Matter 協定：不只解決碎片化，資安準則更吸睛！

■文：任芷萍

物聯網 (IoT) 普及的同時也放大了網路安全 (Cybersecurity) 的衝擊性，各種通訊協定的資安措施更肩負第一線防護任務。去年底剛出爐的「Matter」無線連接標準，雖是以「簡化互操作性、打破智慧家居應用藩籬、消除市場破碎化」為訴求，卻也有業界專家是受到其安全連線機制而吸引，包括：不允許匿名加入、每個裝置皆須經過認證才能連線、入網後可供裝置在不同生態系運作、須經生態系廠商授予證書後才會傳送密鑰、開發者可在 GitHub 上檢查原始碼並修正錯誤，以及嚴格管控限制——由管理者批准裝置的「存取控制清單」(Access Control List, ACL)。

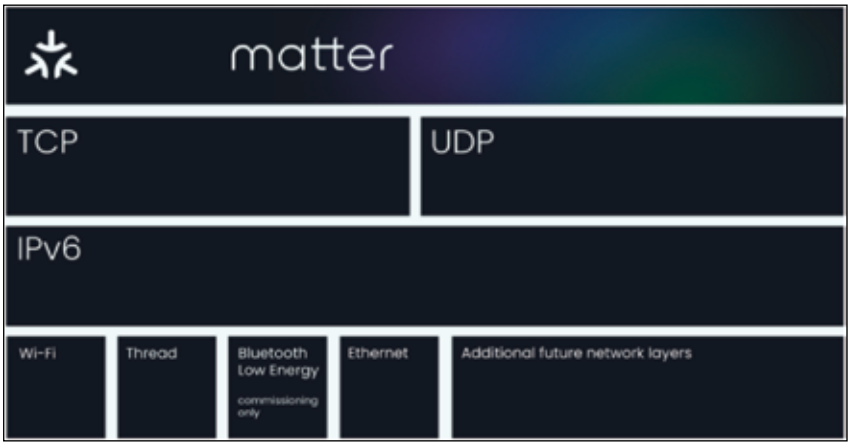
從「應用層」制高點實現身份認證&數位主權

Matter 架構定義部署在設備和控制器上的應用層，並支援基於 IPv6 的網路。它是一個智慧家居開源標準項目，由亞馬遜 (Amazon)、蘋果 (Apple)、谷歌 (Google)、ZigBee 聯盟 (後更名為「連接標準聯盟」，CSA) 聯合發起，旨在開發、推廣一項免專利授權費用的新連線協定，以簡化智慧家居設備商的開發成本，並提高產品之間的相容性；Matter 具有統一的設置流程，打破終端用戶跨廠商平台的壁壘，讓不同的智慧家居設備間，使用 IP 位址作為身份證、互相通訊，最終目的是讓那些功能各不相同的智慧家居有統一的溝通語言，實現一定程度的自動化。

CSA 總裁兼首席執行長 Tobin Richardson 今年初援引世界經濟論壇一份名為《2023 年互聯世界狀況》報告指出，仍有超過 80% 受訪者對於物聯網的個人數據隱私的保護機制抱持存疑，超過 70% 受訪者對於物聯網的安全性沒有信心；而 Matter 這個基於 Zigbee 所發展出來的 IP 通用物聯網協定，在數位主權與一體成形的安全性擁有獨特優勢。有別於 Wi-Fi 或 Thread 等技術採用額外的網路安全措施，Matter 不須依賴任何底層通訊技術便可在允許設備進入網路前，進行身份認證、判斷是否為合法用戶。

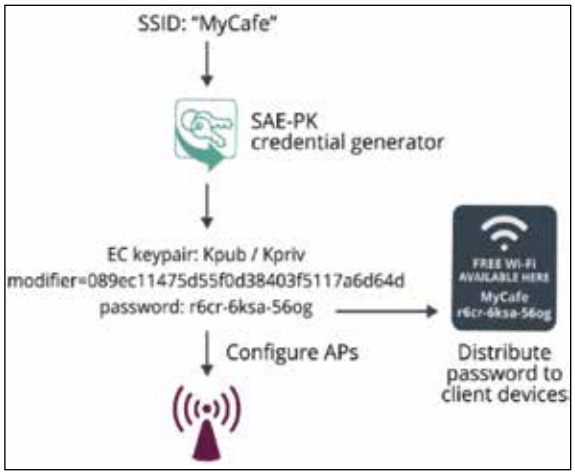
在獲得半導體大廠和 Apple 等終端品牌廠的支持下，Matter 的出現可望打破碎片化市場，又能兼顧用戶的數位主權和數據安全性。儘管 Matter 可單獨存在，但它亦可與 Wi-Fi 實現無縫、可互操作的連接。Wi-Fi 設備上的

圖 1：Matter 建立在互聯網協定 (IP) 之上，以安全和隱私為主要設計原則，可為物聯網提供經驗證的設備身分以及安全的通訊和訪問控制



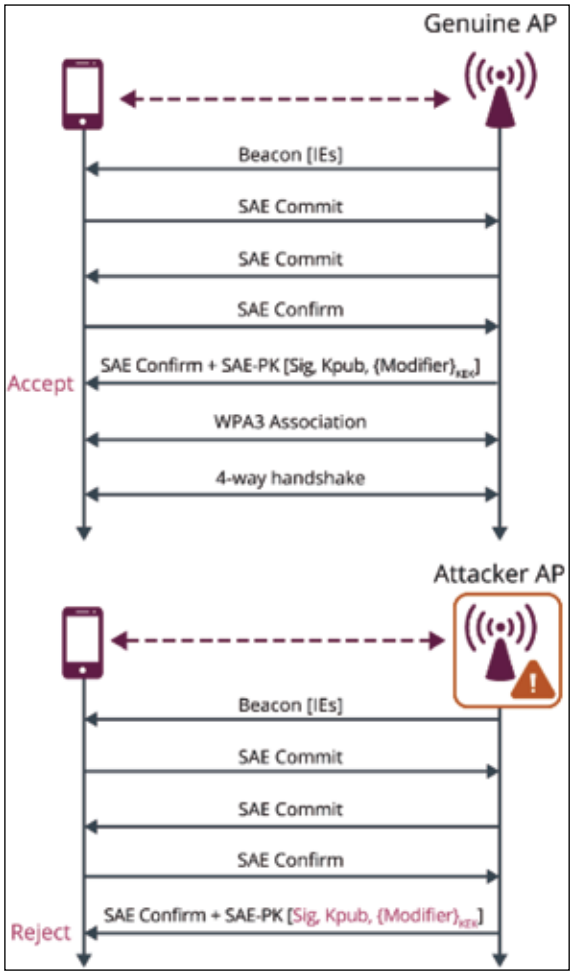
資料來源：https://csa-iot.org/wp-content/uploads/2022/03/Matter_Security_and_Privacy_WP_March-2022.pdf

圖 2：SAE-PK 憑證生成



資料來源：https://www.wi-fi.org/beacon/thomas-derham-nehru-bhandaru/wi-fi-certified-wpa3-december-2020-update-brings-new-0

圖 3：SAE-PK 認證



資料來源：https://www.wi-fi.org/beacon/thomas-derham-nehru-bhandaru/wi-fi-certified-wpa3-december-2020-update-brings-new-0

Matter 認證需要 Wi-Fi CERTIFIED，提供 WPA3 以確保個人和企業安全地交換資訊；可用認證包括：Wi-Fi 6、低功耗 Wi-Fi HaLow，以及允許用戶用二維碼和其他低接觸式連接設備的 Wi-Fi Connect 等核心功能。SAE 公鑰 (SAE-PK) 為公網中使用 WPA3-Personal 的客戶端設備提供針對「邪惡雙胞胎」(Evil Twin) 攻擊的保護。

Arm：PSA Certified 平台安全性架構樹立 Cybersecurity 框架

矽智財 (IP) 與低功耗處理器大廠安謀國際 (Arm) 援引市調機構 ABI Research 指出，預估 2022～2030 年，與 Matter 相容的智慧家庭裝置出貨將逾 55 億台，使 Matter 可望成為下一波物聯網成長的重要推力並建議：保障聯網安全最好在產品設計之初就加入資安概念，從架構、源頭支援安全性規範，以避免後續架構變更或造成額外支出，但這並非易事，因為：缺乏資安參考模式、難以滿足眾多國家的規範、不知如何自我評估及達到不同層級要求等，這將導致設計成本增加。於是，Arm 於 2017 年首次提出 PSA Certified 平台安全性架構。

該架構已將美國 NIST 8259A、歐洲 EN 303 645 等主要通訊協定整合在內，迄今已有逾 130 項認證產品，涵蓋：75 款系統單晶片 (SoC) 和 IC、20 個軟體平台以及 25 家以上的 OEM 產品。主任工程師 Blade Lin 直言，在萬物聯網時代，如何確保有價值的資訊與個人資料不被竊取是最受關注的議題之一；根據他們訪問超過 600 位物聯網相關領域的產品經理發現，有高達 96% 的受訪企業坦承資安功能已成公司最重視的功能之一，有 88% 同意資安問題是當下前三大優先事項。

遵循 PSA 認證四大步驟，開發者能以最經濟實惠的方式取得資安保障：1. 資產評估及威脅評量以定義特定用戶的安全要求；2. 根據上述要求建立架構；3. 使用開放原始碼實作產品軟、硬體和韌體；4. 驗證安全性需求及法規。Blade Lin 說明 PSA 有三大層級：Level 1 適用於所有產品，提供安全標準供廠商自我回覆相關問題；Level 2 與 Level 3 須經過第三方實驗室的認證——前者須經過軟體攻擊測試，後者還須再加上硬體攻擊測試。除了晶片或軟體的功能性認證外，PSA 亦提供應用程式介面 (API) 認

圖 4：PSA Certified 安全認證分為三個層級：Level 1 記錄安全最佳實踐，Level 2 針對遠程軟體攻擊的滲透測試，Level 3 再新增硬體攻擊的滲透測試

資料來源：https://www.psacertified.org/blog/psa-certified-securing-the-future-of-the-iot/

證供操作系統 (OS) 直接使用。

Matter 潛力舞台：智慧城市&工業領域

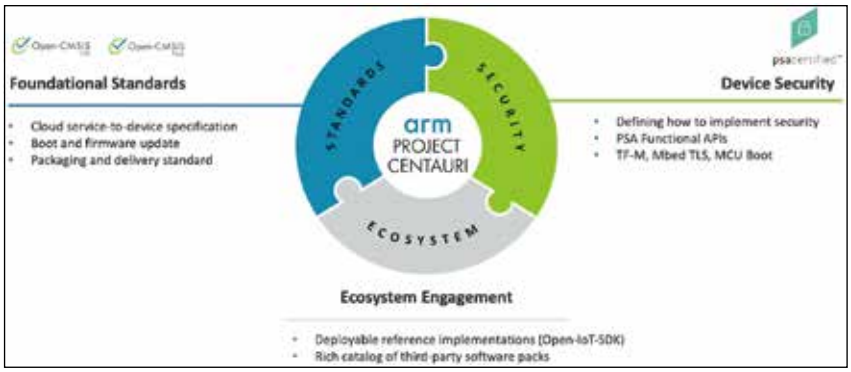
如此一來，可確保程式開發人員使用的是安全性服務，以縮短上市時程、避免軟體破碎化並減少研發資源；另有可信任韌體支援 Cortex-M 和 Cortex-A 建立基本安全性功能，供移植到不同的晶片和平台。正在快速崛起的 Matter 1.0 通訊協定發佈後，PSA 隨即被收錄在 PSA Level 1 的 2.2 版本中。Arm IoT LoB 資深 GTM 經理 Allen Huang 表示，嵌入式系統加入更多智慧功能，且仍在加速之中，這是由兩大因素驅動：一是邊緣運算能力提高，使以往資源受限的 IoT 裝置得以實現複雜功能；二是邊緣設備的數量急速成長，到下個十年可望達到數兆台以上。

Arm 認為，Matter 雖是從智慧家庭出發，但未來可拓展至智慧城市或工業領域，並預告不止 IP，Cortex-A、R、M 系列 MPU 及網路處理器 (NPU) 都將支援 Matter 邊緣及雲端，包括確保 Arm 物聯網整體解決方案的三大區塊與之相容：

1. **Corstone**：預先組合各種底層 IP 且經過驗證的子系統，專為各種特殊應用而設計，從 Corstone-102 到 Corstone-1000 的多個型號，可滿足從智慧檯燈到物聯網閘道器的不同效能和工作負載要求；
2. **Arm 虛擬硬體 (AVH)**：以上述 Corstone 子系統為基礎，於 2021 年 9 月推出的首個產品是基於 Cortex-M55、架構在 Amazon Machine Image (AMI) 伺服器上的 Corstone 300，開發者可透過雲端虛擬方式複製硬體，迅速擴展至數千台裝置，並在晶片未試產 (Tape-out) 前就著手設計軟體；
3. **Project Centauri**：結合標準性、安全性和生態系統，實現軟體再用性 (reuse)，讓開發者專注於創新工作。

Arm 多數 Cortex-M 產品線已可從 AVH 取得，包括 Matter 最常用的 Cortex-M4、M23、M33 等。透過七個 Cortex-M 系列 CPU，AVH 可支援約 800 億台物聯網裝置開發並將工具整合至 GitHub 自定義執行器內，同時強化 Cortex-A 和第三方生態系支援，恩智浦半導體 (NXP)、意法半導體 (ST) 和樹莓派 (Raspberry Pi) 的開發板皆在列，將 AVH 整合到主流的工具和服務中並擴展資料庫，尤其 Cortex-M 模型方便在 AVH 進行開發及測試；開發者在上傳程式碼到資料庫後可就近除錯，同時在資料庫啓動 CI 流程，改變傳統開發物聯網軟體的方式。

圖 5：Project Centauri 將定義基礎標準，以確保物聯網應用程式跨虛實體之間的可攜性



資料來源：https://www.arm.com/zh-TW/markets/iot/project-centauri

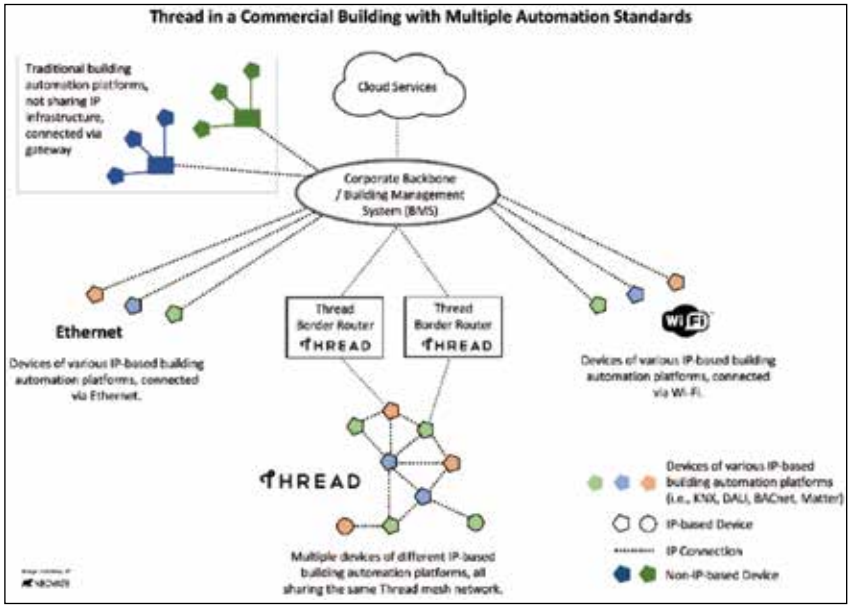
宏觀微電子：軟、硬融合的 IC 設計舉足輕重

宏觀微電子 (Rafael Micro) 行銷副總經理陳嘉修剖析，物聯網是面向應用、服務，且重視垂直應用的廣大市場，受到 Covid-19 疫情影響持續成長，經統計，2022 年全球物聯網整體產值約 1,579 億美元，軟體服務和硬體設備的產值比例約為 7：3，北美、歐洲與中國將三分市場；預估到 2027 年，全球物聯網產值將達 5,250 億美元，期間年複合成長率 (CAGR) 為 22%。雲端運算和人工智慧 (AI) 將透過緣運算和裝置設計改變遊戲規則，AIOT 是資訊科技、營運科技和通訊技術三者的結合，軟、硬融合的 IC 設計極為舉足輕重，而物聯網安全將受到高度關注。

陳嘉修主張，選擇物聯網無線通訊技術的考量，首重不同應用場景：1. 點對點 (P2P) vs. 星狀 (Star) vs. 網格 (Mesh)；2. 授權頻段 vs. 非授權頻段；3. 通訊距離；4. 耗電量；5. 佈建成本及使用成本。談到通訊協定，就不能不提到近來備受矚目的 Matter (前身為 CHIP)。第一代 Matter 標準完全基於現有的網路技術開發，包括：乙太網 (Ethernet)、Wi-Fi、Thread 及藍牙低功耗 (BLE)，其中，Thread 採用 mesh 組網方式，讓網路裡的每個設備都能成為通訊節點，即便某一個設備下線也不會影響其他設備正常工作。

陳嘉修強調，物聯網安全必須立在「零信任」(No Trust) 基礎上，而 Matter 另一項優勢在於：專注於設備身分認證及韌體安全性，安全認證程序嚴謹——所有設備均須完成安全認證，且設備擁有者須提供設備密碼以判斷是否通過認證。支援 Matter 的裝置與雲端連線後會簽發證書，以區塊鏈 (Blockchain) 形式儲存在 Matter 裝置，而 Arm 微控制器 (MCU) 擁有獨特的密鑰執行方式與儲存區域 (TrustZone)，以隔絕外界所有竊取管道，確保密鑰資料安全；同時確保開發環境與軟體更新，同時擁有完整可支援全產業鏈的 Matter 應用開發。

圖 6：Matter 的 IP 基礎意味著它可以用於乙太網、Wi-Fi 和 Thread 網路層，在許多生態系統和設備中提供極大的靈活性和控制



資料來源：https://www.threadgroup.org/news-events/blog/ID/291/Typical-Thread-Network-Topologies--Smart-Homes-with-Matter-Commercial-Buildings#.Y_n3l3ZBy3A

聯發科技：OFDMA + MU-MIMO 是 Matter 絕佳搭檔

特別一提，Matter 與 Wi-Fi 結盟還能獲取以下好處：Wi-Fi 6 和 Wi-Fi 6E 網路可提供複雜的網路效率、診斷、管理和優化功能，使製造機器人和無人機等設備即使在家庭或工業網路中移動或跨區漫遊，也能保持連接；Wi-Fi Location 更可提供公分級的位置資訊，為工業和智慧城市環境提供一系列位置感知的資產管理、網路管理和地理圍欄等物聯網服務。此外，除了經由傳統 Wi-Fi 接入點連接，Wi-Fi EasyMesh、Aware 和 Direct 等個別技術可為不同的物聯網環境提供各種靈活的網路拓撲結構，方便擴展和客製化選項。

聯發科技 (MediaTek) 智慧聯通事業部行銷經理 Porta Fan 宣稱他們從物聯網終端切入，在去年 10 月推出支援 Matter 的 Filogic 130 SDK 3.0。Filogic 130 是高度整合的雙核心晶片，集成 Wi-Fi6、Bluetooth 5、Hi-Fi 4 DSP 和 Arm Cortex-M33；他提到，之所以選用

M33 正是看中其 Armv8-M 32 位元處理器的 TrustZone 資安功能。另 Wi-Fi 6 可額外支援 6GHz 相對乾淨頻段，且其 OFDMA 技術可同時支援不同物聯網裝置；OFDMA + MU-MIMO 對於 Matter 十分關鍵，不僅能同時連結多個裝置、還能在不同頻段供不同裝置使用，在時域、頻域皆有更高自由度。

Silicon Labs：Matter 藉 Thread 擴展支援上百個節點

芯科科技 (Silicon Labs) 資深工程師 Steven Lin 羅列 Matter 有四大願景：易用性、互通性、穩定性、安全性。自從去年 10 月發佈 1.0 規格以來，目前有逾 400 個產品和平台已通過 Matter 測試。Matter 是最上層的應用協定，支援最底層 TCP、UDP、IPv6 等重要傳輸層，即大家熟知的 Wi-Fi、Thread、Ethernet、BLE，但 BLE 只負責入網 (commissioning) 功能。他解釋，Wi-Fi 雖方便，但由於最多只支援 64 個節點，若需擴展則需借助 Thread、可支援上百個節點，且較 Wi-Fi 更為省電；且若其中有節點故障，可經由其他節點繞出，使網路繼續運作。

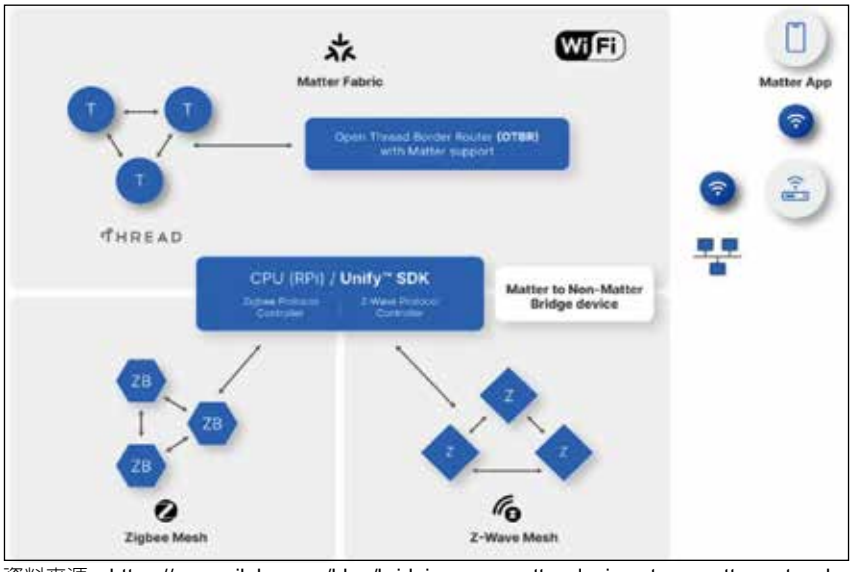
有鑑於此，Silicon Labs 針對 Matter over Thread 力推 MG24 無線 SoC。Steven Lin 指出，更保險的作法是：在網路設置兩個 Thread 與 Wi-Fi 連接的閘道器 (border router)，若其中一個故障，另一個還能將節點設備連到 Wi-Fi。若兩個以上的終端節點使用同一個控制器，則稱作「Fabric」，意指 Google、Apple、三星 (Samsung) 等某個生態系，可讓多個不同陣營的設備互通。「Multi-Admin」是 Matter 另一項卓越功能，當新購一個智慧設備完成設定後，可開啓權限讓其他生態系也能加以控制。

TI：SimpleLink 無線 MCU 力拼最低功耗

在 Matter 構思階段便入列 CSA 的董事會成員的德州儀器 (TI)，亦在第一時間推出支援 Matter 的 Wi-Fi 和 Thread SimpleLink 無線 MCU 全新軟體開發套件。工程師可使用 CC3235SF 和 CC2652R7 等新軟體和無線 MCU，打造超低功率、安全且由電池供電的智慧家庭與工業自動化物聯網應用，順暢連接專用生態系統中的產品。全球幫浦製造商葛蘭富 (Grundfos) 即運用支援 Matter 的 TI 技術推出暖通空調幫浦系列，並與其它智慧家庭產品分享資料，以改善能源消耗、減少碳排放。若門上鎖或電器關閉表示無人在家，幫浦便可進入待機狀態以節省能源。

TI 自稱相較於競品的裝置，新的 TI SimpleLink 無線 MCU 有助於 Thread 應用將待機功耗降低多達 70%，並在使用 5 秒輪詢時將電池續航力延長至 4 年。對於遠端連線應用，這些無線 MCU 的高效率整合式功率放大器可在 +20 dBm 時消耗 101 mA (業界最低的功耗) 實現可靠連線。Matter Wi-Fi 應用的設計人員可運用 TI 的雙頻、多級安全方法來保護裝置資料並防止網路威脅，完全不需額外元件。現可透過索取用於 Thread LP-CC2652R7 (39.99 美元) 和 Wi-Fi LP-CC3235SF (54.99 美元) 的 LaunchPad 開發套件開始原型設計。CTA

圖 7：Silicon Labs 為具有 Wi-Fi 或 Thread 連接的終端產品提供完整的 Matter 協定以及使用無線 SoC 和軟體組合的「OTBR」解決方案，並同時提供 Matter to Zigbee 和 Matter to Z-Wave 橋接解決方案以及功能齊全的 Unify SDK 軟體



資料來源：https://www.silabs.com/blog/bridging-non-matter-devices-to-a-matter-network