iOS 安全性

iOS 12.1

2018 年 11 月

目錄

第 5 頁 **簡介**

第 6 頁 **系統安全性**
安全啟動鏈
系統軟體授權
安全隔離區
作業系統完整保護
Touch ID
Face ID

第 12 頁 **加密與資料保護**
硬體安全性功能
檔案資料保護
密碼
資料保護類別
鑰匙圈資料保護
Keybag

第 20 頁 **App 安全性**
App 程式碼簽署
執行階段程序安全性
延伸功能
App 群組
App 中的資料保護
配件
HomeKit
SiriKit
HealthKit
ReplayKit
安全備忘錄
共享的備忘錄
Apple Watch

第 30 頁 **網路安全性**
TLS
VPN
Wi-Fi
藍牙
單一登入
AirDrop 安全性
Wi-Fi 密碼共享

第 36 頁 **Apple Pay**
Apple Pay 元件
Apple Pay 使用 Secure Element 的方式
Apple Pay 使用 NFC 控制器的方式
信用卡、金融卡及預付卡佈建
付款授權
因交易而異的動態安全碼

使用信用卡和金融卡在商店內付款
使用信用卡和金融卡在 App 內付款
使用信用卡和金融卡在網站上付款
感應式票卡
Apple Pay Cash
交通卡
學生證
停用、移除和清除卡片

第 44 頁　Internet 服務
Apple ID
iMessage
商務聊天
FaceTime
iCloud
iCloud 鑰匙圈
Siri
Safari 建議、搜尋中的「Siri 建議」、查詢字詞、# 影像、「新聞」App 和「新聞」小工具（非適用「新聞」國家或地區）
Safari 智慧型防追蹤

第 55 頁　使用者密碼管理
App 存取已儲存的密碼
自動使用高強度密碼
傳送密碼給其他人或裝置
憑證提供者延伸功能

第 57 頁　裝置控制
密碼保護
iOS 配對模式
設定強制執行
行動裝置管理（MDM）
共享的 iPad
Apple School Manager
Apple Business Manager
裝置註冊
Apple Configurator 2
監管
取用限制
遠端清除
遺失模式
啟用鎖定
螢幕使用時間

第 63 頁　隱私控制
定位服務
存取個人資料
隱私權政策

第 64 頁　安全性認證和計畫
ISO 27001 和 27018 憑證
加密編譯驗證（FIPS 140-2）
Common Criteria Certification（ISO 15408）
機密商業解決方案（CSfC）
安全性設定指南

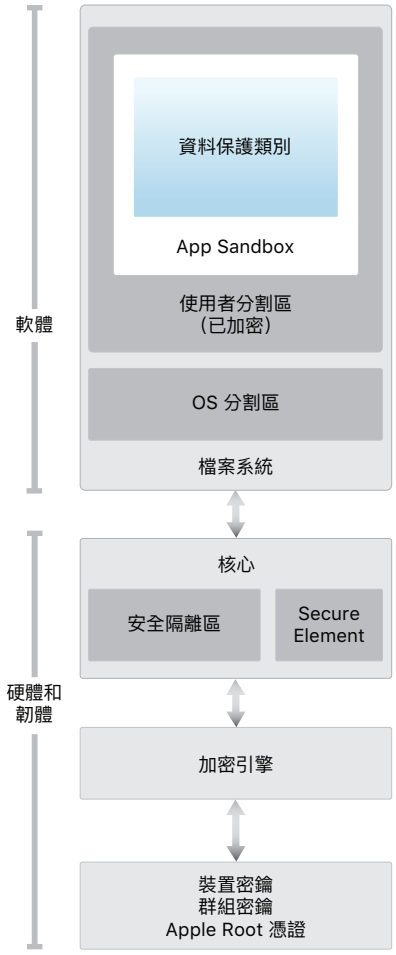
第 66 頁　Apple 安全性獎金

第 67 頁　結論
對安全性的承諾

第 68 頁　詞彙表

第 70 頁　文件版本記錄

簡介



iOS 的安全性架構圖提供視覺化的圖表概覽，以說明本文件中討論的各項技術。

Apple 所設計的 iOS 平台將安全性視為其核心訴求。當我們開始打造可能的最佳行動平台時，我們汲取數十年的經驗來建造一個全新的架構。我們考量了有關桌面系統環境的安全性風險，並在設計 iOS 時建立一套新方式來提升安全性。我們開發並整合創新功能，可加強行動安全性並從一開始便保護整個系統。因此，iOS 對行動裝置而言，在安全性上往前邁進了一大步。

軟體、硬體和服務在每台 iOS 裝置上緊密合作，一同為使用者提供最高的安全性和清楚明確的使用者體驗。iOS 不僅保護裝置和其中的靜態資料，同時也保護了整個生態系統，包含使用者在本機、網路上以及使用重要 Internet 服務所執行的所有操作。

iOS 和 iOS 裝置不僅提供進階的安全性功能，而且還容易使用。許多安全性功能預設便已啟用，因此 IT 部門無須進行繁複的設定。而如裝置加密之類的重要安全性功能則無法設定，因此可避免使用者不小心地停用這些功能。其他功能（如 Face 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。

本文件將詳細介紹 iOS 平台如何運用各種安全性技術與功能，並協助各個公司或機構在其本身的政策和程序中結合 iOS 平台安全性技術與功能，以滿足特定的安全性需求。

本文件主要分為以下幾個主題：

- **系統安全性**：iPhone、iPad 和 iPod touch 上經過整合且安全的軟硬體平台。
- **加密與資料保護**：若裝置遺失或遭竊，或有未經授權的人員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**：可讓 App 安全執行且不犧牲平台完整性的系統。
- **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。
- **Apple Pay**：Apple 的安全付款方式。
- **Internet 服務**：Apple 以網路為基礎的架構，提供傳訊、同步和備份等服務。
- **使用者密碼管理**：密碼取用限制和從其他授權的來源存取密碼。
- **裝置控制**：允許 iOS 裝置管理，防止在未經授權的情況下使用裝置，以及在裝置遺失或遭竊時可進行遠端清除的方式。
- **隱私控制**：iOS 中可用來控制「定位服務」與使用者資料存取權的功能。
- **安全性認證和計畫**：ISO 憑證、加密編譯驗證、Common Criteria Certification 和機密商業解決方案（CSfC）的相關資訊。

系統安全性

進入裝置韌體升級（DFU）模式

在裝置進入 DFU 模式（亦稱為復原模式）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。

首先使用 USB 接線將裝置連接至電腦。

然後依照所用裝置執行以下操作：

iPhone X 或更新機型、iPhone 8 或 iPhone 8 Plus。按下調高音量按鈕並快速放開。按下調低音量按鈕並快速放開。按住側邊按鈕，然後再次按下調低音量按鈕。5 秒後放開側邊按鈕，並繼續按住調低音量按鈕，直到出現復原模式畫面。

iPhone 7 或 iPhone 7 Plus。同時按住側邊按鈕和調低音量按鈕，放開側邊按鈕，並繼續按住調低音量按鈕，直到出現復原模式畫面。

iPhone 6s 和較舊機型、iPad 或 iPod touch。同時按住主畫面按鈕和頂部（或側邊）按鈕，放開頂部（或側邊）按鈕，並繼續按住主畫面按鈕，直到出現復原模式畫面。

注意：裝置處於 DFU 模式時，螢幕上不會顯示任何內容。若顯示 Apple 標誌，表示按住側邊按鈕或睡眠 / 喚醒按鈕的時間過長。

系統安全性旨在確保每部 iOS 裝置的所有核心元件都能為軟體和硬體提供安全保護。這包含啟動程序、軟體更新和「安全隔離區」。此架構是 iOS 安全性的核心，並不會影響裝置的正常使用。

iOS 裝置的硬體、軟體和服務經過緊密的整合，可確保系統的每個元件獲得信任，並對系統整體進行驗證。從初次啟動到 iOS 軟體更新、再到第三方的 App，每個步驟都經過分析和審查，以確保硬體和軟體以最佳方式搭配執行，並適當地使用資源。

安全啟動鏈

啟動程序中每個步驟包含的元件都經過 Apple 加密編譯簽署以確保其完整性，且只有在驗證信任鏈結後，每個步驟才能繼續。這包含啟動程式、核心、核心延伸功能和基頻韌體。此安全啟動鏈有助於確保底層的軟體未經竄改。

開啟 iOS 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 CA 公用密鑰，該公用密鑰用來驗證 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確保下一個步驟經由 Apple 簽署。當 iBoot 完成其任務後，便會驗證和執行 iOS 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。

開機 ROM 載入 LLB（在較舊的裝置上）或 iBoot（在較新的裝置上）失敗會導致裝置進入 DFU 模式。若 LLB 或 iBoot 無法載入或驗證下一個程序，便會暫停啟動，並在裝置螢幕上顯示「連接 iTunes」畫面。此過程稱為復原模式。在這兩種情況下，裝置都必須透過 USB 連接 iTunes，並回復到出廠預設值。

「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：

- **復原模式**：在配備 Apple A10、S2 和較新**晶片式系統（SoC）**的裝置上透過 iBoot 設定
- **DFU 模式**：在配備 A12 SoC 的裝置上透過開機 ROM 設定

如需更多資訊，請參閱本白皮書的「加密與資料保護」章節。

在具有行動數據連線功能的裝置上，基頻子系統也會利用其類似的安全啟動程序，包含已簽署的軟體以及由基頻處理器驗證的密鑰。

「安全隔離區」副處理器也會利用安全啟動程序，以確保其獨立的軟體經過 Apple 驗證和簽署。請參閱本白皮書的「安全隔離區」章節。

如需更多手動進入復原模式的相關資訊，請前往：
support.apple.com/zh-tw/HT201263

系統軟體授權

Apple 會定期釋出軟體更新以解決新產生的安全性問題，同時提供新功能；這些更新會同時提供給所有受支援的裝置。使用者會在裝置上和透過 iTunes 收到 iOS 更新通知，而更新項目可透過無線方式傳送，以鼓勵使用者可儘快採用最新的安全性修正。

上述的啟動程序有助於確保裝置上只能安裝 Apple 簽署的程式碼。為了避免裝置降級到缺少最新安全性更新的較舊版本，iOS 使用了名為「系統軟體授權」的程序。若可將裝置降級，攻擊者一旦有了裝置的擁有權，便會安裝較舊版本的 iOS 並利用舊版本中尚未修復的漏洞進行破壞。

在配備「安全隔離區」的裝置上，「安全隔離區」副處理器也會利用「系統軟體授權」來確保軟體的完整性，並阻止降級的安裝作業。請參閱本白皮書的「安全隔離區」章節。

iOS 軟體更新可使用 iTunes 安裝，或在裝置上採用無線方式（OTA）進行安裝。若使用 iTunes，系統會下載並安裝一份完整的 iOS。若採用 OTA 方式安裝軟體更新，系統將只會下載完成更新所需的元件（而非下載整套 OS），以改善網路效率。此外，在執行 macOS High Sierra 並開啟「內容快取」的 Mac 上可以快取軟體更新，iOS 裝置便無需透過 Internet 重新下載所需的更新。iOS 裝置仍需聯絡 Apple 伺服器以完成更新程序。

在 iOS 升級期間，iTunes（若採用 OTA 軟體更新方式，則為裝置本身）會連接 Apple 安裝授權伺服器，並向其傳送以下資料：要安裝之安裝套件中的各部分加密編譯測量值列表（如 iBoot、核心及 OS 映像檔）、隨機反重播的值（隨機數）以及裝置獨屬的唯一 **Exclusive Chip Identification（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，是否與該簽名所涵蓋的內容相符。這些步驟可確保授權是針對特定裝置進行，並且舊版 iOS 無法從一部裝置拷貝到另一部裝置。隨機數可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。

安全隔離區

「安全隔離區」是內建於晶片式系統（SoC）的副處理器。它使用加密記憶體，並包含一個硬體亂數產生器。「安全隔離區」為 **「資料保護」** 密鑰管理提供所有加密編譯操作，即使在核心遭到入侵的情況下，也可維護「資料保護」的完整性。系統會將「安全隔離區」與應用程式處理器之間的通訊隔離到一個以中斷驅動的信箱和共享的記憶體資料緩衝區中。

「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。

「安全隔離區」會根據 Apple 自定版本的 L4 微核心執行「安全隔離區作業系統」。此「安全隔離區作業系統」由 Apple 簽署，經由「安全隔離區開機 ROM」驗證，並透過個人化的軟體更新程序進行更新。

當裝置啟動時，「安全隔離區開機 ROM」會製作一個臨時記憶體保護密鑰，此密鑰與裝置的 UID 配合使用，用來對裝置記憶體空間的「安全隔離區」部分進行加密。除了在 Apple A7 以外，「安全隔離區」的記憶體也會透過記憶體保護密鑰來認證。在 A11 和較新型以及 S4 SoC 上，會透過儲存在 On-Chip SRAM 中的記憶體保護密鑰和隨機數來認證，使用整合樹狀結構來避免重播安全性關鍵「安全隔離區」記憶體。

由「安全隔離區」儲存到檔案系統的資料會藉由 UID 搭配使用的密鑰和反重播計數器來進行加密。反重播計數器是儲存在專用的非揮發性記憶體**積體電路（IC）**中。

在配備 A12 和 S4 SoC 的裝置上，「安全隔離區」 會與安全儲存區積體電路（IC）配對，以用於反重播計數器儲存。安全儲存區 IC 的設計包含無法更改的 ROM 程式碼、硬體亂數產生器、加密引擎，以及物理篡改偵測。為讀取和更新計數器，「安全隔離區」 和儲存區 IC 會利用安全通訊協定，以確保計數器的獨佔存取權。

針對會標示反重播界限的事件資料，會使用 「安全隔離區」 上的反重播服務來撤銷，包括但不限於以下內容：

- 變更密碼
- 啟用 / 停用 Touch ID 或 Face ID
- 加入 / 刪除指紋
- 重置 Face ID
- 加入 / 移除 Apple Pay 卡片
- 清除所有內容和設定

「安全隔離區」 也負責處理來自 Touch ID 和 Face ID 感應器的指紋和面孔資料，確定是否存在相符的資料後便代表使用者允許存取或購買。

作業系統完整保護

核心完整保護

iOS 核心完成初始化後，便會啟用 「核心完整保護」（KIP）以防止核心和驅動程式碼遭修改。**記憶體控制器**提供受保護的實體記憶體區域，並讓 **iBoot** 用來載入核心和核心延伸功能。開機完成後，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。此外，應用程式處理器的 「記憶體管理單元」（MMU）已設定為防止從受保護記憶體區域外的實體記憶體對應特權碼，以及防止核心記憶體區域內的實體記憶體可寫入對應。

用於啟用 KIP 的硬體會在開機程序完成後被鎖定，以防止重新設定。自 Apple A10 和 S4 起的 SoC 可支援 KIP。

系統副處理器完整保護

系統副處理器是位於與應用程式處理器相同 SoC 上的 CPU。系統副處理器具有特定的用途，iOS 核心會委派許多作業給系統副處理器。範例包含：

- 安全隔離區
- 影像感測器處理器
- 動作副處理器

由於副處理器韌體需處理許多重要系統作業，其安全性是整體系統安全的關鍵。

系統副處理器完整保護（SCIP）會使用與核心完整保護相似的機制來防止副處理器韌體遭修改。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管理單元，以防以下情況：

- 受保護的記憶體區域部分外的可執行對應
- 防止受保護的記憶體區域部分內的可寫入對應

「安全隔離區作業系統」 負責於開機時設定 「安全隔離區」 的 SCIP。

用於啟用 SCIP 的硬體會在開機程序完成後被鎖定，以防止重新設定。自 A12 和 S4 起的 SoC 可支援 SCIP。

指標認證碼

指標認證碼（PAC）是用來防止利用記憶體損壞錯誤的攻擊。系統軟體和內建 App 會使用 PAC 來防止修改函式指標和傳回位址（程式碼指標）。此動作可使許多攻擊的難度提昇。例如，「返回導向程式設計」（ROP）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。

A12 和 S4 SoC 上可支援 PAC。

Touch ID

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

Face ID

只要看一眼，Face ID 便會安全地解鎖配備此功能的 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臉部幾何結構。Face ID 會使用神經網路來判斷螢幕注視、配對和防止造假，您便可以藉由注視螢幕來解鎖手機。Face ID 會自動適應您的外表變化，並嚴密地保護您的生物識別技術資料隱私與安全。

Touch ID、Face ID 和密碼

若要使用 Touch ID 或 Face ID，裝置設定必須為需要密碼以解鎖。當 Touch ID 或 Face ID 偵測到成功的配對時，您的裝置便會自動解鎖，使用者無須輸入裝置密碼。這讓使用更長、更複雜的密碼變得更為實用，因為您無須經常輸入密碼。Touch ID 和 Face ID 並不會取代您的密碼，而是在嚴密的界限和有限的時間內提供更簡便的方式來存取您的裝置。這一點很重要，因為安全性高的密碼是構成 iOS 裝置加密保護資料的基礎。

您可以隨時使用密碼來取代 Touch ID 或 Face ID，但以下操作一律需使用密碼而非生物辨識：

- 更新軟體。
- 清除裝置。
- 檢視或更改密碼設定。
- 安裝 iOS 設定描述檔。

若您的裝置處於以下狀態，也需要使用密碼：

- 裝置剛剛開機或重新啟動。
- 裝置未解鎖的時間超過 48 小時。
- 密碼在過去 156 小時（6 天半）未用來解鎖裝置，且過去 4 小時未使用生物辨識來解鎖裝置。
- 裝置收到了遠端鎖定指令。
- 嘗試生物辨識比對失敗五次後。
- 關機 / 啟動「SOS 緊急服務」後。

當 Touch ID 或 Face ID 啟用時，會在按下側邊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，Touch ID 和 Face ID 便需要成功的配對（或是選擇輸入密碼）。

人群中隨機一人可使用 Touch ID 解鎖您 iPhone 的機率為五萬分之一，使用 Face ID 則為百萬分之一。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。為了進一步保護您的裝置，Touch ID 和 Face ID 皆只允許五次配對失敗，其後便需要輸入密碼才能存取裝置。使用 Face ID 時，雙胞胎或長相與您相似的兄弟姊妹配對錯誤率不盡相同，13 歲以下孩童亦然（因為他們的獨特臉部特徵可能還尚未定型）。若您對此存有疑慮，Apple 建議您使用密碼來認證。

Touch ID 安全性

只有當主畫面按鈕周圍的電容金屬環偵測到手指觸摸時，指紋感應器才會作用，進而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」。處理器與 Touch ID 感應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，該區段密鑰是透過為每個出廠的 Touch ID 感應器和相應的「安全隔離區」佈建共享密鑰來進行交涉。共享密鑰安全性高、具隨機性，且每個 Touch ID 感應器的共享密鑰都不同。區段密鑰的交換會針對雙方使用 AES **密鑰封裝**，並提供一個用來建立作業階段密鑰和使用 AES-CCM 傳輸加密的隨機密鑰。

光柵掃描結果會暫時存放在 「安全隔離區」 加密的記憶體中，同時系統會對其進行向量化處理以便分析，然後便會刪除相關資料。此分析利用皮下**紋路流向角度的對應**，這是一種有損性的程序，會在分析完成後刪除用來重建使用者實際指紋的精細資料。最後產生的節點圖會以一種只能由「安全隔離區」讀取的加密格式進行儲存，其中不含任何身分資訊。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。

Face ID 安全性

Face ID 的設計用意為確認使用者的螢幕注視、提供配對錯誤率低的穩固認證方式，並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您的面孔：當您拿起配備 Face ID 的 Apple 裝置或點按螢幕來喚醒時；當這些裝置嘗試取得您的認證以顯示收到的通知時；或是當支援的 App 要求 Face ID 認證時。當偵測到面孔時，Face ID 會辨認您的眼睛是張開的並注視裝置，確認螢幕注視並進行解鎖；針對輔助使用功能，當啟用 「旁白」 時會停用此功能，並可在需要時個別停用。

確認偵測到注視螢幕的面孔後，原深感測相機會發出並讀取超過 30,000 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，經過數位簽署後傳送到 「安全隔離區」。為了防止數位和物理性造假，原深感測相機會隨機排序擷取到的一系列 2D 影像和深度圖，並發出裝置特定的隨機圖形。A11 和更新 SoC 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徵，並將這個表示式與登記的面孔資料進行比對。這個註冊的面孔資料本身是一個數學表徵，表示在您擺各種姿勢時捕捉到的面孔。

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，我們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 IR 和深度圖。Apple 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。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 iPhone X。

Face ID 資料 (包含您面孔的數學表徵) 經過加密，且僅供 「安全隔離區」 使用。此資料絕對不會流出裝置，不會傳送給 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：

- 登記期間對您的面孔進行計算所產生的數學表徵。
- 某幾次解鎖時對您的面孔進行計算所產生的數學表徵 (如果 Face ID 認為可用於增強未來比對效果)。

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

Touch ID 或 Face ID 如何解鎖 iOS 裝置

若 Touch ID 或 Face ID 已停用，在裝置鎖定時，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。除非輸入密碼來解鎖裝置，否則便無法存取該類別的檔案和**鑰匙圈**項目。

若 Touch ID 或 Face ID 已啟用，則不會在裝置鎖定時捨棄這些密鑰，而是透過提供給「安全隔離區」 中 Touch ID 或 Face ID 子系統的密鑰進行封裝。嘗試解鎖裝置時，若裝置偵測到成功的配對，它便會提供密鑰來解除封裝 「資料保護」 密鑰，裝置便會解鎖。此流程藉由要求 「資料保護」 和 Touch ID 或 Face ID 子系統合作來解鎖裝置，因此提供了額外的保護。

裝置重新啟動時，Touch ID 或 Face ID 解鎖裝置所需的密鑰便會喪失。在需要密碼時，若符合特定條件 (例如 48 小時內未解鎖或嘗試配對失敗達五次)，「安全隔離區」 便會捨棄這些密鑰。

為了改善解鎖效能，以及跟進您面孔和外貌的自然變化，Face ID 會逐漸增強它所儲存的數學表徵。成功解鎖時，如果新計算的數學表徵品質夠好，Face ID 可能會在捨棄該資料

前，使用它來進行有限次數的額外解鎖。相反地，如果 Face ID 無法辨識您，但是配對品質高於特定臨界值，且您在失敗後立即輸入密碼，Face ID 會再次捕捉面孔，並以新計算的數學表徵增強登記的 Face ID 資料。如果您停止用這筆新 Face ID 資料進行配對，以及在進行有限次數的解鎖後，系統便會捨棄這筆資料。這些增強程序可讓 Face ID 跟進您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。

Touch ID、Face ID 和 Apple Pay

Touch ID 和 Face ID 也可以搭配 Apple Pay 使用，方便您在商店、App 內和網路上輕鬆且安全地進行購買。如需更多 Touch ID 和 Apple Pay 的相關資訊，請參閱本白皮書的「Apple Pay」章節。

若要使用 Face ID 授權店內付款，您必須先按兩下側邊按鈕確認付款意圖，然後便可使用 Face ID 進行授權，再將 iPhone X 靠近非接觸式付款讀取器。Face ID 認證後若想選擇其他 Apple Pay 付款方式，則需要重新認證，但是不需要再按兩下側邊按鈕。

若要在 App 內和網路上付款，必須先按兩下側邊按鈕確認付款意圖，然後使用 Face ID 進行認證以授權付款。如果您沒有在按兩下側邊按鈕後 30 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。

Face ID 診斷

Face ID 資料不會流出裝置，且絕不會備份到 iCloud 或其他任何地方。只有在您希望將 Face ID 診斷資料提供給 AppleCare 以取得支援的情況下，才會將這些資訊從您的裝置傳出。啟用「Face ID 診斷」時需使用 Apple 的數位簽署授權，這個授權類似用於軟體更新個人化程序的授權。完成授權後，您就能啟用「Face ID 診斷」，並在支援 Face ID 的裝置上前往「設定」App 開始設定程序。

設定「Face ID 診斷」時，系統會刪除您的 Face ID 登記，並要求您重新登記 Face ID。接下來 10 天內，支援 Face ID 的裝置會開始記錄嘗試認證時捕捉的 Face ID 影像；這段期間過後裝置便會自動停止儲存影像。「Face ID 診斷」不會自動傳送資料給 Apple，傳送給 Apple 之前，您可以審閱和核准在診斷模式下收集的「Face ID 診斷」資料，包含登記和解鎖影像（失敗與成功的影像）在內。「Face ID 診斷」只會上傳經過您核准的「Face ID 診斷」影像。上傳前會先將資料加密，並在上傳完成後立即從裝置上刪除。您拒絕的影像會在當下刪除。

若您沒有藉由審閱影像並上傳任何核准的影像來結束「Face ID 診斷」作業階段，「Face ID 診斷」會在 40 天後自動結束，且所有診斷影像都會從您的裝置上刪除。您也可以隨時停用「Face ID 診斷」。一旦停用，系統會立即刪除所有本機影像，此情況下將不會與 Apple 共享任何 Face ID 資料。

Touch ID 和 Face ID 的其他用途

第三方 App 可使用系統提供的 API 來要求使用者透過 Touch ID 或 Face 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 Touch ID 或 Face ID 時，App 只會收到認證是否成功的通知，無法存取 Touch ID、Face ID 或已登記之使用者的相關資料。Touch ID 或 Face ID 也可用來保護鑰匙圈項目，只有在「安全隔離區」比對成功或裝置密碼正確時才將它們釋出。要求以 Touch ID 或 Face 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 開發者可執行以下操作：

- 要求認證 API 操作可以不再依賴 App 密碼或裝置密碼。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 Touch ID 或 Face ID 當作第二個驗證條件。
- 在「安全隔離區」內產生和使用可由 Touch ID 或 Face ID 保護的 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。

您也可對 Touch ID 或 Face ID 進行設定，以核准從 iTunes Store、App Store 和 Apple Books 購買項目，因此無須輸入 Apple ID 密碼。在 iOS 11 或以上版本上，透過簽署商店要求，受 Touch ID 和 Face ID 保護的「安全隔離區」ECC 密鑰可用來授權購買行為。

加密與資料保護

清除所有內容和設定
「設定」 中的 「清除所有內容和設定」 選項會清除 Effaceable Storage（可抹除儲存空間）中的所有密鑰，導致無法透過加密編譯技術取得裝置上的所有使用者資料。因此，若要將裝置送給別人或送修，此選項便是移除所有個人資訊的理想方式。

重要事項：除非裝置已備份，否則請勿使用「清除所有內容和設定」 選項，因為清除的資料無法復原。

安全啟動鏈、程式碼簽署及執行階段程序安全性，都有助於確保只有受信任的程式碼與 App 可在裝置上執行。iOS 還有其他加密與資料保護功能可保護使用者資料的安全，即使安全性基礎架構的其他部分遭到破壞（例如，在裝置上發生未經授權的修改）仍可予以保護。這對於使用者與 IT 管理者都大有助益，可隨時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。

硬體安全性功能

在行動裝置上，速度與能源效率十分重要。加密編譯操作非常複雜，若在設計與導入時未考慮到這些重要因素，可能會帶來一些效能或電池續航力的問題。

每部 iOS 裝置都配備專屬的 AES-256 加密引擎，其內建於快閃儲存空間與主系統記憶體間的 DMA 路徑中，可讓檔案加密具備高度效率。在 A9 或以上版本 A 系列處理器上，快閃儲存子系統位於獨立的匯流排上，且透過 DMA 加密引擎僅獲得記憶體（其中包含使用者資料）的存取權。

裝置的**唯一識別碼（UID）**與裝置**群組識別碼（GID）**是 AES-256 位元的密鑰，該密鑰已在製作過程中融入（UID）或編譯（GID）到應用程式處理器和 「安全隔離區」 中。任何軟體或韌體都無法直接讀取；只能將 UID 或 GID 用作密鑰，以便查看由矽晶片中建置的專屬 AES 引擎所執行加密或解密操作的結果。應用程式處理器和 「安全隔離區」 都有各自的 UID 和 GID。「安全隔離區」 的 UID 和 GID 只能由 「安全隔離區」 專屬的 AES 引擎使用。UID 和 GID 也無法透過**聯合測試工作群組（JTAG）**或其他除錯介面來使用。

但 Apple A8 和較早的 SoC 不在此限，每個 「安全隔離區」 會在製造過程中自行產生 UID（唯一識別碼）。由於每部裝置的 UID 都是唯一的，且完全是在「安全隔離區」內產生，而非在裝置外的製造系統中產生，因此 Apple 或其他供應商都無法存取或儲存 UID。

在 「安全隔離區」 上執行的軟體可利用 UID 來保護限定於特定裝置的密鑰。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，因此若將記憶體晶片實際從一部裝置移至另一部裝置，檔案則無法存取。UID 與裝置上的任何其他識別碼並不相關。

GID 對同一類別的裝置（例如使用 Apple A8 處理器的所有裝置）的所有處理器是通用的。

除了 UID 和 GID 外，所有其他加密編譯密鑰都是由系統的亂數產生器（RNG）使用以 CTR_DRBG 原始碼為基礎的演算法製作。系統熵是在啟動期間從時間變化以及裝置啟動後從中斷時間來產生的。在 「安全隔離區」 內產生的密鑰會使用其真正的硬體亂數產生器，透過以 CTR_DRBG 處理的多個環型振盪器製作而成。

安全清除儲存的密鑰與產生它們具有同等重要性。在快閃儲存空間上執行此項操作尤其具挑戰性，例如耗損平衡（wear-leveling）可能意味著需要清除多份資料拷貝。為了解決此問題，iOS 裝置內建一種專門用於安全清除資料的功能，稱為 **Effaceable Storage**。此功能利用基礎儲存技術（如 NAND）直接在極低的層次上進行定址和清除小量區塊。

快速交通卡與省電模式

如果 iOS 因為 iPhone 需要充電而未運作，電池中可能仍有足夠的電力以支援 「快速交通卡」 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」 設計的交通卡
- 開啟 「快速模式」 的學生證

按下側邊按鈕會顯示電力不足的圖像，以及表示可使用「快速交通卡」的文字。與 iOS 運作時的情況相同，NFC 控制器仍會執行「快速交通卡」交易，差別在於交易只會以觸覺通知表示。螢幕不會顯示通知。

若是由使用者執行的標準關機，此功能則不會運作。

檔案資料保護

除了 iOS 裝置內建的硬體加密功能，Apple 也使用名為「資料保護」的技術，來進一步保護裝置上快閃記憶體中儲存的資料。「資料保護」可讓裝置回應如來電之類的常見事件，也可以對使用者資料啟用較高層次的加密。「訊息」、「郵件」、「行事曆」、「聯絡資訊」、「照片」和「健康」資料值等主要系統 App 預設都會使用「資料保護」，而安裝於 iOS 7 或以上版本上的第三方 App 可自動獲得此項保護措施。

「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 iOS 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「Apple 檔案系統」(APFS) 的誕生，檔案系統現在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）。

架構概覽

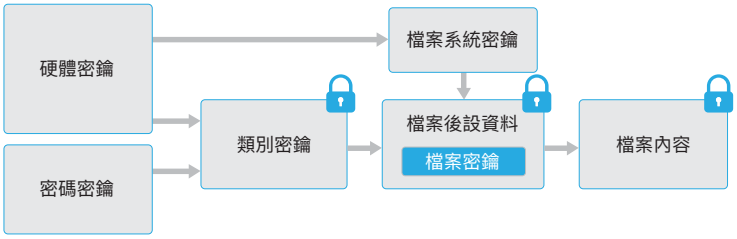
每次在資料分割區上製作檔案時，「資料保護」都會製作一個新的 256 位元密鑰（「檔案專屬」密鑰），並將其提供給硬體 AES 引擎，此引擎會使用該密鑰採用 AES-XTS 模式對寫入快閃記憶體的檔案進行加密。在配備 A7、S2 或 S3 SoC 的裝置上，會使用 AES-CBC。初始化向量使用檔案的區塊偏移量進行計算，它使用**檔案專屬密鑰**的 SHA-1 雜湊進行加密。

依據每個檔案的可存取性情況，檔案（或範圍）專屬密鑰會使用其中一個類別密鑰進行封裝。就像所有其他封裝一樣，這會使用 NIST AES 密鑰封裝、依據 RFC 3394 來執行。封裝的檔案專屬密鑰會儲存在檔案的後設資料中。

以「Apple 檔案系統」格式執行的裝置可能支援檔案複製功能（使用拷貝時寫入技術的零成本拷貝）。檔案複製後，複本的每一半會各自獲得一個用於接受傳入寫入的新密鑰，以便透過新密鑰將新資料寫入媒體。隨著時間推移，檔案可能會包含分別對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，該引擎會在從快閃記憶體中讀取檔案時，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；檔案密鑰永遠不會直接提供給應用程式處理器。在開機時，「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。

檔案系統中所有檔案的後設資料都使用隨機密鑰進行加密，該密鑰是在首次安裝 iOS 或使用者清除裝置時製作而成。在支援「Apple 檔案系統」的裝置上，系統會以「安全隔離區」UID 密鑰封裝檔案系統後設資料密鑰，以利長期儲存。與檔案或範圍專屬密鑰相同，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 Effaceable Storage 中的「無法清除的密鑰」，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機密性，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 MDM 解決方案、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。

密碼

密碼考量事項

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。

藉由設定裝置密碼，使用者可以自動啟用「資料保護」。iOS 支援六位數、四位數和任意長度的英數字元密碼。除了用於解鎖裝置外，密碼還為特定加密密鑰提供熵。這表示攻擊者即使拿到裝置，在沒有密碼的情況下也無法存取特定保護類別中的資料。

密碼與裝置的 UID 之間有關聯性，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。這意味著需要 5 年半的時間才能試完 6 位英數字元密碼的所有組合。

密碼嘗試次數間的延遲

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

使用者密碼的強度越高，加密密鑰就越堅固。Touch ID 和 Face ID 可用來提升這樣的因果關係，因為它可以讓使用者製作一個比實用密碼安全性更高的密碼。這增加了對用於「資料保護」的加密密鑰進行保護的密碼強度，而且不會對一天中多次解鎖 iOS 裝置的使用者體驗產生負面影響。

為了進一步阻止暴力密碼的破解攻擊，系統會延長在鎖定畫面上輸入無效密碼後的延遲時間。若「設定」>「Touch ID 與密碼」>「清除資料」已開啟，裝置將會在嘗試輸入密碼錯誤 10 次後自動清除。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 MDM 解決方案和 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」副處理器會強制執行延遲。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。

為提昇安全性並兼顧可用性，若使用者最近未使用過 USB，iOS 11.4.1 或以上版本需要 Touch ID、Face ID 或密碼輸入才能啟用 USB 介面。這可消除實體連接裝置（例如惡意充電器）的攻擊面，但仍可在合理的時間限制內啟用 USB 配件的用途。若 iOS 裝置鎖定或拔除 USB 接線超過一小時，裝置便不會允許建立任何新連線，直到裝置解鎖。這一小時間：

- 可確保經常連接 Mac 或 PC、USB 配件或有線 CarPlay 的使用者無需在每次連接裝置時輸入密碼。
- 是必要的，因為 USB 配件生態系統並未提供可靠的方式能在建立連線前識別配件。

此外，在 iOS 12 上，如果建立 USB 連線超過三天，裝置會在鎖定後立即拒絕新的 USB 連線。此用意為替不常使用此類連線的使用者增加防護。當裝置處於需要密碼以重新啟用生物辨識認證的狀態時，USB 連線也會被停用。

使用者可以在「設定」中選擇重新啟用永久 USB 連線，設定部分輔助裝置時會自動執行此操作。

DFU 與復原模式

在配備 Apple A10、A11 和 S3 SoC 的裝置上，無法從 「復原模式」 存取受使用者密碼保護的類別密鑰。A12 和 S4 SoC 將此保護擴展到 DFU 模式。

「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數中以建立其他密鑰階層。

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 A12 SoC 上，如果應用程式處理器已進入 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，以防存取受使用者密碼保護的資料。

在 Apple A10、A11、S3 和 S4 SoC 上，如果裝置已進入復原模式，則密碼種子位元會由 「安全隔離區作業系統」 鎖定。「安全隔離區開機 ROM」 和 「安全隔離區作業系統」都會檢查 「開機進度暫存器」 以安全地判定目前的模式。

資料保護類別

在 iOS 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。

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 Touch ID 或 Face ID 解鎖裝置時，才可以存取此類別中的所有資料。

未打開檔案的保護

（`NSFileProtectionCompleteUnlessOpen`）：裝置鎖定時可能需要寫入某些檔案。其中一個不錯的例子是在背景下載的電子郵件附件。此行為是藉由使用非對稱橢圓曲線加密技術（Curve25519 的 ECDH）來達成。一般的檔案專屬密鑰則是使用 One-Pass Diffie-Hellman Key Agreement（如 NIST SP 800-56A 中所述）所衍生的密鑰加以保護。

該協議的臨時公用密鑰與封裝的檔案專屬密鑰一起儲存。KDF 是鏈結密鑰衍生函數（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。SHA-256 則用於雜湊函數。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。

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。

無保護

（`NSFileProtectionNone`）：此類別密鑰僅受到 UID 的保護，並且儲存在 Effaceable Storage 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 裝置上的所有資料一樣）。

資料保護類別密鑰

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)
類別 D	無保護	(NSFileProtectionNone)

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，如密鑰和登入代號。iOS 鑰匙圈提供了儲存這些項目的安全方式。

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（祕密金鑰）。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）會以祕密金鑰加密。後設資料密鑰受「安全隔離區」處理器保護，但會從應用程式處理器中快取，以允許快速查詢鑰匙圈。秘密金鑰一律需要在「安全隔離區」處理器中來回。

鑰匙圈是以儲存在檔案系統中的 SQLite 資料庫的方式導入。只有一個資料庫，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。管理方式是要求第三方 App 使用存取群組，並使用透過 Apple Developer Program（Apple 開發者計畫）或透過應用程式群組來為其分配前置碼。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（Apple 開發者計畫）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，但使用的密鑰不同，所屬 API 的名稱也不同。

可用性	檔案資料保護	鑰匙圈資料保護
未鎖定時	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
鎖定時	NSFileProtectionCompleteUnlessOpen	N/A
首次解鎖後	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
總是	NSFileProtectionNone	kSecAttrAccessibleAlways
密碼已啟用	N/A	kSecAttrAccessible WhenPasscodeSetThisDeviceOnly

利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，然而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；它們：

- 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。

鑰匙圈項目的元件

除了存取群組，每個鑰匙圈項目還包含管理後設資料（如「製作時間」和「上次更新時間」的時間戳記）。

其中也包含屬性的 SHA-1 雜湊，用來查詢項目（如帳號和伺服器名稱），以在無須解密每個項目的情況下即可進行查找。最後，它還包含加密資料，其中包括下列項目：

- 版本編號
- 連線權限控制列表（ACL）資料
- 指出項目所屬保護類別的值
- 以保護類別密鑰加以封裝的項目專屬密鑰
- 描述項目的屬性字典（傳遞到 SecItemAdd），編碼為二進位 plist 並使用項目專屬密鑰加密

在 GCM（Galois/Counter Mode）模式下加密為 AES-256；存取群組會納入屬性中，並受加密期間計算的 GMAC 標記保護。

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 需要這些資訊的時間來選擇鑰匙圈類別，妥善地在安全性與可用性之間取得平衡。例如，VPN 憑證必須隨時可供使用，這樣裝置才能保持連續的連線，但 VPN 憑證屬於「不可遷移」類別，因此無法將其移至另一部裝置。

對於 iOS 所製作的鑰匙圈項目，將會強制執行下列類別保護：

項目	可存取
Wi-Fi 密碼	首次解鎖後
郵件帳號	首次解鎖後
Exchange 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」廣播加密密鑰	首次解鎖後
iCloud 代號	首次解鎖後
家人共享密碼	未鎖定時
「尋找我的 iPhone」代號	總是
語音信箱	總是
iTunes 備份	解鎖時，不可遷移
Safari 密碼	未鎖定時
Safari 書籤	未鎖定時
VPN 憑證	總是，不可遷移
Bluetooth® 密鑰	總是，不可遷移
Apple 推播通知服務代號	總是，不可遷移
iCloud 憑證和專用密鑰	總是，不可遷移
iMessage 密鑰	總是，不可遷移
由設定描述檔所安裝的憑證和專用密鑰	總是，不可遷移
SIM PIN	總是，不可遷移

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，方法是指定使用 Touch ID、Face 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 Touch ID 或 Face 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。

Keybag

檔案和「鑰匙圈資料保護」類別的密鑰會收集在 Keybag 中加以管理。iOS 使用下列 Keybag：使用者、裝置、備份、託管和「iCloud 備份」。

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。它是儲存在「無保護」類別中的二進位屬性列表（.plist）檔案，其內容是使用 Effaceable Storage 中儲存的密鑰來加密。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。`AppleKeyStore` 核心延伸功能會管理使用者 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 是用來儲存操作相關裝置特定資料的封裝類別密鑰。設定為共用的 iOS 裝置有時候需要存取憑證，才能讓使用者登入，因此需要未受使用者密碼保護的 Keybag。iOS 不支援使用者專屬檔案系統內容的加密編譯區分，即系統將使用來自裝置 Keybag 的類別密鑰來封裝檔案專屬密鑰。不過，鑰匙圈會使用來自使用者 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 iOS 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 是在 iTunes 進行加密備份時製作，其儲存在裝置進行備份的電腦中。新 Keybag 是使用一組新的密鑰製作而成，備份的資料會以這些新密鑰來重新加密。如前面所述，不可遷移的鑰匙圈項目仍會使用 UID 衍生的密鑰加以封裝，以使其可以回復到最初備份它們的裝置，但在其他裝置上則無法存取。

系統會使用 iTunes 中設定的密碼來保護 Keybag，其執行了一千萬次 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 iTunes 備份，那麼無論備份檔案屬於哪一種 「資料保護」 類別，備份檔案都不會加密，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 會用於 iTunes 同步和行動裝置管理（MDM）。此 Keybag 允許 iTunes 執行備份和同步，使用者無須輸入密碼，它還允許 MDM 解決方案遠端清除使用者密碼。它儲存在用來與 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，在該期間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 iTunes 時，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。這就是重新啟動後首次使用 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。它們會使用來自「安全隔離區」 中單調計數器目前值所衍生的密鑰、Keybag 的 UUID 和 「安全隔離區」 的 UID 來進行加密。

在 「安全隔離區」 中增加 「一次性解鎖代號」 計數器的數字會使任何現有的代號失效。在使用代號時、重新啟動裝置的第一次解鎖後、（由使用者或系統）取消軟體更新時或代號的規則計時器到期時，計數器都會遞增。

手動軟體更新的「一次性解鎖代號」會在 20 分鐘後到期。此代號可從「安全隔離區」輸出，並寫入 Effaceable Storage 中。若裝置在 20 分鐘內未重新開機，規則計時器會遞增計數器。

系統會在以下情況偵測到有可用更新時執行自動軟體更新：

- 已在 iOS 12 中設定自動更新。

  或者

- 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」，並在接下來解鎖時重新建立。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 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），因此可以在背景執行 iCloud 備份。對於 「無保護」 以外的所有 「資料保護」 類別，加密的資料會從裝置中讀取並傳送至 iCloud。對應的類別密鑰會以 iCloud 密鑰加以保護。鑰匙圈類別的密鑰會使用 UID 衍生的密鑰進行封裝，方式與未加密的 iTunes 備份相同。非對稱式 Keybag 也可用於 「iCloud 鑰匙圈」 其相關鑰匙圈復原作業的備份中。

App 安全性

App 是現代行動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。

有鑑於此，iOS 提供了多重保護來確保 App 經過簽署和驗證，且以 Sandbox 技術限制，進而保護使用者資料。這些要素為 App 提供了穩定且安全的平台，讓成千上萬的開發者能夠在 iOS 上提供數十萬款的 App，而不會影響系統的完整性。使用者可以在其 iOS 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。

App 程式碼簽署

iOS 核心啟動後，它將控制可執行哪些使用者程序和 App。為了確保所有 App 均來自核准的已知來源且未經竄改，iOS 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。

若要在 iOS 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 開發者計畫）。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，以確保它們可以如所述方式執行，且沒有明顯的程式錯誤或其他問題。除了已討論過的技術外，此挑選過程還會讓客戶對所購買的 App 的品質更加放心。

iOS 允許開發者將程式框架嵌入 App 中，以便供 App 本身或 App 內嵌入的延伸功能使用。為了保護系統並防止其他 App 在其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名驗證。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，或其程式碼簽名中具有相同團隊識別碼的資源庫平台來成為主要執行檔。因為作為系統一部分發佈的可執行檔不具有團隊識別碼，所以它們只能連結到隨系統本身發佈的資源庫。

企業也可以編寫供組織內部使用的企業內部 App，並分發給員工。企業和組織可以使用 D-U-N-S 編號申請加入 Apple Developer Enterprise Program（ADEP，Apple 開發者企業計畫）。Apple 會在驗證申請者的身分和資格後核准其要求。組織成為 ADEP 的成員後，便可以註冊以獲得一個「佈建描述檔」，該描述檔允許企業內部 App 在其授權的裝置上執行。使用者必須安裝「佈建描述檔」才能執行企業內部 App。這可以確保只有組織要求的使用者能夠將 App 載入到其 iOS 裝置上。透過 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。第一次啟動任一企業級 App 時，裝置必須從 Apple 收到允許執行 App 的肯定確認。

與其他行動平台不同，iOS 不允許使用者安裝來自網站可能有惡意性質且未經簽署的 App，或者執行不受信任的程式碼。執行時，會在載入所有可執行記憶體頁面後對其進行程式碼簽名檢查，以確保 App 自安裝或上次更新後未遭修改過。

執行階段程序安全性

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

所有第三方的 App 均會以 Sandbox 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。這樣可以防止 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 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 保持區隔。iOS 的大部分操作與所有第三方的 App 一樣，以非特殊權限使用者「mobile」的身分執行。整個作業系統分割區都裝載為唯讀。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 本身。

系統使用宣告的授權來控制第三方 App 對使用者資訊與功能（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。授權已經過數位簽署，因此無法更改。系統 App 和服務程式廣泛使用授權來執行特定權限的操作，如果不使用授權，則需要以根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（ASLR）可防止利用記憶體損壞錯誤的攻擊。內建 App 會使用 ASLR 來確保啟動時隨機安排所有記憶體區域。藉由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，便降低遭到許多複雜攻擊的可能性。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 作為 iOS 開發環境，可自動編譯啟用了 ASLR 支援的第三方 App。

iOS 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 對其 JavaScript JIT 編譯器使用了此功能。

延伸功能

iOS 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。系統會在安裝時自動偵測延伸功能，並讓使用相符系統的其他 App 使用這些延伸功能。

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。擴充點有「今天」小工具、「分享」、「自定」動作、「照片編輯」、「文件提供程式」和「自定鍵盤」。

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 Sandbox 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 對隱私控制具有相同的存取權限。因此，若使用者對 App 授予「聯絡資訊」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。

自定鍵盤是一種特殊類型的延伸功能，因為是由使用者啟用並適用於整個系統。一旦啟用後，該鍵盤延伸功能將會用於所有的文字欄位，但密碼輸入和任何安全文字的顯示方式除外。為了限制使用者資料的傳送，在預設情況下自定鍵盤是在一個十分受限的 Sandbox 中執行，該 Sandbox 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。自定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 Sandbox 中執行延伸功能。

對於在 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」規則。例如，MDM 解決方案可阻止使用者將受管理 App 中的文件輸出到未受管理的「文件提供程式」，或阻止他們在受管理的 App 中使用未受管理的鍵盤。此外，App 開發者可避免在其 App 中使用第三方的鍵盤延伸功能。

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）可保證「App 群組 ID」在整個 App 生態系統中是唯一的。

App 中的資料保護

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，協助確保在 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）、「聯絡資訊」、「提醒事項」、「備忘錄」、「訊息」和「照片」會導入「資料保護」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」。

配件

Made for iPhone, iPad, and iPod touch（MFi）授權計畫允許經過審查的配件製造商存取 iPod Accessories Protocol（iAP）和必要的支援硬體元件。

當 MFi 配件使用 Lightning 接頭或透過藍牙與 iOS 裝置進行通訊時，裝置會要求配件使用 Apple 提供的憑證（裝置會對此憑證進行驗證）進行回應，以證明配件經過 Apple 授權。然後，裝置會傳送一個質詢，配件必須使用已簽署的回應來回應。這個過程完全由 Apple 提供給經核准配件製造商的自定積體電路（IC）處理，而且對於配件本身是透明的。

配件可以要求存取不同的傳輸方式和功能；例如透過 Lightning 接線存取數位音訊串流，或透過藍牙存取位置資訊。認證積體電路會確保只有經過核准的配件才能取得對裝置的完全存取權限。如果配件不支援認證，其存取權限僅限於類比音訊和一小部分的序列（UART）音訊播放控制。

AirPlay 也會利用認證積體電路來驗證接收器已經過 Apple 核准。AirPlay 音訊和 CarPlay 視訊串流使用 MFi-SAP（安全關聯通訊協定），此通訊協定使用 AES-128 在計數器 (CTR) 模式下對配件和裝置之間的通訊進行加密。臨時密鑰則使用 ECDH 密鑰交換（Curve25519）進行交換，並使用認證電路的 1024 位元 RSA 密鑰來簽署，以作為端到端（STS）通訊協定的一部分。

HomeKit

HomeKit 提供家庭自動化的基礎架構，利用 iCloud 與 iOS 安全性來保護與同步私密資料，無須將其透露給 Apple。

HomeKit 身分

HomeKit 身分與安全性是以 Ed25519 公用 - 專用密鑰組為基礎。iOS 裝置會為 HomeKit 的每位使用者產生 Ed25519 密鑰組，這些密鑰組會變成他們的 HomeKit 身分，用於認證 iOS 裝置之間以及 iOS 裝置與配件之間的通訊。

密鑰會儲存在鑰匙圈中，並只會納入加密的鑰匙圈備份之中。密鑰會在使用「iCloud 鑰匙圈」（若可用）的裝置間同步。HomePod 和 Apple TV 會依照以下敘述的「點一下來設定」或設定模式來接受密鑰。密鑰會由 iPhone 透過 Apple 識別服務（IDS）分享給配對的 Apple Watch。

與 HomeKit 配件的通訊

HomeKit 配件會產生其自己的 Ed25519 密鑰組，以用於與 iOS 裝置的通訊。若將配件回復成原廠設定，便會產生新的密鑰組。

為了在 iOS 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，利用配件製造商所提供並由使用者於 iOS 裝置上輸入的八位數代碼，然後使用 CHACHA20-POLY1305 AEAD 與 HKDF-SHA-512 產生的密鑰來加密。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 iOS 裝置與 HomeKit 配件在使用期間進行通訊時，每個項目會使用上述過程中交換的密鑰來認證另一個項目。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-SHA-512 衍生密鑰來進行加密。這同時適用於 IP 型與低功耗藍牙配件。

針對支援廣播通知的低功耗藍牙裝置，配件會由配對的 iOS 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，這些資料是透過低功耗藍牙廣播傳送通知。廣播加密密鑰是一種 HKDF-SHA-512 衍生密鑰，資料會由 CHACHA20-POLY1305 Authenticated Encryption with Associated Data（用於關聯資料的認證加密，AEAD）演算法進行加密。廣播加密密鑰會定期由 iOS 裝置變更並使用 iCloud 同步至其他裝置，如以下「裝置和使用者之間的資料同步」章節描述。

本機資料儲存

HomeKit 會在使用者的 iOS 裝置上儲存家庭、配件、情境和使用者的相關資料。儲存的資料會使用自使用者 HomeKit 身分密鑰所衍生的密鑰加上隨機數來進行加密。此外，HomeKit 資料會使用「資料保護」類別的「首次使用者認證前的保護」來儲存。HomeKit 資料只會在加密的備份資料中進行備份，因此舉例來說，未加密的 iTunes 備份便不包含 HomeKit 資料。

裝置和使用者之間的資料同步

可以使用 iCloud 和「iCloud 鑰匙圈」在同一名使用者的 iOS 裝置間同步 HomeKit 資料。同步期間，HomeKit 資料會使用自使用者 HomeKit 身分與隨機數衍生的密鑰來進行加密。此資料在同步期間會以不透明二進位大型物件來處理。最近的物件會儲存在 iCloud 中以啟用同步，但不會用於任何其他用途。因為它是使用僅可於使用者 iOS 裝置上取得的密鑰進行加密，因此它的內容在傳輸與 iCloud 儲存期間是無法存取的。

HomeKit 資料也會在同一家庭的多位使用者間進行同步。此處理會使用認證與加密，就像 iOS 裝置與 HomeKit 配件間使用的一樣。認證是以 Ed25519 公用密鑰為基礎，當使用者加入家庭時，便會在裝置間交換這些密鑰。在新使用者加入家庭後，所有進一步的通訊都會使用端到端的通訊協定與每一作業階段的密鑰進行認證和加密。

一開始在 HomeKit 中建立家庭的使用者或具有編輯權限的其他使用者可以新增使用者。持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控制中心以完成操作。

當使用者登入 iCloud 時，便會自動執行佈建 Apple TV 的程序以搭配 HomeKit 使用。iCloud 帳號需要啟用雙重認證。Apple TV 與持有者的裝置會透過 iCloud 交換臨時 Ed25519 公用密鑰。當持有者的裝置與 Apple TV 連接相同區域網路時，臨時密鑰會使用端到端的通訊協定與各區段的密鑰來保護區域網路的連線。此處理會使用認證與加密，就像 iOS 裝置與 HomeKit 配件間使用的一樣。透過安全的區域網路，持有者的裝置會將使用者的 Ed25519 公用 - 專用密鑰組傳送至 Apple TV。這些密鑰之後會用來保護 Apple TV 與 HomeKit 配件間的通訊，還有 Apple TV 和其他 iOS 裝置（HomeKit 家庭的一部分）間的通訊。

若使用者沒有多部裝置，且拒絕將其家庭的存取權限授予其他使用者，便不會將 HomeKit 資料同步至 iCloud。

家庭資料與 App

App 對家庭資料的存取權是受使用者的「隱私權」設定所控制。當 App 要求提供家庭資料時（類似於「聯絡資訊」、「照片」和其他 iOS 資料來源），系統會要求使用者會授予存取權。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資訊，網址為：developer.apple.com/homekit

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。如需更多資訊，請參閱本白皮書「Internet 服務」中的「Siri」一節。

HomeKit 網路攝影機

HomeKit 中的網路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 裝置。系統會使用在 iOS 裝置和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 iOS 裝置所在位置不在區域網路上，則會經由家庭控制中心將加密的串流傳遞至 iOS 裝置。家庭控制中心不會解密串流，且只扮演 iOS 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 無權從此串流擷取螢幕畫面。

HomeKit 配件的 iCloud 遠端存取

HomeKit 配件可直接與 iCloud 連接，讓 iOS 裝置在無法使用藍牙或 Wi-Fi 通訊時控制配件。

「iCloud 遠端存取」經過精密設計，因此無須向 Apple 透露所傳送的配件種類、命令內容和通知內容，即可控制配件和傳送通知。HomeKit 不會透過「iCloud 遠端存取」來傳送有關住家的資訊。

當使用者使用 iCloud 遠端存取來傳送指令時，配件和 iOS 裝置會彼此認證，而資料會使用專為區域連線所設定的相同程序來進行加密。通訊的內容會經過加密，且不會對 Apple 顯示。透過 iCloud 設定位址的作業是基於在設定程序期間所註冊的 iCloud 識別碼。

支援 iCloud 遠端存取的配件會在配件的設定處理期間加以佈建。佈建處理會在使用者登入 iCloud 時開始。接著，iOS 裝置會要求配件使用「Apple 認證副處理器」（內建於所有 Built for HomeKit 配件）來簽署詢問。配件也會產生 prime256v1 橢圓曲線密鑰，而公用密鑰則會連同簽署的詢問和認證副處理器的 X.509 憑證，一起傳送至 iOS 裝置。這些會用來從 iCloud 佈建伺服器要求配件的憑證。憑證會由配件儲存，但不會包含配件的相關識別資訊，除非已將存取權限授予 HomeKit iCloud 遠端存取。執行佈建的 iOS 裝置也會傳送 bag 至配件，其中包含要連接 iCloud 遠端存取伺服器所需的 URL 和其他資訊。此資訊不特定於任何使用者或配件。

每個配件都會向 iCloud 遠端存取伺服器註冊所允許使用者的列表。這些使用者已向將配件加入住家的人員取得控制配件的權限。使用者會取得由 iCloud 伺服器授予的識別碼並可對應到 iCloud 帳號，以從配件傳送通知訊息和回應。同樣地，配件具有 iCloud 發出的識別碼，但這些識別碼難以識別且不會顯示有關配件本身的任何資訊。

當配件連接至 HomeKit iCloud 遠端存取伺服器時，便會提供其憑證與通行證。通行證是從不同的 iCloud 伺服器中取得，且並非對每個配件都是唯一的。當配件要求通行證時，其會在要求中包含製造商、型號和韌體版本。此要求中並不會傳送任何使用者識別或住家識別的資訊。與通行證伺服器的連線不會經過認證，以協助保護隱私。

配件會使用 HTTP/2 來連接至 iCloud 遠端存取伺服器，並使用 TLS v1.2 及 AES-128-GCM 和 SHA-256 加以保護。配件會讓其與 iCloud 遠端存取伺服器的連線保持開啟，以便其接收傳入的訊息和將回應與外寄通知傳送給 iOS 裝置。

HomeKit 電視遙控器配件

第三方 HomeKit「電視遙控器」配件可為透過「家庭」App 綁定的 Apple TV 提供 HID 事件和 Siri 音訊。HID 事件在 Apple TV 與「遙控器」之間是透過安全的作業階段傳送。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。其中的各個音訊分段會透過 Apple TV 與「遙控器」之間專用的區域網路連線直接傳送到 Apple TV。區域網路連線會以每一作業階段 HKDF-SHA-512 衍生密鑰組加密，該密鑰組會透過 Apple TV 與「遙控器」之間的 HomeKit 作業階段進行交涉。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。

SiriKit

Siri 使用「iOS 延伸功能」機制來與第三方 App 進行通訊。雖然 Siri 可存取 iOS 聯絡資訊與裝置的目前位置，Siri 在提供該資訊給 App 前，會先針對包含延伸功能的 App，檢查受 iOS 保護的使用者資料存取權，以確認 App 是否具有存取權。Siri 僅會傳遞原始使用者查詢文字的相關片段給延伸功能。例如，如果 App 沒有 iOS 聯絡資訊的存取權，Siri 將不會在使用者要求（如「用『付款』App 付給媽媽 10 美元」）中解析關係。在此情況下，延伸功能的 App 僅會透過傳遞給它的原始話語片段看到「媽媽」一詞。然而，如果 App 確實具有 iOS 聯絡資訊的存取權，便會收到該使用者媽媽的 iOS 聯絡資訊。如果在訊息內文中參照某筆聯絡資訊，例如「傳『訊息』App 跟媽媽說哥哥最好了」，無論 App 的 TCC 為何，Siri 將不會解析「哥哥」一詞。App 所呈現的內容可能會傳送至伺服器，以便 Siri 瞭解使用者可能會在 App 中使用的詞彙。使用者的要求若需要從使用者的連絡資訊擷取位置資訊（例如「使用 <App 名稱 > 叫車送我到媽媽家」），無論 App 的位置或聯絡資訊存取權為何，Siri 都會提供所需位置資訊給 App 的延伸功能，但僅限用於該要求。

Siri 在執行時允許啟用 SiriKit 的 App 針對應用程式實例提供一組自定單字。這些自定單字會與本白皮書中「Siri」一節中所討論的隨機識別碼綁定，並具有相同的時限。

HealthKit

在取得使用者許可後，HealthKit 便可儲存和整合來自健康與健身 App 的資料。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。

健康資料

HealthKit 可讓使用者儲存並整合各種來源的健康資料，例如 App、裝置和醫療機構。此資料會儲存在「資料保護」類別的「未打開檔案的保護」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 Touch ID 或 Face ID 來解鎖裝置時，即可再次存取資料。

HomeKit 也會彙總管理資料，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。

臨時日誌檔會儲存健康記錄，當裝置鎖定時便會產生這些記錄（例如當使用者從事運動時）。這些臨時日誌檔會儲存在「資料保護」類別的「未打開檔案的保護」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。設定 iCloud 儲存時，系統會在裝置間同步健康資料，並透過加密保護靜態與傳輸中的資料，確保安全無虞。健康資料只會包含在加密的 iTunes 備份中，不會包含在未加密的 iTunes 備份或「iCloud 備份」中。

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，以取得臨床健康記錄的複本。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，便會透過 TLS v1.2 受保護的連線直接從醫療機構下載臨床健康記錄資料。下載資料後，臨床健康記錄會安全地與其他「健康」資料一起儲存。

資料完整性

儲存在資料庫中的資料包含追蹤每筆資料記錄出處的後設資料。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，選擇性的後設資料項目可包含記錄的數位簽署副本。此用意是提供記錄（由受信任之裝置所產生）的資料完整性。用於數位簽章的格式為 IETF RFC 5652 中所指定的加密編譯訊息語法（Cryptographic Message Syntax，CMS）。

第三方 App 的存取

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 也必須提供隱私權政策給使用者，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 要求提供健康資料時（類似於「聯絡資訊」、「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「健康」App 的「來源」標籤頁中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。這可避免 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。

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。

您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「資料保護」類型的「無保護」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。此資料會備份到「iCloud 備份」，且不會使用 CloudKit 在裝置之間同步。

ReplayKit

ReplayKit 是允許開發者在其 App 中加入錄製與即時廣播功能的程式框架。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。
- **螢幕畫面與音訊擷取**：螢幕畫面與音訊擷取是在 App 的處理程序外、於 ReplayKit 的服務程式 **replayd** 中進行。這會確保錄製的內容從不讓 App 處理程序存取。
- **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 UI 來預覽與共享影片。UI 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。

廣播

- **螢幕畫面與音訊擷取**：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 UI 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

此架構可確保託管的 App 對廣播的影片和音訊內容沒有權限，只有 ReplayKit 和第三方廣播延伸功能具有存取權。

- **廣播選擇器**：為了選取要使用的廣播服務，ReplayKit 提供檢視控制器（類似於 UIActivityViewController），而開發者可在其 App 中呈現。檢視控制器會使用 UIRemoteViewController SPI 來導入，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。
- **系統廣播選擇器**：可允許使用者直接從 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 UI）。UI 會使用 UIRemoteViewController SPI 來導入，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**：第三方廣播服務會導入上傳延伸功能，以在廣播期間處理影片和音訊內容，而上傳延伸功能可透過兩種方式來接收內容：
  - 小型已編碼 MP4 剪輯片段
  - 原始未編碼的樣本緩衝
    - **MP4 剪輯片段處理**：在此處理模式期間，小型已編碼 MP4 剪輯片段會由 **replayd** 產生並儲存在只供 ReplayKit 子系統存取的私密位置。產生影片剪輯片段後，**replayd** 會將影片剪輯片段的位置透過 NSExtension 要求 SPI（XPC 型）傳遞至第三方上傳延伸功能。**replayd** 還會產生一個一次性 Sandbox 代號，並同樣傳遞至上傳延伸功能，以便在延伸功能要求期間提供延伸功能存取權給特定影片剪輯片段。
    - **樣本緩衝處理**：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。

安全備忘錄

「備忘錄」 App 包含安全備忘錄功能，可讓使用者保護特定備忘錄的內容。安全備忘錄是以使用者提供的密語加密，為檢視 iOS、macOS 裝置和 iCloud 網站上的備忘錄所需。

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。備忘錄的內容會使用 AES-GCM 進行加密。系統會在 「核心資料」 和 CloudKit 中建立新記錄，以便儲存加密的備忘錄、標記和初始化向量，並且刪除原始備忘錄記錄；加密的資料不會就地寫入。附件也會以相同的方式加密。支援的附件包含影像、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。

當使用者成功輸入密語時，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。在開啟時，使用者無需輸入密語或使用 Touch ID 或 Face ID，便可檢視或保護其他備忘錄。不過，如果部分備忘錄的密語不同，安全作業階段僅會套用至使用目前密語保護的備忘錄。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 分鐘時。
- 裝置鎖定時。

忘記其密語的使用者若有在裝置上啟用 Touch ID 或 Face ID，仍可以檢視安全備忘錄或保護其他備忘錄。此外，「備忘錄」 會在嘗試輸入密語失敗三次後，顯示使用者提供的提示。使用者必須知道目前的密語才能更改密語。

若使用者忘記目前的密語，可以重置密語。此功能可讓使用者以新的密語製作新的安全備忘錄，但將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

「備忘錄」 可與其他人共用。共享的備忘錄未經過端對端加密。使用者加入 Apple 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 / 解密彼此資料的程序。

Apple Watch

Apple Watch 使用為 iOS 打造的安全性功能與技術來協助保護裝置上的資料，同時亦保護與已配對 iPhone 和 Internet 的通訊。這包含如 「資料保護」 與鑰匙圈存取控制等技術。使用者的密碼也會與裝置 ID 結合以建立加密密鑰。

將 Apple Watch 與 iPhone 配對是使用頻外（OOB）處理加以保護以交換公用密鑰，其後面並接著低功耗藍牙（BLE）連結共享密鑰。Apple Watch 會顯示動畫圖形，該動畫圖形是使用 iPhone 上的相機捕捉。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 密鑰項目」（Standard BLE Passkey Entry）會用作備用配對方式。

一旦建立低功耗藍牙作業階段並使用 「藍牙核心規格」 提供的最高層級安全通信協定加密後，Apple Watch 和 iPhone 會使用改寫自 Apple 識別服務（IDS）的程序來交換密鑰，如本白皮書 「Internet 服務」 中的 「iMessage」 一節所述。密鑰交換後，便會捨棄藍牙作業階段密鑰，且 Apple Watch 與 iPhone 間的所有通訊都會使用 IDS 進行加密，而加密後的藍牙、Wi-Fi 與行動數據連結則提供第二加密層。低功耗藍牙位址每 15 分鐘便會輪動，以減少流量洩漏的風險。

為了支援需要連續傳輸資料的 App，會使用本白皮書 「Internet 服務」 中的 「FaceTime」 一節提到的方式來提供加密，使用由已配對 iPhone 所提供的 IDS 服務或直接 Internet 連線。

Apple Watch 會為檔案與鑰匙圈項目導入以硬體加密的儲存空間與類別式保護，如本白皮書的「加密與資料保護」一節所述。也會一併使用鑰匙圈項目的存取控制 Keybag。手錶與 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。

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）。接著便可在 Apple Watch 上於「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 Internet 與配對的 iPhone 同步「郵件」資料。針對 Gmail 帳號，使用者需要在 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，即可用來擷取「郵件」。此 OAuth 代號絕不會用來從配對的 iPhone 連接到 Gmail 伺服器。

Apple Watch 可藉由按住側邊按鈕來手動加以鎖定。此外，除非停用手腕偵測功能，否則會在使用者將手錶從手腕取下不久後自動鎖定裝置。Apple Watch 鎖定時，使用者只能藉由輸入手錶的密碼才能使用 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 MDM 解決方案來強制執行。

若正穿戴著手錶，也可使用已配對的 iPhone 來解鎖手錶。這是使用在配對期間建立的密鑰進行認證連線來解鎖。iPhone 會傳送密鑰，而手錶會使用該密鑰來解鎖其資料保護密鑰。iPhone 無從得知手錶密碼，系統也不會傳輸手錶密碼。此功能可在 iPhone 上使用 Apple Watch App 關閉。

Apple Watch 一次只能與一部 iPhone 配對。在取消配對時，iPhone 會傳遞指示以清除 Apple Watch 的所有內容和資料。

Apple Watch 可設定為在當晚進行系統軟體更新。如需深入瞭解如何儲存 Apple Watch 密碼以在更新期間使用，請參閱本文件中的「Keybag」章節。

在已配對 iPhone 上啟用「尋找我的 iPhone」也會在 Apple Watch 上使用「啟用鎖定」。「啟用鎖定」可讓 Apple Watch 在遺失或遭竊時，其他人無法輕易使用或銷售。「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。

網路安全性

除了 Apple 用於保護 iOS 裝置上所儲存資料的內建安全保護，也有許多網路安全措施可供企業組織採用並確保資訊從 iOS 裝置來回傳輸時安全無虞。

行動使用者必須能在全球各處存取公司網路，因此很重要的一點是確保他們獲得授權並且其資料在傳輸期間受到保護。iOS 使用標準網路通訊協定並使開發者能夠存取這些通訊協定，以進行受認證、已授權且已加密的通訊。為了達成這些安全性的目標，iOS 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。

在其他平台上，需要用防火牆軟體來保護開放式通訊埠以防止入侵。因為 iOS 透過限制監聽埠以及移除不必要的網路工具程式（如 telnet、Shell 或網頁伺服器），使受攻擊的範圍減小，因此在 iOS 裝置上不需要額外的防火牆軟體。

TLS

iOS 支援傳輸層安全性（TLS v1.0、TLS v1.1、TLS v1.2）和 DTLS，同時支援 AES-128 和 AES-256，且偏好使用提供完美前向安全性的加密套件。Safari、「行事曆」、「郵件」 和其他 Internet 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（Network.framework）則提供精細的控制。CFNetwork 不允許 SSLv3，而使用 WebKit 的 App（如 Safari）也禁止進行 SSLv3 連線。

在 iOS 11 或以上版本及 macOS High Sierra 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 Sierra 中的 RC4 對稱加密套件已淘汰。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，以使用新型且安全的加密套件。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 Certificate Transparency 記錄中，才允許用來進行 TLS 連線。

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安全性的套件，特別是 GCM 與 CBC 模式中的 ECDHE_ECDSA_AES 和 ECDHE_RSA_AES。App 可針對各網域停用前向安全性要求，停用後便會將 RSA_AES 加入可用加密集中。

伺服器必須支援 TLS v1.2 和前向安全性，且憑證必須有效並使用 SHA-256 加以簽署，或是最好使用 2048 位元 RSA 密鑰或 256 位元橢圓曲線密鑰的最低限度。

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 或以上版本編譯的 App。

VPN

與虛擬私人網路類似的安全網路服務通常只需要簡單的設定和配置，便可配合 iOS 裝置使用。與 iOS 裝置搭配使用的 VPN 伺服器支援以下通訊協定和認證方式：

- IKEv2/IPSec，透過共享密鑰、RSA 憑證、**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
- Cisco IPSec，透過密碼進行使用者認證，並藉由共享密鑰和憑證進行機器認證
- L2TP/IPSec，透過 MS-CHAPV2 密碼進行使用者認證，並藉由共享密鑰進行機器認證

iOS 支援以下 VPN 使用方式：

- **隨選即用 VPN**，適用於使用以憑證為基礎的認證網路。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。MDM 可為每個受管理的 App 和 Safari 中特定的網域指定連線。這有助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公司網路。
- **總是開啟 VPN**，可針對透過行動裝置管理（MDM）解決方案管理的裝置設定此項，並使用 Apple Configurator 2、Apple School Manager 或 Apple Business Manager 加以監督。這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。「總是開啟 VPN」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。預設通道的通訊協定 IKEv2 使用資料加密對流量傳輸進行安全保護。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 Internet 存取權。

Wi-Fi

iOS 支援包含「WPA2 企業級」在內的業界標準 Wi-Fi 通訊協定，可針對無線企業網路提供連線認證服務。「WPA2 企業級」使用 AES-128 位元加密，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，確保使用者的資料始終受到保護。有了 802.1X 的支援，可將 iOS 裝置整合到各種 RADIUS 認證環境中。iPhone 和 iPad 上支援的 802.1X 無線認證方式包括 EAP-TLS、EAP-TTLS、EAP-FAST、EAP-SIM、PEAPv0、PEAPv1 和 LEAP。

除了資料保護外，iOS 擴充 WPA2 層級保護，以透過 802.11w 中參考的「管理訊框保護」服務來單點發送與多點發送管理訊框。PMF 支援適用於 iPhone 6 和 iPad Air 2 或更新機型。

當 iOS 沒有與 Wi-Fi 網路產生關聯，iOS 會在執行 Wi-Fi 掃描時，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偏好的 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 掃描並不是隨機的。

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，iOS 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。

此時因為裝置中斷某個 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 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。iPhone 4s 或更早機型上不支援 Wi-Fi MAC 位址隨機載入。

在 iPhone 6s 或更新機型上，已知 Wi-Fi 網路的隱藏屬性會自動識別與更新。如果 Wi-Fi 網路的服務集識別碼（SSID）已廣播，iOS 裝置將不會傳送要求中包含 SSID 的探測。這樣可避免裝置廣播非隱藏網路的網路名稱。

為了保護裝置不受網路處理器韌體的漏洞影響，包含 Wi-Fi 和基頻在內的網路介面限制了對應用程式處理器記憶體的存取。使用 USB 或 SDIO 與網路處理器互動時，網路處理器無法起始「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 IOMMU 會限制網路處理器對含有其網路封包或控制結構的記憶體頁面進行 DMA 存取。

藍牙

iOS 的藍牙支援旨在提供實用的功能，而不會增加對私密資料不必要的存取。iOS 裝置支援 Encryption Mode 3、Security Mode 4 和 Service Level 1 連線。iOS 支援以下藍牙描述檔：

- 免持描述檔（HFP）
- 電話簿存取描述檔（PBAP）
- 訊息存取描述檔（MAP）
- 進階音訊分配描述檔（A2DP）
- 音訊 / 視訊遠端控制描述檔（AVRCP）
- 個人區域網路描述檔（PAN）
- 人機介面裝置描述檔（HID）

對這些描述檔的支援因設備而異。

如需更多資訊，請前往：support.apple.com/zh-tw/HT204387

單一登入

iOS 支援透過單一登入（SSO）對企業網路進行認證。SSO 搭配以 Kerberos 為基礎的網路使用，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。同時還支援以憑證為基礎（PKINIT）的認證作業。

iOS SSO 利用 SPNEGO 代號和 HTTP Negotiate 通訊協定，與以 Kerberos 為基礎的認證閘道和支援 Kerberos 申請單的 Windows Integrated Authentication 系統配合使用。SSO 的支援以開放原始碼 Heimdal 專案為基礎。

支援下列加密類型：

- 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 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 支援設定描述檔的承載資料，允許 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。

接續互通

「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、撥打和接聽電話通話、傳送和接收簡訊，以及共享行動數據 Internet 連線。

接力

當使用者的 Mac 和 iOS 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 4.2 配對。各個訊息會採用與 iMessage 相似的加密方式。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低功耗藍牙廣播，其會在 GCM 模式下使用 AES-256 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低功耗藍牙連線，並執行廣播加密密鑰的交換。此連線使用標準的低功耗藍牙 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，這些訊息會使用 APNs，而非低功耗藍牙。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 的原生 App 繼續存取由 App 開發者合法控制之網域中的網頁。「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透過共用網頁憑證的機制來建立。如需詳細資訊，請參閱本白皮書 「使用者密碼管理」 一節中的 「App 存取已儲存的密碼」。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（如本節前文所述）。

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 「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，方式與 AirDrop 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 使用此功能時，兩部裝置間會開始交換，如同使用 「接力」 傳送一樣（請參閱前面章節）。不過，在使用低功耗藍牙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。此連線會使用 TLS 加密以交換其 iCloud 身分憑證。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」 安全地跨裝置傳送剪貼板內容，因此使用者可以在一部裝置上拷貝並在另一部裝置上貼上。剪貼板內容會如其他 「接力」 資料一樣受到保護，並依照預設與 「通用剪貼板」 分享，App 開發者選擇不允許分享時不在此限。

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執行的 App（必須以 iCloud 登入裝置來建立此存取權）。

自動解鎖

支援 「自動解鎖」 功能的 Mac 電腦會使用低功耗藍牙與點對點 Wi-Fi，以便安全地允許使用者的 Apple Watch 解鎖 Mac。支援此功能且與 iCloud 帳號綁定的每部 Mac 與 Apple Watch 皆必須使用雙重認證（TFA）。

啟用 Apple Watch 來解鎖 Mac 時，便會建立使用 「自動解鎖識別身分」 的安全連結。Mac 會建立一次性隨機解鎖密鑰，並透過連結將其傳輸至 Apple Watch。此密鑰會儲存在 Apple Watch 上，且僅可在 Apple Watch 解鎖時存取（請參閱 「加密與資料保護」 一節中的 「資料保護類別」 部分）。新密鑰不得為使用者的密碼。

在解鎖操作期間，Mac 會使用低功耗藍牙來建立與 Apple Watch 的連線。接著在初次啟用時，兩部裝置間會使用共享密鑰來建立安全連結。Mac 與 Apple Watch 之後會使用點對點 Wi-Fi 和安全密鑰（從安全連結所衍生）來判斷兩部裝置間的距離。若裝置位於範圍內，便會使用安全連結來傳送預先共享的密鑰，以解鎖 Mac。順利解鎖後，Mac 會將目前的解鎖密鑰取代為一次性使用的新解鎖密鑰，並將新解鎖密鑰透過連結傳輸至 Apple Watch。

iPhone 行動數據通話中繼

Mac、iPad 或 iPod touch 若連上與 iPhone 相同的 Wi-Fi 網路，即可透過 iPhone 行動數據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，會透過 **「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。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 iPhone 的音訊。

在一部裝置上接聽來電時，會透過低功耗藍牙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。

撥出的通話也將透過 「Apple 推播通知服務」 中繼到 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 行動數據通話」 來停用裝置的電話中繼功能。

iPhone 訊息轉寄

「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、iPod touch 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。或者會藉由輸入由 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，此作業使用的方式如本白皮書中本節的 「iMessage」 部分所述。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

支援 「即時熱點」 的 iOS 裝置使用低功耗藍牙來搜尋裝置並與其進行通訊，前提是裝置必須使用相同的 iCloud 帳號進行登入。與 「即時熱點」 相容且執行 OS X Yosemite 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 iOS 裝置，並與其進行通訊。

當使用者進入 iOS 裝置上的 「Wi-Fi 設定」 時，裝置會發出包含一個識別碼的低功耗藍牙廣播，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，以表示其處於可用狀態。

當使用者選擇可用於 「個人熱點」 的裝置時，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（使用標準低功耗藍牙加密方法）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低功耗藍牙連結，使用相同訊息專屬加密方式來回應 「個人熱點」 的連線資訊。

AirDrop 安全性

支援 AirDrop 的 iOS 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 功能並執行 OS X 10.11 或以上版本的 Mac 電腦。Wi-Fi 訊號用來在裝置之間進行直接通訊，無需使用任何 Internet 連線或 Wi-Fi 存取點。

當使用者啟用 AirDrop 後，裝置上就會儲存一個 2048 位元的 RSA 識別身分。此外，裝置還會依據與使用者的 Apple ID 綁定的電子郵件位址和電話號碼，建立一個 AirDrop 識別身分的雜湊值。

當使用者選擇使用 AirDrop 共享項目時，設備會透過低功耗藍牙發出 AirDrop 訊號。附近處於喚醒狀態且開啟了 AirDrop 的其他裝置偵測到此訊號後，便會使用其持有人的識別身分雜湊值的簡短版本進行回應。

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。在「只限聯絡人」模式下，接收到的識別身分雜湊值會與發起者的「聯絡資訊」App 中人員的雜湊值進行比對。若找到相符項目，發送裝置會建立一個點對點 Wi-Fi 網路，並使用 Bonjour 告知已建立 AirDrop 連線。接收裝置會使用此連線將其完整的識別身分雜湊值傳送給發起者。如果完整雜湊值仍與「聯絡資訊」相符，接收者的名字和照片（如果「聯絡資訊」中有的話）便會顯示在 AirDrop 共享表單中。

使用 AirDrop 時，由傳送方使用者選擇要與其共享內容的對象。發送裝置會與接收裝置建立一個加密（TLS）連線，此連線會交換它們的 iCloud 識別身分憑證。憑證中的識別身分會針對每位使用者的「聯絡資訊」App 進行驗證。然後會要求接收方使用者接受來自經識別的人員或裝置所傳送的內容。如果選擇了多位接收者，則會針對每個目標重複此過程。

在「所有人」模式中，會使用相同的程序，但若未能在「聯絡資訊」中找到相符項目，接收裝置會顯示在 AirDrop 傳送表單中，並帶有一個小圖像和裝置名稱，該名稱可在「設定」>「一般」>「關於本機」>「名稱」中找到。

對於 AirDrop 的使用，組織可針對使用 MDM 解決方案來管理的裝置和 App 進行限制。

Wi-Fi 密碼共享

支援 Wi-Fi 密碼共享的 iOS 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，會使用低功耗藍牙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 64 個字元的 PSK 給要求者，此 PSK 也可用來加入網路。

對於 Wi-Fi 密碼共享的使用，組織可針對透過 MDM 解決方案所管理的裝置和 App 進行限制。

Apple Pay

使用 Apple Pay，使用者可以使用受支援的 iOS 裝置、Apple Watch 和 Mac 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。使用者也可將具備 Apple Pay 功能的交通卡加入 「錢包」。對於使用者來說很容易，且在硬體和軟體方面皆具備整合性的安全措施。

Apple Pay 的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

Secure Element：Secure Element 符合工業標準、受認證的晶片，於 Java Card 平台上運作，符合金融業的電子付款要求。

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

錢包：「錢包」 可用來加入和管理信用卡、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，且可能可以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 「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 上的 「設定輔助程式」 和 「設定」
- 用來設定 Apple Watch 的 Watch App
- Mac 上的 「錢包與 Apple Pay」 系統偏好設定面板。

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

安全隔離區：在 iPhone、iPad 以及 Apple Watch 上，「安全隔離區」 會管理認證程序並使付款交易生效。

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 伺服器會管理信用卡、金融卡、交通卡和學生證在 「錢包」 中的設定和佈建，以及儲存在 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 內的付款重新加密付款憑證。

Apple Pay 使用 Secure Element 的方式

Secure Element 主控著一種特殊設計的 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、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 的安全性功能保護。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。

Apple Pay 使用 NFC 控制器的方式

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

卡片持有人使用 Touch ID、Face 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、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 磁場。因此，非接觸式付款交易的付款授權詳細資料會限制在本機 NFC 磁場內，且絕對不會向應用程式處理器暴露。相反地，App 內和網路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、金融卡及預付卡佈建

當使用者加入信用卡、金融卡或預付卡（包含商店卡）到「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的服務供應商。透過此資訊，發卡機構會判定是否要核准將該卡片加入「錢包」。

Apple Pay 會使用三種伺服器端調用來傳送和接收與發卡機構或網路之間的通訊，作為卡片佈建程序的一部分：必要欄位、卡片檢查與連結和佈建。發卡機構或網路會使用這些調用來驗證、核准卡片以及將卡片加入「錢包」。這些主從式架構作業階段皆使用 TLS v1.2 進行加密。

完整卡號不會儲存在裝置或 Apple 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，且與一般信用卡或金融卡號不同，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」與 iOS 和 watchOS 相隔離，且絕對不會儲存在 Apple 伺服器上，亦不會備份至 iCloud。

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、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七天後，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。

手動將信用卡或金融卡加入 Apple Pay

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」內、「錢包」App 或 Apple Watch App，使用者可以藉由打字方式或使用裝置上的相機來輸入該資訊。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。所有資訊會經過加密並傳送到 Apple Pay 伺服器。

若「卡片檢查」程序傳回使用條款 ID，則 Apple 會下載發卡機構的使用條款與條件，並顯示給使用者閱覽。如果使用者接受使用條款，Apple 便會將所接受條款的 ID 連同 CVV 傳送至「連結」和「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，像是您 iTunes 和 App Store 帳戶活動的相關資訊（例如您是否在 iTunes 內有長期的交易記錄）、您裝置的資訊（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 iOS 裝置），以及加入卡片時的大略位置（若您已啟用「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金融卡的 「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 帳號將信用卡或金融卡加入 Apple Pay

若要使用向 iTunes 登記的信用卡或金融卡，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，裝置會下載並顯示使用條款，並連帶條款 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，以避免資訊遭 iOS 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。

其他驗證

發卡機構有權決定信用卡或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，使用者需從發卡機構存檔的聯絡資訊中選擇。接著會傳送一組代碼，使用者必須將其輸入 「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。

付款授權

在配備 「安全隔離區」 的裝置上，Secure Element 只會在從 「安全隔離區」 接收到授權後，才會允許付款。在 iPhone 或 iPad 上，此作業則包含確認使用者已透過 Touch ID、Face ID 或裝置密碼授權的動作。若裝置適用 Touch ID 或 Face ID，其便為預設方法；但使用者隨時都可以使用密碼。在三次嘗試比對指紋失敗後，或是兩次嘗試比對面孔失敗後，會自動建議改用密碼；而嘗試失敗五次後，則必須輸入密碼。當使用者未設定 Touch ID 或 Face ID，或是沒有針對 Apple Pay 啟用 Touch ID 或 Face ID 時，也需要輸入密碼。在 Apple Watch 上，裝置必須使用密碼解鎖且必須按兩下側邊按鈕才能進行付款。

「安全隔離區」 和 Secure Element 之間的通訊會在序列介面上進行，Secure Element 會連接到 NFC 控制器，接著再連接到應用程式處理器。即使未直接連接，「安全隔離區」和 Secure Element 也可以使用共享的密鑰組來安全地通訊，此密鑰組是在製造過程中佈建的。通訊的加密和認證是基於 AES，兩端的通訊方皆會使用加密編譯隨機數來防止重播攻擊。密鑰組是從 「安全隔離區」 內的 UID 密鑰和 Secure Element 的唯一識別碼產生。密鑰組接著會安全地從「安全隔離區」傳送至工廠內的**硬體安全性模組（HSM）**，其中包含所需的密鑰材料，再將密鑰組植入 Secure Element。

當使用者授權交易時，「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（非接觸式付款或 App 內）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，AR 受 「安全隔離區」 的加密和反復原機制的保護。它會透過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示為已刪除。

只有在 Secure Element 使用與加入卡片時相同的密鑰組和 AR 值出示授權時，才能使用加入到 Secure Element 的信用卡、金融卡和預付卡。這使 iOS 在下列情況發出指令，讓「安全隔離區」將 AR 拷貝標示為無效，將卡片轉譯為無法使用的狀態：

- 當密碼停用時。
- 使用者登出 iCloud 時。
- 使用者選擇「清除所有內容和設定」時。
- 裝置從復原模式回復時。

使用 Apple Watch 時，卡片會在下列情況標示為無效：

- 手錶的密碼已停用時。
- 手錶已與 iPhone 取消配對時。

使用密鑰組及其目前 AR 值的拷貝，Secure Element 會先驗證從「安全隔離區」接收到的授權，才會啟用付款 Applet 來進行非接觸式付款。在 App 內進行交易時，會擷取來自付款 Applet 的加密付款資料，此時亦會套用此程序。

因交易而異的動態安全碼

來自付款 Applet 的付款交易包含付款密碼及「裝置帳號號碼」。這組密碼是一次性安全碼，計算方式是使用隨每筆新交易遞增的交易計數器，以及個人化期間付款 Applet 所佈建且付款網路和 / 或發卡機構已知的密鑰。視付款方案而定，也可能會使用其他資料來進行計算，包含下列資料：

- 進行 NFC 交易時使用 Terminal Unpredictable Number
- 在 App 內交易時使用 Apple Pay 伺服器隨機數

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所完成交易的類型而有所不同。

使用信用卡和金融卡在商店內付款

如果 iPhone 已開機且偵測到 NFC 磁場，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「錢包」App 並選擇卡片，或當裝置鎖定時：

- 在配備 Touch ID 的裝置上按兩下主畫面按鈕
- 在配備 Face ID 的裝置上按兩下側邊按鈕

接下來，在發送付款資訊前，使用者必須使用 Touch ID、Face 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，皆不會將完整的實際信用卡或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。

使用信用卡和金融卡在 App 內付款

Apple Pay 也可以用來在 iOS App 及 Apple Watch App 內進行付款。當使用者以 Apple Pay 在 App 內付款時，Apple 會收到加密的交易資訊，並以開發者特定密鑰再次加密，才會傳送給開發者或商家。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特定密鑰再次加密，才會將交易傳遞給商家。

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 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 Touch ID、Face 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。

當使用者授權付款時，系統會呼叫 Apple Pay 伺服器以取得加密編譯隨機數，這與進行店內交易時 NFC 終端機傳回的數值類似。隨機數和其他交易資料會傳遞到 Secure Element 以產生付款憑證，此付款憑證會以 Apple 密鑰進行加密。當加密的付款憑證從 Secure Element 發出後，會傳遞到 Apple Pay 伺服器，伺服器會解密憑證、比對憑證中的隨機數與原來由 Apple Pay 伺服器發送的隨機數，然後使用與「商家 ID」關聯的商家密鑰重新加密付款憑證。接著付款憑證會傳回裝置，透過 API 傳送回 App。App 接下來會將付款憑證傳遞到商家系統進行處理。商家便可以使用其專用密鑰解鎖付款憑證以進行處理。這會結合來自 Apple 伺服器的簽名，允許商家驗證交易是針對此特定商家所進行的。

API 會要求一個授權，此授權用來指定支援的「商家 ID」。App 也可能包含要傳送至 Secure Element 進行簽署的其他資料（例如訂單號碼或客戶身分），以確保交易無法轉移到其他客戶。此程序需由 App 開發者執行，其能指定 PKPaymentRequest 上的 applicationData。此資料的雜湊值會包含在加密的付款資料中。商家接著會負責驗證 applicationData 雜湊值是否與付款資料內包含的內容相符。

使用信用卡和金融卡在網站上付款

使用者可透過 iOS 裝置、Apple Watch 和 Mac 使用 Apple Pay 在網站上付款。Apple Pay 交易也可在 Mac 上開始，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。Apple 伺服器會執行網域名稱驗證並發出 TLS 用戶端憑證。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。商家作業階段簽名經過驗證後，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、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 iOS 和 macOS 的 Safari 隱私設定中停用 Apple Pay 查詢。

商家作業階段經過驗證後，所有安全性與隱私措施皆與使用者在 App 內付款時相同。

在 Mac 對 iPhone 或 Apple Watch 的「接力」作業中，Apple Pay 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。IDS 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。使用者卡片的特定裝置帳號不會共享，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的聯絡資訊、送貨及帳單地址。

使用者使用 Touch ID、Face 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。

只有位於彼此附近的裝置可要求和完成付款。鄰近位置是透過低功耗藍牙廣播來加以決定。

感應式票卡

「錢包」 支援使用 「加值服務」 (VAS) 通訊協定來將資料從支援的票卡傳送至相容的 NFC 終端機。VAS 通訊協定可在感應式終端機上導入，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。若使用者擁有帶有商店識別碼的票卡，系統會要求使用者透過 Touch ID、Face 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 密鑰會與商家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。

使用者也可手動選取票卡，並透過 Touch ID、Face ID 或密碼授權使用，然後再向 NFC 終端機出示該卡。

Apple Pay Cash

在 iOS 11.2 或以上版本及 watchOS 4.2 或以上版本上，可在 iPhone、iPad 或 Apple Watch 上使用 Apple Pay 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 Pay Cash 帳號中，且可在使用者已用 Apple ID 登入的合格裝置上，前往 「錢包」 或 「設定」 > 「錢包與 Apple Pay」 使用該款項。

若要使用個人對個人付款和 Apple Pay Cash，使用者必須在與 Apple Pay 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。

設定 Apple Pay Cash 時，您加入信用卡或金融卡時提供的資訊，可能會與我們的合作銀行 Green Dot Bank 和 Apple Payments Inc. 共享，Apple Payments Inc. 是我們專為保護您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。

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 Pay Cash 餘額。如有必要，會從使用者加入 「錢包」 中的第二信用卡或金融卡提取額外款項。

「錢包」 中的 Apple Pay Cash 卡片可搭配 Apple Pay 使用，以便在商店、App 內和網路上進行付款。Apple Pay 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 「錢包」 中的金融卡或預付卡為 Apple Pay 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. 會儲存且可能使用您的交易資料。Apple 與其餘子公司無從得知您的付款、收款對象或是使用 Apple Pay Cash 卡片進行購買的地點。

當你透過 Apple Pay 付款、將款項加入 Apple Pay 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隨機數，這個隨機數與 App 中針對 Apple Pay 傳回的數值類似。隨機數和其他交易資料會傳遞到 Secure Element 以產生付款簽名。付款簽名從 Secure Element 傳出時，會傳遞至 Apple Pay 伺服器。Apple Pay 伺服器會透過付款簽名和隨機數驗證交易的認證、完整性和正確性。接著就會啟動轉帳程序，並在交易完成時通知您。

如果交易包含使用信用卡或金融卡為 Apple Pay Cash 加值、付款給另一位使用者，或在 Apple Pay Cash 餘額不足時提供補充款項，那麼系統會產生一個加密付款憑證並傳送至 Apple Pay 伺服器，這與在 App 和網站中用於 Apple Pay 的憑證類似。

Apple Pay Cash 帳號的餘額超過一定金額後，或是當偵測到異常活動，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（例如確認您先前所居住的街道名稱）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。

交通卡

在中國和日本，使用者可在支援的 iPhone 和 Apple Watch 機型上將支援的交通卡加入「錢包」中。方法為從實體卡片將餘額和定期券轉移至其數位「錢包」代表票卡中，或是從發卡機構的 App 佈建新交通卡到「錢包」中。將交通卡加入「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。在日本，Suica 還能用來付款。

加入的交通卡會與使用者的 iCloud 帳號綁定。如果使用者加入超過一張卡片至「錢包」，Apple 或交通卡發卡機構可能可以連結卡片間的使用者個人資訊和相關帳號資訊。例如 MySuica 卡可以與匿名 Suica 卡連結。交通卡和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「錢包」的過程中，使用者必須輸入卡片序號的識別數字。使用者也需要提供個人資訊來證明卡片持有人身分。例如，如果使用 MySuica 卡或包含定期券的 Suica 卡，則使用者也必須輸入出生日期。將票卡從 iPhone 轉移至 Apple Watch 時，轉移過程中兩部裝置都必須處於上線狀態。

可透過「錢包」從信用卡和預付卡或從交通卡發卡機構的 App 進行加值。使用 Apple Pay 時重新載入餘額的安全性，於本白皮書中「使用信用卡和金融卡在 App 內付款」一節說明。

從交通卡發卡機構的 App 內佈建交通卡的程序，於本白皮書中「從發卡機構的 App 加入信用卡或金融卡」一節中說明。

交通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。通過驗證後，系統可為 Secure Element 建立「裝置帳號號碼」，並在「錢包」中啟用新加入且含有轉移餘額的票卡。在日本，完成從實體卡片佈建後，實體 Suica 卡便會停用。

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。交通業者擁有密鑰，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，使用者可享有流暢的「快速交通卡」體驗，無須使用 Touch ID、Face 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。使用者若要啟用 Touch ID、Face 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。

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

- 透過「尋找我的 iPhone」從遠端清除裝置
- 透過「尋找我的 iPhone」啟用「遺失模式」
- 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「錢包」移除所有卡片
- 在發卡機構的 App 中移除卡片

Apple Pay 伺服器會通知交通業者停用這些卡片。針對 Suica 卡，如果裝置在使用者嘗試清除時處於離線狀態，Suica 卡可能仍可在某些終端機上使用，直到隔天凌晨 12:01（日本標準時間）才會失效。在中國，如果使用者的裝置處於離線狀態，交通卡會繼續開放使用。

如果使用者移除了交通卡，可將餘額加回以相同 Apple ID 登入的裝置上來收回餘額。

學生證

在 iOS 12 中，參與方案的院校所屬教職員生可將其在校相關證件加入「錢包」中，以便進出校園設施及在接受其證件的地方付款。

使用者透過證件發卡機構或參與學校提供的 App，將其證件加入「錢包」中。此操作的技術程序，與本指南上文「從發卡機構的 App 加入信用卡或金融卡」中所述的程序相同。此外，發卡機構的 App 必須支援對保護其證件存取權的帳號使用雙重認證。最多可同時在以相同 Apple ID 登入的任兩部支援 Apple 裝置上設定同一張卡片。

若將學生證加入「錢包」，系統會預設開啟「快速模式」。處於「快速模式」的學生證無需 Touch ID、Face ID 或密碼驗證便可與接受終端機互動。使用者可以按一下「錢包」中證件正面的「更多」按鈕，然後關閉「快速模式」來停用此功能。重新啟用「快速模式」必須使用 Touch ID、Face ID 或密碼。

可藉由以下方式停用或移除學生證：

- 透過「尋找我的 iPhone」從遠端清除裝置
- 透過「尋找我的 iPhone」啟用「遺失模式」
- 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「錢包」移除所有卡片
- 在發卡機構的 App 中移除卡片

停用、移除和清除卡片

使用者可以使用「尋找我的 iPhone」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「尋找我的 iPhone」、iCloud.com 或直接在裝置上使用「錢包」來清除 Apple Pay 中的卡片。在 Apple Watch 上，可以使用 iCloud 設定、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。

此外，當使用者透過「清除所有內容和設定」、使用「尋找我的 iPhone」來清除整部裝置，或在復原模式下將裝置回復時，iOS 會指示 Secure Element 將所有卡片標記為已刪除。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 標示為無效，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，以確保 Secure Element 中的所有卡片皆已清除。

Internet 服務

製作高強度的 Apple ID 密碼
Apple ID 會用來連接許多服務，包含 iCloud、FaceTime 和 iMessage。為了協助使用者製作高強度密碼，所有新帳號都必須包含下列密碼屬性：

- 至少有八個字元
- 至少有一個字母
- 至少有一個大寫字母
- 至少有一個數字
- 連續的相同字元不得超過三個
- 不能與帳號名稱相同

Apple 已內建一套強大的服務來協助使用者更充分地使用裝置並提高生產力，其中包含 iMessage、FaceTime、「Siri 建議」、iCloud、「iCloud 備份」和「iCloud 鑰匙圈」。

這些 Internet 服務都具備了 iOS 在整個平台上推動的安全性目標。這些目標包含安全處理資料，無論是裝置上儲存的靜態資料或是透過無線網路傳輸的資料；保護使用者的個人資訊；以及對資料和服務的惡意或未經授權的存取威脅加以防護。每項服務在使用其本身的強大安全性架構時，絲毫不影響 iOS 整體的易用性。

Apple ID

Apple ID 是一組帳號，用來登入 Apple 服務，如 iCloud、iMessage、FaceTime、iTunes Store、Apple Books、App Store 等。對使用者而言，安全地保護其 Apple ID 以防止帳號遭未經授權的存取，是十分重要的。為了達成此目標，Apple 要求使用長度至少為八個字元的安全密碼，同時包含字母和數字，連續的相同字元不得超過三個，且不能為常用的密碼。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。Apple 也會要求使用者設定三個安全問題，以在持有者要更改帳號資訊或重置忘記的密碼時，用來協助驗證其身分。

在對帳號進行重要更動（例如密碼或帳單資訊經變更），或使用 Apple ID 來在新裝置上登入時，Apple 也會向使用者發送電子郵件和推播通知。若有任何事件看似異常，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 因應任何可能影響客戶安全的新資訊。

雙重認證

為協助使用者進一步保護其帳號，Apple 提供了雙重認證，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。

透過雙重認證，使用者的帳號只能在信任的裝置上存取，例如使用者的 iPhone、iPad 或 Mac。若要在任何新裝置上首次登入，則需要兩項資訊：Apple ID 密碼以及自動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、macOS、tvOS、watchOS 和 Apple 網站使用的認證系統。

如需更多雙重認證的相關資訊，請前往：support.apple.com/zh-tw/HT204915

雙步驟驗證

自 2013 年開始，Apple 也提供了類似的安全性方式，稱為雙步驟驗證。啟用雙步驟驗證後，使用者必須藉由發送至其中一部受信任裝置的臨時代碼來驗證其身分，才有權更改其 Apple ID 帳號資訊、登入 iCloud、iMessage、FaceTime 或 Game Center，以及在新裝置的 iTunes Store、Apple Books 或 App Store 中進行購物。若使用者忘記密碼或無法存取其受信任的裝置，也可以使用存放在安全位置、由 14 個字元組成的「復原密鑰」。雖然我們大多鼓勵新使用者使用雙重認證，但仍有某些情況會改為建議使用雙步驟驗證。

如需更多 Apple ID 雙步驟驗證的相關資訊，請前往：
support.apple.com/zh-tw/HT204152

管理式 Apple ID

「管理式 Apple ID」 會以類似於 Apple ID 的方式運作，但是由教育機構所持有並控制。機構可以重置密碼、限制購買和通訊（如 FaceTime 和 「訊息」），以及替教職員、教師和學生設定以角色為基礎的權限。

「管理式 Apple ID」 會停用部分 Apple 服務，如 Apple Pay、「iCloud 鑰匙圈」、HomeKit 和 「尋找我的 iPhone」。

如需更多 「管理式 Apple ID」 的相關資訊，請前往：
help.apple.com/schoolmanager/#/tes78b477c81

稽核管理式 Apple ID

「管理式 Apple ID」 亦支援稽核，可讓機構遵守法律和隱私法規。管理者、經理或教師帳號可授予特定 「管理式 Apple ID」 的稽核權限。稽核者只能監視學校階層中層級低於自己的帳號。亦即教師可以監視學生；經理可以稽核教師和學生；管理者可以稽核經理、教師和學生。

在使用 Apple School Manager 要求稽核憑證時，系統會核發一個特殊帳號，其僅能存取要求稽核的 「管理式 Apple ID」。稽核權限會在七天後到期。在這期間，稽核者可以讀取並修改使用者儲存在 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 School Manager 中。記錄會顯示誰是稽核者、稽核者要求存取的 「管理式 Apple ID」、要求的時間，以及是否有執行稽核。

如需更多稽核 「管理式 Apple ID」 的相關資訊，請前往：
help.apple.com/schoolmanager/#/tesd8fcbdd99

管理式 Apple ID 和個人裝置

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

iMessage

Apple 的 iMessage 是一項適用於 iOS 裝置、Apple Watch 和 Mac 電腦的傳訊服務。iMessage 支援文字以及照片、聯絡資訊、位置資訊等附件。資訊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 充分使用了 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。

當使用者在裝置上打開 iMessage 後，裝置會產生以下兩對密鑰供服務使用：用於加密的 1280 位元 RSA 密鑰和 NIST P-256 曲線上用於簽署的 256 位元 ECDSA 密鑰。每一組密鑰的專用密鑰會儲存在裝置的鑰匙圈中，公用密鑰則與裝置的 APNs 位址一起傳送至 Apple 識別服務（IDS），在目錄服務中，公用密鑰會與使用者的電話號碼或電子郵件位址相關聯。

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 位址及所關聯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位址，系統會藉由傳送確認連結來驗證這些電子郵件位址。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，還有多個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位址加入時，使用者所有已註冊的裝置都會顯示一則提示訊息。

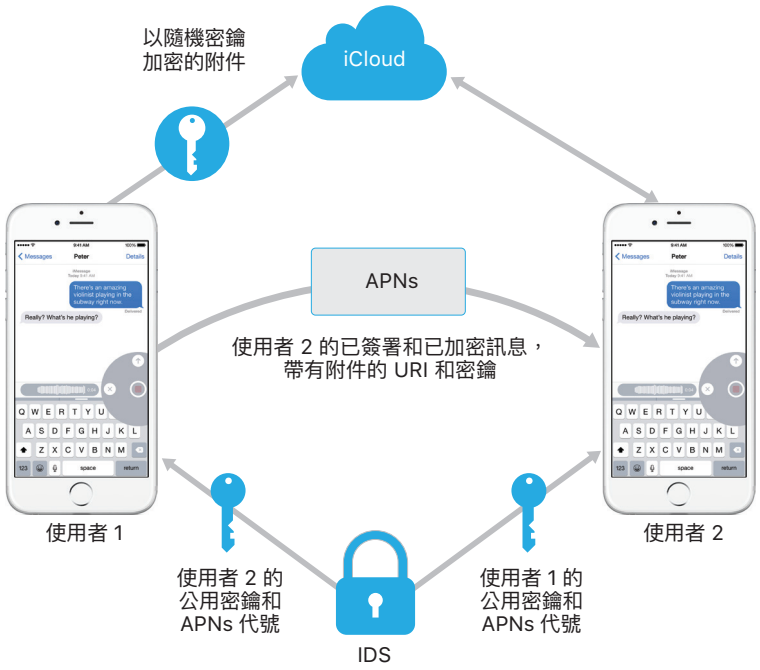
在 iOS 12 或以上版本上，從連結至同一個 Apple ID 的不同位址傳來的訊息，在接收訊息的裝置上會顯示為單一對話。此功能使用向 IDS 擷取的帳號識別碼，以及電子郵件位址或電話號碼的公用密鑰和 APNs 位址。

iMessage 傳送和接收訊息的方式

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位址，裝置就會聯絡 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，裝置會先利用使用者的「聯絡資訊」App 來收集與該名字綁定的電話號碼和電子郵件位址，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 RSA 加密密鑰會從 IDS 擷取。針對每部接收裝置，傳送裝置會產生隨機 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 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，而雜湊值會使用傳送裝置的專用簽署密鑰以 ECDSA 進行簽署。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 版本而定，APNs 最多只可以中繼大小為 4KB 或 16KB 的訊息。若訊息文字過長或隨附附件（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 **URI（統一資源識別碼）**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機密性和完整性，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位址與接收者的聯絡資訊相符，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。目前訊息最多可儲存 30 天。

商務聊天

「商務聊天」 是讓使用者可使用 「訊息」 App 來與商家通訊的傳訊服務。只有使用者可發起對話，而商家會收到難以識別該使用者的識別碼。商家不會收到使用者的電話號碼、電子郵件位址或 iCloud 帳號資訊。當您與 Apple 聊天時，Apple 會收到與您的 Apple ID 綁定的 「商務聊天 ID」。使用者保有是否要繼續通訊的控制權。刪除 「商務聊天」 對話會將其從使用者的 「訊息」 App 中移除，並阻止商家繼續傳送訊息給使用者。

傳送給商家的訊息會在使用者裝置和 Apple 的傳訊伺服器之間分別加密，而 Apple 的傳訊伺服器會將這些訊息解密，再透過 TLS 轉送給商家。商家的回覆機制也雷同，會透過 TLS 傳送至 Apple 的傳訊伺服器，伺服器會重新加密訊息再傳送至使用者的裝置。若使用 iMessage，訊息可排入佇列最多 30 天，等待傳送給離線的裝置。

FaceTime

FaceTime 是 Apple 的視訊和語音通話服務。與 iMessage 類似，FaceTime 通話使用 「Apple 推播通知」 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。這個共享密鑰會透過 「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和 HMAC-SHA1 使用 AES-256 來加密 SRTP 封包。完成初始連線和安全性設定後，FaceTime 便會使用 STUN 與「Internet 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。雖然重複使用了許多一對一 FaceTime 的基礎架構和設計，不過 「群組 FaceTime」 通話採用以 IDS 所提供的確實性為基礎的全新密鑰建立機制。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。作業階段密鑰是透過 AES-SIV 來封裝，並使用 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位址加入進行中的 「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。

iCloud

iCloud 會儲存使用者的聯絡資訊、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。使用者設定 iCloud 的方式為使用 Apple ID 登入，然後選擇想使用的服務。IT 管理者可透過 MDM 設定描述檔來停用 iCloud 功能，包括 「我的照片串流」、「iCloud 雲碟」 和 「iCloud 備份」 等。該服務無法得知正在儲存的內容，並會以位元組集合的方式對所有檔案進行處理。

每個檔案都會區分為區塊，並由 iCloud 使用 AES-128 以及從利用 SHA-256 的各區塊內容所衍生的密鑰進行加密。這些密鑰與檔案的後設資料會由 Apple 儲存在使用者的 iCloud 帳號中。檔案的加密區塊會使用 Apple 和第三方的儲存服務進行儲存，不會含有任何使用者的識別資訊。

iCloud 雲碟

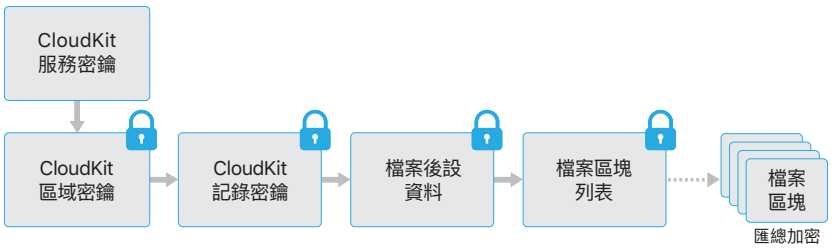
「iCloud 雲碟」 會加入以帳號為基礎的密鑰來保護儲存在 iCloud 中的文件。和現有的 iCloud 服務一樣，「iCloud 雲碟」 會將檔案內容分塊並進行加密，然後使用第三方的服務來儲存這些加密區塊。不過，檔案內容密鑰是由記錄密鑰所封裝，與「iCloud 雲碟」後設資料儲存在一起。而這些記錄密鑰則由使用者的 「iCloud 雲碟服務密鑰」 保護，

儲存在使用者的 iCloud 帳號中。使用者可以藉由與 iCloud 進行認證來存取其 iCloud 文件後設資料，但也必須擁有「iCloud 雲碟服務密鑰」才能顯示「iCloud 雲碟」儲存空間中受保護的部分。

CloudKit

CloudKit 允許 App 開發者在 iCloud 中儲存鍵值資料、結構資料和資產。對 CloudKit 的存取是使用 App 授權來加以控制。CloudKit 同時支援公用和專用資料庫。公用資料庫是由 App 的所有拷貝使用，通常用於一般資產，且並未加密。專用資料庫則會儲存使用者的資料。

如同使用「iCloud 雲碟」一樣，CloudKit 會使用以帳號為基礎的密鑰來保護存放在使用者專用資料庫中的資訊，就像其他 iCloud 服務，檔案會使用第三方的服務加以切割、加密並儲存。CloudKit 使用的是階層式密鑰（與「資料保護」類似）。檔案專屬密鑰是以 CloudKit 記錄密鑰加以封裝。「記錄」密鑰則會依序由整個區域的密鑰加以保護，其受到使用者的 CloudKit 服務密鑰所保護。「CloudKit 服務密鑰」會存放在使用者的 iCloud 帳號，且僅可在使用者已向 iCloud 認證後才可使用。



CloudKit 端對端的加密

Apple Pay Cash、「健康」資料、使用者密碼、Siri 智慧和「嘿 Siri」均使用 CloudKit 端對端的加密，並搭配受 iCloud 鑰匙圈同步保護的「CloudKit 服務密鑰」。對這些 CloudKit 容器而言，密鑰階層根生於 iCloud 鑰匙圈中，因此擁有與 iCloud 鑰匙圈相同的安全特徵：密鑰只能在使用者的受信任裝置上使用，Apple 或任何第三方均無法使用。若失去 iCloud 鑰匙圈資料的存取權（請參閱本白皮書下文的「託管安全性」章節），CloudKit 中的資料就會重置，如果資料可以從受信任的本機裝置存取，便會重新上傳至 CloudKit。

iCloud 雲端「訊息」也使用 CloudKit 端對端的加密，並搭配由「iCloud 鑰匙圈」同步功能保護的「CloudKit 服務密鑰」。如果使用者已啟用「iCloud 備份」，系統便會將用於 iCloud 雲端「訊息」容器的「CloudKit 服務密鑰」備份至 iCloud，如此一來，即使使用者無法存取「iCloud 鑰匙圈」和受信任裝置，仍可復原其訊息。每當使用者關閉「iCloud 備份」，這個「iCloud 服務密鑰」就會變換。

iCloud 備份

iCloud 還會每天通過 Wi-Fi 備份資訊，包括裝置設定、App 資料、「相機膠卷」中的照片和影片，以及「訊息」App 中的對話。透過 Internet 傳送內容時，iCloud 會對其進行加密，以加密的格式儲存並使用安全代號進行認證，進而保護內容。只有當裝置處於鎖定狀態、連接到電源且可透過 Wi-Fi 連接 Internet 時，「iCloud 備份」才會進行。多虧 iOS 中所使用的加密技術，系統經過精心設計，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。

以下是 iCloud 備份的項目：

- 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 iOS 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、Apple Books 或 App Store 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 相關聯。

復原選項

情況	CloudKit 端對端加密的使用者復原選項
可取用受信任的裝置	可透過受信任的裝置或「iCloud 鑰匙圈」復原功能來復原資料。
無受信任的裝置	只能透過「iCloud 鑰匙圈」復原功能來復原資料

復原選項

情況	iCloud 雲端「訊息」的使用者復原選項
已啟用「iCloud 備份」且可取用受信任的裝置	可透過「iCloud 備份」、取用受信任的裝置或「iCloud 鑰匙圈」復原功能來復原資料。
已啟用「iCloud 備份」且無法取用受信任的裝置	可透過「iCloud 備份」和「iCloud 鑰匙圈」復原功能來復原資料。
已停用「iCloud 備份」且可取用受信任的裝置	可透過受信任的裝置或「iCloud 鑰匙圈」復原功能來復原資料。
已停用備份且無受信任的裝置	只能透過「iCloud 鑰匙圈」復原功能來復原資料。

- 使用者 iOS 裝置上的照片與影片。請注意，若使用者在其 iOS 裝置（iOS 8.1 或以上版本）或 Mac（OS X 10.10.3 或以上版本）上開啟「iCloud 照片圖庫」，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」中。
- 聯絡資訊、行事曆行程、提醒事項和備忘錄
- 裝置設定
- App 資料
- 通話記錄和鈴聲
- 主畫面和 App 整理
- HomeKit 設定
- Visual Voicemail 密碼（備份時需要可運作的 SIM 卡）
- iMessage、「商務聊天」、簡訊（SMS）與 MMS 訊息（備份時需要可運作的 SIM 卡）

注意：若已啟用 iCloud 雲端「訊息」，iMessage、「商務聊天」、簡訊（SMS）與 MMS 訊息都會從現有的「iCloud 備份」中移除，改為儲存在「訊息」的端對端加密 CloudKit 容器中。使用者的「iCloud 備份」會保留該容器的密鑰。如果使用者之後停用了「iCloud 備份」，該容器的密鑰就會變換，新密鑰只會儲存在「iCloud 鑰匙圈」中（Apple 和任何第三方均無法存取），且寫入該容器的新資料無法用舊的容器密鑰解密。

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。檔案會以其原始的加密狀態備份至 iCloud。資料保護類別為「無保護」的檔案會在傳輸期間進行加密。

「iCloud 備份」Keybag 內含每個「資料保護」類別的非對稱（Curve25519）密鑰，這些密鑰用於加密檔案專屬密鑰。如需更多備份 Keybag 和「iCloud 備份」Keybag 內容的相關資訊，請參閱本白皮書「加密與資料保護」一節中的「鑰匙圈資料保護」。

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。）

當使用者的鑰匙圈資料庫備份至 iCloud 時，仍會受到與 UID 連結的密鑰保護。這樣可讓鑰匙圈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）都無法讀取使用者的鑰匙圈項目。

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，進而根據其「資料保護」類別對其重新加密。

iCloud 鑰匙圈

Safari 與 iCloud 鑰匙圈的整合
Safari 可以產生加密編譯的高安全性隨機字串來用作網站密碼，然後將其儲存在鑰匙圈中並與您的其他裝置同步。鑰匙圈項目透過 Apple 伺服器在不同的裝置之間傳輸，但會嚴格進行加密，Apple 和其他裝置均無法讀取其內容。

iCloud 鑰匙圈可讓使用者在 iOS 裝置和 Mac 電腦之間安全地同步其密碼，不會將此資訊提供給 Apple。除了強大的隱私保護和安全性，易用性和回復鑰匙圈的功能對「iCloud 鑰匙圈」的設計和架構也具有重要影響。「iCloud 鑰匙圈」由兩項服務組成：鑰匙圈同步和鑰匙圈復原。

Apple 設計的「iCloud 鑰匙圈」和鑰匙圈復原可確保使用者的密碼在下列情況下仍然受到保護：

- 使用者的 iCloud 帳號被盜。
- 外部攻擊者或員工危害了 iCloud 的安全性。
- 第三方存取使用者帳號。

鑰匙圈同步

當使用者第一次啟用「iCloud 鑰匙圈」時，裝置將建立信任圈並為自己製作同步身分。同步身分包括專用密鑰和公用密鑰。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金鑰（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。

已簽署的同步信任圈會置於使用者的 iCloud 密鑰值儲存區域。如果不知道使用者的 iCloud 密碼，就無法對其進行讀取，如果沒有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。

當使用者在其他裝置上開啟「iCloud 鑰匙圈」時，這部裝置察覺使用者之前在 iCloud 中建立的一個同步信任圈並非成員。該裝置會製作其同步身分的成對密鑰組，然後製作應用程式申請單以要求加入該信任圈。該申請單包括裝置的同步身分公用密鑰，系統將要求使用者以其 iCloud 密碼進行認證。橢圓密鑰產生參數會從 iCloud 取回並產生用於簽署應用程式申請單的密鑰。最終，應用程式申請單會置於 iCloud 中。

當第一部裝置接收到應用程式申請單時，會顯示一則通知，讓使用者確認新裝置正在要求加入同步信任圈。該使用者輸入其 iCloud 密碼，應用程式申請單則藉由比對專用密鑰的簽名進行驗證。這樣便確認產生了加入信任圈要求的人員，在發出要求時輸入了使用者的 iCloud 密碼。

使用者核准將新裝置加入到信任圈後，第一部裝置會將新成員的公用密鑰加入到同步信任圈，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名。

假設簽名信任圈有兩個成員，並且每個成員擁有與其配對的公用密鑰。他們現在開始透過 iCloud 鍵值儲存空間來交換個別的鑰匙圈項目，或儲存在 CloudKit 中（如適用）。如果兩個信任圈成員擁有相同的項目，將同步修改日期最近的項目。如果另一個成員擁有該項目且修改日期相同，則將略過這些項目。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 均無法對其進行解密。

當新裝置加入同步信任圈時，將會重複該過程。例如，當第三部裝置加入時，另外兩名使用者的裝置上均會出現確認訊息。使用者可以從其中任一部裝置來核准新成員。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，以確保所有成員擁有相同的鑰匙圈項目。

但是整個鑰匙圈不會進行同步。某些項目專屬於特定裝置（例如 VPN 身分），這些項目不會離開裝置。僅會同步具有 `kSecAttrSynchronizable` 屬性的項目。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）、Wi-Fi 網路密碼以及 HomeKit 加密密鑰設定了此屬性。

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`。

鑰匙圈復原

鑰匙圈復原功能讓使用者可以將其鑰匙圈交由 Apple 託管，但不允許 Apple 讀取密碼和鑰匙圈包含的其他資料。即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。當使用 Safari 來為 Web 帳號產生隨機且安全的密碼時，這尤其重要，因為這些密碼的唯一記錄位於鑰匙圈中。

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安全密碼進行加密，只有在滿足一系列嚴格的條件時，託管服務才會提供鑰匙圈拷貝。

當 iCloud 鑰匙圈已開啟時，若使用者的帳號啟用了雙重認證，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。

然後，iOS 裝置會匯出使用者的鑰匙圈拷貝，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性模組（HSM）叢集公用密鑰進行封裝。這會變成使用者的「iCloud 託管記錄」。

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

除了建立安全碼，使用者必須註冊電話號碼。這在鑰匙圈復原期間提供了第二層的身分認證。使用者將會收到一則簡訊，必須回覆此簡訊才能繼續復原程序。

託管安全性

iCloud 為鑰匙圈託管提供了安全的基礎架構，可確保只有經過授權的使用者和裝置才能執行復原作業。iCloud 背後部署的是 HSM 叢集，可保護託管記錄。叢集的每位成員都有一個密鑰，用來對其監管的託管記錄進行加密，如本白皮書中前文所述。

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 iCloud 安全碼來將用於加密使用者鑰匙圈的隨機密鑰解除封裝。有了該密鑰，您便可解密從 iCloud 鍵值儲存空間擷取的鑰匙圈，並將其回復到裝置上。最多允許對託管記錄認證和擷取 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持有人將會收到訊息，通知他們已失去其託管記錄。他們之後可以選擇重新註冊。

Siri

使用者只需自然地開口說話，即可透過 Siri 來傳送訊息、排程會議、撥打電話以及執行其他操作。Siri 使用語音辨識、文字到語音轉換和主從式架構，以回應各種要求。Siri 支援的工作經過專門設計，可確保盡量只使用最少的個人資訊，並對這些資訊提供完善的保護。

Siri 開啟後，裝置將會製作隨機識別碼，以用於語音辨識和 Siri 伺服器。這些識別碼僅用於 Siri 內部，並用來改善服務。如果隨後關閉了 Siri，裝置將會產生新的隨機識別碼，以便在 Siri 重新開啟時使用。

為了改進 Siri 的功能，系統會將裝置中的某些使用者資訊傳送給伺服器。這些資訊包括：音樂資料庫（歌曲名稱、演出者和播放列表）、「提醒事項」列表名稱以及「聯絡資訊」中定義的姓名和關係。裝置與伺服器所進行的所有通訊均透過 HTTPS 來完成。

啟動 Siri 對話後，系統會將使用者的名字和姓氏（來自「聯絡資訊」）以及約略的地理位置傳送至伺服器。如此一來 Siri 便可使用姓名回應或回答只需要大概位置的問題，例如天氣相關資訊。

如果需要更精確的位置（例如附近電影院的確切位置），伺服器將會要求裝置提供更精確的位置。以上範例說明了在預設情況下，如何將資訊傳送至伺服器（僅限於為了處理使用者要求而有必要傳送的情況下）。在任何情況下，只要 10 分鐘內沒有任何動作，系統就會捨棄對話資訊。

若 Siri 要求是來自 Apple Watch，手錶會製作其本身的隨機專屬識別碼，如前文所說明。然而，該要求也會傳送已配對 iPhone 的 Siri 識別碼來作為使用者資訊的參考，而非再次傳送使用者的資訊。

系統會將使用者的說話內容錄音傳送至 Apple 的語音辨識伺服器。如果任務僅涉及聽寫，系統便會將辨識出的文字傳送回裝置中。否則，Siri 會對文字進行分析，必要時會將其與來自裝置相關之描述檔的資訊相結合。例如，如果要求是「發訊息給媽媽」，便會使用從「聯絡資訊」上傳的關係和姓名。然後會將已確認動作的指令傳送回要執行指令的裝置。

許多 Siri 功能是由裝置依照伺服器的指示來完成的。例如，當使用者要求 Siri 朗讀收到的訊息時，伺服器就會要求裝置朗讀其未讀訊息的內容。訊息的內容和傳送者資訊不會傳送到伺服器。

使用者的語音錄音將保存 6 個月，讓辨識系統能夠加以利用，以便更有效地理解使用者的語音內容。6 個月後，將會儲存另一份不含識別碼的拷貝，以供 Apple 持續改善和開發 Siri，保存時間最長為兩年。兩年過後，不包含識別碼的小型錄製子集、聽寫記錄和相關資料仍可能會繼續由 Apple 用於持續改進和確保 Siri 的品質。此外，某些引用音樂、運動隊伍和隊員以及商家或興趣點的錄音同樣會儲存，以用於改善 Siri。

無需動手，透過語音也可以啟動 Siri。語音觸發偵測會在本機裝置上進行。在此模式下，只有當傳入的音訊模式十分符合指定觸發詞語的原聲時，Siri 才會啟動。偵測到語音觸發詞語後，對應的音訊（包括後續的 Siri 指令）會傳送到 Apple 的語音辨識伺服器作進一步處理，此過程所遵循的規則，與透過 Siri 執行其他使用者語音錄音時遵循的規則相同。

使用者也可拿起手錶靠近嘴邊並說出 Siri 要求，來啟動 Apple Watch 上的 Siri。當同時發生以下兩種情況，就能以這個方式啟動 Siri：

- 裝置上機器學習模型偵測到裝置附近出現人類語音原聲
- 第二個裝置上機器學習模型識別到符合「抬起說話」手勢的動作軌跡和裝置姿勢

偵測到這個動作和語音組合時，對應的音訊會傳送到 Apple 的語音辨識伺服器做進一步處理，此過程所遵循的規則，與透過 Siri 執行其他使用者語音錄音時遵循的規則相同。

Siri 建議

針對 App 和捷徑的 Siri 建議是由裝置上機器學習功能產生。不會有任何資料傳送至 Apple，除非資訊無法用於識別使用者的哪些訊號為捷徑或 App 啟動的有用預測。

Siri 的捷徑

加入 Siri 的捷徑會使用 iCloud 在所有 Apple 裝置上同步，並使用 CloudKit 端對端加密技術來加密。與捷徑相關聯的語句會同步至 Siri 伺服器以進行語音辨識，並與「Siri」一節中所說明的隨機 Siri 識別碼綁定。Apple 不會收到捷徑的內容，這些內容儲存在本機的資料保險箱中。

「捷徑」App

您可使用 iCloud 選擇性將「捷徑」App 中的自定捷徑同步到不同 Apple 裝置上。您也可透過 iCloud 與其他使用者分享捷徑。

自定捷徑包羅萬象，類似於指令碼或程式。從 Internet 下載的捷徑會透過隔離系統遭到隔離。使用者第一次使用捷徑時會收到警告，且有機會可檢查捷徑，包含其來源等資訊在內。

若從共享工作表啟動，自定捷徑也可在 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），系統會下載更新版惡意軟體定義以即時識別惡意程式碼。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。

Safari 建議、搜尋中的「Siri 建議」、查詢字詞、# 影像、「新聞」App 和「新聞」小工具（非適用「新聞」國家或地區）

Safari 建議、搜尋中的「Siri 建議」、查詢字詞、# 影像、「新聞」App 和「新聞」小工具（非適用「新聞」國家或地區）會顯示裝置本身以外的使用者建議，來源包括維基百科、iTunes Store、當地新聞、「地圖」結果及 App Store；甚至會在使用者開始輸入文字前提供建議。

當使用者開始在 Safari 位址列中輸入、在搜尋打開或使用「Siri 建議」、使用「查詢字詞」、打開 # 影像、在「新聞」App 中使用「搜尋」或使用「新聞」小工具（非適用「新聞」國家或地區）時，會使用 HTTPS 來加密下列內容並傳送給 Apple，以向使用者提供相關的結果：

- 每 15 分鐘替換的識別碼，用於保護隱私。
- 使用者的搜尋查詢。
- 最有可能的完整查詢建議（根據內容和於本機快取的過去搜尋記錄得出）。
- 其裝置的大略位置，如果使用者已為「基於位置的建議」開啟「定位服務」。位置模糊的程度取決於對裝置所在位置所估算的人口密度；例如，鄉村位置的模糊程度較高，那裡使用者的地理位置可能相距較遠，而在市中心的模糊程度較低，因為那裡的使用者彼此之間的距離通常較靠近。使用者可以在「設定」中關閉「基於位置的建議」的「定位服務」，停止將所有位置資訊傳送給 Apple。若「定位服務」已關閉，Apple 便可能使用裝置的 IP 位址來推測大略位置。
- 裝置的類型以及是否在「搜尋」、Safari、「查詢字詞」、「新聞」App 或「訊息」中使用「Siri 建議」所進行的搜尋。
- 連線類型。
- 裝置上最近使用過的三個 App 資訊（提供額外的搜尋內容）。只會納入由 Apple 維護的熱門 App 允許名單中的 App，以及最近 3 小時內曾存取過的 App。
- 裝置上熱門應用程式的列表。
- 地區語言、地區設定及輸入法偏好設定。
- 如果使用者的裝置可存取音樂或影片訂閱服務，則這些訂閱服務的名稱或訂閱類型等資訊可能會傳送給 Apple。使用者的帳號名稱、編號及密碼不會傳送給 Apple。
- 興趣主題的總結與彙總表示。

當使用者選擇某項結果，或未選擇結果即退出 App 時，部分資訊會傳送給 Apple 以協助改善未來搜尋結果的品質。此資訊僅會與同一個 15 分鐘的作業階段識別碼綁定，並不會與特定使用者綁定。回饋包含部分上述內容資訊與互動資訊，例如：

- 每次互動與每次網路搜尋要求的間隔時間。
- 建議的排名與顯示順序。
- 結果 ID 與選擇的動作（若結果非當地結果），或者所選取當地結果的類別（若結果為當地結果）。
- 標示使用者是否選擇結果的旗標。

Apple 會將「建議」記錄與查詢、內容和回饋保留 18 個月。一小部分的記錄最長會保留五年，例如查詢、地區設定、網域、約略位置和彙總指標。

在某些情況下，「建議」可能會將常見單字或詞句的查詢轉送給合格的合作廠商，以接收和顯示合作廠商的搜尋結果。Apple 會對這些查詢使用代理服務，因此合作廠商不會收到使用者的 IP 位址或搜尋回饋。與合作廠商進行的通訊是透過 HTTPS 來加密。針對頻繁發生的查詢，Apple 提供城市層次的位置、裝置類型及用戶端語言作為搜尋內容，以供合作廠商改善搜尋表現。

若要就地理位置層面和跨各種網路瞭解和改善「建議」的表現，就必須記錄下列資訊（不含作業階段識別碼）：

- 部分 IP 位址（IPv4 位址不含後 8 個位元、IPv6 位址不含後 80 個位元）
- 大略位置
- 大略的查詢時間
- 等待時間 / 傳送率
- 回應大小
- 連線類型
- 地區設定
- 裝置類型和要求的 App

Safari 智慧型防追蹤

「智慧型防追蹤」（ITP）屬於 Safari 友善隱私權的預設 Cookie 和網站資料政策其中一環。它可限制存取 Cookie 和其他網站資料，藉此預防跨網站追蹤。

ITP 會收集資源負載（影像、指令碼等）與使用者互動（例如點按次數和文字輸入項目）的統計資料。系統使用機器學習模型，根據所收集的統計資料在裝置上分類哪些網域名稱有能力跨網站追蹤使用者。

當網域被分類為具有追蹤能力，如果使用者先前曾作為第一方與該網域互動，ITP 會立即隔離其 Cookie；至於使用者尚未與其互動的已分類網域，ITP 會立刻開始封鎖其 Cookie。例如：

- video.example 提供無廣告訂閱服務，且其有大量影片嵌入其他網站中
- 使用者登入 video.example，然後登入含有 video.example 嵌入內容的其他網站
- ITP 將 video.example 分類為具有追蹤能力，因此隔離了其 Cookie
- 當使用者造訪包含 video.example 嵌入內容的 newspaper.example 時，提供給 video.example 的 Cookie 為 newspaper.example 上 video.example 專屬的隔離 Cookie

嵌入的第三方內容可能會透過「儲存空間存取 API」，要求使用者提供其第一方 Cookie 的存取權。當使用者點按使用「儲存空間存取 API」的嵌入第三方內容時，Safari 會顯示提示，詢問使用者是否要允許第三方存取其 Cookie 和網站資料，以便允許第三方在第一方網域上追蹤它們。如果使用者選取「允許」，便會允許嵌入的第三方內容在該次造訪頁面期間存取其第一方 Cookie；之後造訪時，使用者與嵌入的內容互動且內容呼叫「儲存空間存取 API」後，嵌入的第三方內容便可取得其第一方 Cookie 的存取權。此外，由於使用者先前已允許這項存取，因此不會再次顯示提示。系統會保留使用者對這個第一與第三方組合的決定，且會在使用者清除 Safari 瀏覽記錄時隨之清除。

如果使用者活躍使用 Safari 30 天期間，沒有直接或透過「儲存空間存取 API」與已分類為具有追蹤能力的網域互動，系統便會清除其現有 Cookie。30 天無互動後，分類為具有追蹤能力的網域也無法設定新 Cookie。Safari 絕不允許在第三方內容中存取其他第一方網站資料。

藉由 ITP 隔離第一方和第三方資料，有助於防止有心人士基於跨網站追蹤目的使用 Cookie 和網站資料。Apple 無從得知特定裝置已擷取統計資料或分類為具有追蹤能力的網域名稱。

除了封鎖分類為具有追蹤能力的網域之第三方 Cookie，ITP 還會將傳送給分類為具有追蹤能力的網域之 HTTP 參照位址資訊裁剪為僅含頁面的來源。

使用者密碼管理

iOS 提供多種功能，讓使用者可安全且便利地輕鬆驗證使用密碼進行驗證的第三方 App 及網站。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「設定」>「密碼與帳號」>「網站與 App 密碼」中管理。若無使用者許可，App 無法存取「密碼自動填寫」鑰匙圈。儲存在「密碼自動填寫」鑰匙圈中的憑證會透過「iCloud 鑰匙圈」（若已啟用）在不同裝置間同步。

「iCloud 鑰匙圈」密碼管理員和「密碼自動填寫」提供以下功能：

- 在 App 和網站中填寫憑證
- 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

App 存取已儲存的密碼

共享 Web 憑證 API

如果 iOS App 可使用以下兩個 API 與「密碼自動填寫」鑰匙圈互動：

`SecRequestSharedWebCredential`

`SecAddSharedWebCredential`

只有 App 開發者和網站管理者核准且使用者同意後，才會授予存取權限給 iOS App。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 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 才會將網站和 App 標示為具有信任關係。只有在具有信任關係的情況下，才會呼叫這兩個 API 並向使用者發出提示，使用者同意後，才會將密碼核發給 App、更新或刪除。

對 App 使用「密碼自動填寫」

iOS 允許使用者在 App 的憑證相關欄位中輸入儲存的使用者名稱和密碼，方法為點一下 iOS 鍵盤的「快速輸入」列上顯示的「鑰匙」。系統會運用 apple-app-site-association 檔案提供的相同 App 與網站關聯機制，為 App 和網站建立穩固的關聯。這個介面不會向 App 提供任何憑證資訊，除非使用者同意釋出憑證給 App。當 iOS 將網站和 App 標示為具有受信任關係，「快速輸入」列也會直接建議填入 App 中的憑證。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 App 不需要採用 API。

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 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。

自動使用高強度密碼

當「iCloud 鑰匙圈」已啟用，iOS 會在使用者於 App 中或 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。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「iCloud 鑰匙圈」已啟用的裝置間同步。

iOS 產生的密碼預設長度為 20 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。

iOS 會根據啟發法在 App 和 Safari 中產生密碼，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密碼內容是否適用於製作密碼，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"。

App 和網站可提供規則給 iOS，以確認產生的密碼相容於相關服務。iOS 會盡可能產生符合這些規則且強度最高的密碼。開發者使用 UITextInputPasswordRules 或 <input> 元素中的 passwordrules 屬性來提供規則。

傳送密碼給其他人或裝置

AirDrop

當 iCloud 已啟用，使用者可使用 AirDrop 將已儲存的憑證傳送至其他裝置，包含儲存憑證的網站、其使用者名稱和密碼。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。（請參閱「AirDrop 安全性」以取得更多資訊。）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。

Apple TV

「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 會顯示提示，邀請使用者與 Apple TV 分享一組憑證。使用相同 iCloud 帳號的 iPhone 和 Apple TV 會在進行此程序的過程中加密兩部裝置間的通訊。如果 iPhone 登入不同的 iCloud 帳號，那麼 Apple TV 會：

- 使用 PIN 碼來建立加密連線
- iPhone 必須解鎖並靠近與該 Apple TV 配對的 Siri Remote 才會收到此提示。

使用藍牙 LE 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

使用者可指定符合的第三方應用程式，做為「密碼與帳號」設定中「自動填寫」的憑證提供者。這個機制建立在延伸功能之上。憑證提供者延伸功能必須提供選擇憑證的畫面，且可選擇性提供有關已儲存憑證的 iOS 後設資料，以便直接在「快速輸入」列上提供。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。使用者選擇將密碼填入 App 中或 Safari 中的網站上時，iOS 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 Sandbox 內，且 App 解除安裝時會自動移除。

裝置控制

iOS 支援具彈性的安全性原則和設定，讓使用者容易實施與管理。這可讓各機構保護公司資訊並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）。

公司可以使用密碼保護、設定描述檔、遠端清除和第三方 MDM 解決方案等資源來管理裝置流通並協助確保公司的資料安全，甚至在員工使用私人的 iOS 裝置存取資料時，亦能保障安全。

密碼保護

依照預設，使用者的密碼可定義為數值的 PIN。在配備 Touch ID 或 Face ID 的裝置上，密碼長度至少需有四位數。使用者可在「設定」>「密碼」中的「密碼選向」中選取「自定英數密碼」，來指定較長的英數字元密碼。較長且複雜的密碼比較難以猜測或攻擊，建議使用此類密碼。

管理者可以使用 MDM 或 Exchange ActiveSync，或是要求使用者手動安裝設定描述檔，來強制實施複雜密碼要求和其他原則。可使用下列密碼原則：

- 允許簡易數值
- 需要英數數值
- 最短密碼長度
- 最短複雜字元數量
- 最長密碼使用期限
- 密碼總覽
- 自動鎖定逾時
- 無需密碼的裝置鎖定時間
- 嘗試失敗的次數上限
- 允許 Touch ID 或 Face ID

如需各規則的管理者詳細資訊，請前往：
help.apple.com/deployment/mdm/#/mdm4D6A472A

如需各規則的開發者詳細資訊，請前往：
developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef

iOS 配對模式

iOS 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 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 中，需要配對的服務會等到裝置已由使用者解鎖後才會啟動。

此外，在 iOS 10 或以上版本中，部分服務（包含照片同步）會要求裝置解鎖後才會開始。

在 iOS 11 或以上版本中，除非裝置最近剛解鎖，否則服務不會啟動。

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 11 或以上版本中，使用者還必須輸入密碼。使用者完成此步驟後，主機和裝置會交換並儲存 2048 位元的 RSA 公用密鑰。主機會得到 256 位元密鑰，可解鎖儲存在裝置上的託管 Keybag（請

參閱本白皮書「Keybag」章節中的「託管 Keybag」）。在裝置將受保護的資料傳送到主機或啟動服務（iTunes 同步、檔案傳送、Xcode 開發等）前，需要使用交換的密鑰來啟動加密 SSL 作業階段。裝置需透過 Wi-Fi 與主機連線，以將此加密作業階段用於所有通訊，因此在這之前必須先透過 USB 配對。配對也會啟用一些診斷功能。在 iOS 9 中，若配對記錄已超過六個月未使用，便會過期。在 iOS 11 或以上版本中，這個時限縮短為 30 天。

如需更多資訊，請前往：support.apple.com/zh-tw/HT203034

部分服務（包含 com.apple.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。

如需更多資訊，請前往：support.apple.com/zh-tw/HT202778

設定強制執行

設定描述檔為 XML 檔案，可讓管理者分配設定資訊到 iOS 裝置。使用者無法更改由已安裝的設定描述檔定義的設定。如果使用者刪除設定描述檔，亦會移除描述檔所定義的所有設定。如此一來，管理者便可以藉由將規則與 Wi-Fi 和資料存取綁定的方式，來強制執行設定。例如，提供電子郵件設定的設定描述檔也可以指定裝置密碼規則。使用者的密碼必須符合管理者的需求，否則無法存取郵件。

iOS 設定描述檔包含幾項可指定的設定，包含：

- 密碼原則
- 裝置功能的限制（例如，停用相機）
- Wi-Fi 設定
- VPN 設定
- 郵件伺服器設定
- Exchange 設定
- LDAP 目錄服務設定
- CalDAV 行事曆服務設定
- Web Clip
- 憑證和密鑰
- 進階行動數據網路設定

如需查看目前管理者列表，請前往：
help.apple.com/deployment/mdm/#/mdm5370d089

如需查看目前開發者列表，請前往：
developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef

設定描述檔可以簽署並加密來驗證其來源，以確保其正當性並保護內容。設定描述檔使用支援 3DES 和 AES-128 的 CMS（RFC 3852）進行加密。

設定描述檔也可以鎖定到裝置上，以徹底防範遭移除，或要求輸入密碼才能移除。由於許多企業的使用者皆持有私人的 iOS 裝置，可以移除將裝置綁定至 MDM 解決方案的設定描述檔，但這麼做也會移除所有受管理的設定資訊、資料和 App。

使用者可以使用 Apple Configurator 2 直接在裝置上安裝設定描述檔，也可以透過 Safari 下載、藉由電子郵件傳送，或使用 MDM 解決方案以無線方式傳送來取得設定描述檔。使用者在 Apple School Manager 或 Apple Business Manager 中設定裝置時，裝置會下載並安裝用於 MDM 註冊的描述檔。

行動裝置管理（MDM）

iOS 支援 MDM，可讓企業為整個組織安全地設定和管理大量 iPhone、iPad、Apple TV 和 Mac 部署。設定描述檔、無線註冊和 Apple 推播通知服務等現有的 iOS 技術均內建 MDM 功能。例如，APNs 可用來喚醒裝置，以便其可透過安全連線與 MDM 解決方案直接進行通訊。機密或所有權資訊不會透過 APNs 傳輸。

使用 MDM，IT 部門便可以為企業環境中的 iOS 裝置註冊、以無線方式設定配置和更新設定、監控公司政策的遵守狀況、管理軟體更新政策，甚至可以遠端清除或鎖定受管理的裝置。

如需更多 MDM 的相關資訊，請前往：

- www.apple.com/tw/iphone/business/it/management.html
- help.apple.com/deployment/ios/#/ior07301dd60
- help.apple.com/deployment/mdm/#/mdmbf9e668

共享的 iPad

「共享的 iPad」是在 iPad 教育部署中使用的一種多重使用者模式。可讓學生共用 iPad，而不會混雜文件和資料。每位學生可獲得專屬的主目錄，這個主目錄是以 APFS 卷宗形式建立，且受到使用者的憑證保護。「共享的 iPad」需要使用由學校核發且持有的「管理式 Apple ID」。「共享的 iPad」可讓學生登入任何由組織持有，且設為讓多名學生共用的裝置。學生資料會分割至個別的主目錄，每個主目錄都位於其專屬的資料保護網域中，且受 UNIX 權限和 Sandbox 技術保護。

登入「共享的 iPad」

當學生登入時，Apple 的識別身分伺服器會使用 SRP 通訊協定認證「管理式 Apple ID」。若成功，則會授予一個該裝置特定的短暫存取代號。如果學生先前使用過裝置，他們便已有使用相同憑證解鎖的本機使用者帳號。

如果學生先前未使用過裝置，則會佈建新的 UNIX 使用者 ID、含有使用者主目錄的 APFS 卷宗以及邏輯鑰匙圈。如果裝置未連接 Internet（例如當學生正在參加戶外教學），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的使用者可以登入。這個時限過後，即使本機帳號已存在，學生仍需於線上進行認證。

學生的本機帳號解鎖或建立後，若進行遠端認證，由 Apple 伺服器核發的短暫代號便會轉換為 iCloud 代號，以允許登入 iCloud。接著學生的設定會回復，且其文件和資料會從 iCloud 同步。

當學生的作業階段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，背景同步機制可確保更動會在學生登出後推播至 iCloud。該使用者的背景同步作業完成後，系統會卸載其 APFS 卷宗，且若沒有提供使用者的憑證，就無法再次裝載。

登出「共享的 iPad」

學生登出「共享的 iPad」時，系統會立即鎖定學生的使用者 Keybag，並關閉所有 App。為了加快新學生登入的速度，系統會暫時延遲部分的一般登出操作，並向新學生顯示「登入視窗」。如果學生在這段期間（約 30 秒）登入，「共享的 iPad」會執行延遲的清除，做為新學生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。

「共享的 iPad」升級

「共享的 iPad」從 iOS 10.3 以下版本升級為 10.3 或以上版本時，系統會執行一次性檔案系統轉換，以便將 HFS+ 資料分割區轉換為 APFS 卷宗。此時，如果系統上存在任何使用者主目錄，這些主目錄會保留在主資料卷宗上，而非轉換為單獨的 APFS 卷宗。

其他學生登入時，其主目錄也會存在於主資料卷宗上。如上文所述，在刪除主資料卷宗上的所有使用者帳號前，系統不會以使用者的專屬 APFS 卷宗製作新的使用者帳號。因此，為了確保使用者獲得 APFS 提供的額外保護和配額，應利用清除再重新安裝的方式將 iPad 升級至 10.3 或以上版本，或是透過「Delete User」 MDM 指令來刪除裝置上的所有帳號。

如需更多「共享的 iPad」的相關資訊，請前往：
help.apple.com/deployment/mdm/#/cad7e2e0cf56

Apple School Manager

Apple School Manager 是一項適用於教育機構的服務，可讓機構購買內容、設定在 MDM 解決方案中自動註冊裝置、建立學生和職員的帳號，以及設定 iTunes U 課程。Apple School Manager 可在網路上取用，是專為技術經理和 IT 管理者與教職員所設計。

如需更多 Apple School Manager 的相關資訊，請前往：
help.apple.com/schoolmanager

Apple Business Manager

Apple Business Manager 是簡便的網頁式入口網站，供 IT 管理者用來集中部署 iOS、macOS 和 tvOS 裝置。若搭配行動裝置管理（MDM）解決方案使用，您可以配置裝置設定及購買和分發 App 與書籍。Apple Business Manager 可在網路上取用，且專為 IT 管理者所設計。

如需更多 Apple Business Manager 的相關資訊，請前往：
help.apple.com/businessmanager

裝置註冊

Apple School Manager 和 Apple Business Manager 提供快速又簡便的方式，方便組織部署直接向 Apple 或 Apple 授權的零售商購買的 iOS 裝置。購買後也可使用 Apple Configurator 2，將搭載 iOS 11 或以上版本及 tvOS 10.2 或以上版本的裝置加入 Apple School Manager 或 Apple Business Manager。

在使用者得到裝置前，公司可以在 MDM 中自動註冊裝置，無需實際操作或準備。在註冊方案後，管理者需登入方案網站，並將方案連結到其 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。設定裝置期間，如果確實實施適當的安全措施，將能提高敏感資料的安全性。例如：

- 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。

指定使用者後，所有 MDM 專屬的設定、限制或控制項目便會自動安裝。裝置與 Apple 伺服器之間所有傳輸中的通訊皆會透過 HTTPS（SSL）加密。

藉由移除 iOS、tvOS 和 macOS 上「設定輔助程式」中的特定步驟，使用者的設定程序可以更加簡化，方便他們快速使用。管理者也可以控制使用者是否可從裝置上移除 MDM 描述檔，並確定裝置限制從一開始時即已就緒。裝置經開箱和啟用後，會於組織的 MDM 解決方案中註冊，然後安裝所有管理設定、App 和書籍。

Apple Configurator 2

除了 MDM 以外，macOS 的 Apple Configurator 2 也可輕鬆設定和預先設定 iOS 裝置與 Apple TV，再分發給使用者。可利用 Apple Configurator 2 快速為裝置預先設定 App、資料、限制和設定。

Apple Configurator 2 可讓您使用 Apple School Manager 或 Apple Business Manager 來在 MDM 解決方案中註冊裝置，使用者無需使用「設定輔助程式」。購買後也可使用 Apple Configurator 2 來將 iOS 裝置和 Apple TV 加入 Apple School Manager 或 Apple Business Manager。

如需更多 Apple Configurator 2 的相關資訊，請前往：
help.apple.com/configurator/mac

監管

在裝置設定期間，組織可設定要監管的裝置。監管意味著裝置列入機構所有，這樣會對其設定和限制提供額外的控制權。透過 Apple School Manager 或 Apple Business Manager，在 MDM 註冊流程中得以無線方式在裝置上啟用監管，或是使用 Apple Configurator 2 來手動啟用。若要監管某部裝置，必須清除該裝置並重新安裝作業系統。

如需更多使用 MDM 或 Apple Configurator 2 來設定和管理 iOS 裝置與 Apple TV 的相關資訊，請前往：help.apple.com/deployment/ios

取用限制

管理者可視情況啟用或停用「取用限制」，以防止使用者存取特定 App、服務或裝置功能。系統會將取用限制承載附加在設定描述檔中，藉此將取用限制傳送給裝置。取用限制可套用至 iOS、tvOS 和 macOS 裝置。受管理 iPhone 上的某些取用限制可能會反映在配對的 Apple Watch 上。

如需查看目前 IT 管理者列表，請前往：
help.apple.com/deployment/mdm/#/mdm0F7DD3D8

遠端清除

管理者或使用者可以遠端清除 iOS 裝置。藉由從 Effaceable Storage 安全地刪除區塊儲存裝置加密密鑰，讓所有資料無法讀取，即可執行立即遠端清除。遠端清除可由 MDM、Exchange 或 iCloud 起始。

當 MDM 或 iCloud 觸發遠端清除指令時，裝置會傳送確認通知並執行清除作業。若是透過 Exchange 執行遠端清除，裝置會在執行清除之前登入 Exchange 伺服器。

使用者也可以使用「設定」App 來清除他們的裝置。如前面提到的，可以將裝置設定為在連續多次輸入密碼失敗後，自動清除裝置。

遺失模式

如果裝置遺失或遭竊，MDM 管理者可以在安裝 iOS 9.3 或以上版本的受監管裝置上遠端啟用「遺失模式」。當「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定的訊息，例如顯示電話號碼，以便在尋獲裝置時撥打。當裝置設為「遺失模式」時，管理者可以要求裝置傳送其目前位置，且可選擇播放聲音。當管理者關閉「遺失模式」時（這是離開此模式的唯一方式），使用者會在鎖定畫面上看見此動作的通知訊息，或在主畫面上收到提示。

啟用鎖定

當「尋找我的 iPhone」開啟時，若沒有輸入持有人的 Apple ID 憑證或裝置之前使用的密碼，便無法重新啟用裝置。

若裝置為組織所有，建議組織監管裝置，讓「啟用鎖定」可由組織管理，而非藉由個別使用者輸入其 Apple ID 憑證來重新啟用裝置。

在受監管的裝置上，相容的 MDM 解決方案會在 「啟用鎖定」 啟用時儲存略過代碼，或在稍後需要清除裝置並指定給新的使用者時，使用此代碼來自動清除 「啟用鎖定」。

依照預設，使用者即使開啟了 「尋找我的 iPhone」，監管的裝置也不會啟用 「啟用鎖定」。但是，MDM 解決方案可能會擷取略過代碼並在裝置上允許 「啟用鎖定」 啟用。在 MDM 解決方案啟用了 「啟用鎖定」 時，若 「尋找我的 iPhone」 已開啟，「啟用鎖定」便會在此時啟用。如果 MDM 伺服器啟用 「啟用鎖定」 時，「尋找我的 iPhone」 為關閉狀態，則會在下一次使用者啟用 「尋找我的 iPhone」 時啟用 「啟用鎖定」。

若裝置用於教育機構且透過 Apple School Manager 建立 「管理式 Apple ID」，則 「啟用鎖定」 可綁定至管理者 Apple ID，而非使用者 Apple ID，或是使用裝置的略過代碼停用。

螢幕使用時間

「螢幕使用時間」 是 iOS 12 的功能，可讓使用者瞭解和控制自己或子女的 App 和網路用量。使用者可以：

- 檢視用量資料
- 設定 App 或網路用量限制
- 設定停用時間
- 執行其他取用限制

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（同步功能預設為關閉）才能使用此功能。「螢幕使用時間」 取代了 iOS 先前版本中的 「取用限制」 功能。

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 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變更。子女在 18 歲生日當天（以所在國家或地區為準）可關閉這個監控功能。

可使用 Apple 識別服務（IDS）的端對端加密連線，在家長和子女的裝置間傳輸用量資料和配置設定。加密的資料會暫時存放在 IDS 伺服器上，直到接收裝置讀取這筆資料（例如當 iPhone/iPad 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
- 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

Apple 不會收集特定 App 或網路用量資料。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。

隱私控制

Apple 十分重視客戶的隱私，且具備許多內建控制項目和選項，可讓 iOS 使用者決定 App 可以如何使用其資訊、於何時使用，以及可以使用哪些資訊。

定位服務

「定位服務」會使用 GPS、藍牙、公用 Wi-Fi 熱點和基地台位置來判定使用者的約略位置。「定位服務」可以使用「設定」中的單一切換來關閉，使用者也可以對使用定位服務的各個 App 核准此功能。使用者可以讓 App 只有在使用時才要求接收位置資料，或是隨時都可以接收位置資料。使用者可以選擇不允許使用定位服務，也可以隨時在「設定」中更改選擇。使用者可以依照 App 要求的定位用途，在「設定」中將定位服務設為永不允許、在使用時允許或總是允許。此外，當有權隨時使用定位服務的 App 在背景中運作時，系統會提醒使用者已核准定位服務，且可以更改 App 的存取權。

另外，使用者可細微控制系統服務對定位資訊的使用權。這可讓使用者關閉以下資訊中所涵蓋的定位資訊：分析服務所收集且供 Apple 用於改善 iOS 的資訊、與基於位置的 Siri 資訊、「Siri 建議」搜尋結果中基於位置的內容、當地交通狀況，以及過去曾造訪的重要位置資訊。

存取個人資料

iOS 可防止 App 未經授權存取使用者的個人資訊。此外，使用者可以在「設定」中查看哪些 App 有權存取特定資訊，亦可授予或撤銷往後的任何存取權。包含以下項目的存取權：

- 聯絡資訊
- 行事曆
- 提醒事項
- 照片
- 動態活動與健身
- 定位服務
- Apple Music
- 您的音樂與影片活動
- 麥克風
- 相機
- HomeKit
- 健康
- 語音辨識
- 藍牙共享
- 您的媒體資料庫

如果使用者登入 iCloud，依照預設便會授予 App 存取「iCloud 雲碟」的權限。使用者可以在「設定」中控制每個 App 的 iCloud 存取權。此外，iOS 所提供的取用限制可防止資料在 MDM 解決方案和使用者所安裝的 App 和帳號之間移動。

隱私權政策

如需參閱 Apple 的隱私權政策，請前往：www.apple.com/tw/legal/privacy

安全性認證和計畫

注意：如需 iOS 安全性認證、驗證及指引的最新資訊，請前往：
support.apple.com/zh-tw/HT202739

ISO 27001 和 27018 憑證

針對支援下列產品與服務的基礎架構、開發和操作，Apple 已依據 2017 年 7 月 11 日發佈的 Statement of Applicability v2.1 適用性聲明，取得「資訊安全管理系統」的 ISO 27001 和 ISO 27018 憑證：Apple School Manager、iTunes U、iCloud、iMessage、FaceTime、管理式 Apple ID、Siri，和 Schoolwork。Apple 對 ISO 標準的合規狀況已經英國標準協會認證。英國標準協會的網站就 ISO 27001 和 ISO 27018 列有合規證書。若要檢視這些憑證，請前往：

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

加密編譯驗證（FIPS 140-2）

iOS 中的加密模組經過重複驗證，符合美國聯邦資訊處理標準（FIPS）140-2 規範（自 iOS 6 起的每次發行版本）。隨著每次主要版本的發行，Apple 會在 iOS 作業系統發行時，向 CMVP 提交這些模組進行重新驗證。此計畫會針對適當使用 iOS 加密編譯服務和核准演算法的 Apple App 和第三方 App，驗證加密操作的完整性。

Apple 已取得嵌入式硬體模組的 FIPS 140-2 驗證，稱為「**Apple 安全隔離區處理器（SEP）安全密鑰存放區（SKS）加密編譯模組**」，因此經核准可使用由 SEP 產生和管理的密鑰。Apple 將繼續致力為後續每個主要 iOS 版本實現更高級別的硬體模組。

Common Criteria Certification（ISO 15408）

自 iOS 9 起，Apple 依據 Common Criteria Certification 計畫，為每個主要 iOS 版本達成 ISO 認證，並擴展涵蓋範圍以納入下列各項：

- Mobile Device Fundamental Protection Profile
  - Extended Package for Mobile Device Management Agents
  - Extended Package for Wireless LAN Clients
  - PP-Module for VPN Client
- Protection Profile for Application Software
  - Extended Package for Web Browsers

iOS 12 預計為以下各項取得額外認證：

- Extended Package for Email Clients

Apple 計劃對後續每個主要 iOS 版本擴展涵蓋範圍。

Apple 在 International Technical Community（ITC）中扮演積極角色，開發目前仍無法取得的「合作保護描剖繪」（cPP），致力於評估關鍵行動安全性技術。Apple 會依據目前可取得和開發中之新版本與更新版本的 cPP 來持續評估和爭取認證。

機密商業解決方案（CSfC）

在合適的情況下，Apple 也已提交 iOS 平台與各種服務，以納入機密商業解決方案（CSfC）計畫元件列表。因為 Apple 平台與服務具備 Common Criteria Certification，他們也會依據 CSfC 計畫元件列表來提交以便納入。

若要查看最新列出的元件，請前往：
www.nsa.gov/resources/everyone/csfc/components-list

安全性設定指南

Apple 已與世界各地的政府合作，旨在開發能提供指導與建議的指南，以維護一個更安全的環境，也就是針對高風險環境進行所謂的「裝置強化」（device hardening）。這些指南會針對在 iOS 中設定與使用內建功能，提供已定義且經過審核的資訊，以增強保護。

Apple 安全性獎金

若研究人員將嚴重問題告知 Apple，Apple 將會予以酬謝。為取得 Apple 安全性獎金的資格，研究者需提供明確的報告以及其概念的實例證明。此漏洞必須影響到現行最新的 iOS 版本，並涉及最新硬體。實際付款金額會經 Apple 審查後予以決定。獎勵條件包含新穎度、安全性問題暴露的可能性，以及需要使用者互動的程度。

問題經妥善告知後，Apple 會盡快優先解決已證實的問題。Apple 會在適當的情況下公開表彰，除非另有要求。

類別	付款上限（USD）
保護開機韌體元件	$200,000
擷取受「安全隔離區」保護的機密資料	$100,000
使用核心權限執行任意程式碼	$50,000
未經授權存取 Apple 伺服器上的 iCloud 帳號資料	$50,000
從 Sandbox 程序存取位於該 Sandbox 以外的使用者資料	$25,000

結論

對安全性的承諾

Apple 致力於以最先進的隱私與安全性技術保護個人資訊，進而保障客戶的安全；並採用全方位的方式來保護企業環境中的公司資料。

iOS 本身便具有安全性防護。包括平台、網路，再到 App，企業所需的一切都可以在 iOS 平台上完成。這些元素造就了 iOS 在業界安全性的領先地位，同時兼顧優良的使用者體驗。

Apple 在 iOS 和 iOS App 生態系統之間運用一致且統合的安全性基礎架構。硬體式儲存加密可在裝置遺失時提供遠端清除的功能；並讓使用者在將裝置贈予或轉讓給其他人時，徹底移除所有公司和個人資訊。診斷資訊也會以匿名方式收集。

Apple 在設計 iOS App 時便將提昇安全性納入考量。例如，iMessage 和 FaceTime 提供用戶端對用戶端的加密。第三方 App，結合必要的程式碼簽署、Sandbox 技術限制和授權可為使用者提供業界首屈一指的保護，免受病毒、惡意軟體和其他入侵程式的危害。App Store 的提交流程會先審核每個 iOS App，通過審核後才能供應，這個流程可以進一步保障使用者免受這些風險的威脅。

為了充分利用 iOS 與生俱來的強大安全性功能，我們建議企業審核其 IT 部門和安全性原則，以確保可充分使用到此平台所提供的多重安全性技術。

Apple 擁有一個專業的安全性團隊，專門為所有的 Apple 產品提供支援。這個團隊會為開發中和已發佈的產品提供安全性審核和測試。Apple 團隊亦提供安全性工具和訓練，並積極監控新的安全性問題和威脅報告。Apple 為「資安事件應變小組論壇」（Incident Response and Security Teams, FIRST）的成員。

若要深入瞭解如何向 Apple 提報問題以及訂閱安全性通知的相關資訊，請前往：support.apple.com/zh-tw/HT201220

詞彙表

位址空間配置隨機載入（ASLR）	iOS 使用的一項技術，可讓透過軟體漏洞肆虐的惡意程式成功率大幅降低。藉由確保記憶體位址和位移無法預測，入侵程式代碼便無法對這些值進行硬式編碼。在 iOS 5 或以上版本中，所有系統 App 和資料庫的位置都是隨機安排的，而所有第三方 App 均編譯為不受位置限制即可執行。
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位址的目錄，用於查詢密鑰和裝置位址。
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 iOS 裝置。
開機進度暫存器（BPR）	一組 SoC 硬體旗標，軟體可用來追蹤裝置進入的開機模式，例如「DFU 模式」和「復原模式」。「開機進度暫存器」 旗標一旦設定就無法清除。這可讓之後的軟體取得系統狀態的信任指標。
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。
資料保護	iOS 的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。
裝置韌體升級（DFU）	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 的電腦時，便會顯示以下提示：「iTunes 偵測到一台正處於復原模式的 iPad。若要與 iTunes 一同使用，您必須回復 iPad。」
ECDSA	以橢圓曲線加密技術為基礎的數位簽章演算法。
Effaceable Storage	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，Effaceable Storage 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。
Elliptic Curve Diffie-Hellman Exchange（ECDHE）	搭配臨時密鑰的 Elliptic Curve Diffie-Hellman Exchange。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。
Exclusive Chip Identification（ECID）	每部 iOS 裝置處理器中的一個 64 位元唯一識別碼。在一部裝置上接聽來電時，會透過低功耗藍牙 4.0 短暫傳播來終止附近與 iCloud 配對的裝置鈴聲。傳播位元組會使用與 「接力」 傳播相同的方式進行加密。用作個人化程序的一部分，此識別碼並非機密。
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 Effaceable Storage 中以進行快速清除，而不視為機密。
群組識別碼（GID）	類似 UID，同一類別中每個處理器的 GID 皆相同。
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。
iBoot	用來載入 XNU 的代碼，作為安全啟動鏈的一部分。視 SoC 是第幾代的而定，iBoot 可能由 LLB 載入或直接由開機 ROM 載入。
積體電路（IC）	亦稱為微晶片。
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。

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（在 iOS 5 中設為 3） – 類型（系統、備份、託管或「iCloud 備份」） – Keybag UUID – 如果 Keybag 已簽署則包含 HMAC – 用於封裝類別密鑰的方式：與 UID 或 PBKDF2，以及 salt 和反覆運算次數相配合 • 類別密鑰列表： – 密鑰 UUID – 類別（所屬的檔案或鑰匙圈資料保護類別） – 封裝類型（僅限 UID 衍生密鑰、UID 衍生密鑰和密碼衍生密鑰） – 封裝的類別密鑰 – 非對稱式類別的公用密鑰
鑰匙圈	iOS 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。
密鑰封裝	使用一個密鑰來加密另一個密鑰。iOS 依照 RFC 3394 使用 NIST AES 密鑰封裝。
Low-Level Bootloader（LLB）	在具有雙階段開機架構的系統上，由開機 ROM 呼叫的代碼，接著會載入 iBoot，作為安全啟動鏈的一部分。
記憶體控制器	用於在檔案系統上加密檔案的 AES 256 位元密鑰。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。
檔案專屬密鑰	用於在檔案系統上加密檔案的 AES-256 位元密鑰。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。
佈建描述檔	一個由 Apple 簽署的 plist，其包含一組實體和授權，允許在 iOS 裝置上安裝並測試 App。開發「佈建描述檔」會列出開發者選擇要用來臨機操作分配的裝置；分配「佈建描述檔」中包含企業開發 App 的 App ID。
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徵。
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。一旦設定鎖定位元，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。
系統副處理器完整保護（SCIP）	系統副處理器是位於與應用程式處理器相同 SoC 上的 CPU。
晶片式系統（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。
Tangling	使用者的密碼轉換為加密編譯密鑰，並使用裝置 UID 強化的過程。這可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。Tangling 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）。
統一資源識別碼（URI）	一個可識別網頁式資源的字元字串。
唯一識別碼（UID）	在製造過程便直接燒入每個處理器的 A 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。
XNU	iOS 和 macOS 作業系統中央的核心。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、Sandbox 技術限制、授權檢查和 ASLR。

文件版本記錄

日期	摘要
2018 年 11 月	**已更新適用於 iOS 12.1** • 群組 FaceTime
2018 年 9 月	**已更新適用於 iOS 12** • 安全隔離區 • 作業系統完整保護 • 快速交通卡與省電模式 • DFU 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	**已更新適用於 iOS 11.4** • 生物辨識政策 • HomeKit • Apple Pay • 商務聊天 • iCloud 雲端 「訊息」 • Apple Business Manager
2017 年 12 月	**已更新適用於 iOS 11.2** • Apple Pay Cash **已更新適用於 iOS 11.1** • 安全性認證和計畫 • Touch ID/Face ID • 共享的備忘錄 • CloudKit 端對端的加密 • TLS • Apple Pay、在網路上使用 Apple Pay 付款 • Siri 建議 • 共享的 iPad 如需更多 iOS 11 安全性內容的相關資訊，請前往： support.apple.com/zh-tw/HT208112

日期	摘要
2017 年 7 月	**已更新適用於 iOS 10.3** • 系統隔離區 • 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 • 隱私控制 如需更多 iOS 10.3 安全性內容的相關資訊，請前往： support.apple.com/zh-tw/HT207617
2017 年 3 月	**已更新適用於 iOS 10** • 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、在網路上使用 Apple Pay 付款 • 信用卡、金融卡及預付卡佈建 • Safari 建議 如需更多 iOS 10 安全性內容的相關資訊，請前往： support.apple.com/zh-tw/HT207143
2016 年 5 月	**已更新適用於 iOS 9.3** • 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 School Manager、共享的 iPad 如需更多 iOS 9.3 安全性內容的相關資訊，請前往： support.apple.com/zh-tw/HT206166

日期	摘要
2015 年 9 月	**已更新適用於 iOS 9** • 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 如需更多 iOS 9 安全性內容的相關資訊，請前往： support.apple.com/zh-tw/HT205212

2018 年 11 月