新聞稿

意法半導體推出Secure Manager軟硬體安全方案
使開發安全的嵌入式應用變得更簡單

- *市場上首款經過認證的即用型 MCU 安全保護服務，簡化嵌入式應用開發*
- *利用 Arm® TrustZone®以及 ST 和合作夥伴攜手開發的技術，其符合 PSA 和 SESIP 第三級 安全規範之應用*

【臺北訊，2023年3月21日】—服務橫跨多重電子應用領域的全球半導體領導廠商意法半導體（STMicroelectronics，簡稱ST；紐約證券交易所代碼：STM）推出業界首款微控制器系統晶片安全解決方案，此命名為「STM32TrusTEE Secure Manager」（安全管理器）可簡化嵌入式應用開發流程，確保其能「開箱即用」安全保護功能。STM32TrusTEE Secure Manager解決方案第一個使用在STM32H5系列微控制器，能進一步省去開發者自行編寫、驗證安全程式碼，同時還能根據需求提供最佳實作範例的安全服務。

意法半導體微控制器和數位IC產品部旗下通用微控制器子業務部執行副總裁Ricardo De Sa Earp表示，「社會日益重視應用安全，客戶要求快速提供經過認證安全以及高性能的應用。這些趨勢促使我們與授權合作夥伴ProvenRun密切合作，開發出STM32Trust TEE Secure Manager。該安全管理器能保護使用者、資產和資料安全，加強安全保護，同時簡化客戶在開發專案中增加具有價值的安全功能，還能為應用認證帶來更多便利性。」

身為Arm的主要開發合作夥伴，意法半導體支援在Cortex®-M33內核心上開發符合PSA和GlobalPlatform SESIP第三級認證之安全規範的應用。此外，意法半導體還與微軟Azure合作開發高安全性的中介軟體，亦與ProvenRun合作開發在ProvenCore-M可信任執行環境作業系統上運行的STM32Trust TEE Secure Manager。

ProvenRun總裁暨創始人Dominique Bolignano進一步表示，「我們與ST合作開發安全管理器，將其變成STM32Cube生態系統中目標大眾市場之好用的安全解決方案。我們相信，隨著時間的推移，再整合ProvenCore-M技術將可協助客戶顯著提升應用安全的穩定性。」

此外，意法半導體在STM32Trust TEE Secure Manager上預先整合並認證意法半導體授權合作夥伴Kudelski IoT的Kudelski IoT keySTREAM™信任根，支援憑證生命週期遠端系統管理服務。因此，這是一個安全外掛程式解決方案，其提供軟體隔離、加密、金鑰儲存和初始憑證等安全服務。

Kudelski IoT資深副總裁Hardy Schmidbauer指出，「數位身份、設定檔和憑證管理是物聯網裝置安全的核心。意法半導體在安全管理器中預整合和驗證IoT keySTREAM，可以提升裝置的安全性，同時達到現場零接觸配置，以緩解設備廠商在複雜和不安全的生產環境中管理憑證的痛點。」

在STM32H5導入STM32TrusTEE Secure Manager後，意法半導體計畫將其推廣到不同系列的STM32微控制器。

更多資訊，請造訪：www.st.com/stm32trustee-sm。

關於意法半導體

意法半導體擁有48,000名半導體技術的創造者和創新者，掌握半導體供應鏈和先進的製造設備。身為一家半導體垂直整合製造商（IDM），意法半導體與逾二十萬家客戶、數千名合作夥伴一起研發產品和解決方案，共同建立生態系統，協助利益關係人因應各種挑戰和新機會，滿足世界對永續發展之更高的需求。意法半導體的技術讓人們出行更智慧，電力和能源管理更高效，物聯網和互聯技術應用更廣泛。意法半導體承諾將於2027年實現碳中和。詳情請瀏覽意法半導體公司網站：www.st.com。