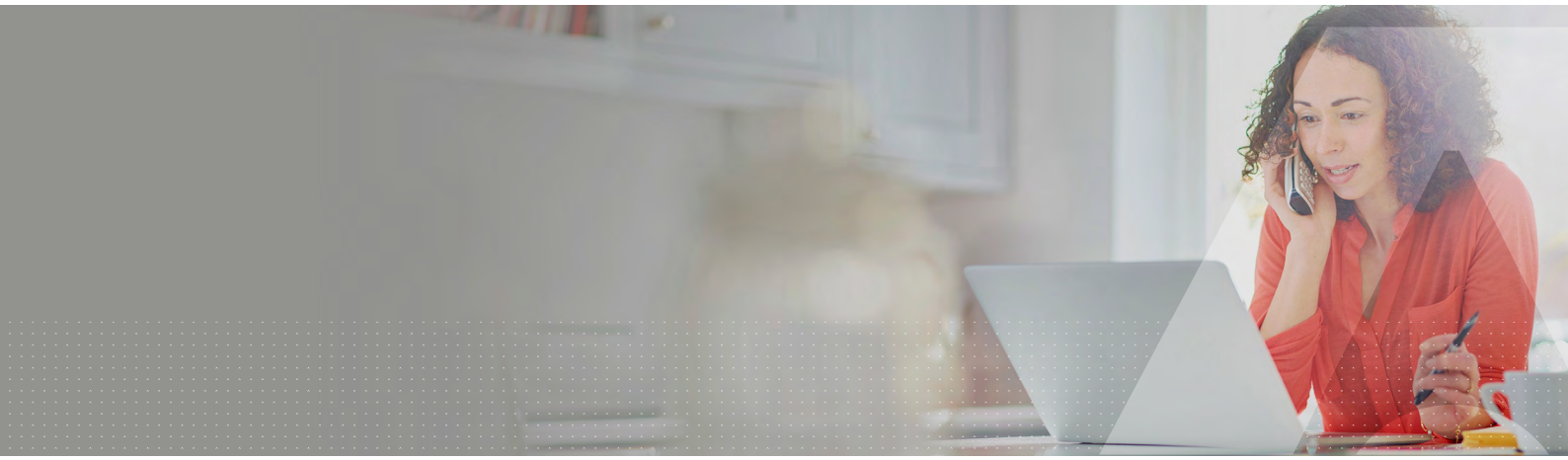
cpl.thalesgroup.com

Google Workspace | THALES
Building a future we can all trust

針對Google Workspace設計的Thales安全解決方案

採用Google Workspace用戶端加密與Thales身分識別和資料保護方案以強化隱私和機密性



強化Google Workspace金鑰管理

在數位轉型和雲端應用程式的現今世界中，雲端服務供應商和企業正在尋求更強大的雲端安全性與法規遵循方案。針對這項挑戰，Google Workspace藉由用戶端加密(beta版即將問世)以強化隱私和機密性－該方案讓企業客戶能夠透過SafeNet Trusted Access 信任存取和CipherTrust雲端金鑰管理器完全掌控他們的加密金鑰。

在共同承擔安全責任的概念下，Google建議客戶採用外部金鑰管理器(EKM)和身分識別供應者(IDP)以確保唯有授權且身分驗證合法的使用者可以存取受保護的文件。唯有Thales開發一套獨立IDP與金鑰管理方案。

Google Workspace用戶端加密與Thales身分識別保護和金鑰管理：更強的組合

採用Google Workspace用戶端加密的客戶可以藉由Thales的整合式端對端方案達到更強安全性和較低的部署負荷，Thales方案保護身分識別並管控與雲端機敏資料分離的加密金鑰。

用戶端加密金鑰讓服務供應商可以容納加密資料但不會予以解密，保護使用者的隱私。使用者擷取他們的檔案時，相對應的資料加密金鑰唯有在使用者通過客戶管控的身分驗證程序之後才會使用客戶提供的金鑰進行解密。

Thales的SafeNet Trusted Access 信任存取(STA)搭配CipherTrust雲端金鑰管理器為客戶提供一個源自單一廠商的獨立IDP與金鑰管理方案，協助您以更流暢的部署、傑出的使用者體驗和更優價值實現商業目標。

Thales是可信任的多重雲端夥伴。STA與CipherTrust雲端金鑰管理器讓企業能夠維持對存取安全和加密金鑰的管控而不會被廠商套牢－這點對於數位轉型計畫的多重雲端環境支援而言非常重要。

集成/整合方案的運作流程

使用者登入Google Workspace然後被重導至STA以接受身份驗證和身分識別確認。

- STA驗證使用者身分並建立一個身分驗證token。
- 當使用者建立一個用戶端加密檔，由STA產生的身分驗證token和另一個由Google產生的授權碼將傳送到CipherTrust雲端金鑰管理器，同時CipherTrust雲端金鑰管理器也會取得一個由Google產生的資料加密金鑰(DEK)。
- CipherTrust雲端金鑰管理器以STA對STA產生的身分驗證token進行確認，並由Google對Google產生的授權碼進行確認。
- 如果二個代碼都通過認證，CipherTrust雲端金鑰管理器將使用一個由CipherTrust產生的金鑰加密鑰(KEK)對DEK進行加密 – 然後將加密的DEK送回Google。
- 此後檔案不論開啟或儲存都將需要由CipherTrust雲端金鑰管理器進行認證，通過認證才能允許被授權者打開KEK和存取DEK與檔案。

關鍵優勢

將工作負荷與應用程式轉移到雲端的企業經常運用一些協同合作套件例如Google Workspace。這提供很大的效益包括簡易性、可以從任何地方使用任何裝置存取等，而若增加外部身分識別與加密就能夠自行管控加密金鑰，以及為儲存在雲端的機敏公司資產增加額外的隱私和安全性。

Thales是唯一提供獨立IDP、認證與金鑰管理的安全方案供應商，協助企業在透過用戶端加密保護Google Workspace的同時符合最佳雲端安全實務原則。

Thales整合式存取與金鑰管理方案提供實質的效益，包括：

- **安全性：**讓企業擁有自己的存取安全和金鑰管理，降低資料外洩及受懲罰的風險。
- **流暢部署：**單一廠商方案與Google Workspace整合，確保快速流暢的部署。
- **卓越的用戶體驗：**使用者受惠於Google Workspace及其他雲端服務與應用的單一登入方便性。

關鍵功能

用戶端加密的身分識別保護

STA當成一個獨立的第三方IDP，對Google Workspace使用者進行身分認證。STA藉由OIDC整合，為Google Workspace用戶端加密提供身分驗證。

強化身分驗證並確保Google Workspace存取安全

STA藉由SAML整合以與Google Workspace建立聯合身分識別，提供單一登入，並於使用者登入Google服務時執行適當層級的認證。

簡單而強大的身分驗證

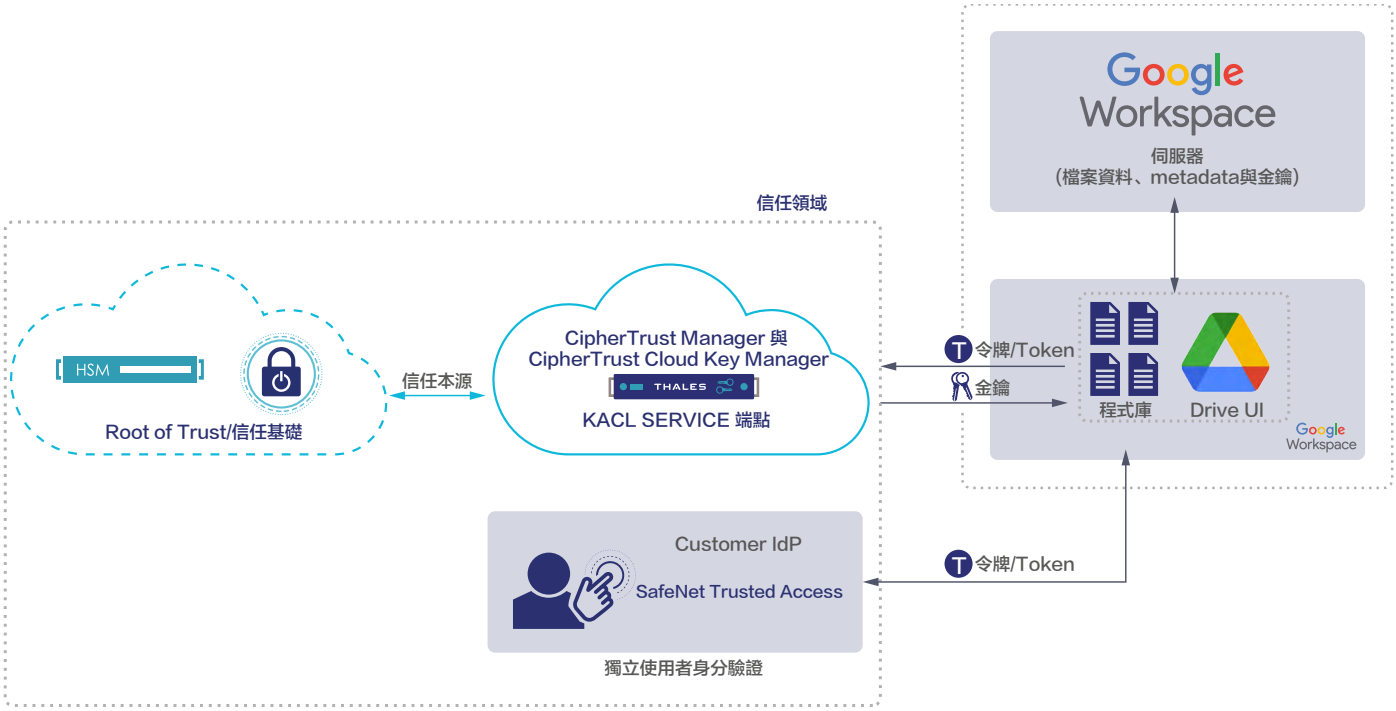
運用零信任安全模式，遵循先認證後存取的概念，對所有資源提供強大且連續的認證、單一登入和多因子認證。認證方法包括：FIDO、硬體代碼、軟體代碼(OTP apps)、out-of-band (OOB)推播認證、憑證認證(CBA)、型態認證、簡訊與電子郵件OOB以及脈絡認證。

便利和簡易

在預設的時間內，可設定使用既有的憑證進行再認證 – 減少使用者抗拒而不會犧牲安全性。

Google Workspace金鑰管理

CipherTrust雲端金鑰管理器提供外部金鑰管理與策略管控，確保唯有授權使用者才能存取加密文件。



關於Google Workspace用戶端加密

Google Workspace用戶端加密協助客戶強化資料機密性，並解決廣泛的資料主權與法規遵循要求。客戶可以直接管控加密金鑰，以及他們選擇用來存取那些金鑰的身分識別服務。客戶資料無法被Google解密，而使用者可以繼續享有協同合作效益、在行動裝置存取內容、以及在外部分享加密檔案。

關於Google Workspace

Google Workspace是一個統合的協同合作與通訊平台，為各大小規模企業提供連接、建立與協同合作所需的一切。Google Workspace 包括應用程式例如 Gmail、 Google Meet、 Calendar、 Drive、 Docs、 Sheets、 Slides等。詳細資訊請參觀 workspace.google.com。

關於Thales存取管理

Thales領先業界的存取管理與認證方案讓企業藉由一種零信任模式以集中管理和確保企業IT、Web與雲端應用程式的存取安全。以政策為基礎的條件式存取、強韌單一登入、以及共通的認證方法，協助企業有效預防入侵，安全轉移至雲端以及簡化法規遵循。

關於Thales資料保護

CipherTrust資料安全平台是一組支援雲端的產品方案，協助資安團隊舒緩許多資安挑戰以實現他們的多重雲端策略。該平台提供無與倫比的方案廣度，解決資料安全與加密金鑰管理挑戰。CipherTrust雲端金鑰管理器是該平台的元件之一。

關於Thales

不論任何企業都仰賴Thales保護他們的資料。企業在維護資料安全上面對越來越多重要的決策，不論是建置加密策略、移轉到雲端、或者符合資料法規的遵循等，您可以仰賴Thales來保護您邁向數位轉型。

Thales為關鍵決策提供關鍵技術。