解決方案簡介

THALES
CYBERSECURITY



運用 Thales Luna HSMs 保護數位資產

因應日益升高的風險與
持續演進的監管要求，
打造數位信任的
硬體基礎

cpl.thalesgroup.com

THALES

CYBERSECURITY

什麼是數位資產？

數位資產是以數位形式呈現並進行交易的任何形式價值，包括用於支付與交易的加密貨幣與穩定幣，以及證券、存款或現實世界資產等代幣化資產。這些資產在區塊鏈等分散式平台上建立、管理與交換，透過去中心化、可程式化貨幣與數位所有權，構成現代數位金融的基礎。



導言：數位資產快速普及，金融風險日益升高

數位資產已成爲全球金融體系的重要一環。目前穩定幣的交易金額已超過 Visa 與 Mastercard 的交易金額總和，而國際區塊鏈結算量每年已超過 6 兆美元 (Delphi Digital，2025)。此外，現實世界資產與金融資產，在分散式帳本平台上的代幣化也正快速發展，機構試點持續擴大，涵蓋資本市場、支付及跨境結算等領域 (國際清算銀行，2024)。因此，銀行、支付及資本市場等金融機構，正加速推動數位資產策略，以滿足客戶需求，並在快速演進的市場環境中維持競爭力。

這波成長也凸顯強大安全基礎的重要性。2025 年，加密貨幣相關駭客攻擊造成的損失約達 34 億美元，更加凸顯當機構擴大數位資產業務時，健全的金鑰管理與安全控制措施的重要性。即使是已具備成熟安全機制的集中式平台，私鑰仍是暴露風險的關鍵途徑。在 2025 年第一季，包括託管交易所與資產平台在內的集中式服務，佔所有遭竊資金的 88%，凸顯在硬體層級保護私鑰作業的重要性 (Chainalysis，2025)。

隨著數位資產的規模與複雜度持續提升，金融機構需要建立以核心私鑰保護爲設計核心的安全架構。值得信賴且經驗證的硬體安全模組 (HSM) 可提供此一基礎，透過可靠的硬體式信任根保護金鑰，並支援以金鑰爲核心的數位資產工作流程。



挑戰：安全缺口與全球監管要求持續擴大

即使數位資產相關計畫持續加速，許多機構仍難以達成，在大規模營運下維持安全所需的控制措施。私鑰必須以能防止未經授權存取的方式產生、儲存與使用，同時支援大量交易簽署、多方核准工作流程，以及職責分離。以軟體爲基礎的金鑰儲存模式日益欠缺防護，尤其當攻擊者將竊取私鑰視爲進行詐欺與竊盜的主要途徑時，更是難以阻擋。

同時，全球主要金融中心的監管要求日益嚴格，且趨於一致。香港 SFC《虛擬資產交易平台指引》、新加坡金融管理局 (MAS) 相關通知、歐盟《加密資產市場法規》(MiCA)、德國聯邦金融監管局 (BaFin) 指引，以及瑞士金融市場監督管理局 (FINMA) 相關要求，都對資產託管控制、金鑰管理、營運韌性及可稽核性提出明確要求。如今，機構必須證明其數位資產基礎架構能在各種部署模式下，持續落實一致的政策執行、可驗證的金鑰保護，以及透明的治理機制。

滿足這些要求，需要一個值得信賴的安全基礎，以保護私鑰、控制交易簽署，並在不阻礙創新的情況下支援合規。經認證的 HSM 基礎架構，可透過在具防竄改能力的硬體中保護關鍵作業，同時提供監管機構與機構風險管理團隊所要求的安全保障。

解決方案：以 Luna HSM 打造機構級數位資產安全防護

Thales Luna HSM 透過提供硬體信任根保護數位資產，確保私鑰與簽署作業受到經認證、具防竄改能力的硬體保護，並可採地端部署或以服務形式提供，以符合現代數位資產平台的需求。Luna HSM 提供經驗證的安全金鑰產生機制，並在客戶自有且通過 FIPS 驗證的硬體中保護用於應用程式簽署的私鑰，確保金鑰與應用程式層、線上系統及雲端環境完全隔離，而這些環境正是多數攻擊的來源。

透過在防竄改硬體中執行金鑰建立、儲存與簽署，Luna HSM 可強化各類數位資產託管模式。早期許多數位資產平台著重於單純以軟體爲主的便利性，如今機構客戶與監管機關則日益要求以經認證的 HSM 保護私鑰。Luna HSM 可部署於企業內部環境或以服務形式提供，並透過標準 API 將硬體安全能力整合至既有架構，在不造成架構限制的情況下，支援不斷演進的數位資產託管模式。企業可爲軟體金鑰管理流程建立可驗證的信任根，降低單一故障點的風險，並確保核准流程、簽署政策與治理規範獲得一致且有效的執行。此方法可爲機構級數位資產營運提供所需的控管能力與安全保障。

Luna HSM 可與領先的託管平台、區塊鏈基礎架構、錢包技術及代幣化引擎整合。客戶可將 Luna HSM 部署於地端、雲端，以服務形式提供，或透過 Thales Data Protection on Demand (DPoD) 雲端服務市集使用，同時維持一致的安全性、治理與營運控制。靈活選擇部署模式，加上具備密碼敏捷性與量子就緒能力的安全防護，爲機構擴展數位資產能力提供強大基礎，同時強化信任、效能與法規遵循。

Luna HSM 數位資產部署模式

爲數位資產提供靈活的 Luna HSM 部署選項，可部署於雲端、地端或混合環境：

優勢：

完整的金鑰所有權與經認證的安全保障： 金鑰在客戶自有、通過 FIPS 驗證及 Common Criteria 認證的 Luna HSM 內產生、儲存與使用。交易簽署則在具備最高安全保障等級的硬體中執行。Luna HSM 內建密碼敏捷性，包括支援 NIST 標準化的後量子演算法，以及採用未來新興演算法的彈性。

與機構環境無縫整合： Luna HSM 可與受監管的基礎架構整合，並連接支援多元託管架構的託管平台，以及區塊鏈系統，降低安全、治理與稽核團隊在營運上的負擔。

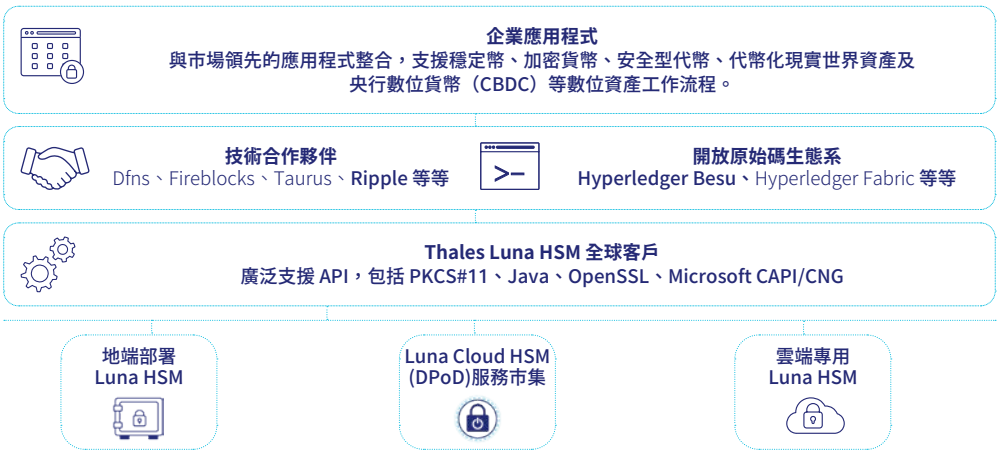
支援熱、溫、冷錢包簽署工作流程： 機構可透過受控機制執行即時線上核准，或完全離線的交易簽署。此彈性可支援不同的風險模型與託管方式。

進階治理與政策控制： Luna HSM 可執行細緻的控制措施，包括多方核准簽署、地址白名單及交易額度限制。不可變更的日誌則支援可稽核性與監管透明度。

資產代幣化與智慧合約支援： Luna HSM 保護代幣化資產在鏈上的完整生命週期，並支援智慧合約互動的簽署作業，包括穩定幣及現實世界資產代幣化。

跨數位資產生態系連結： Luna HSM 可與入金通道、出金通道、流動性供應商、發行商及結算平台整合，同時讓私鑰持續受到硬體完整保護

爲全球法規遵循做好準備： Luna HSM 支援符合 SFC、MAS、MiCA、BaFin 及 FINMA 等監管框架的要求。透過細緻的金鑰、租戶與政策隔離，可將不同環境對應至特定業務單位、區域及監管要求。



多元部署模式，將 Luna HSM 的安全防護延伸至數位資產環境



Luna HSM 提供經認證的硬體信任根，可用於數位資產生態系中的金鑰產生、存取控制與交易簽署，並支援多種部署形式。

總結

隨著數位資產逐漸成爲機構金融的核心，私鑰保護的重要性前所未有，而金鑰遭到入侵仍是數位資產平台財務損失的主要原因之一。Thales Luna HSM 透過在經認證、客戶自有的硬體中執行金鑰產生、保護與交易簽署，爲機構提供值得信賴的風險因應方式。將金鑰保留在通過 FIPS 驗證及 Common Criteria 認證的 HSM 中，可強化安全防護、支援監管要求，並大幅降低金鑰遭誤用或竊取的風險。Luna HSM 可與領先的託管平台、區塊鏈與代幣化平台，以及更廣泛的數位資產生態系整合。以具備密碼敏捷性與量子安全能力的基礎爲核心，並提供靈活的部署模式，Luna HSM 爲數位資產採用提供信任根，協助機構在展現對客戶與監管機構控制能力的同時，安全地擴展業務規模。

關於 Thales

Thales 是全球網路安全領導者，協助企業、政府及全球最受信賴的組織，在任何環境中以大規模方式保護關鍵應用程式、機敏資料、身分與軟體，並實現最高投資報酬率。Thales 擁有超過 30,000 家客戶，其中包括 58% 的《財星》全球 500 大企業，解決方案遍及全球 148 個國家。透過創新服務與整合式平台，Thales 協助客戶更全面掌握風險、抵禦網路威脅、彌補合規缺口，並爲全球數十億消費者每天提供值得信賴的數位體驗。

Learn more about Luna HSMs

Free trial for Luna Cloud HSM for Hyperledger Fabric on DPoD

cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us

© Thales - March 2026 • AC v8