上，則加密的訊息會最多快取 30 天，以便使用者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 天後，未傳遞的快取訊息將會過期並被永久刪除。

## FaceTime 安全性

FaceTime 是 Apple 的視訊和語音通話服務。與 iMessage 相似，FaceTime 通話使用「Apple 推播通知服務」(APNs) 服務來與使用者已註冊的裝置建立初始連線。FaceTime 通話的語音/視訊內容受到端對端的加密保護，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，這個基礎架構負責中繼使用者已註冊的裝置之間的資料封包。藉由透過中繼連線使用 APNs 通知與「用於 NAT 的作業階段周遊公用程式」STUN 訊息，裝置會驗證其識別憑證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 加以認證。在初始連線和安全性設定後，FaceTime 便會使用 STUN 與「網際網路連接建立」(ICE) 來建立裝置間的點對點連線 (若適用)。

「群組 FaceTime」延伸 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端對端加密。雖然「群組 FaceTime」重複使用許多一對一 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安全性，這表示即便使用者的裝置遭入侵，也不會洩漏過去通話的內容。作業階段密鑰是使用 AES-SIV 來封裝，並使用橢圓曲線整合加密機制 (ECIES) 架構搭配臨時 P-256 ECDH 密鑰來在成員間分送。

當有新電話號碼或電子郵件地址加入進行中的「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」功能的安全性

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」結合到一個 App 中 (iOS、iPadOS 和 macOS)。「尋找」可協助使用者定位遺失的裝置 (即使是處於離線的 Mac)。在線上的裝置可以直接透過 iCloud 向使用者報告其位置。「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。然後，這些附近的裝置會將偵測到之遺失裝置的位置中繼傳送到 iCloud，以便使用者在「尋找」App 中找到它，同時保護所有相關使用者的隱私權和安全性。「尋找」甚至適用於處於離線和睡眠狀態的 Mac。

藉由使用藍牙和世界各地不計其數處於活躍使用狀態的 iOS、iPadOS 和 macOS 裝置，使用者可以定位他們遺失的裝置，即使沒有連接 Wi-Fi 或行動網路也可找到。在「尋找」中啟用「離線尋找」的任何 iOS、iPadOS 或 macOS 裝置，都能作為「尋找者裝置」使用。這表示裝置可以使用藍牙偵測其他遺失的離線裝置，然後使用其網路連線來向裝置擁有者回報約略位置。當裝置啟用離線尋找功能，就代表該裝置的位置也可被其他參與者以相同方式定位。整個互動是端對端加密、匿名，且設計要提高電池和資料效率。對電池壽命和行動數據方案使用的影響最小，並且使用者隱私得到更好的保護。

**【注意】**「尋找」可能未在所有國家或地區提供。

#### 端對端加密

「尋找」的建置基礎為先進的公用密鑰加密編譯技術。當「尋找」設定中的離線尋找啟用時，會直接在裝置上產生用橢圓曲線 (EC) P-224 專用加密密鑰組，其標註為  $\{d, P\}$  ( $d$  表示專用密鑰， $P$  則為公用密鑰)。此外，256 位元密碼  $SK_0$  和計數器  $i$  會初始化為零。這組專用密鑰和該密碼絕不會傳送給 Apple，且會使用「iCloud 鑰匙圈」，只在使用者的其他裝置間以端對端加密方式同步。密碼和計數器用於透過下列遞迴建構來衍生目前的對稱密鑰  $SK_i: SK_i = \text{KDF}(SK_{i-1}, \text{"update"})$ 。

根據密鑰  $SK_i$ ，兩個大整數  $u_i$  和  $v_i$  會透過  $(u_i, v_i) = \text{KDF}(SK_i, \text{"diversify"})$  來計算。接下來會使用與兩個整數相關的離線關聯，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分為  $P_i$  且驗證  $P_i = u_i * P + v_i * G$ 。

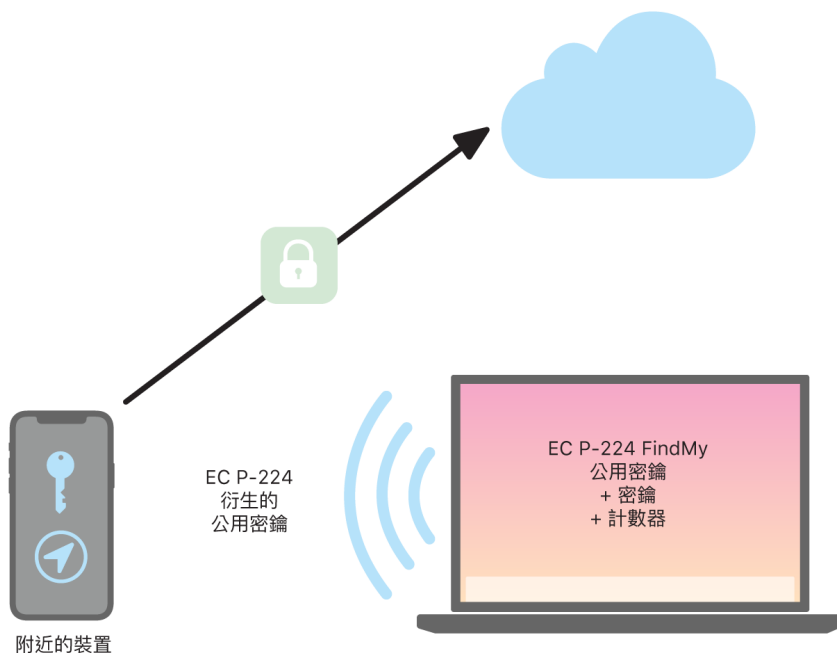
當裝置遺失且無法連接 Wi-Fi 或行動網路時 (例如將 MacBook Pro 遺落在公園長椅上時)，裝置會於有限期間內，在藍牙承載資料中開始定期廣播衍生的公用密鑰  $P_i$ 。藉由使用 P-224 公用密鑰的表示資料可以容納在單一的藍牙承載單位中。這樣周圍的裝置便能將離線裝置的位置加密到公用密鑰來協助尋找該裝置。大約每隔 15 分鐘，系統就會使用計數器的增量值和上述的程序來以新的公用密鑰取代原有的，因此無法透過持久性識別碼來追蹤使用者。衍生機制的設計用意在於防止多個公用密鑰  $P_i$  連結至相同裝置。

## 讓使用者和裝置保持匿名狀態

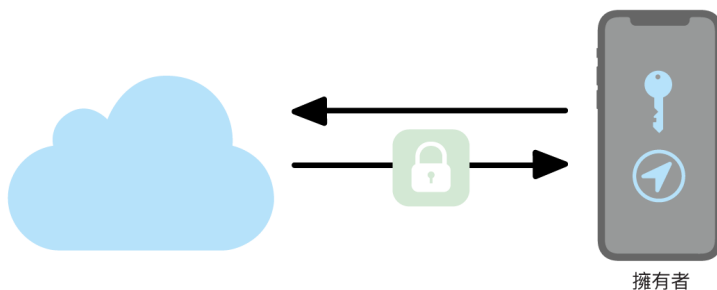
除了確保完全加密位置資訊和其他資料，參與者的身分也會對彼此和 Apple 保密。在尋找者裝置傳送至 Apple 的資料中，內容或標頭均不含任何認證資訊，因此 Apple 無從得知尋找者是誰，也不知道誰的裝置被找到。此外，Apple 不會記錄可能揭露尋找者身分的資訊，也不會保留可能讓任何人建立尋找者和擁有者之間關聯的資訊。裝置擁有者只會收到加密位置資訊 (在「尋找」App 中解密並顯示)，不會顯示誰找到了裝置。

## 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訊並轉送至 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 雜湊計算所得出。Apple 絕對不會擁有解密密鑰，因此 Apple 無法讀取尋找者加密的位置。遺失裝置的擁有者可重新建構索引和解密加密的位置。



嘗試定位遺失的裝置時，系統會為位置搜尋期間估算預期的計數值範圍。知道搜尋期間計數值範圍中的原始專用 P-224 密鑰  $d$  和密碼值  $SK_i$ ，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裝置之擁有者，便可使用索引值組  $\text{SHA256}(P_i)$  和從伺服器下載加密位置。再來「尋找」App 會使用相符的專用密鑰  $d_i$  來在本機解密加密位置，並在 App 中顯示遺失裝置的約略位置。擁有者的 App 會將從多部尋找者裝置回報的位置結合在一起，以產生更精準的位置。



## 定位已離線的裝置

如果使用者已在裝置上啟用「尋找我的 iPhone」，當裝置升級至 iOS 13 或以上版本、iPadOS 13.1 或以上版本和 macOS 10.15 或以上版本時，會預設啟用離線尋找功能。這樣的設計可確保所有使用者都能獲得找回遺失裝置的最高可能性。但是，如果使用者不想參與，可以隨時在裝置上的「尋找」設定中停用離線尋找。當離線尋找停用時，裝置就不能再擔任尋找者，也無法被其他尋找者裝置偵測到。但是只要裝置有連接 Wi-Fi 或行動網路，使用者仍可定位裝置。

成功定位遺失的離線裝置時，使用者會收到通知和電子郵件訊息，通知他們裝置已找到。若要檢視遺失裝置的位置，使用者需打開「尋找」App 並選取「裝置」標籤頁。「尋找」會連同約略地址和在多久前偵測到裝置的資訊顯示地圖位置，而非如同成功定位裝置前在空白地圖上顯示裝置。如果收到更多回報的位置，目前的位置和時間戳記都會自動更新。雖然使用者無法在離線裝置上播放聲音或從遠端清除，他們可以使用位置資訊來回溯經過的路線，或是採取其他行動來協助找回裝置。

## 接續互通

### 「接續互通」安全性概覽

「接續互通」運用 iCloud、藍牙和 Wi-Fi 等技術，可讓使用者從一部裝置到另一部裝置繼續作業、撥打和接聽電話、傳送和接收簡訊，以及共享行動數據網際網路連線。

### 「接力」安全性

Apple 安全地處理原生 App 和網站之間的接力，無論是從一台裝置到另一台裝置，甚至是大量資料的接力。

### 「接力」如何安全運作

當使用者的 iOS、iPadOS 和 macOS 裝置彼此接近時，使用者可以使用「接力」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。使用者可以使用「接力」功能來切換裝置並立即繼續作業。

當使用者在第二部支援「接力」功能的裝置上登入 iCloud 時，兩部裝置會透過 APNs 來建立頻外低功耗藍牙 (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。在某些情況下，會使用 APNs 而非 BLE 來傳送這些訊息。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「接力」功能

「接力」功能允許 iOS、iPadOS 或 macOS 的原生 App 在由 App 開發者合法控制之網域中的網頁上繼續使用者的操作。「接力」也允許原生 App 的使用者活動在網頁瀏覽器中繼續進行。

為了協助阻止原生 App 要求繼續存取非受開發者控制的網站，App 必須證明擁有要繼續存取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。如需詳細資訊，請參閱：[App 對已儲存密碼的存取權限](#)。在允許 App 接受使用「接力」功能的使用者活動前，系統必須驗證 App 的網域名稱控制。

使用「接力」功能傳送的網頁來源可以是任何採用了「接力」API 的瀏覽器。當使用者檢視網頁時，系統會使用加密的「接力」廣播位元組來廣播網頁的網域名稱。只有使用者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「接力」，並將該原生 App 圖像顯示為「接力」選項。啟動後，原生 App 會接收完整的 URL 和網頁標題。瀏覽器中的其他資訊則不會傳送到原生 App。

相反地，若「接力」接收裝置未安裝相同的原生 App，原生 App 可能會指定後援 URL。在此情況下，系統會將使用者的預設瀏覽器顯示為「接力」App 選項（若該瀏覽器已採用「接力」API）。要求使用「接力」時，系統會啟動瀏覽器並使用來源 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「接力」傳送較龐大的資料

除了使用「接力」的基本功能外，部分 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 來支援接力功能，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「接力」傳送一樣。不過，在使用低功耗藍牙（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。此連線經過加密（使用 TLS），並透過「iCloud 鑰匙圈」共享的身分獲得信任。憑證中的識別標誌會針對每位使用者的身分進行驗證。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「接力」安全地跨裝置傳送使用者的剪貼板內容，因此他們可以在一部裝置上拷貝並在另一部裝置貼上。剪貼板內容會如其他「接力」資料一樣受到保護，除非 App 開發者選擇不允許分享，否則這些內容會依照預設與「通用剪貼板」分享。

無論使用者是否已將剪貼板內容貼至 App 中，App 皆可存取剪貼板資料。透過「通用剪貼板」，此資料存取會延伸至使用者其他裝置上的 App（必須以 iCloud 登入裝置來建立此存取權）。

## iPhone 行動網路通話轉接安全性

當使用者的 Mac、iPad 或 HomePod 若連上與其 iPhone 相同的 Wi-Fi 網路，即可透過 iPhone 行動網路連線來撥打和接聽電話。設定會要求裝置使用相同的 Apple ID 帳號同時登入 iCloud 和 FaceTime。

收到來電時，會使用「Apple 推播通知服務」（APNs）來通知所有已設定的裝置，每個通知都會使用與 iMessage 相同的端對端加密機制。位於相同網路上的裝置會顯示來電通知使用者介面。使用者接聽電話時，會使用安全的點對點連線技術，在兩部裝置間無縫傳輸使用者 iPhone 的音訊。

在一部裝置上接聽來電時，會使用低功耗藍牙（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「接力」傳播相同的方式進行加密。

撥出的通話也將使用 APNs 轉接到 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。使用者可以在 FaceTime 設定中關閉「iPhone 行動網路通話」來停用裝置的電話轉接功能。

## iPhone 訊息轉寄安全性

「訊息轉寄」會自動將 iPhone 上收到的 SMS 文字簡訊傳送到使用者已註冊的 iPad 或 Mac 上。每部裝置都必須使用相同的 Apple ID 帳號登入 iMessage 服務。當「訊息轉寄」開啟時，若啟用了雙重認證，系統會自動在使用者信任圈內的裝置上進行註冊作業。或者，可在每部裝置上輸入由 iPhone 產生的隨機六位數驗證碼來驗證註冊作業。

裝置完成連結後，iPhone 便會加密傳入的 SMS 簡訊並轉寄至每部裝置，此作業的操作方式如 [iMessage 安全性概覽](#) 所述。回覆會以相同方式傳回到 iPhone，然後 iPhone 可使用電信業者的 SMS 傳輸機制以簡訊來傳送回覆。「訊息轉寄」功能可在「訊息」設定中開啟或關閉。

## 「即時熱點」安全性

「即時熱點」會將其他 Apple 裝置連接到個人 iPhone 和 iPad 熱點。支援「即時熱點」的 iPhone 和 iPad 裝置使用低功耗藍牙 (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 帳號或「家人共享」所使用的帳號 (iOS 13 和 iPadOS) 進行登入。與「即時熱點」相容且系統為 OS X 10.10 或以上版本的 Mac 電腦，可使用相同的技術來搜尋支援「即時熱點」的 iPhone 和 iPad 裝置，並與其進行通訊。

當使用者一開始進入裝置上的 Wi-Fi 設定時，其會發出包含一個識別碼的 BLE 廣播，所有登入相同 iCloud 帳號的裝置均接受該識別碼。該識別碼由與 iCloud 帳號綁定的 DSID (Destination Signaling Identifier) 產生，且會定期更新。當其他登入相同 iCloud 帳號的裝置彼此接近且支援「個人熱點」時，這些裝置會偵測到訊號並加以回應，以表示其可使用「即時熱點」。

當非「家人共享」成員的使用者選擇 iPhone 或 iPad 用於「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。裝置接著會透過相同的 BLE 連結，使用相同訊息專屬加密方式來回應「個人熱點」的連線資訊。

使用者若有使用「家人共享」，系統會以某種機制安全地共享「個人熱點」連線資訊，此機制類似於 HomeKit 裝置用於同步資訊的機制。具體而言，在使用者之間共享熱點資訊的連線，受到 ECDH (Curve25519) 臨時密鑰的保護，這個臨時密鑰是透過使用者的個別裝置專用 Ed25519 公用密鑰進行認證。所使用的公用密鑰之前已在「家人共享」建立時，使用 IDS 於「家人共享」成員之間同步。

# 網路安全性

## 網路安全性概覽

除了 Apple 用於保護 Apple 裝置上所儲存資料的內建安全保護，也有許多措施可供企業組織採用並確保資訊在裝置間來回傳輸時安全無虞。所有保護機制和措施均屬於網路安全範疇。

由於使用者必須能從全球任何地方取用企業網路，協助確保使用者取得授權，並使其資料在傳輸過程中獲得妥善保護，是相當重要的。為了達成這些安全目標，iOS、iPadOS 和 macOS 將經過實證的技術和 Wi-Fi 及行動數據網路連線的最新標準整合在一起。正因如此，我們的作業系統使用（並使開發者得以運用）標準網路通訊協定來進行經認證、授權及加密的通訊。

## TLS 安全性

iOS、iPadOS 和 macOS 支援傳輸層安全性 (TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3) 和資料包傳輸層安全性 (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、「行事曆」和「郵件」等網際網路 App 會自動使用此通訊協定，在裝置和網路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 或以上版本及 macOS 10.13 或以上版本上，除非受到使用者信任，否則不再允許使用 SHA-1 憑證進行 TLS 連線，也不允許使用 RSA 密鑰短於 2048 位元的憑證。iOS 10 和 macOS 10.12 已淘汰 RC4 對稱加密套件。依照預設，以 SecureTransport API 建置的 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 傳輸安全性

「App 傳輸安全性」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 傳輸安全性」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) 與密碼區塊連結 (CBC) 模式中的 ECDHE\_ECDSA\_AES 和
- ECDHE\_RSA\_AES

App 可針對各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路連線作業將會失敗，除非 App 覆寫「App 傳輸安全性」。無效憑證隨時會造成嚴重的作業失敗和連線中斷。「App 傳輸安全性」會自動套用到針對 iOS 9 或以上版本及 macOS 10.11 或以上版本編譯的 App。

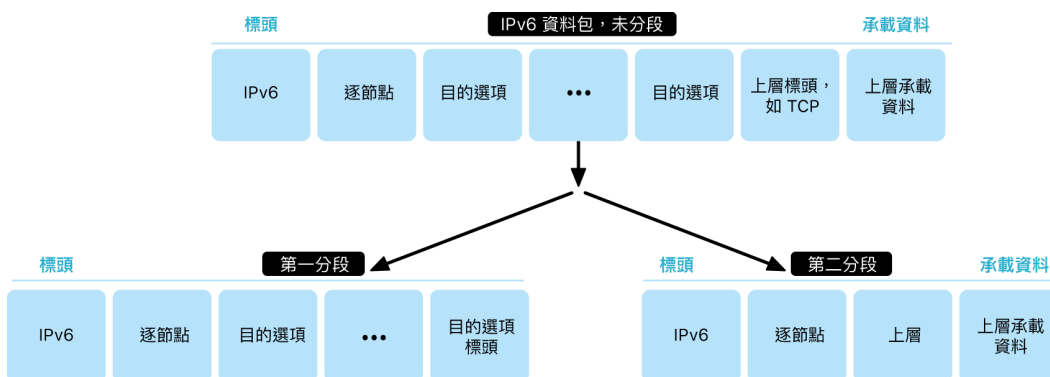
## 憑證有效性檢查

評估 TLS 憑證的受信任狀態的程序是依據行之多年的業界標準 (RFC 5280 中所立)，且結合 RFC 6962 (憑證透明度) 等新興標準。在 iOS 11 或以上版本及 macOS 10.13 或以上版本中，Apple 裝置會定期更新至最新的撤銷與受限的憑證列表。此列表是由憑證撤銷列表 (CRL) 彙集而成，而這些 CRL 為 Apple 信任每個內建憑證授權單位及其附屬 CA 核發者所公佈。此列表可能包含 Apple 所決定的其他限制。每當網路 API 函式用於安全連線時，都會查閱這些資訊。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 安全性

所有 Apple 作業系統皆支援 IPv6 並導入數種機制，以保護使用者的隱私與網路堆疊的穩定性。使用「無狀態位址自動設定」(SLAAC) 時，會產生所有介面的 IPv6 位址，其方式可協助防止跨網路裝置追蹤，同時藉由確保網路沒有變動時的位址穩定性來提供絕佳使用者體驗。位址產生演算法是根據 RFC 3972 的加密編譯產生位址，並藉由介面專屬的修飾元增強，以保證即使相同網路上有不同介面，最終將具有不同的位址。此外，所建立的臨時位址其偏好存留期為 24 小時，在預設情況下，這些臨時位址會用於任何新的連線。配合 iOS 14、iPadOS 14 和 watchOS 7 推出的專用 Wi-Fi 位址功能，系統會為裝置加入的每個 Wi-Fi 網路產生一個不重複的連結本機位址。網路的 SSID 會合併作為產生位址的額外元素，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 延伸標題和分段相關的攻擊，Apple 裝置導入了 RFC 6980、RFC 7112 和 RFC 8021 中指定的保護措施。這些措施尤其可阻止攻擊，在攻擊中僅可在第二個片段中可以找到上層標題 (如下所示)，其反過來可能導致對安全控制 (如無狀態封包過濾器) 產生模糊空間。



此外，為了協助確保 Apple 作業系統的 IPv6 堆疊的可靠性，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。

## 虛擬專用網路 (VPN) 安全性

虛擬專用網路 (VPN) 等安全網路服務，通常只需要基本的設定與配置，即可搭配 iPhone、iPad 和 Mac 裝置使用。

### 支援的通訊協定

這些裝置可搭配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、橢圓曲線數位簽章算法 (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 密碼進行使用者認證，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 進行使用者認證，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**：適用於使用憑證式認證的網路。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。行動裝置管理 (MDM) 解決方案可為每個受管理的 App 和 Safari 中特定的網域指定連線。這有助於確保具安全考量的資料始終以安全的方式透過企業網路進出，而使用者的個人資料並不會進出企業網路。

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 校務管理」、「Apple 商務管理」或「Apple 商務必備」加以監管的裝置。「總是開啟 VPN」可讓使用者在連接到行動數據與 Wi-Fi 網路時，不需要手動開啟 VPN 即可啟用保護功能。透過將所有 IP 流量回傳至組織，讓組織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。組織可以監控並過濾傳入其裝置或自其裝置傳出的流量、保護組織網路內的資料安全，並限制裝置的網際網路存取權。

## Wi-Fi 安全性

### 安全存取無線網路

所有 Apple 平台均支援業界標準 Wi-Fi 認證與加密通訊協定，以便在連接下列安全無線網路時提供經認證的存取權與保密性：

- WPA2 個人級
- WPA2 企業級
- WPA2/WPA3 Transitional
- WPA3 個人級
- WPA3 企業級
- WPA3 企業級 192 位元安全性

WPA2 和 WPA3 會認證每個連線，並提供 128 位元 AES 加密功能，可協助確保以無線方式傳送的資料保密無虞。這可為使用者提供最高等級的安全保障，在透過 Wi-Fi 網路連線傳送和接收通訊時，可確保使用者的資料始終受到保護。

### WPA3 支援

以下 Apple 裝置支援 WPA3：

- iPhone 7 或後續機型
- iPad 第五代或後續機型
- Apple TV 4K 或後續機型
- Apple Watch Series 3 或後續機型

- Mac 電腦 (2013 年末或後續機型, 採用 802.11ac 或以上版本)

較新型的裝置支援透過 WPA3 企業級 192 位元安全性進行認證, 包含支援連線至相容無線連接點 (AP) 時使用 256 位元 AES 加密。此加密為以無線方式傳送的流量提供強度更高的保密防護。所有 iPhone 11 或後續機型、iPad 第七代以後的所有 iPad 機型, 以及所有配備 Apple 晶片的 Mac 電腦, 都支援 WPA3 企業級 192 位元安全性。

## PMF 支援

除了保護以無線方式傳送的資料以外, Apple 平台也透過 802.11w 中定義的「受保護管理框架」(PMF) 服務, 將 WPA2 和 WPA3 等級的保護延伸至單點發送與多點發送管理框架。以下 Apple 裝置提供 PMF 支援:

- iPhone 6 或後續機型
- iPad Air 2 或後續機型
- Apple TV HD 或後續機型
- Apple Watch Series 3 或後續機型
- Mac 電腦 (2013 年末或後續機型, 採用 802.11ac 或以上版本)

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、EAPv0 和 PEAPv1。

## 平台保護

Apple 作業系統會保護裝置, 抵禦網路處理器韌體中的漏洞。這表示使用 Wi-Fi 的網路控制器已限制存取「應用程式處理器」記憶體。

- 使用 USB 或 SDIO (安全數位輸入輸出) 與網路處理器互動時, 網路處理器無法啟動直接記憶體存取 (DMA) 交易至「應用程式處理器」。
- 使用 PCIe 時, 每個網路處理器位於其獨立的 PCIe 匯流排上。各 PCIe 匯流排上的安全數位輸入輸出 (IOMMU) 會進一步限制網路處理器的 DMA 存取權限, 只允許存取含有其網路封包和控制結構的記憶體和資源。

## 過時通訊協定

Apple 產品支援以下過時的 Wi-Fi 認證與加密通訊協定:

- WEP Open, 搭配 40 位元和 104 位元密鑰
- WEP Shared, 搭配 40 位元和 104 位元密鑰
- Dynamic WEP
- 臨時密鑰完整性通訊協定 (TKIP)
- WPA
- WPA/WPA2 Transitional

這些通訊協定已被認定為不安全, 基於相容性、可靠性、效能與安全理由, 極度不建議使用。目前僅基於回溯相容性目的支援上述通訊協定, 未來的軟體版本中可能會予以移除。

建議所有 Wi-Fi 網路均移轉至 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 隱私權

### 隨機 MAC 位址

在沒有與 Wi-Fi 網路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」(MAC 位址)。系統會執行這些掃描以尋找和連接已知的 Wi-Fi 網路，或為使用地理柵欄的 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 網路時進行的 Wi-Fi 掃描未經過隨機化處理。iPhone 5 或後續機型支援 Wi-Fi 隨機 MAC 位址。

當裝置沒有與 Wi-Fi 網路產生關聯或裝置的處理器處於睡眠狀態時，Apple 平台在執行 ePNO (enhanced Preferred Network Offload) 掃描時，也會使用隨機 MAC 位址。當裝置上針對會利用地理柵欄的 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 網路的連線時其 MAC 位址會更改，即使裝置已連接行動網路，Wi-Fi 流量的被動觀察程式亦無法使用該位址持續追蹤裝置。Apple 已告知 Wi-Fi 製造商，iOS 和 iPadOS Wi-Fi 掃描會使用隨機 MAC 位址，且 Apple 及製造商皆無法預測這些隨機 MAC 位址。

在 iOS 14 或以上版本、iPadOS 14 或以上版本，以及 watchOS 7 或以上版本中，當 iPhone、iPad 或 Apple Watch 連接至 Wi-Fi 網路時，會依據個別網路以唯一 (隨機) MAC 位址自我識別。此功能可由使用者停用，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 位址。

如需更多資訊，請參閱 Apple 支援文章：[在 iPhone、iPad 和 Apple Watch 上使用專用 Wi-Fi 位址](#)。

### 隨機 Wi-Fi 框架序號

Wi-Fi 框架包含一個序號，用於低等 802.11 通訊協定以啟用有效且可靠的 Wi-Fi 通訊。由於這些序號會隨著每次傳輸框架遞增，因此可在進行 Wi-Fi 掃描期間，用來尋找已傳輸訊息與相同裝置所傳輸框架的關聯。

為防範這種情況，每當 MAC 位址更改為新的隨機位址時，Apple 裝置都會使用隨機序號。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序號功能：

- iPhone 7 或後續機型
- iPad 第五代或後續機型
- Apple TV 4K 或後續機型
- Apple Watch Series 3 或後續機型
- iMac Pro (2017 年; Retina 5K; 27 吋) 或後續機型
- MacBook Pro (2018 年; 13 吋) 或後續機型
- MacBook Pro (2018 年; 15 吋) 或後續機型
- MacBook Air (2018 年; Retina; 13 吋) 或後續機型
- Mac mini (2018 年) 或後續機型
- iMac (2019 年; Retina 4K; 21.5 吋) 或後續機型
- iMac (2019 年; Retina 5K; 27 吋) 或後續機型
- Mac Pro (2019 年) 或後續機型

### 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 位址。隨機產生的位址也會用於 iOS 和 iPadOS (裝有 SIM 卡) 中的「個人熱點」和 macOS 中的「網際網路共享」。

每當這些網路介面啟動時，都會產生新的隨機位址，且會視需要為每個介面產生獨立的唯一位址。

## 隱藏的網路

Wi-Fi 網路的識別方式為透過名為**服務組織別元 (SSID)**的網路名稱。某些 Wi-Fi 網路設定為隱藏 SSID，這會導致無線連接點不會廣播網路的名稱。這些網路便稱為**隱藏的網路**。iPhone 6s 和後續機型的裝置會自動偵測隱藏的網路。如果網路已隱藏，iOS 或 iPadOS 裝置就會傳送含有 SSID 的探查要求；若未隱藏則不會傳送。這可協助防止裝置廣播使用者先前曾連接但已隱藏的網路，進一步確保隱私。

## 藍牙安全性

Apple 裝置具備兩種藍牙類型：傳統藍牙和低功耗藍牙 (BLE)。兩種版本的藍牙安全性模式都包含以下不同的安全功能：

- **配對**：建立一或多個共用秘密密鑰的程序
- **綁定**：儲存配對期間所建立密鑰的作業，此密鑰用於後續的連線以成立受信任裝置配對
- **認證**：驗證兩部裝置具有相同密鑰
- **加密**：訊息保密性
- **訊息完整性**：防止訊息偽造
- **安全簡易配對**：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	低功耗藍牙
配對	P-256 橢圓曲線	FIPS 核准的演算法 (AES-CMAC 和 P-256 橢圓曲線)
綁定	配對資訊儲存在 iOS、iPadOS、macOS、tvOS 和 watchOS 裝置中的安全位置	配對資訊儲存在 iOS、iPadOS、macOS、tvOS 和 watchOS 裝置中的安全位置
認證	FIPS 核准的演算法 (HMAC-SHA256 和 AES-CTR)	FIPS 核准的演算法
加密	AES-CCM 加密編譯，在控制器中執行	AES-CCM 加密編譯，在控制器中執行
訊息完整性	AES-CCM 用於確保訊息完整性	AES-CCM 用於確保訊息完整性
安全簡易配對：防止被動竊聽	橢圓曲線 Diffie-Hellman Exchange Ephemeral (ECDHE)	橢圓曲線 Diffie-Hellman 交換 (ECDHE)
安全簡易配對：防禦中間人 (MITM) 攻擊	兩種使用者協助的數值方式：數值比較或通行密鑰輸入	兩種使用者協助的數值方式：數值比較或通行密鑰輸入 進行配對需要使用者回應，包含所有非 MITM 配對模式在內
藍牙 4.1 或以上版本	iMac 2015 年底或後續機型 MacBook Pro 2015 年初或後續機型	iOS 9 或以上版本 iPadOS 13.1 或以上版本 macOS 10.12 或以上版本 tvOS 9 或以上版本 watchOS 2.0 或以上版本

支援	傳統藍牙	低功耗藍牙
藍牙 4.2 或以上版本	iPhone 6 或後續機型	iOS 9 或以上版本 iPadOS 13.1 或以上版本 macOS 10.12 或以上版本 tvOS 9 或以上版本 watchOS 2.0 或以上版本

## 低功耗藍牙隱私權

為了協助保護使用者的隱私，BLE 包含下列兩項功能：隨機位址和跨傳輸密鑰衍生。

**隨機位址**功能可藉由經常更改藍牙裝置位址，來減少在一段時間內追蹤 BLE 裝置的可行性。為了讓裝置使用隱私功能來重新連接已知裝置，裝置位址（稱為**專用位址**）必須能由其他裝置解析。需使用配對程序中交換的裝置的身分解析密鑰來產生專用位址。

iOS 13 或以上版本和 iPadOS 13.1 或以上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，透過 BLE 產生的連結密鑰可用來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 的超寬頻安全性

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 或更新的 iPhone 機型可精準定位其他配備 U1 的 Apple 裝置。「超寬頻」技術使用隨機資料機制，此機制與其他支援的 Apple 裝置所採用的相同：

- 隨機 MAC 位址
- 隨機 Wi-Fi 框架序號

## 單一登入安全性

### 單一登入

iOS 和 iPadOS 支援透過單一登入 (SSO) 對企業網路進行認證。SSO 搭配 Kerberos 型網路使用，針對使用者獲授權存取的服務對使用者進行認證。SSO 可用於各種網路活動，從安全的 Safari 區段到第三方的 App。同時還支援憑證式認證（例如 PKINIT）。

macOS 支援使用 Kerberos 對企業網路進行認證。App 可使用 Kerberos 來針對使用者獲授權存取的服務對使用者進行認證。Kerberos 也可用於各種網路活動，例如安全 Safari 作業階段、網路檔案系統驗證及第三方 App。支援憑證式認證，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 網路連線 API 的第三方 App 也可進行設定來使用。為了設定 SSO，iOS 和 iPadOS 支援設定描述檔的承載資料，允許行動裝置管理 (MDM) 解決方案向下推播必要的設定。其中包括：設定使用者主要名稱 (即 Active Directory 使用者帳號) 和 Kerberos 領域設定，以及設定應允許哪些 App 和 Safari Web URL 使用 SSO。

## 可延伸的單一登入功能

App 開發者可使用 SSO 延伸功能提供自己的單一登入實作。當原生或 Web App 需要使用某些身分提供者以進行使用者認證時，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，以及使用挑戰/回應機制 (例如 Kerberos) 的延伸功能。這讓可延伸的單一登入功能可支援 OpenID、OAuth、SAML2 和 Kerberos 認證架構。SSO 延伸功能也藉由採用原生 SSO 通訊協定 (可在 macOS 登入期間擷取 SSO 代號) 來支援 macOS 認證。

若要使用單一登入延伸功能，App 可以使用認證服務 API，也可依賴作業系統提供的 URL 攔截機制。WebKit 和 CFNetwork 提供攔截層，以便為任何原生或 WebKit App 提供順暢的單一登入支援。為了叫用單一登入延伸功能，必須透過行動裝置管理 (MDM) 描述檔安裝管理者提供的設定。除此之外，重新導向類型的延伸功能必須使用「相關聯的網域」承載資料，證明其支援的身分伺服器知悉其存在。

隨作業系統提供的唯一延伸功能為 Kerberos SSO 延伸功能。

## AirDrop 安全性

支援 AirDrop 的 Apple 裝置使用低功耗藍牙 (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訊，包括具有 AirDrop 功能且系統為 iOS 7 或以上版本的 iOS 裝置和 iPad 裝置，以及系統為 OS X 10.11 或以上版本的 Mac 電腦。Wi-Fi 無線電用來在裝置之間進行直接通訊，無需使用任何網際網路連線或無線連接點 (AP)。此連線經過 TLS 加密。

在預設情況下，AirDrop 的共享設定為「只限聯絡人」。使用者也可以選擇使用 AirDrop 與所有人進行共享，或者完全關閉此功能。組織或部門可針對行動裝置管理 (MDM) 解決方案所控管的裝置和 App，限制其 AirDrop 的使用權。

## AirDrop 作業

AirDrop 使用 iCloud 服務來協助使用者進行認證。當使用者登入 iCloud 時，2048 位元 RSA 身分會儲存在裝置上，而當使用者開啟 AirDrop 時，系統會根據與使用者 Apple ID 綁定的電子郵件地址和電話號碼來製作簡短 AirDrop 識別身分雜湊值。

當使用者選擇使用 AirDrop 共享項目時，發送裝置會透過 BLE 發出 AirDrop 訊號，其中包含使用者的簡短 AirDrop 識別身分雜湊值。附近處於喚醒狀態並開啟 AirDrop 的其他 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分。

在「只限聯絡人」模式下，接收裝置會將收到的簡短 AirDrop 識別身分雜湊值與裝置上「聯絡人」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 來以裝置的識別身分資訊予以回應。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「聯絡人」App 中找到比對成功的項目，接收裝置也會回應。

接著發送裝置會使用點對點 Wi-Fi 來起始 AirDrop 連線，並使用此連線傳送完整的識別身分雜湊值給接收裝置。如果完整識別身分雜湊值與接收者「聯絡人」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分雜湊值予以回應。

如果雜湊值經過驗證，接收者的名字和照片（如果「聯絡人」中有的話）便會顯示在傳送者的 AirDrop 共享表單中。在 iOS 和 iPadOS 中，會顯示在「聯絡人」或「裝置」區域中。未通過驗證或認證的裝置會顯示在傳送者的 AirDrop 分享表單上，並帶有一個輪廓圖像和裝置名稱，該名稱可在「設定」>「一般」>「關於本機」>「名稱」中設定。在 iOS 和 iPadOS 中，這些項目位於 AirDrop 分享表單的「其他人」區域中。

接著傳送方使用者可選擇要分享的對象。使用者選擇後，發送裝置會與接收裝置建立一個加密 (TLS) 連線，此連線會交換彼此的 iCloud 識別身分憑證。憑證中的識別身分會針對每位使用者的「聯絡人」App 進行驗證。

如果憑證通過驗證，系統就會要求接收方使用者接受來自經識別的使用者或裝置所傳送的内容。如果選擇了多位接收者，則會針對每個目標重複此程序。

## iPhone 和 iPad 的 Wi-Fi 密碼共享安全性

支援 Wi-Fi 密碼共享的 iPhone 和 iPad 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。

當使用者選擇了 Wi-Fi 網路（要求者），且系統提示要求輸入 Wi-Fi 密碼時，Apple 裝置會啟動低功耗藍牙 (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 網路的密碼之其他 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）需要要求者的「聯絡人」資訊，且要求者必須使用類似 AirDrop 的機制證明其身分。證明身分後，提供者會傳送密碼給要求者，此密碼可用來加入網路。

組織可針對透過行動裝置管理 (MDM) 解決方案控管的裝置和 App，限制對 Wi-Fi 密碼共享功能的使用權限。

## macOS 的防火牆安全性

macOS 包含內建防火牆，可防止 Mac 遭網路存取並防禦拒絕服務攻擊。若要進行此設定，可前往「系統設定」>「隱私權與安全性」（macOS 13 或以上版本）、「系統偏好設定」的「安全性與隱私權」面板（macOS 12 或較早版本），或是使用手動安裝或 MDM 解決方案提供的設定描述檔（含有防火牆承載資料）。支援下列設定：

- 封鎖任何 App 的所有傳入連線。
- 自動允許內建的軟體接收傳入連線。
- 自動允許已下載和已簽署的軟體接收傳入連線。
- 根據使用者指定的 App 加入或拒絕連線。
- 阻止 Mac 回應 ICMP（網際網路控制訊息通訊協定）探查和連接埠掃描要求。

# 開發者套件安全性

## 開發者套件安全性概覽

Apple 提供多種「套件」架構以支援第三方開發者延伸 Apple 服務。以下架構的核心為保護使用者隱私與安全性：

- HomeKit
- CloudKit
- SiriKit
- WidgetKit
- DriverKit
- ReplayKit
- ARKit

## HomeKit 安全性

### HomeKit 通訊安全性

HomeKit 提供家庭自動化的基礎架構，利用 iCloud 與裝置安全功能來保護與同步隱私資料，無須透露給 Apple。

HomeKit 身分與安全性是以 Ed25519 公用密鑰與專用密鑰的組合為基礎。Ed25519 密鑰配對是在使用者的裝置上產生，會成為其 HomeKit 身分。密鑰配對會成為 HomeKit 配件通訊協定 (HAP) 的一部分，用於驗證使用者的 Apple 裝置和 HomeKit 配件之間的直接通訊。

如果共享家庭有設定家庭中樞，其成員可以透過這個家庭中樞傳送指令到配件。系統會使用 Apple 識別服務 (IDS)，對這些命令執行端對端加密和驗證，並從使用者裝置傳送到家庭中樞，然後使用 HomeKit 配件通訊協定 (HAP) 或 Matter (智慧家庭連線標準) 轉送至相關配件上。

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」的裝置間保持最新狀態。

### HomeKit 配件之間的通訊

HomeKit 配件會產生自己的 Ed25519 密鑰組，用於與 Apple 裝置通訊。若將配件回復成原廠設定，便會產生新的密鑰組。

為了在 Apple 裝置與 HomeKit 配件之間建立關係，系統會使用「安全遠端密碼」(3072 位元) 通訊協定來交換密鑰，並在使用者裝置上輸入配件製造商提供的八位數代碼，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 或以上版本上建立軟體認證的支援。



當裝置與 HomeKit 配件在使用期間進行通訊時，各自會使用上述過程中交換的密鑰來認證對方。每個區段都會使用端到端的通訊協定來建立，並使用以各個區段 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，配件會由配對的裝置透過安全的作業階段以廣播加密密鑰佈建。此密鑰會用於加密有關配件狀態變更的資料，這些資料是使用 BLE 廣播傳送通知。廣播加密密鑰是一種 HKDF-SHA512 衍生密鑰，資料會透過 ChaCha20-Poly1305 AEAD 演算法進行加密。廣播加密密鑰會定期變更並使用 iCloud 更新至其他裝置，如 [HomeKit 資料安全性](#) 所說明。

## 與 Matter 配件通訊

Matter 配件的身分與安全性是以憑證為基礎。針對 Apple 家庭，信任根憑證授權管理中心 (CA) 是在初始使用者裝置 (即「擁有者」) 上產生，而 CA 的專用密鑰會儲存在其「iCloud 鑰匙圈」中。家庭中的每部 Apple 裝置都會使用 NIST P256 產生憑證簽署要求 (CSR)。擁有者的裝置會摘要這個 CSR，進而為使用其 CA 專用密鑰的裝置建立 Matter 識別身分憑證。此憑證之後會用於驗證使用者裝置和配件之間的通訊。

配件配對期間，Matter 配件會產生自己的 NIST P256 密鑰配對和 CSR，並收到來自 CA 的憑證。產生密鑰配對之前，Matter 配件和家庭擁有者的裝置會交換密鑰 (使用 SPAKE2+ 通訊協定搭配配件製造商提供的 PIN)，並執行裝置認證程序。接著系統會透過此通道交換 CSR 和憑證 (使用 AES-CCM 與 HKDF-SHA256 衍生密鑰進行加密)。如果配件回復成出廠設定，系統會產生新的密鑰配對和 CSR，並在配對期間為配對核發新憑證。

當 Apple 裝置和 Matter 配件在使用期間進行通訊時，各自會使用自己的憑證來認證對方。每個工作階段都會使用三階段 (sigma) 通訊協定來建立，並使用以各個工作階段 P256 密鑰為基礎的 HKDF-SHA256 衍生密鑰來進行加密。

如需更多關於 Apple 裝置如何與 Matter 配件安全互動的資訊，請參閱 Apple Developer 網站上的 [iOS 16 的 Matter 支援](#)。

## HomeKit 和 Siri

Siri 可用來查詢和控制配件，並可啟動情境。匿名提供給 Siri 的家庭配置資訊會盡量最小化，以提供房間名稱、配件和指令辨識所需的情境。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

使用者可以使用「家庭」App 在支援 Siri 的配件上啟用 Siri 等新功能，以及計時器、鬧鐘、對講機和門鈴等其他 HomePod 功能。啟用這些功能後，配件會與本機網路上託管這些 Apple 功能的已配對 HomePod 進行協調。音訊是使用 HomeKit 和 AirPlay 通訊協定透過加密通道在裝置間交換。

開啟「聆聽嘿 Siri」後，配件會使用本機執行的觸發字詞偵測引擎來聽取「嘿 Siri」字詞。如果此引擎偵測到該字詞，它會使用 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，如果字詞似乎不包含觸發字詞，則可能會取消音訊分段。

開啟「觸碰使用 Siri」後，使用者可以按下配件上的專用按鈕來開始與 Siri 對話。音訊分段會直接傳送到配對的 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 本身的使用者呼叫，使用相同安全性、隱私和加密保護措施，來滿足使用者的意圖。如果 Siri 有音訊回覆，則 Siri 的回覆會透過 AirPlay 音訊通道傳送到配件。部分 Siri 要求需要使用者提供其他資訊 (例如，詢問使用者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方式傳輸到 HomePod。

配件需有一個視覺指示器，以便在其主動聆聽時向使用者發出訊號 (例如，LED 指示器)。除了取用音訊串流之外，配件並不清楚 Siri 要求的意圖，且配件上不會儲存任何使用者資料。

## HomeKit 資料安全性

家庭如果已升級至新 HomeKit 架構 (適用於 iOS 16.2 和 iPadOS 16.2)，系統會利用 iCloud 和「iCloud 鑰匙圈」在使用者 Apple 裝置之間安全同步 HomeKit 資料。在此同步過程中，會使用 iCloud 端對端加密機制將 HomeKit 資料加密，且 Apple 無法存取。

如果使用者是一開始在 HomeKit 中建立家庭的使用者 (即「擁有者」)，或是具有編輯權限的其他使用者，則可以新增使用者。擁有者的裝置會使用新使用者的公用密鑰來設定配件，以便讓配件可認證和接受來自新使用者的指令。當具有編輯權限的使用者新增使用者時，系統便會將此程序委派至家庭中樞以完成操作。

### 家庭資料與 App

使用者可在「隱私權」設定中控制 App 對家庭資料的存取權。當 App 要求提供家庭資料時，系統會要求使用者授予存取權，過程類似於要求提供「聯絡人」、「照片」和其他 iOS、iPadOS 和 macOS 資料來源。若使用者核准，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 開發者說明文件中所載明的其他詳細資訊，網址為：<https://developer.apple.com/homekit/>。

### 本機資料儲存

HomeKit 會在使用者的 Apple 裝置上儲存家庭、配件、情境和使用者的相關資料。系統會使用「資料保護」類別「首次使用者認證前的保護」，將此資料儲存在 Data Vault 內。HomeKit 資料不會備份到本機備份檔中。

## 用 HomeKit 保護路由器的安全

使用者可以使用支援 HomeKit 的路由器來提高家庭網路的安全性。透過這些路由器，使用者可以管理 HomeKit 配件對區域網路和網際網路的 Wi-Fi 存取權。路由器也支援專用 PSK (PPSK) 認證，因此可以使用配件特定的密鑰將配件加入 Wi-Fi 網路，並可視需要撤銷。PPSK 認證藉由不將主要的 Wi-Fi 密碼提供給配件，以及允許路由器安全地識別配件 (即使更改了其 MAC 位址)，也可以提高安全性。

使用者可以用「家庭」App 來設定配件群組的存取限制，如下所示：

- **無限制：**允許不受限制地存取網際網路和區域網路。
- **自動：**此為預設的設定。根據配件製造商提供給 Apple 的網際網路網站和本機連接埠列表，允許存取網際網路和區域網路。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「無限制」。)
- **限制家庭權限：**除了 HomeKit 用來從區域網路 (包含從家庭中樞到支援遠端遙控) 搜尋和控制配件所需的連線之外，無法存取其他網際網路或區域網路。

PPSK 是高強度、針對配件提供的 WPA2 個人級密語，由 HomeKit 自動產生，如果以後將配件從家庭中移除，則會撤銷。當透過 HomeKit 路由器所設定之家庭中的 HomeKit 將配件加到 Wi-Fi 網路時，就會使用 PPSK；這個加入的配件會反映為 Wi-Fi 憑證：HomeKit 受管理 (位於「家庭」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 網路的配件將重新設定為使用 PPSK，否則它們將保留其現有憑證。

作為一項額外的安全措施，使用者必須使用路由器製造商的 App 來設定 HomeKit 路由器，以便讓該 App 驗證使用者是否有權存取路由器，以及將其加到「家庭」App 中。

## HomeKit 攝影機安全性

HomeKit 中具有網際網路通訊協定位址 (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路上存取該串流的 iOS、iPadOS、tvOS 和 macOS 裝置。系統會使用在裝置和「網際網路通訊協定」攝影機 (或網路攝影機) 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。若裝置未連接區域網路, 則會經由家庭中樞將加密的串流傳遞至裝置。家庭中樞不會解密串流, 且只扮演裝置和網路攝影機之間的中繼站角色。App 向使用者顯示 HomeKit 網路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 無權從此串流擷取截圖。

### HomeKit 安全錄影

HomeKit 提供了端對端的安全和專用機制, 可記錄、分析和檢視 HomeKit 網路攝影機的剪輯片段, 而無需將該影片內容呈現給 Apple 或任何第三方。當網路攝影機偵測到動作時, 影片剪輯片段將透過該家庭中樞和網路攝影機之間的專用區域網路連線, 直接傳送到作為家庭中樞的 Apple 裝置。區域網路連線會以每一作業階段 HKDF-SHA512 衍生密鑰組加密, 該密鑰組會透過家庭中樞與網路攝影機之間的 HomeKit 作業階段進行交涉。HomeKit 會將家庭中樞上的音訊和影片串流進行解碼, 並在本機分析影片影格中是否有任何重大事件。如果偵測到重大事件, HomeKit 將使用 AES-256-GCM (含有隨機產生的 AES256 密鑰) 對影片剪輯片段進行加密。HomeKit 還會為每個剪輯片段產生封面影格, 並使用相同的 AES256 密鑰對這些封面影格進行加密。經過加密的封面影格以及音訊和影片資料將會上傳到 iCloud 伺服器。每個剪輯片段的相關後設資料 (包括加密密鑰) 都會使用 iCloud 端對端加密上傳到 CloudKit。

對於臉部分類, HomeKit 會使用 iCloud 端對端加密在 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訊 (例如姓名) 以及代表該人員臉部的影像。這些臉部影像可以選擇從使用者的「照片」中取得, 也可以從以前分析過的網路攝影機視訊中收集。「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路攝影機接收之安全視訊串流中的臉部, 並將該識別資訊納入在前面所提到的剪輯片段後設資料中。

當使用「家庭」App 檢視攝影機的剪輯片段時, 會從 iCloud 下載資料, 而解密串流的密鑰則會使用 iCloud 端對端解密在本機解除封裝。加密的影片內容會從伺服器連續播送, 並在 iOS 裝置本機上解密, 然後在檢視器中顯示。每個影片剪輯片段的作業階段可分為多個子區段, 每個子區段會使用其專屬的密鑰對內容串流進行加密。

## Apple TV 的 HomeKit 安全性

HomeKit 可安全地將一些第三方遠端配件連接到 Apple TV, 並支援為家庭 Apple TV 的擁有者加入使用者個人檔案。

### 搭配 Apple TV 使用第三方的遙控器配件

部分第三方遙控器配件可為使用「家庭」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。當使用者以遙控器上專用的 Siri 按鈕特地啟用麥克風時, 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路連線, 直接將音訊分段傳送到 Apple TV。每一作業階段 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, 藉此加密區域網路連線。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 音訊輸入相同的隱私權保護措施處理。

### HomeKit 家庭的 Apple TV 描述檔

當 HomeKit 家庭的使用者將其描述檔加入家庭擁有者的 Apple TV, 便可提供取用其電視節目、音樂和 Podcast 的權限給該使用者。每個使用者用於 Apple TV 的描述檔設定, 會使用 iCloud 端對端加密來分享至擁有者的 iCloud 帳號。這些資料為各使用者所有, 擁有者只擁有讀取權限。家庭的每位使用者都可以在「家庭」App 中更改這些值, 而擁有者的 Apple TV 會使用這些設定。

開啟設定時, 使用者的 iTunes 帳號就可在 Apple TV 上使用。關閉設定時, 所有與該使用者有關的帳戶和資料都會從 Apple TV 上刪除。由使用者裝置所起始的初始 CloudKit 共享, 以及用於建立安全 CloudKit 共享的代號, 會透過家庭使用者間同步資料所用的相同安全頻道來傳送。

## iOS、iPadOS 和 watchOS 的 SiriKit 安全性

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 可存取使用者的聯絡人資訊和裝置的目前位置。但是 Siri 必須先檢查 App 受使用者控制的權限，才能提供受保護的資料給該 App。根據這些權限，Siri 只會傳遞使用者原始話語的相關片段給 App 延伸功能。例如，如果 App 沒有聯絡資訊的存取權，Siri 就不會在使用者要求中解析關係（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。

但是如果使用者授予 App 存取聯絡資訊的權限，該 App 就可收到有關使用者母親的解析資訊。如果在訊息的一部分提及某個關係，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。

支援 SiriKit 的 App 可以傳送 App 專用或使用者專屬的詞彙給 Siri，例如使用者的聯絡人名稱。這些資訊能讓 Siri 的語音辨識和自然語言理解功能辨識該 App 的詞彙，且與隨機識別碼有關聯。只要識別碼使用中，自訂資訊就持續可用，直到使用者在「設定」中停用 App 的 Siri 整合，或是解除安裝支援 SiriKit 的 App。

若說出「使用『共乘』App 叫車送我到媽媽家」這類語句，需要使用者聯絡人的位置資料才能處理要求。無論使用者對該 App 設定的位置或聯絡資訊權限為何，Siri 都會僅針對該要求提供必要的資訊給 App 的延伸功能。

## WidgetKit 安全性

WidgetKit 是開發人員用來提供小工具和手錶複雜功能的架構。兩者都可能顯示敏感資訊，尤其在「永遠顯示」的裝置上可能會非常顯眼。

在 iOS 中，使用者可以設定是否要在鎖定畫面和「永遠顯示」下顯示敏感資料。在「設定」中，他們可以在「設定」>「Face ID 與密碼」的「鎖定時允許取用」部分中停用鎖定畫面小工具的資料取用。

在 Apple Watch 上，使用者可以選擇「設定」>「螢幕顯示與亮度」>「永遠顯示」>「隱藏敏感性複雜功能」來設定是否要在「永遠顯示」下顯示敏感資料。他們也可以選擇對所有或個別的複雜功能顯示已遮蔽的內容。

如果使用者選擇隱藏他們認為是私人的內容，WidgetKit 會呈現暫存區或遮蔽。若要設定遮蔽，開發者必須：

1. 建置 `redacted(reason:)` 回呼。
2. 朗讀 `privacy` 屬性。
3. 提供自訂暫存區顯示方式。

開發者也可以使用 `unredacted()` 顯示方式修改器將顯示區呈現為未遮蔽的狀態。

作為將個別顯示方式標記為隱私敏感的替代方案，例如，如果整個小工具內容都是隱私敏感的，開發者可以將「資料保護」功能加入小工具延伸功能中。WidgetKit 將顯示暫存區而非小工具內容，直到使用者解鎖其裝置以符合所選的隱私權等級。開發者必須在 Xcode 中為小工具延伸功能啟用「資料保護」功能，然後設定 `Data Protection` 授權數值，以符合他們希望提供的隱私權等級：

- `NSFileProtectionComplete`
- `NSFileProtectionCompleteUnlessOpen`

WidgetKit 會在裝置受密碼鎖定時隱藏這些小工具內容，並在使用者重新啟動裝置後顯示暫存區，直到使用者進行認證。另外，這些 iOS 小工具在 Mac 上能夠以 iPhone 小工具的形式提供。

## macOS 的 DriverKit 安全性

DriverKit 架構讓開發者可製作供使用者安裝在 Mac 上的裝置驅動程式。透過 DriverKit 建立的驅動程式會在使用者空間中執行，而非作為核心延伸功能，因此可提升系統安全性與穩定性。這讓安裝程序變得更簡單，且提高了 macOS 的穩定性和安全性。

使用者只需下載 App (使用系統延伸功能或 DriverKit 時不需要安裝程式)，而延伸功能只會在需要時啟用。在許多使用情況中這些延伸功能取代了 kexts，而其需要在「/系統/資源庫」或「/資源庫」中安裝的管理者權限。

IT 管理者若使用需要核心延伸功能的裝置驅動程式、雲端儲存解決方案、網路和安全性 App，建議其改用以系統延伸功能建置的新版本。這些新版本可大幅減少 Mac 上的核心陷入混亂的可能性，以及縮小攻擊面積。這些新的延伸功能會在使用者空間中執行，不需要特殊的權限即可安裝，且當綁定的 App 被移到「垃圾桶」中時會自動移除。

DriverKit 架構針對 I/O 服務、裝置比對、記憶體描述元和分送佇列提供 C++ 類別。也可為數字、集合、字串和其他常見類型定義 I/O 適用的類型。使用者可搭配家庭專用的驅動程式架構 (例如 USBDriverKit 和 HIDDriverKit) 使用上述類別。使用「系統延伸功能」架構來安裝和升級驅動程序。

## iOS 和 iPadOS 的 ReplayKit 安全性

ReplayKit 程式框架允許開發者在其 App 中加入錄製與即時廣播功能。此外，它允許使用者運用裝置的前鏡頭和麥克風來為其錄製的內容和廣播加上註解。

### 影片錄製

錄製影片中打造的安全性層級有數層：

- **權限對話框**：在錄製開始前，ReplayKit 會提供使用者同意警示，要求使用者確認其錄製螢幕畫面、麥克風及前置相機的意圖。系統會針對每個 App 處理程序顯示此警示一次，且若 App 停留在背景超過 8 分鐘，將會再次顯示。
- **螢幕與音訊擷取**：螢幕與音訊擷取是在 App 的處理程序外、於 ReplayKit 的服務程式 `replayd` 中進行。此設計可確保錄製的內容從不讓 App 處理程序存取。
- **App 內的螢幕與音訊擷取**：這可讓 App 取得影片和樣本緩衝，且受到權限對話框的保護。
- **影片製作與儲存**：影片檔會直接寫入目錄，只有 ReplayKit 的子系統可存取，且從不讓任何 App 存取。這樣可協助防止錄製內容未經使用者同意而遭第三方使用。
- **終端使用者預覽與共享**：使用者可使用 ReplayKit 提供的使用者介面來預覽與共享影片。使用者介面會透過「iOS 延伸功能」基礎架構跨處理序呈現，並可存取產生的影片檔。

### ReplayKit 廣播

廣播影片中打造的安全性層級有數層：

- **螢幕與音訊擷取**：廣播期間的螢幕與音訊擷取機制與影片錄製相同，且會發生於 `replayd` 中。
- **廣播延伸功能**：若要讓第三方服務參與 ReplayKit 廣播，它們需要建立兩個新延伸功能 (以 `com.apple.broadcast-services` 端點加以設定)：
  - 允許使用者設定其廣播的使用者介面延伸功能
  - 上傳延伸功能，可處理上傳影片與音訊資料至服務的後端伺服器

該架構可協助確保託管 App 對廣播的影片和音訊內容沒有特權。只有 ReplayKit 和第三方廣播延伸功能具有存取權。

- **廣播選擇器**：使用廣播選擇器，使用者可直接從 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使用者介面)。系統會使用專用 API 來導入使用者介面，且其為位於 ReplayKit 程式框架中的延伸功能。其為來自託管 App 的跨處理序延伸功能。
- **上傳延伸功能**：第三方廣播服務會實作延伸功能，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傳延伸功能。影片資料完成編碼的方式是藉由從影片樣本緩衝擷取 `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 安全性

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 設計的相機重視使用者的隱私，第三方 App 必須取得使用者的同意才能取用相機。在 iOS 和 iPadOS 中，當使用者授予 App 相機的取用權限時，該 App 可從前後相機取用即時影像。若無法讓使用者明確知道相機正在使用中，App 就不允許使用相機。

用相機拍攝的照片和影片可能包含其他資訊，例如拍攝地點、景深和 OverCapture。如果使用者不希望「相機」App 拍攝的照片和影片包含位置，可以隨時前往「設定」>「隱私權」>「定位服務」>「相機」控制此設定。如果使用者不希望分享照片和影片時包含位置，可以在分享表單裡的「選項」選單中關閉位置。

使用 ARKit 的 App 可使用其他相機的世界或臉部追蹤資訊，以便為使用者提供更優異的 AR 體驗。世界追蹤會在使用者的裝置上使用演算法來處理來自這些感測器的資訊，以便判斷其與實體空間的相對位置。世界追蹤用於提供「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、tvOS 和 watchOS 支援具彈性的安全政策和設定，讓使用者容易實施與管理。各機構可透過這些功能保護公司資訊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) 計畫時）。

組織可以使用由行動裝置管理 (MDM) 解決方案建置的 MDM 架構來強制執行密碼要求、配置設定、限制功能，甚至在受管理的裝置上遠程清除企業資料。這有助於維護企業資料的安全性，即使員工使用他們的個人裝置來取用這些資料。

## iPhone 和 iPad 的配對模式安全性

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 或以上版本中，服務具有以下特性：

- 需要配對的服務會等到裝置已由使用者解鎖後才會啟動
- 除非裝置最近剛解鎖，否則服務不會啟動
- 可能 (包含照片同步) 會要求裝置解鎖後才會開始

配對程序需要使用者解鎖裝置並接受來自主機的配對要求。在 iOS 9 或以上版本中，使用者也需要輸入其密碼，輸入後主機和裝置才會交換及儲存 2048 位元 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前 (iTunes 或 Finder 同步、檔案傳送、Xcode 開發等)，需要使用交換的密鑰來啟動加密 SSL 作業階段。若要將這個加密的作業階段用於所有通訊，裝置需要透過 Wi-Fi 從主機連線，因此先前必須已透過 USB 完成配對。配對也會啟用一些診斷功能。在 iOS 9 中，若配對記錄已超過 6 個月未使用，便會過期。在 iOS 11 或以上版本中，此期限縮短為 30 天。

部分服務 (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 或以上版本中，Apple TV 可使用「安全遠端密碼」通訊協定來以無線方式建立配對關係。

使用者可以使用「重置網路設定」或「重置定位服務與隱私權」選項來清除信任的主機列表。

## 行動裝置管理

### 行動裝置管理安全性概覽

Apple 作業系統支援行動裝置管理 (MDM)，此解決方案讓組織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

設定、無線註冊和「Apple 推播通知服務」(APNs) 等作業系統技術均內建 MDM 功能。例如，APNs 可用來喚醒裝置，並觸發裝置透過安全連線與 MDM 解決方案直接進行通訊。任何機密或私密資訊皆不會透過 APNs 傳輸。

使用 MDM，IT 部門便可以為企業或教育環境中的 Apple 裝置註冊、以無線方式設定配置和更新設定、監控遵守狀況、管理軟體更新，甚至可以遠端清除或鎖定受管理的裝置。

在 iOS 13、iPadOS 13.1 和 macOS 10.15 或以上版本中，Apple 裝置支援專為「員工自攜裝置」BYOD 計畫設計的新註冊選項。「使用者註冊」讓使用者在其擁有的裝置上擁有更多自主權，同時以加密編譯方式將受管理的資料隔離，增強了企業資料的安全性。這讓 BYOD 計畫在安全性、隱私和使用者體驗之間達到更平衡的狀態。在 iOS 17、iPadOS 17 和 macOS 14 或以上版本中，為基於帳號的「裝置註冊」加入了類似的資料隔離機制。

## 註冊類型

- **使用者註冊：**「使用者註冊」專為使用者擁有的裝置所設計，且與管理式 Apple ID 整合以在裝置上建立使用者識別身分。起始註冊需要管理式 Apple ID，使用者必須成功認證才能順利註冊。管理式 Apple ID 可搭配使用者已登入的個人 Apple ID 使用。受管理的 App 和帳號使用管理式 Apple ID，而個人 App 和帳號則使用個人 Apple ID。
- **裝置註冊：**「裝置註冊」允許組織讓使用者手動註冊裝置，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」也有較大範圍的設定和取用限制可套用至裝置。當使用者移除註冊描述檔，所有配置、設定，以基於該註冊描述檔的受管理 App 都會移除。與「使用者註冊」類似，「裝置註冊」也可以與管理式 Apple ID 整合。這種基於帳號的「裝置註冊」還提供了使用「管理式 Apple ID」與個人 Apple ID 並行的能力，並以加密編譯方式將企業資料隔離。
- **自動裝置註冊：**「自動裝置註冊」讓組織在裝置開箱的當下即可進行設定及管理。這些裝置稱為**受監管**，且使用者可選擇讓使用者無法移除 MDM 描述檔。「自動裝置註冊」是為了由組織擁有的裝置所設計。

## 裝置取用限制

取用限制可由管理者啟用，或在部分情況下停用，以協助防止使用者取用特定 App、服務，或在 MDM 解決方案中註冊的 iPhone、iPad、Mac、Apple TV 或 Apple Watch 的功能。取用限制會傳送至取用限制承載資料中的裝置，其為設定的一部分。iPhone 上的某些取用限制可能會反映在配對的 Apple Watch 上。

## 密碼與密碼設定管理

依照預設，在 iOS、iPadOS 和 watchOS 上，使用者的密碼可定義為數值的 PIN。在配備 Face ID 或 Touch ID 的 iPhone 和 iPad 裝置上，預設密碼長度是六位數，最少四位數。由於較長且複雜的密碼比較難以猜測或攻擊，因此建議使用此類密碼。

管理者可以使用 MDM 或在 iOS 和 iPadOS 上使用 Microsoft Exchange，強制實施複雜的密碼要求和其他規則。若 macOS 密碼規則承載資料是以手動方式安裝，則需使用管理者密碼。密碼規則可能需要特定的密碼長度、組成內容或其他屬性。

Apple Watch 預設使用數字密碼。如果套用至受管理 Apple Watch 的密碼規則要求使用非數字字元，則需要使用配對的 iPhone 來解鎖裝置。

## 設定強制執行

設定是 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。如果組織需要設定大量裝置或為大量裝置提供許多自訂的電子郵件設定、網路設定或憑證，則設定是一種安全可靠的方式。



## 設定

設定是遵循特定結構且包含承載資料的 XML 描述檔或 json 格式檔案，可將設定和授權資訊載入 Apple 裝置。設定會自動處理設定、帳號、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。在組織將設定傳送到 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。

**【注意】** Mac 版 Apple Configurator 只能用來管理 iPhone、iPad 和 Apple TV 裝置上的設定描述檔。

## 註冊描述檔

註冊描述檔是 MDM 承載資料的設定，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到裝置並查詢裝置的特定層面。當使用者移除註冊描述檔，所有設定、包含的設定項目，還有以該註冊描述檔為基礎的受管理 App (根據註冊類型和使用的設定) 都會一併移除。在裝置上一次只能存在一個註冊描述檔。

## 設定範例

設定中包含可指定特定承載資料中的多個設定項目，包括 (但不限於)：

- 密碼規則
- 裝置功能的取用限制 (例如停用相機)
- 網路與 VPN 設定
- Microsoft Exchange 設定
- 「郵件」設定
- 帳號設定
- LDAP 目錄服務設定
- CalDAV 行事曆服務設定
- 憑證和識別身分
- 憑證
- 軟體更新

## 描述檔簽署與加密

設定描述檔可簽署來驗證其來源，以及加密來協助確保其完整性和保護其內容。iOS 和 iPadOS 的設定描述檔是使用 [RFC 5652](#) (支援 3DES 和 AES128) 中指定的「加密編譯訊息語法」(CMS) 所加密。

## 描述檔安裝

設定可使用 MDM 解決方案或由使用者手動安裝在裝置上。或者，也可使用 Mac 版 Apple Configurator 來將設定部署到 iOS、iPadOS 和 tvOS 裝置。某些設定必須使用 MDM 解決方案進行安裝。如需移除描述檔的相關資訊，請參閱「Apple 平台部署」中的 [行動裝置管理簡介](#)。

**【注意】** 在監管的裝置上，設定描述檔也可鎖定至裝置。此設計可防止移除設定描述檔，或是允許僅透過密碼移除。

## 自動裝置註冊

在使用者收到裝置前，公司可以在行動裝置管理 (MDM) 解決方案中自動註冊 iOS、iPadOS、macOS 和 tvOS 裝置，無需操作實體或準備。註冊「Apple 校務管理」、「Apple 商務管理」或「Apple 商務必備」其中一項服務後，管理者需登入服務網站，並將服務連結到其 MDM 解決方案。接著便可透過 MDM 將他們購買的裝置指定給使用者。裝置設定過程中，裝置會向 Apple 伺服器查詢指派的 MDM，如發生此情況，便會連線至 MDM 解決方案以執行註冊。使用「自動裝置註冊」和相容的 MDM 解決方案，可讓組織實作下列安全措施：

- 將使用者認證納入 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的初步設定，及要求進行其他裝置設定才能存取敏感資料。
- 註冊前要求裝置執行最低作業系統版本。
- 在 Mac 電腦上強制執行「檔案保險箱」。

透過 MDM 註冊裝置後，所有設定、限制或控制項目便會自動安裝。

藉由移除裝置上「設定輔助程式」中的特定步驟，使用者的設定程序更加簡化，方便他們快速使用。如果跳過步驟，就會使用更加保護隱私的設定。例如，如果跳過了設定定位服務的窗格，就不會在「設定輔助程式」執行期間啟用服務。

管理者也可以控制使用者是否可從裝置上移除 MDM 描述檔，並協助確保設定和取用限制在裝置的生命週期內均有效。

## Apple 校務管理、Apple 商務管理和 Apple 商務必備

「Apple 校務管理」、「Apple 商務管理」和「Apple 商務必備」是專供 IT 管理者使用的服務，用於部署組織直接向 Apple 或 Apple 授權的經銷商和電信業者購買的 Apple 裝置。

使用 MDM 解決方案時，管理者可以簡化使用者的設定程序、配置裝置設定，以及分發你在這三項服務中購買的 App 和書籍。「Apple 校務管理」也直接或使用 SFTP 與「學生資訊系統」(SIS) 整合，且全部三項服務都支援目錄同步處理和聯合驗證，因此可根據組織的識別身分供應商 (IdP) 自動佈建、更新和取消佈建帳號。

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。這些認證針對範圍內系統的 Apple 資訊隱私權和安全性作法，為客戶提供了獨立證明。如更多資訊，請參閱「Apple 平台認證」中的 [Apple 網際網路服務安全性認證](#)。

**【注意】**若要瞭解 Apple 計畫在特定國家或地區的供應情況，請參閱 Apple 支援文章：[適用於教育機構和企業的 Apple 計畫和付款方式供應情況](#)。

## 裝置監管

**監管**通常表示裝置是歸組織所有，並提供其額外的裝置設定和取用限制的控制權限。如需更多資訊，請參閱「Apple 平台部署」中的[關於 Apple 裝置監管](#)。

使用「自動裝置註冊」時，裝置上的監管功能會自動啟用。

## 啟用鎖定安全性

Apple 執行「啟用鎖定」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 安全晶片的 Intel 架構式 Mac。

### 在 iPhone 和 iPad 上如何運作

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「啟用鎖定」。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。已啟用鎖定的裝置會提示使用者輸入 iCloud 帳號和密碼，這組帳號和密碼必須屬於當初開啟「啟用鎖定」的使用者。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 上如何運作

在配備 Apple 晶片的 Mac 上，LLB 會驗證該裝置是否存在有效的 LocalPolicy，以及 LocalPolicy 規則的反重放值是否與「安全儲存元件」中儲存的值相符。如果出現以下情況，Low-Level Bootloader (LLB) 會開機進入 RecoveryOS：

- 目前的 macOS 沒有 LocalPolicy

- 該 macOS 的 LocalPolicy 無效
- LocalPolicy 反重放值雜湊值與「安全儲存元件」中儲存的值不相符

RecoveryOS 偵測到 Mac 電腦未啟用，就會與啟用伺服器聯絡以取得啟用憑證。如果裝置處於已啟用鎖定的狀態，則 RecoveryOS 會提示使用者輸入 iCloud 帳號和密碼，這組帳號和密碼必須屬於當初開啟「啟用鎖定」的使用者。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。除非存在有效的 LocalPolicy，否則 LLB 將不會允許 macOS 開機。

## 在採用 Intel 架構的 Mac 電腦上如何運作

在採用 Intel 架構並配備 T2 晶片的 Mac 中，T2 晶片韌體會先驗證是否存在有效的啟用憑證，再允許電腦開機至 macOS。如果不存在有效的啟用憑證，則由 T2 晶片載入的 UEFI 韌體會負責向 T2 晶片查詢裝置的啟用狀態，並開機進入 RecoveryOS 而不是 macOS。RecoveryOS 偵測到 Mac 沒有啟用，就會與啟用伺服器聯絡以取得啟用憑證。如果裝置處於已啟用鎖定的狀態，則 RecoveryOS 會提示使用者輸入 iCloud 帳號和密碼，這組帳號和密碼必須屬於當初開啟「啟用鎖定」的使用者。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遠端清除

「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，可透過遠端方式加以鎖定或清除。

### 受管理的遺失模式

如果系統為 iOS 9 或以上版本的受監管 iOS 或 iPadOS 裝置遺失或遭竊，行動裝置管理 (MDM) 管理者可從遠端啟用該裝置上的「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，目前的使用者會被登出裝置且無法解鎖。螢幕會顯示一則可由管理者自訂的訊息，例如顯示電話號碼，以便在尋獲裝置時撥打。管理者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。當管理者關閉「受管理的遺失模式」時（此為結束此模式的唯一方式），使用者會從鎖定畫面上的訊息或主畫面上的提示獲知此動作。

### 遠端清除

管理者或使用者可從遠端清除 iPhone、iPad、Mac、Apple TV 和 Apple Watch 裝置，讓所有資料無法讀取。

當 MDM 或 iCloud 觸發遠端清除指令時，裝置會傳回確認通知並執行清除作業。若是透過 Microsoft Exchange ActiveSync 執行遠端清除，裝置會在執行清除之前登入 Microsoft Exchange Server。

遠端清除在以下情況中無法使用：

- 透過「使用者註冊」
- 當帳號是透過「使用者註冊」安裝時使用 Microsoft Exchange ActiveSync
- 如果裝置受監管則使用 Microsoft Exchange ActiveSync

使用者也可以使用「設定」（iPhone 和 iPad）或「系統設定」（Mac）來清除所持有的受支援裝置。如前面提到的，可以將 iPhone、iPad 和 Apple Watch 裝置設定為在連續多次輸入密碼失敗後，自動清除裝置。

配備 Apple 晶片的 Mac 電腦，以及配備 Apple T2 安全晶片或已開啟「檔案保險箱」的 Mac 電腦，可執行立即遠端清除。執行立即遠端清除的方式為安全捨棄媒體密鑰。

## iPadOS 中「共享的 iPad」安全性

「共享的 iPad」是在 iPad 部署中使用的多重使用者模式。此模式可讓使用者共享一部 iPad，同時讓每位使用者的文件和資料維持獨立狀態。每位使用者可獲得專為他們保留的儲存位置，這個位置是以 APFS（Apple 檔案系統）卷宗形式導入，且受到使用者的憑證保護。「共享的 iPad」需使用由組織核發並擁有的管理式 Apple ID。

使用「共享的 iPad」，可讓使用者登入任何組織擁有且設為供多重使用者使用的裝置。使用者資料會分割至獨立的目錄中，而每個目錄都位於其專屬的資料保護網域中，且受到 UNIX 權限和沙盒技術保護。在 iPadOS 13.4 或以上版本中，使用者也可登入暫時操作階段。當使用者登出暫時操作階段，使用者的 APFS 卷宗會被刪除，而且保留的空間會歸還給系統。

## 登入「共享的 iPad」

當登入「共享的 iPad」時，同時支援原生和同盟管理式 Apple ID。第一次使用同盟帳號時，系統會將使用者重新導向至身分提供者 (IdP) 的登入口網站。經過認證後，會核發一個有效期短的存取代碼以支援管理式 Apple ID，而登入程序會繼續執行，類似於原生管理式 Apple ID 登入程序。登入後，「共享的 iPad」上的「設定輔助程式」會提示使用者建立一組密碼 (憑證)，用來在未來保護裝置上的本機資料及認證登入畫面。在單一使用者裝置上，使用者會使用同盟帳號登入一次其管理式 Apple ID，然後用自己的密碼解鎖其裝置；同樣地，在「共享的 iPad」上，使用者會使用同盟帳號登入一次，此後便使用自行建立的密碼。

當使用者不是透過聯合驗證登入時，「Apple 識別服務」(IDS) 會使用 SRP 通訊協定認證該管理式 Apple ID。若認證成功，則會授予一個該裝置專用的短效期存取代碼。如果使用者先前使用過裝置，他們便已有使用相同憑證解鎖的本機使用者帳號。

如果使用者之前沒有用過裝置或正在使用暫時操作階段功能，則「共享的 iPad」會佈建一個新的 UNIX 使用者 ID、一個用於儲存使用者個人資料的 APFS 卷宗，以及一個本機鑰匙圈。由於建立 APFS 卷宗時會為使用者分配 (保留) 儲存空間，因此可能沒有足夠空間建立一個新卷宗。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使用者，並讓該使用者退出裝置，以便讓新使用者登入。萬一全部現有的使用者都尚未完成上傳其雲端資料，新的使用者登入程序便會失敗。若要登入，新的使用者需要等待一位使用者的資料同步完成，或請管理者強制刪除一個現有的使用者帳號，而這麼做會有資料遺失的風險。

如果裝置未連接網際網路 (例如使用者沒有 Wi-Fi 連接點時)，則可能會在有限天數內針對本機帳號進行認證。在這種情況下，只有擁有先前已存在本機帳號或暫時操作階段的使用者可以登入。這個時限過後，即使本機帳號已存在，使用者仍需於線上進行認證。

使用者的本機帳號解鎖或建立後，若進行遠端認證，由 Apple 伺服器核發的短效期代碼便會轉換為 iCloud 代碼，以允許登入 iCloud。接著使用者的設定會回復，且其文件和資料會從 iCloud 同步。

當使用者的作業為作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，使用者登出之後，背景同步機制可協助確保更動會推送至 iCloud，或是使用 NSURLSession 背景作業的其他 Web 服務。該使用者的背景同步作業完成後，系統會卸載其 APFS 卷宗，且若使用者沒有重新登入，就無法再次裝載。

暫時操作階段不會與 iCloud 同步資料，且雖然暫時操作階段可以登入第三方同步服務 (例如 Box 或 Google 雲端硬碟)，但並沒有在暫時操作階段結束時繼續同步資料的功能。

## 登出「共享的 iPad」

使用者登出「共享的 iPad」時，系統會立即鎖定該使用者的 Keybag，並關閉所有 App。為了加快新使用者登入的速度，iPadOS 會暫時延遲部分的一般登出操作，並向新使用者顯示登入視窗。如果使用者在這段期間 (約 30 秒) 登入，「共享的 iPad」會執行延遲的清除，做為新使用者登入帳號程序的一部分。但是如果「共享的 iPad」維持閒置狀態，便會觸發延遲的清除程序。執行清除階段期間，「登入視窗」會重新啟動，就像是發生另一個登出操作。

當暫時操作階段結束時，「共享的 iPad」會執行完整的登出程序，並立即刪除暫時操作階段的 APFS 卷宗。

# Apple Configurator 安全性

Mac 版 Apple Configurator 採用彈性、安全並以裝置為中心的設計，讓管理者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)，再將裝置交給使用者。使用 Mac 版 Apple Configurator，管理者可以更新軟體、安裝 App 和設定描述檔、重新命名與更改裝置上的桌布、輸出裝置資訊和文件等等。

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 安全晶片的 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。使用者在任何時候都無法在 Apple Configurator 之外檢閱或使用此檔案。

管理者也可使用 Mac 版 Apple Configurator 或 iPhone 版 Apple Configurator，選擇將裝置加入「Apple 校務管理」、「Apple 商務管理」或「Apple 商務必備」，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。當管理者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，包含強制性監管和行動裝置管理 (MDM) 註冊。針對並非直接購買的裝置，使用者有 30 天的緩衝期可以將裝置從這些服務之一、監管和 MDM 中釋出。

若 iOS、iPadOS 和 tvOS 裝置完全沒有網際網路連線而在設定時已連接具備網際網路連線的主機 Mac，組織也可以使用 Mac 版 Apple Configurator 來將其啟用。管理者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 或行動網路。此功能不允許管理者略過非共享式啟用期間通常所需的任何現有「啟用鎖定」要求。

## 「螢幕使用時間」安全性

「螢幕使用時間」是一項內建功能，用於查看和管理成人及其孩童在 App、網站等上花費的時間。有兩種使用者類型：成人與 (受管理的) 孩童。

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，因此瞭解其如何在這方面保障隱私和安全性是相當重要的。「螢幕使用時間」是 iOS 12 或以上版本、iPadOS 13.1 或以上版本、macOS 10.15 或以上版本的功能，以及 watchOS 6 或以上版本的部分功能。

下表說明了「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
執行其他取用限制	iOS iPadOS macOS watchOS
設定網路用量限制	iOS iPadOS macOS
設定 App 限制	iOS iPadOS macOS watchOS
設定停用時間	iOS iPadOS macOS watchOS

使用者若要管理自己的裝置使用情況，可使用 CloudKit 端對端的加密，在與同一個 iCloud 帳號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。使用者的帳號必須啟用雙重認證（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「取用限制」功能，以及舊版 macOS 中找到的「分級保護控制」功能。

在 iOS 13 或以上版本、iPadOS 13.1 或以上版本和 macOS 10.15 或以上版本中，「螢幕使用時間」使用者和受管理的子女會自動在裝置間分享其使用情況（若其 iCloud 帳號已啟用雙重認證）。使用者清除 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」來瞭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更動。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。

系統會使用端對端加密的「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 或 iPad 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

如果使用者開啟「分享 iPhone 與 Apple Watch 分析」，則系統只會收集下列匿名資料，以便讓 Apple 更瞭解「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
- 為「類別」用量設定限制後的用量變化（90 天內）
- 是否已開啟「螢幕使用時間」
- 是否已開啟「停用時間」
- 使用「要求增加時間」需求的次數
- App 限制的數量
- 使用者在「螢幕使用時間」設定中檢視用量的次數，依使用者類型和檢視類型（本機、遠端、小工具）分類
- 使用者忽略限制的次數，依使用者類型分類
- 使用者刪除限制的次數，依使用者類型分類

Apple 不會收集特定 App 或網站用量資料。當使用者在「螢幕使用時間」用量資訊中看到 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。若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分，以執行快速清除並提高安全性。

**安全儲存元件** 此晶片的設計包含無法更改的 RO 程式碼、硬體亂數產生器、加密引擎，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，以用於儲存反重複值。為讀取和更新反重複值，「安全隔離區」和儲存晶片會利用安全通訊協定，以協助確保反重複值的獨佔存取權。此技術已歷經多個世代更迭，提供不同的安全性保證。

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

**佈建描述檔** 由 Apple 簽署的佈建描述檔 (.plist 檔案)，其包含一組實體和授權，允許在 iOS 和 iPadOS 裝置上裝並測試 App。開發用的佈建描述檔會列出開發者選擇用來參與臨時發佈的裝置；發佈佈建描述檔中包含企業開發 App 的 App ID。

**位址空間配置隨機載入 (ASLR)** 作業系統使用的一項技術，可讓程式錯誤遭到不當利用的成功率大幅降低。藉由確保記憶體位址和位移無法預測，入侵的程式碼便無法對這些值進行硬式編碼。

**系統副處理器完整保護 (SCIP)** Apple 用來防止副處理器韌體遭修改的機制。

**系統軟體授權** 此程序結合了硬體內建的加密編譯密鑰與線上服務，以檢查升級時只會提供和安裝來自 Apple 的合法軟體 (適用性取決於支援的裝置)。

**系統單晶片 (SoC)** 一種積體電路 (IC)，可將多重元件整合到單片晶片上。應用程式處理器「安全隔離區」和其他副處理器是 SoC 的元件。

**直接記憶體存取 (DMA)** 此功能可讓硬體子系統略過 CPU 直接存取主記憶體。

**門禁** 在 macOS 中，設計來協助確保使用者的 Mac 上只會執行受信任的軟體。

**指紋紋路角度對應** 從指紋的一部分擷取出，描述紋路走向和寬度的數學表示資料。

**記憶體控制器** 系統單晶片中的子系統，負責控制系統單晶片與其主記憶體之間的介面。

**唯一晶片識別碼 (ECID)** 每部 iPhone 或 iPad 處理器中的一個 64 位元唯一識別碼。

**唯一識別碼 (UID)** 在製造過程中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體讀取，只能由處理器的硬體 AES 引擎使用。若要取得實際密鑰，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矽晶片。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」的一種技術，可透過系統軟體上的測量值和僅存於硬體中的密鑰 (例如「安全隔離區」中的 UID) 來保護或密封加密密鑰。

**密碼衍生密鑰 (PDK)** 衍生密鑰，衍生自使用者密碼與長期 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 和 iPadOS 遵循 [RFC 3394](#) 使用 NIST AES 密鑰封裝。

**啟動切換** 支援在受支援的 Mac 電腦上安裝 Microsoft Windows 的 Mac 工具程式。

**軟體種子位元** 「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。每個軟體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」開機 ROM 和作業系統便可獨立變更每個軟體種子位元的值。設定鎖定位元後，軟體種子位元和鎖定位元均無法修改。「安全隔離區」重新啟動時，軟體種子位元和其鎖定位元會重置。

**媒體密鑰** 加密密鑰階層的一部分，可協助安全並即時的清除。在 iOS、iPadOS、tvOS 和 watchOS 中，媒體密鑰會封裝資料卷宗上的後設資料（因此若缺少媒體密鑰便無法存取所有檔案專屬密鑰，讓使用「資料保護」防護的檔案無法存取）。在 macOS 中，媒體密鑰會封裝密鑰材料、所有後設資料，以及受「檔案保險箱」保護的卷宗上的所有資料。在任一情況下，清除媒體密鑰都會使加密的資料無法存取。

**復原模式** 如果無法識別使用者的裝置，復原模式可用於復原許多 Apple 裝置，讓使用者能重新安裝作業系統。

**硬體安全模組 (HSM)** 專門用來防止竄改的電腦，可保護並管理數位密鑰。

**統一可延伸韌體介面 (UEFI) 韌體** 此技術取代 BIOS，用於將韌體連接至電腦的作業系統。

**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 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分，無論是 Apple 或攻擊者皆無法對其進行修改。

**開機進度暫存器 (BPR)** 一組系統單晶片 (SoC) 硬體旗標，可讓軟體追蹤裝置進入哪種開機模式，例如裝置韌體升級 (DFU) 模式和復原模式。「開機進度暫存器」旗標設定後就無法清除。這可讓之後的軟體取得系統狀態的信任指標。

**群組識別碼 (GID)** 類似 UID，同一類別中每個處理器的 GID 皆相同。

**裝置韌體升級 (DFU) 模式** 裝置的開機 ROM 程式碼在等待透過 USB 回復時所處的模式。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，會顯示以下提示：「Finder (或 iTunes) 偵測到一台處於復原模式中的 iPhone 或 iPad。若要與 Finder (或 iTunes) 一同使用，使用者必須復原此 iPhone 或 iPad。」

**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。

**增強型序列週邊介面 (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。

**橢圓曲線數位簽章算法 (ECDSA)** 以橢圓曲線加密技術為基礎的數位簽章算法。

**積體電路 (IC)** 亦稱為微晶片。

**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/輸出裝置和週邊設備的位址空間存取。

**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進行快速清除，而不視為機密。

**檔案專屬密鑰** 由「資料保護」用來加密檔案系統上之檔案的密鑰。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體除錯工具。

**纏結** 使用者的密碼轉換為加密編譯密鑰，並使用裝置 UID 強化的程序。此程序可協助確保暴力密碼破解攻擊必須在指定裝置上才能執行，進而降低發生率，且可避免多部裝置同時受到攻擊。纏結演算法為 PBKDF2，其使用 AES 密鑰搭配裝置 UID，作為每次反覆運算的偽隨機函式 (PRF)。

**鑰匙圈** Apple 作業系統和第三方 App 用來儲存和擷取密碼、密鑰和其他敏感性憑證的基礎架構和 API 組。

**AES 加密引擎** 實作 AES 的專用硬體元件。

**AES-XTS** IEEE 1619-2007 中定義的一種 AES 模式，專門用於加密儲存媒體。



**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 和採用 macOS 10.13 或以上版本的 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 安全性獎金** Apple 提供給研究人員的獎勵，研究人員回報的漏洞若會影響最新發佈的作業系統及相關最新硬體，便可獲得此獎勵。

**Apple 校務管理** 是一個易於使用的入口網站，能提供快速、簡化的方式讓 IT 管理者為組織部署直接購自 Apple 或與 Apple 合作之授權經銷商或電信業者的 Apple 裝置。他們可以在其行動裝置管理 (MDM) 解決方案中自動註冊裝置，無須在使用者取得前實際操作或準備裝置。

**Apple 商務管理** 是一個易於使用的入口網站，能提供快速、簡化的方式讓 IT 管理者為組織部署直接購自 Apple 或與 Apple 合作之授權經銷商或電信業者的 Apple 裝置。他們可以在其行動裝置管理 (MDM) 解決方案中自動註冊裝置，無須在使用者取得前實際操作或準備裝置。

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

**Apple 識別服務 (IDS)** Apple 的 iMessage 公用密鑰、APNs 位址、電話號碼和電子郵件地址的目錄，用於查詢密鑰和裝置位址。

**CKRecord** 鍵值組的字典，其中包含儲存至 CloudKit 或從 CloudKit 擷取的資料。

**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載入程式。用來載入 XNU 的程式碼，作為安全開機鏈的一部分。每一代系統單晶片 (SoC) 的 iBoot 可能在載入方式上有差異，有些是由 Low Level Bootloader 載入，有些則直接由開機 ROM 載入。

**Keybag** 用於儲存一組類別密鑰的資料結構。每種類型 (使用者、裝置、系統、備份、託管或「iCloud 備份」) 的格式皆相同。

標題包含以下內容：版本 (iOS 12 或以上版本中設為 4)、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 salt 和反覆運算次數纏結)。

類別密鑰列表：密鑰 UUID、類別 (哪個檔案或「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)、封裝類別密鑰和非對稱式類別的公用密鑰。

**Low Level Bootloader (LLB)** 在具有雙階段開機架構的 Mac 電腦上，LLB 包還由開機 ROM 叫用的程式碼，接著會作為安全開機鏈的一部分載入 iBoot。

**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 (固態硬碟) 的硬體子系統。

**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、沙盒技術限制、授權檢查和位址空間配置隨機載入 (ASLR)。

**XProtect** 在 macOS 中，根據簽章偵測和移除惡意軟體的防毒技術。

# 文件版本記錄

## 文件版本記錄

### 2024 年 5 月

新增主題：

- [Cryptex1 Image4 資訊檔雜湊 \(spih\)](#)
- [Cryptex1 世代 \(stng\)](#)
- [用於訊息和 IDS 的 BlastDoor](#)
- [「封閉模式」安全性](#)
- [關於 App Store 安全性](#)
- [WidgetKit 安全性](#)

更新主題：

- [Apple 平台安全性簡介](#)
- [Apple SoC 安全性](#)
- [安全隔離區](#)
- [Face ID、Touch ID 和密碼](#)
- [面孔比對安全性](#)
- [Face ID 和 Touch ID 的用途](#)
- [可使用備用電量的快速卡片](#)
- [作業系統完整性](#)
- [安全啟動資料連線](#)
- [驗證 iPhone 和 iPad 的配件](#)
- [watchOS 的系統安全性](#)
- [密碼](#)
- [資料保護概覽](#)
- [資料保護的 Keybag](#)
- [替用開機模式保護密鑰的機制](#)
- [遭遇攻擊時保護使用者資料](#)

- [在 macOS 中管理檔案保險箱](#)
- [iOS 和 iPadOS 的 App 安全性簡介](#)
- [macOS 的門禁與執行階段保護](#)
- [管理式 Apple ID 安全性](#)
- [iCloud 加密](#)
- [帳號復原聯絡人安全性](#)
- [遺產聯絡人安全性](#)
- [「iCloud 鑰匙圈」安全性概覽](#)
- [保護鑰匙圈同步](#)
- [「iCloud 鑰匙圈」的託管安全性](#)
- [卡片佈建的安全性概覽](#)
- [將信用卡或簽帳金融卡加入 Apple Pay](#)
- [以卡片進行 Apple Pay 付款](#)
- [Apple Card 安全性](#)
- [「iPhone 卡緊收」的安全性](#)
- [使用 Apple 錢包存取](#)
- [申領密鑰類型](#)
- [Apple 錢包中的身分證](#)
- [「Apple 錢包」中的身分證安全性](#)
- [開發者套件安全性概覽](#)
- [HomeKit 通訊安全性](#)
- [行動裝置管理安全性概覽](#)
- [設定強制執行](#)

## 2022 年 12 月

新增主題：

- [iCloud 的進階資料保護](#)

更新主題：

- [iCloud 安全性概覽](#)
- [iCloud 加密](#)
- [「iCloud 備份」的安全性](#)
- [帳號復原聯絡人安全性](#)
- [遺產聯絡人安全性](#)

## 2022 年 5 月

更新對象：

- iOS 15.4
- iPadOS 15.4
- macOS 12.3
- tvOS 15.4
- watchOS 8.5

新增主題：

- [配對 RecoveryOS 的限制](#)
- [本機作業系統版本 \(love\)](#)
- [健康分享](#)
- [帳號復原聯絡人安全性](#)
- [遺產聯絡人安全性](#)
- [「iPhone 卡緊收」的安全性](#)
- [使用 Apple 錢包存取](#)
- [申領密鑰類型](#)
- [Apple 錢包中的身分證](#)
- [支援 Siri 的 HomeKit 配件](#)

更新主題：

- [配備 Touch ID 的巧控鍵盤](#)
- [Face ID、Touch ID 和密碼](#)
- [面孔比對安全性](#)
- [可使用備用電量的快速卡片](#)
- [配備 Apple 晶片的 Mac 所具備的開機模式](#)
- [配備 Apple 晶片的 Mac 上的 LocalPolicy 檔案內容](#)
- [簽署系統卷宗安全性](#)
- [watchOS 的系統安全性](#)
- [Apple 安全研究裝置](#)
- [Apple 檔案系統的角色](#)
- [保護 App 對使用者資料的存取](#)
- [macOS 的 App 安全性簡介](#)
- [在 macOS 中防禦惡意軟體](#)
- [iCloud 安全性概覽](#)
- [保護鑰匙圈同步](#)
- [保護「iCloud 鑰匙圈」復原](#)
- [以卡片進行 Apple Pay 付款](#)

- [Apple Pay 中的感應式票卡](#)
- [停用卡片的 Apple Pay 功能](#)
- [Apple Card申請](#)
- [Apple Cash 安全性](#)
- [將交通卡和 eMoney 卡加入到 Apple 錢包](#)
- [Apple Messages for Business 安全性](#)
- [FaceTime 安全性](#)
- [iOS 中的汽車鑰匙安全性](#)
- [Apple Configurator 安全性](#)

移除主題：

- [HomeKit 配件和 iCloud](#)

## 2021 年 5 月

更新對象：

- [iOS 14.5](#)
- [iPadOS 14.5](#)
- [macOS 11.3](#)
- [tvOS 14.5](#)
- [watchOS 7.4](#)

新增主題：

- [配備 Touch ID 的巧控鍵盤](#)。
- [安全意圖以及與「安全隔離區」的連線](#)。
- [自動解鎖與 Apple Watch](#)。
- [CustomOS Image4 Manifest Hash \(coih\)](#)。

更新主題：

- [可使用備用電量的快速卡片](#)中新增兩種「快速模式」交易。
- 已編輯[安全隔離區功能摘要](#)。
- 已將軟體更新內容加入[安全多重開機 \(smb3\)](#)。
- [密封密鑰保護 \(SKP\)](#) 新增內容。

## 2021 年 2 月

### 更新對象：

- iOS 14.3
- iPadOS 14.3
- macOS 11.1
- tvOS 14.3
- watchOS 7.2

### 新增主題：

- 為 iBoot 加入記憶體安全機制
- 在配備 Apple 晶片的 Mac 上進行開機程序
- 配備 Apple 晶片的 Mac 所具備的開機模式
- 配備 Apple 晶片的 Mac 所提供的「啟動磁碟」安全性規則控制機制
- LocalPolicy 簽署密鑰的建立與管理
- 配備 Apple 晶片的 Mac 上的 LocalPolicy 檔案內容
- 簽署系統卷宗安全性
- Apple 安全研究裝置
- 密碼監視
- IPv6 安全性
- iOS 中的汽車鑰匙安全性

### 更新主題：

- 安全隔離區
- 硬體麥克風斷線功能
- 採用 Intel 架構的 Mac 所適用的 RecoveryOS 和診斷環境
- Mac 電腦的直接記憶體存取保護
- 在 macOS 中安全延伸核心
- 系統完整保護
- watchOS 的系統安全性
- 在 macOS 中管理檔案保險箱
- App 對已儲存密碼的存取權限
- 密碼安全性建議
- Apple Cash 安全性
- Apple Messages for Business 安全性
- Wi-Fi 隱私權
- 啟用鎖定安全性
- Apple Configurator 安全性

## 2020 年 4 月

更新對象：

- iOS 13.4
- iPadOS 13.4
- macOS 10.15.4
- tvOS 13.4
- watchOS 6.2

更新內容：

- iPad 麥克風斷線功能已新增至**硬體麥克風斷線功能**。
- Data Vault 已新增至**保護 App 對使用者資料的存取**。
- 在 **macOS 中管理檔案保險箱**以及命令列工具更新。
- 在 **macOS 中防禦惡意軟體**中新增「惡意軟體移除工具」。
- 已更新 **iPadOS 中「共享的 iPad」安全性**。

## 2019 年 12 月

合併 iOS 安全性指南、macOS 安全性概覽和 Apple T2 安全晶片概覽

更新對象：

- iOS 13.3
- iPadOS 13.3
- macOS 10.15.2
- tvOS 13.3
- watchOS 6.1.1

已移除隱私權控制、Siri 和 Siri 建議，以及 Safari 智慧型防追蹤。請參訪 <https://www.apple.com/tw/privacy/> 以取得這些功能的最新資訊。

## 2019 年 5 月

針對 iOS 12.3 進行更新

- 支援 TLS 1.3
- 修訂 AirDrop 安全性的說明
- DFU 模式與復原模式
- 配件連線的密碼需求

## 2018 年 11 月

針對 iOS 12.1 進行更新

- 群組 FaceTime

## 2018 年 9 月

針對 iOS 12 進行更新

- 安全隔離區
- OS 完整保護
- 可使用備用電量的快速卡片
- DFU 模式與復原模式
- HomeKit 電視遙控器配件
- 感應式票卡
- 學生證
- Siri 建議
- Siri 的捷徑
- 「捷徑」App
- 使用者密碼管理
- 螢幕使用時間
- 安全性認證和計畫

## 2018 年 7 月

針對 iOS 11.4 進行更新

- 生物辨識政策
- HomeKit
- Apple Pay
- 商務聊天
- iCloud 雲端「訊息」
- Apple 商務管理

## 2017 年 12 月

針對 iOS 11.2 進行更新

- Apple Pay Cash



## 2017 年 10 月

針對 iOS 11.1 進行更新

- 安全性認證和計畫
- Touch ID/Face ID
- 共享的備忘錄
- CloudKit 端對端加密
- TLS 更新
- Apple Pay、在網站上使用 Apple Pay 付款
- Siri 建議
- 共享的 iPad

## 2017 年 7 月

針對 iOS 10.3 進行更新

- 安全隔離區
- 檔案資料保護
- Keybag
- 安全性認證和計畫
- SiriKit
- HealthKit
- 網路安全性
- 藍牙
- 共享的 iPad
- 遺失模式
- 啟用鎖定
- 隱私權控制

## 2017 年 3 月

針對 iOS 10 進行更新

- 系統安全性
- 資料保護類別
- 安全性認證和計畫
- HomeKit、ReplayKit、SiriKit
- Apple Watch
- Wi-Fi、VPN
- 單一登入
- Apple Pay、在網站上使用 Apple Pay 付款
- 信用卡、簽帳金融卡及預付卡佈建
- Safari 建議

## 2016 年 5 月

針對 iOS 9.3 進行更新

- 管理式 Apple ID
- Apple ID 雙重認證
- Keybag
- 安全性認證
- 遺失模式、啟用鎖定
- 安全備忘錄
- Apple 校務管理
- 共享的 iPad

## 2015 年 9 月

針對 iOS 9 進行更新

- Apple Watch 啟用鎖定
- 密碼原則
- Touch ID API 支援
- A8 上的資料保護使用 AES-XTS
- 自動軟體更新的 Keybag
- 認證更新
- 企業級 App 的信任模型
- Safari 書籤的資料保護
- App 傳輸安全性
- VPN 規格
- HomeKit 的 iCloud 遠端存取
- Apple Pay 酬賓卡、Apple Pay 發卡機構的 App
- Spotlight 裝置上索引編列
- iOS 配對模式
- Apple Configurator 2
- 取用限制

# 版權聲明

© 2024 Apple Inc. 保留一切權利。

在未經 Apple 書面同意的情況下將 Apple 標誌的字元符號用於商業用途 (可透過 Option + Shift + K 的鍵盤組合鍵輸入)，將違反美國聯邦和州法律，並構成侵犯商標權和公平競爭行為。

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、Find My、Handoff、HealthKit、HomeKit、HomePod、HomePod mini、iMac、iMac Pro、iMessage、iPad、iPadOS、iPad Air、iPad Pro、iPhone、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 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® 文字商標和標誌是 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。對於非 Apple 製造之產品相關資訊，或是非 Apple 控制或測試之獨立網站，不得解釋 Apple 為其推薦或背書。Apple 對於第三方網站或產品的選擇、效能或使用，概不負責。Apple 對於第三方網站的準確性或可靠性不具有任何立場。如需更多資訊，請聯絡廠商。

部分 App 不適用於部分地區。App 的供應狀況會有所變動。

TA028-00780