解決方案簡介

THALES
CYBERSECURITY

Fireblocks



透過 Thales 與 Fireblocks 將數位資產私鑰安全儲存於客戶自有的認證 HSM

掌握數位資產的
所有權與控制權

cpl.thalesgroup.com

THALES
CYBERSECURITY

Fireblocks

- 將現有經認證的 HSM 基礎架構，延伸至數位資產工作流程，例如穩定幣、加密貨幣、安全型代幣、代幣化現實世界資產及央行數位貨幣（CBDC）。
- 支援靈活的熱、溫與冷錢包簽署工作流程 •
- 用於交易簽署的私鑰始終受到客戶自有及管理、具備後量子密碼學（PQC）就緒能力的 Luna HSM 保護，符合審查與法規要求。

受監管機構所面臨的挑戰

隨著數位資產的採用加速，受監管機構必須在嚴格的合規要求與內部控制規範下，因應安全交易處理的複雜挑戰。既有基礎架構、日益嚴格的監管審查，以及機構風險管理政策，往往成爲創新的阻礙。

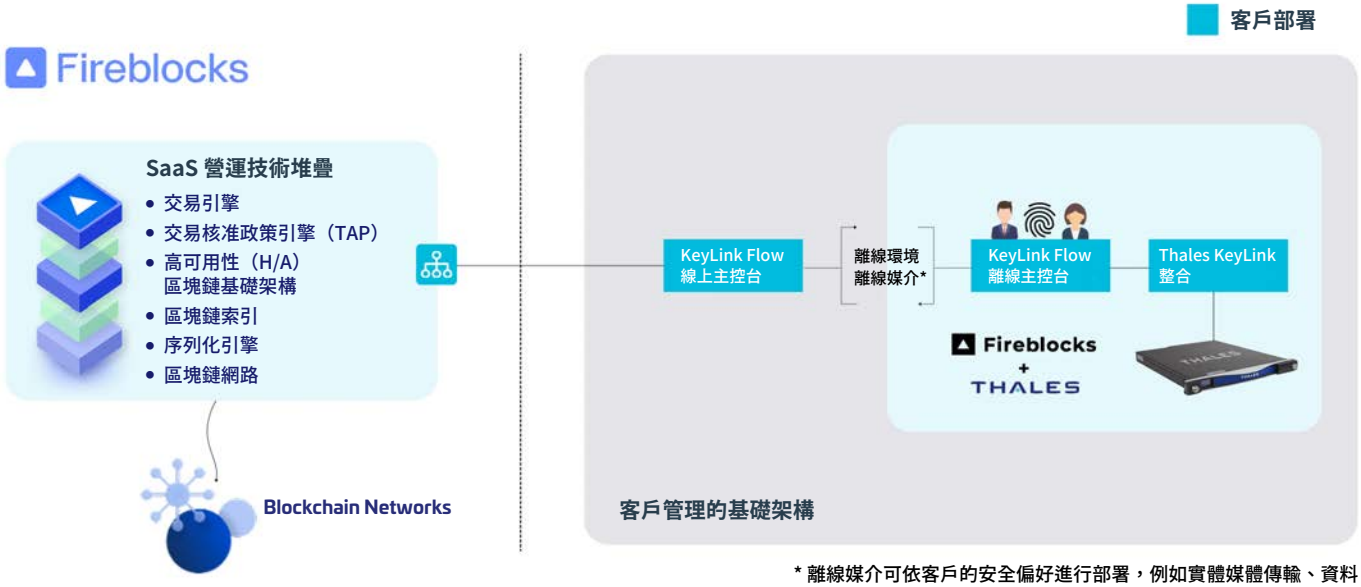
若要成功推動數位資產業務，相關解決方案必須與既有的機構控制框架無縫整合，在維持可稽核性、效能及與企業系統完整整合的同時，提供靈活的簽署工作流程。

Thales 與 Fireblocks：安全且合規的數位資產簽署解決方案

Fireblocks 與 Thales 的合作，讓銀行、託管機構及交易所等受監管機構，能透過完全整合至既有基礎架構的加密簽署流程，管理數位資產交易。此解決方案運用安全的中介軟體層 Fireblocks KeyLink，將 Fireblocks Digital Asset Platform 連接至 Thales Luna HSM。Luna HSM 讓機構能在通過 FIPS 140-3 Level 3 與 Common Criteria 認證的硬體中，安全儲存及管理加密金鑰，確保私鑰始終保留在 HSM 內，並符合嚴格的合規與監管要求。此聯合解決方案兼具地端硬體的安全性，以及 Fireblocks Digital Asset Platform 的彈性與擴充性。此組合讓機構能完整掌握金鑰所有權，符合最高等級的安全與合規標準，無縫整合彈性的交易簽署流程，無論是自動化簽署或氣隙隔離（Air-Gapped）環境皆適用。

主要功能與優勢

- 完整金鑰所有權，以及經 FIPS 驗證的數位資產簽署信任根
  - 加密金鑰始終保留在安全且具防竄改能力的 Thales Luna HSM 環境中。
  - 交易簽署在通過 FIPS 140-3 Level 3 驗證、Common Criteria EAL4+ 認證及符合 eIDAS 規範的 Thales Luna HSM 硬體中執行。
  - Luna HSM 透過將 NIST 標準化的後量子密碼（PQC）演算法直接整合至核心韌體，保護量子安全加密金鑰，實現密碼敏捷性與後量子密碼學就緒能力。
- 與既有基礎架構無縫整合
  - 運用已嵌入受監管、銀行級環境中的安全架構。
  - 將安全、治理與稽核流程所需的營運負擔降至最低。
- 熱錢包或冷錢包簽署選項
  - 支援即時線上交易核准。
  - 透過安全機制（例如 USB、SFTP、資料二極體）支援氣隙隔離的離線工作流程。
- 進階治理與政策控制
  - 提供細緻且完全可自訂的控制措施，包括多方核准規則、地址白名單及交易額度限制。
  - 完整且不可變更的日誌，可提供稽核軌跡與監管佐證。
- 原生支援代幣化與智慧合約
  - 安全管理代幣化資產在鏈上的完整生命週期。
  - 相容於智慧合約交易核准及鏈上資產邏輯。
- 數位資產與穩定幣生態系連結
  - 在維持完整金鑰控制權的同時，安全地與數位資產及穩定幣生態系互動，涵蓋入金通道、出金通道、流動性提供者及發行商。
- 爲全球法規遵循而打造
  - 設計用於因應香港金融管理局（HKMA）、香港證券及期貨事務監察委員會（HKSFC）及日本金融廳（JFSA）等主要監管框架。
  - 支援依業務單位、地理區域或監管轄區進行組織分區。



Integrating Thales Luna HSM with Fireblocks' KeyLink strengthens the security and efficiency of digital asset operations.

總結

Fireblocks KeyLink 搭配 Thales Luna HSM，讓機構能運用符合其監管與內部安全標準的基礎架構，安全管理數位資產工作流程。此混合式方法同時支援既有 HSM 系統與現代化編排平台，提供彈性、信心與面對未來的準備。對於需要靈活簽署控制、與既有基礎架構無縫整合，以及拓展至數位資產與穩定幣生態系的機構而言，這是一套安全的數位信任基礎。

關於 Fireblocks

Fireblocks 是全球深受信賴的數位資產基礎架構公司，協助各種規模的組織在區塊鏈上建立、營運並拓展業務。Fireblocks 提供業界安全性、擴充性與完整性兼具的平台，簡化託管、代幣化、支付、結算及交易作業，服務全球規模最大的交易所、託管機構、銀行、支付服務提供者及穩定幣發行商生態系。全球超過 2,400 家組織，包括超過 60 家全球銀行，例如 BNY、BNP Paribas、SCB、SMBC、Wenia 及 BTG Pactual，均信賴 Fireblocks，透過其平台在超過 100 條區塊鏈及逾 3 億個錢包上，保護超過 10 兆美元的數位資產交易。更多資訊請參閱 fireblocks.com。

關於 Thales

Thales 是全球網路安全領導者，協助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、資料、身分與軟體。透過 Thales 整合式平台，客戶能更全面掌握風險、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。

© Thales - November 2025 • AC v5