cpl.thalesgroup.com

THALES
Building a future we can all trust

亞太地區領先的金融安全集團與 Thales 合作，實現數位化轉型和合規性

Thales 解決方案協助金融安全集團應對關鍵業務挑戰

摘要

亞太地區一家領先的金融安全集團，部署高可擴展的 Thales 解決方案用於保護靜態資料，以及保護不同環境中的分散式資料和金鑰管理；同時提供模組化管理，無論它們在何處運營，都能實現當地法規遵循的合規性。

企業背景

該集團被譽為亞太地區領先的金融安全集團之一。它的業務以亞洲地區為主，透過人壽和健康保險解決方案，協助客戶專注於結構性增長市場。該集團在亞太地區擁有強大的影響力，在新加坡、香港、印尼、韓國、日本和越南等多個國家擁有數百萬客戶。

目前，該集團正從部署在全球40多個不同地點的 Thales 解決方案中獲益。

業務需求

數位化轉型正在推動該集團的業務需求，期望能利用數據分析、商業應用和基礎設施提供的雲端優勢。該集團需要高度可擴展的解決方案，可同時在混合和多雲環境中執行，並在不同環境中提供資料保護和金鑰管理。

該集團還必須為客戶提供一個安全管道，以實現監管的合規性，同時將資料轉移到雲端，執行共同責任模式。

強制性法規規範包括以下內容：

- 個人資料保護法 (PDPA)
- 健康保險流通與責任法案 (HIPAA)
- 支付卡產業資料安全標準 (PCI DSS)
- 歐盟一般資料保護規範 (GDPR EU)

挑戰

作為金融業的一部分，該集團要處理大量的個人、健康和財務資料。作為一家保險公司，該集團的法律責任是保護所有客戶資料不受任何侵犯，同時實現合規性，以應對關鍵的稽核挑戰。任何不符合他們所處國家/地區的當地資料隱私法的行為都將面臨嚴重的後果。例如，根據 PCI 安全標準委員會（PCI Security Standards Council）的說法，不合規的團體可能會遭受巨大的法律成本與和解費，導致銷售額的降低。

Thales 在眾多國家執行業務，能為不同國家客戶提供具策略性的在地隱私法律建議。

Thales 被選為該集團的第一家也是唯一一家供應商，透過提供靜態資料保護工具來加強他們現有的基礎設施，並確保該資料的金鑰在硬體信任根中安全的產生、儲存和管理。

解決方案

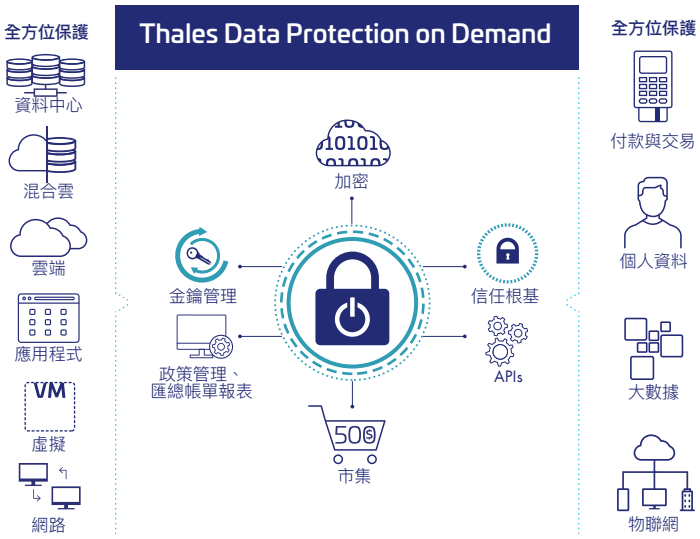
Thales 熟知該集團在數位化轉型和法規遵循方面面臨的業務挑戰，並提供以下解決方案，透過靜態資料保護工具的優勢來加強集團的安全基礎設施。

滿足法規遵循的要求

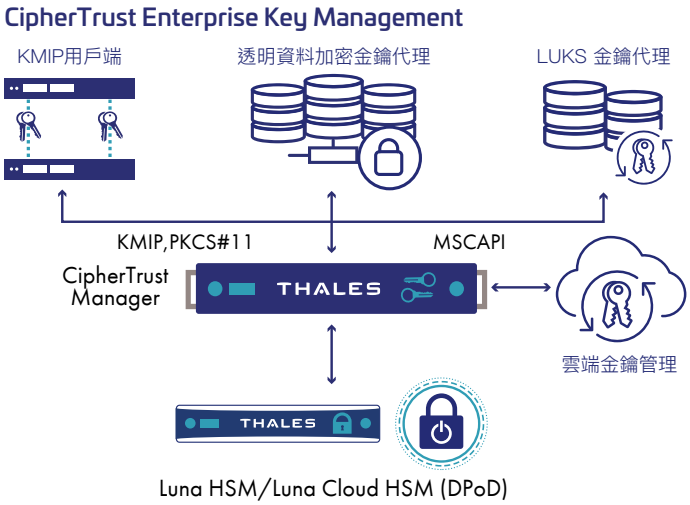
鑒於個人資料在使用、儲存和處理方式的脆弱性，確保資料安全勢在必行。為了保護資料和 HIPAA、GDPR 和 PCI-DSS 等法規的到位，可解決資料安全問題和隱私法規。

該集團採取分階段的方式以實現他們的目標。第一階段是實現法規遵循，客戶選擇了 Thales Data Protection on Demand Luna Cloud HSM 服務和 CipherTrust Manager，以協助該集團透過經驗證的 **FIPS 140-2 3** 級認證加密解決方案，滿足其資料安全合規性需求。

- Thales Data Protection on Demand 雲端平台，透過簡易的線上市集，提供各式的雲端硬體安全模組 Luna Cloud HSM和 CipherTrust 金鑰管理服務。有了 Data Protection On Demand(DPoD)，不必再購買、部署或維護任何硬體，讓資安管理變得更加簡易、符合成本效益且便利。只需幾個按鍵，便能在幾分鐘內部署所需的保護措施、提供服務、新增資安政策並且查看使用狀況報告。DPoD 提供各種的基於雲端的 Luna HSM 服務，允許客戶在雲端中儲存和管理用於資料加密的加密金鑰，同時保留對金鑰的完全控制，以滿足各種使用情況和跨環境整合。Luna HSMs 在一個業經強化、防篡改、並經 FIPS 140-2 驗證的設備中安全地管理、處理和儲存加密金鑰和功能，該設備可作為本地硬體，也可在雲端和混合環境中使用。
- CipherTrust Manager 提供了領先業界的企業金鑰管理解決方案，使企業能夠集中管理加密金鑰，提供精細的存取控制和配置安全性原則。CipherTrust Manager 是 CipherTrust 資料安全平台的中央管理點。它管理金鑰的生命週期任務，包括生成、輪換、銷毀、導入和導出，為金鑰和金鑰管理策略提供以角色界定的存取控制； 並支持穩健的稽查和報告，並提供對開發者友善的 REST API。



CipherTrust Manager 可用於虛擬和實體設備，與符合 FIPS 140-2 Level 3 標準的 Thales Luna HSM（在企業內部，通過 DPoD 作為雲服務，或在混合環境中一起使用）或與協力廠商硬體安全模組（HSM）整合，以安全的方式儲存具最高信任根的金鑰。



無保險庫代碼化將資料從本地安全的轉移到雲端基礎設施

在第 2 階段，Thales 建議使用**無保險庫代碼化**將資料安全的從本地端轉移到雲端基礎設施。

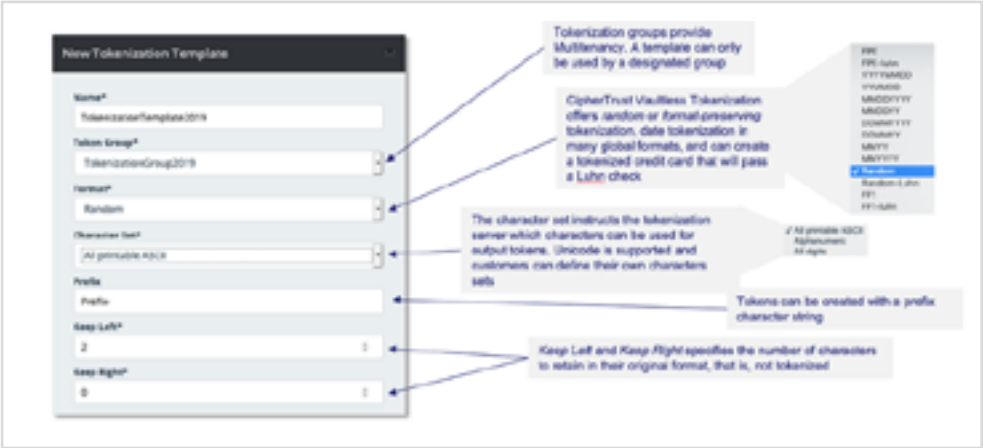
代碼化有效降低安全政策遵循與監管要求所需的成本和工作負載，如歐盟的一般資料保護規範（GDPR）和支付卡產業資料安全標準（PCI-DSS）。

- CipherTrust Tokenization 以兩種便利的解決方案，提供應用層代碼化服務，為客戶提供完全的靈活性：帶有動態資料遮罩的無保險庫代碼化和有保險庫代碼化。無論它們是位於資料中心、大數據環境還是在雲端，兩項解決方案都可以保護機敏資產並使其匿名化。

自帶金鑰 (BYOK)

Thales為該集團部署了 **CipherTrust Cloud Key Manager**（CCKM），以利用公有雲解決方案供應商的金鑰庫中的BYOK方法。該集團部署 Thales CCKM 的主要目的是確保，用來加密存放在雲端的資料、及網路協作軟體中使用的資料的金鑰的所有權，而不是完全任由公有雲解決方案供應商來生成與儲存這把金鑰。這個解決方案使該集團能夠實踐強大的金鑰管理，同時滿足嚴格的稽核和合規性。

在為期兩年的 BYOK 部署之後，該集團已經從自帶金鑰（BYOK）轉移到最高級別的**自帶加密 (BYOE)**。

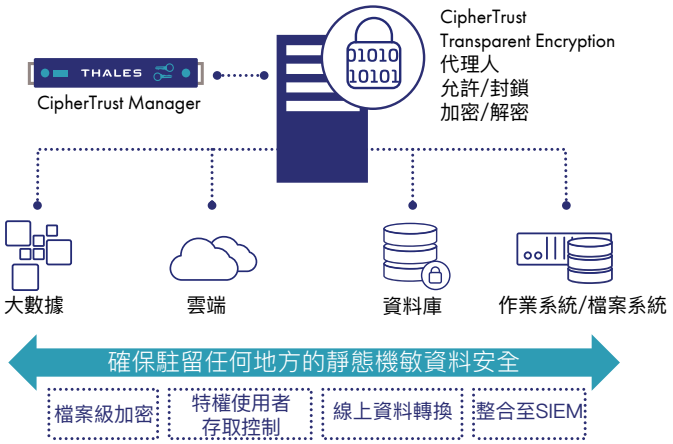


無保險庫代碼化提供了集中的配置，以實現明確的職責分工。

變動環境的資料庫加密

保護機敏資料不僅只是保護資料中心的內部資料庫和文件。在部署 CipherTrust Manager 的同時，我們還推薦 CipherTrust Transparent Encryption，以支援該集團的數位化轉型的過程，同時保護大量的個人、健康和財務資料。

CipherTrust Transparent Encryption



- CipherTrust Transparent Encryption 透過集中的金鑰管理、特權用戶存取控制和詳細的資料存取稽核日誌，以提供靜態資料加密。無論資料位於何處，都能協助企業達到保護資料的法規遵循和最佳執行要求。

  CipherTrust Transparent Encryption 還允許企業使用已經驗證的硬體加速加密解決方案，以符合加密、存取控制和資料存取紀錄的合規性和最佳執行要求。該解決方案可確保文件、資料庫和連結雲端儲存的安全，同時在實體、虛擬和雲端環境中支援存取控制和資料存取稽核記錄。

優勢

加強安全性和合規性

Thales 的資料保護產品和解決方案可以滿足一系列安全和隱私要求，包括電子身分認證與歐盟電子身分識別（eIDAS）、支付卡產業資料安全標準（PCI DSS）、歐盟一般資料保護規範（GDPR）、健康保險流通與責任法案（HIPAA）、聯邦資訊安全管理法（FISMA）以及區域資料保護和隱私法。

優化員工和資源效率

Thales 提供業界最廣泛的資料安全，支援任何產業案例的使用，透過產品協同設計、單一連線的全球支援、可靠的追踪記錄以保護免受不斷變化的威脅，以及擁有業界最大的資料安全合作夥伴關係生態系統。 在 Thales，我們高度關注易用性、自動化 API 和回應式管理，以確保您的團隊能夠快速部署、保護和監控業務的保障。 此外，我們的專業服務和合作夥伴可提供設計、實施和培訓的協助，以確保員工花費最短時間即能快速、可靠地部署執行。

降低總體擁有成本

Thales 的資料保護組合提供了一套全面的資料安全產品和解決方案，這些產品和解決方案可輕鬆進階擴展到新的使用案例，並且在保護新技術和傳統技術方面有著良好的成效。藉助 Thales，在降低運營成本和資本支出的同時，你可以證明你的投資是經得起未來考驗的。

關於Thales

不論任何人在個資保護的技術上都透過 Thales 保護他們的資料。在資料安全方面，企業面臨著越來越多的決定性時刻。 無論是建置加密策略，移轉到雲端還是滿足合規性要求，在邁向數位化轉型時，您可以依靠 Thales 來保護您的有價資料。

關鍵時刻，關鍵技術。