PRODUCT
產品介紹

HiSecure
身分確認服務
目錄服務
附卡授權API
Hicos卡片管理工具

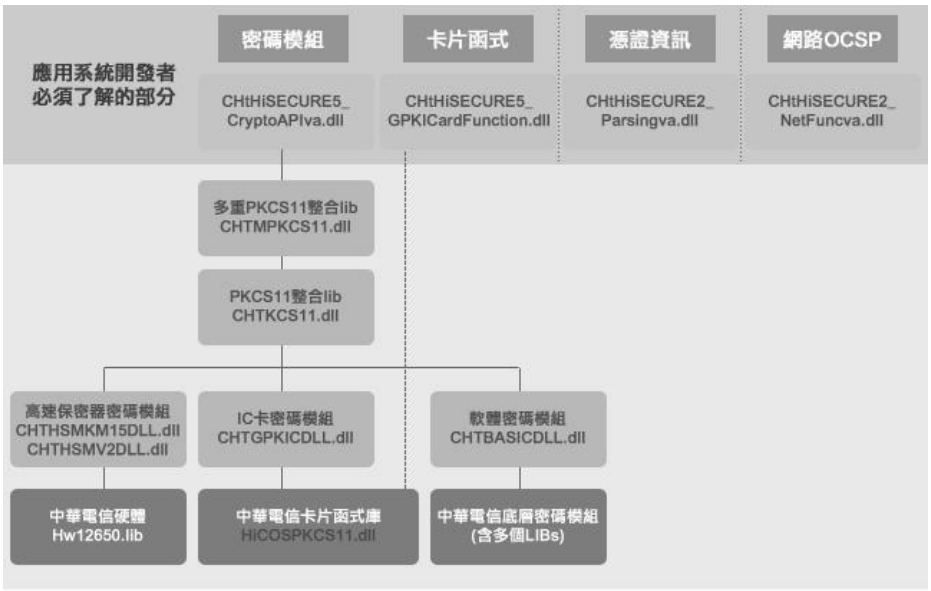
Hisecure

開發一個 PKI的應用系統，是需要一些技術來輔助的。例如密碼模組的技術，憑證資訊的解析等，再加上種種技術及規範不斷地更新之下，如果沒有一個好的開發工具，勢必使得PKI架構難以推行。中華電信HiSECURE便是提供相關的技術給應用系統的開發廠商，使其可以最迅速便捷的方式來開發PKI的應用系統。
HiSecure依據GPKI技術規範、憑證及憑證廢止清冊格式剖繪、公鑰憑證處理安全事項檢查表以及相關國際相關標準，提供開發電子認證應用系統所需之安全保密函式，可呼叫編譯後提供數位簽章以及檢驗簽章、加密與解密、憑證解析、憑證廢止清冊查訊下載與檢驗、憑證線上狀態查詢等功能。以解決資訊安全上身份鑑別、資料完整性、系統真確性、機密性、不可否認性、存取控制、可歸責性之問題。

提供對象：廠商或政府開發**PKI**運用

提供函式功能如下：

程式語言 功能	C語言	JAVA 語言
資料加解密	對稱與非對稱	對稱 -DES/DES3/AES等非對稱-RSA
數位簽章與驗證	SHA1 with RSA	SHA1/MD5withRSA/Raw RSA
憑證資訊的取得	序號、發行者、持有者、身份證末碼、統編、憑證類別、主體類型、效期	序號、發行者、持有者、身份證末碼、統編、憑證類別、主體類型、效期
憑證廢止驗證	CRL 及 OCSP	CRL 及 OCSP



HiSecure C語言函式介面架構圖