中華資安國際
CHT Security

CypherCom

端對端加密通訊系統

通訊技術 | 資安專業 | 國際認證 | 自主研發

- 硬體晶片加密確保金鑰不外洩
- 適用現有 4G/5G/Wi-Fi 上網環境
- 通過FIPS 140-2 Level 3安全認證
- PKI憑證技術確認通話者身分
- 直接使用原有手機裝置
- 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
02-2343-1628 SERVICE@CHTSECURITY.COM

EMPOWER YOUR SECURITY

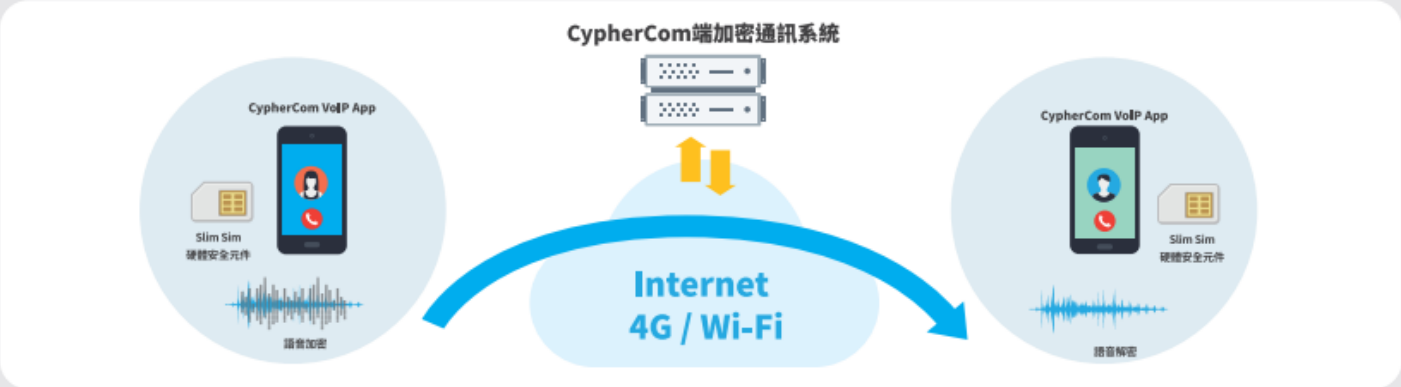
產品簡介

CypherCom為一套端對端加密通訊系統，將安全認證從傳統的「設備」角度延伸到「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，著眼於零信任之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，完成端點對端點的秘密通訊。

CypherCom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，確保通訊使用之金鑰受到高強度保護，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通話，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，包含語音加密通訊之CypherCom Server、VoIP APP、通過FIPS 140-2 Level 3安全驗證之Slim SIM硬體憑證載具等，確保封包無法被還原或竊聽。

- CypherCom Server：傳送VoIP通話、發行與管理使用者Slim Sim安全元件、與確認安全元件之有效性
- SecuTex Slim SIM：儲存使用者之通訊私鑰
- VoIP App：採用 TLS & SRTP 協定，提供端對端加密通話

服務模式

提供雲端(Cloud)以及本地部署(On-Premises)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
02-2343-1628 SERVICE@CHTSECURITY.COM