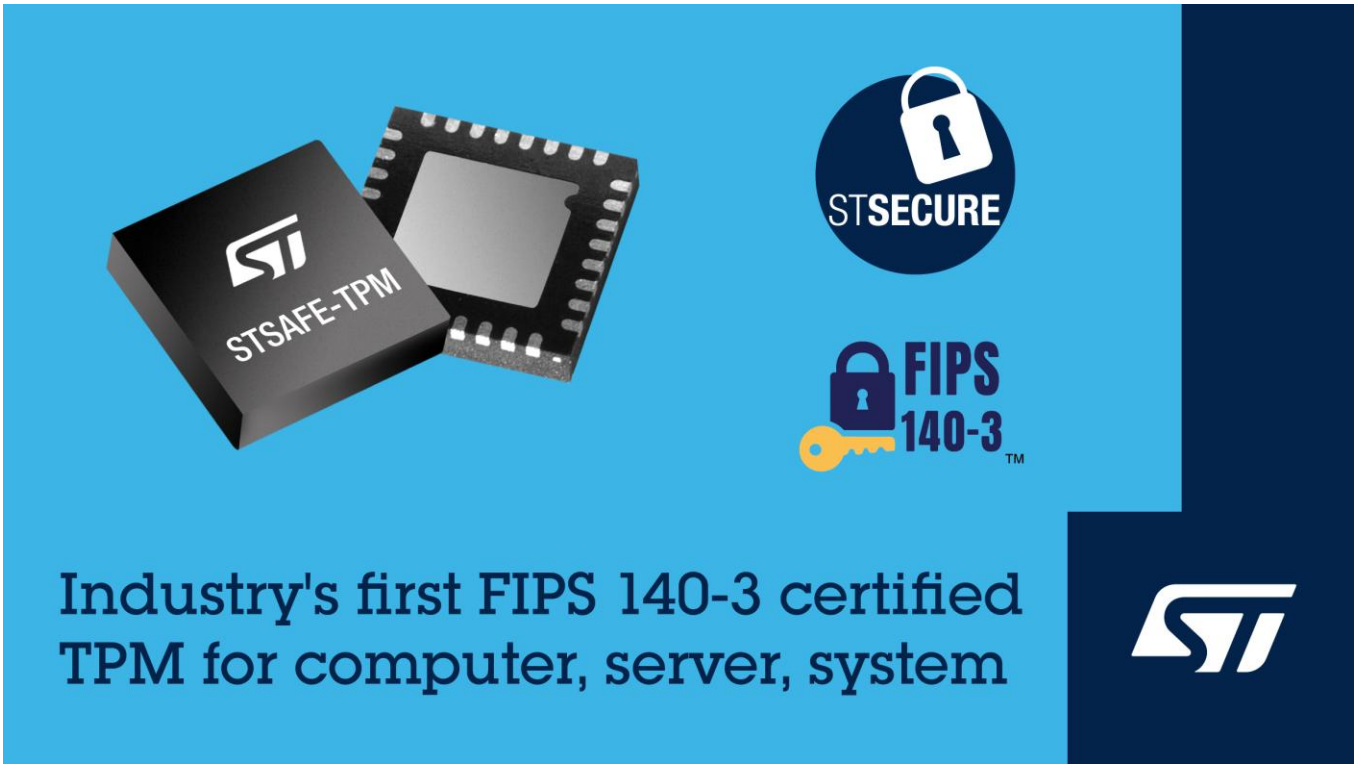
新聞稿



意法半導體推出業界首款通過FIPS 140-3認證的TPM可信賴平台模組，適用於電腦、伺服器和嵌入式系統

先進的保護技術已通過最新的資訊安全認證標準，該標準在全球廣受認可，並且為美國聯邦採購必要條件

【臺北訊，2024年10月30日】服務橫跨多重電子應用領域之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）宣布STSAFE-TPM可信賴平台模組（TPM）已獲得FIPS 140-3認證，是市面上首款獲得此認證的標準化加密模組。

獲得最新認證的可信賴平台模組包括ST33KTPM2X、ST33KTPM2XSPI、ST33KTPM2XI2C、ST33KTPM2I和 ST33KTPM2A，可提供加密資產保護以滿足關鍵資訊系統的安全和法規要求。其可用於個人電腦、伺服器、連網與IoT設備，以及高安全保護醫療設備和基礎建設。其中，ST33KTPM2I適用於長壽命的工業系統，而ST33KTPM2A以名為STSAFE-V100-TPM的產品系列，取得車規AEC-Q100認證，適用於車用產品的安全性整合。

FIPS 140-3取代了FIPS 140-2，是聯邦資訊處理標準（Federal Information Processing Standards，FIPS）中最新的加密模組規範。意法半導體連網部門安全行銷總監Laurent Degauque表示，「所有FIPS 140-2認證預計將於2026年9月到期。我們的TPM取得了FIPS 140-3認證，已為新產品設計做好準備，讓客戶能夠打造安全且互通的設備，擴充產品和認證的可靠性。

此TPM產品系列支援安全啟動、遠端 / 匿名認證和安全儲存等應用，並擁有擴充至200KB的使用者內部儲存。此外，每款產品皆支援安全韌體更新，以新增PQC等加密算法，確保使用者使用最先進的資產保

護加密技術。

STSAFE-TPM產品系列符合多項產業安全標準，其中包括適用於可信賴平台模組的Trusted Computing Group TPM 2.0、通用標準Common Criteria EAL4+（通過CC框架最嚴格的漏洞分析測試AVA_VAN.5），以及目前FIPS 140-3具備安全等級1級認證和物理安全3級認證，提供TCG定義的標準化加密服務（最高384位元ECDSA和ECDH加密演算法、最高4096位元RSA加密演算法（包括金鑰生成）、最高256位元AES演算法、SHA1、SHA2和SHA3演算法），並與FIPS 140-3認證軟體組件或技術相容。

意法半導體也提供配置服務，以載入設備密鑰和證書，進而降低整體解決方案的成本和上市時間，並確保供應鏈的安全性。

更多資訊，請瀏覽：www.st.com/st33ktpm。

關於意法半導體

意法半導體匯聚超過 5 萬名半導體技術的創造者和製造者，掌握半導體供應鏈和先進的製造設備。做為一家整合元件製造商（IDM），意法半導體與逾 20 萬家客戶與數千個合作夥伴一起研發產品和解決方案，攜手建立生態系統，協助客戶因應挑戰和新機會，滿足世界對於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，電源和能源管理更高效，物聯網和連接技術的使用更廣泛。意法半導體致力於 2027 年達成碳中和（適用於範圍 1 和範圍 2 ，以及部分範圍 3 ）之目標。更多資訊，請瀏覽意法半導體官方網站：www.st.com。