# CypherCom

# 端對端加密通訊系統

## 硬體加密確保零信任網路通訊安全

**國際認證 | 通訊技術 | 硬體加密 | 整合 VoIP 與 IM**

- 硬體晶片加密確保金鑰不外洩
- 直接使用原有手機裝置
- 整合VoIP與即時通訊軟體
- PKI 憑證技術確認通話者身分
- 通過 FIPS 140-2 Level 3 安全認證
- 適用現有 4G/5G/Wi-Fi 上網環境
- 語音、文字、照片、影片及檔案加密傳輸
- 中華電信集團自主研發加解密元件

中華資安國際
CHT Security

www.chtsecurity.com
SERVICE@CHTSECURITY.COM 02-2343-1628 | 04-2369-2214 | 07-262-6260

EMPOWER YOUR SECURITY

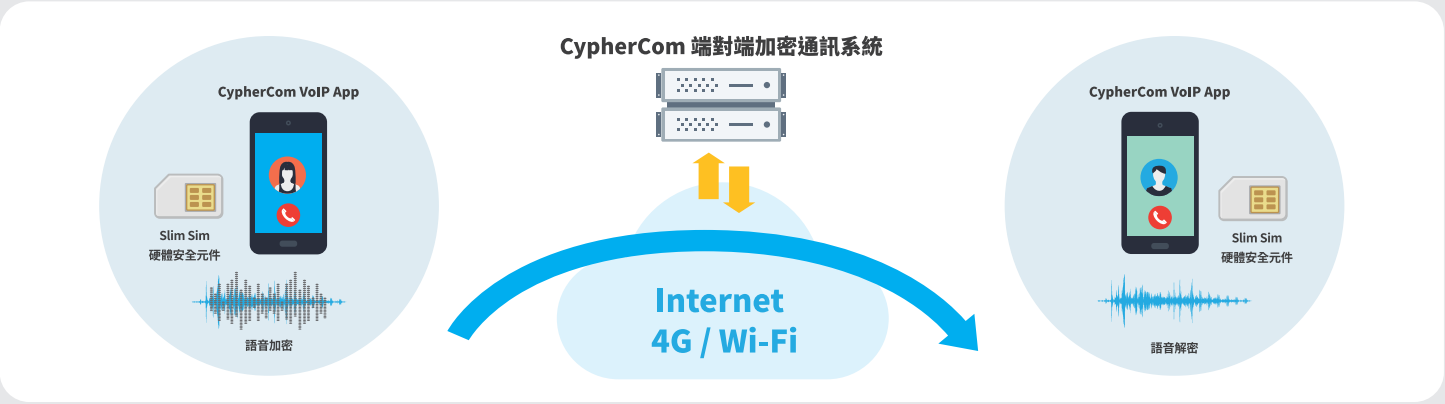
## 產品簡介

CypherCom 是一套端對端加密通訊系統，相較於過去的安全通訊方案著重於網路與設備點對點的認證，CypherCom 將安全認證從傳統的「設備」角度更延伸到「使用者」的層面，確實保障使用者間通信內容的保密性與完整性，基於零信任的精神，於既有行動通訊網路上，建構一套安全的、不被竊聽的通訊系統，通訊過程全程加密，過程中不儲存明文訊息，亦無法解密，完成端點對端點的秘密通訊。

CypherCom 端對端加密通訊系統之 Slim Sim 硬體安全元件與其 applet 皆通過 FIPS 140-2 Level 3 安全驗證，確保通訊使用之私鑰受到高強度保護，並且通訊過程均採硬體加密模式，確保使用者通訊安全。

使用本套端對端加密通訊系統，終端用戶不需轉換手機，只須連網便可以進行安全的 VoIP 語音通話及 Instant Messaging (IM) 訊息傳送，包括語音、照片、影片、檔案皆加密保護，並整合現有通訊錄功能，使用簡便且安全。

## 架構說明




整套通訊系統採用中華電信集團自行研發之軟硬體元件，包含 CypherCom Server、APP、通過 FIPS 140-2 Level 3 安全驗證之 Slim SIM 或 Bluetooth Token* 硬體憑證載具等，確保封包無法被還原或竊聽，「持續驗證、不輕易信任」，達成零信任網路 (Zero Trust Network) 通訊安全。

★ Bluetooth Token 僅支援 iOS

- CypherCom Server : 傳送通訊之語音、照片、影片、檔案，發行與管理使用者 Slim Sim 安全元件，並確認安全元件之有效性
- Slim SIM : 儲存使用者之通訊私鑰
- CypherCom App : 採用 TLS & SRTP 協定，提供端對端加密通訊

## 服務模式

提供雲端 (Cloud) 由專業資訊安全代管服務商協助管理以及本地部署 (On-Premises) 建置於企業內部兩種模式，適用於所有對於通訊安全高度重視之用戶。

## 產品規格

| Slim SIM 硬體安全元件 | 通訊安全 |
|---|---|
| · 符合 Java Card Platform Specification 3.0.4 | · 通訊間連線均採用 TLS 加密保護確保機敏性 |
| · 符合 GlobalPlatform Specification 2.2.1 | · 私密金鑰採用 ECC P-256 金鑰 |
| · 支援非對稱加密演算法及金鑰：RSA、ECDSA、ECDH 等簽章演算法 | · 簽章演算法採用 ECDSA with SHA-256 演算法 |
| · 晶片通過 Common Criteria EAL5+ 與 FIPS 140-2 Level 3 安全認證 | · 金鑰交換皆採用 ECDHE-ECDSA |
| · 卡片作業系統與 PKI Applet 通過 FIPS 140-2 Level 3 安全認證 | · 資料加密採用 AES-128-GCM |


中華資安國際
CHT Security

www.chtsecurity.com
SERVICE@CHTSECURITY.COM 02-2343-1628 | 04-2369-2214 | 07-262-6260