Chunghwa Telecom

HiSECURE C/C++ API 檢測程式

使用手冊

Ver 1.0

Chunghwa Telecom Co., Ltd.
Telecommunication Lab

2009/10/15

Table of Contents

1. Introduction

HiSECURE C/C++ API 之中文名稱為安全保密函式庫 C 語言版本(以下簡稱本函式庫)，本函式庫係依據 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、數位信封加密與解密、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。

本函式庫係由中華電信研究所開發，匯集了先進的網路安全標準與多年的資訊安全及密碼學之研發經驗，其智慧財產權屬於中華電信公司所有。為配合電子化政府基礎建設的網路安全需求，使眾多植基於政府機關公開金鑰基礎建設(GPKI)的應用系統能儘速進行開發測試，將此保密及憑證模組應用程式介面作版權的分級，在不同等級的 API 中作不同的版權以及程式散佈之保護。目前本函式庫之標準版版權為中華電信公司所有；研考會規劃使用，程式散佈亦由研考會控管。

而 HiSECURE C/C++ API 檢測程式(以下簡稱本檢測程式)係為一套提供給用戶端測試本函式庫之函式功能是否正常的測試工具。中華電信研究所的服務範圍主要針對本函式庫中各函式功能是否符合預期、是否有 Bug 的相關問題提供技術支援。上層應用系統可能利用本函式庫建立 PKI 應用服務，當有問題發生時，為了能更明確、快速界定是否為本函式庫的問題，並縮小用戶反應問題的可能原因範圍，以便於協助用戶能更迅速釐清、解決問題，我們提供了本測試程式。

2. Getting Started

2.1 環境需求(Requirements)

使用密碼模組檢測程式前，須先完成以下事項：

(1) 安裝HiCOS卡片管理工具後，HiCOS PKCS#11版本須為2.0.9.36691以上版本。

(2) 安裝讀卡機和備妥卡片。

(3) 卡片內已有憑證。

2.2 HiCOS卡片管理工具

(1) HiCOS 卡片管理工具是一種 CSP(Cryptography Service Provider)，係提供 IC 卡之憑證註冊至作業系統的工具，以利安全電子郵件或憑證應用應用系統使用密碼學之簽章或加密等功能，下載安裝後除 HiCOS 卡片管理工具外，並包含用戶端環境檢測工具、UP2Date Agent 等程式與相關手冊。

(2) 來源：GRCA 下之各政府憑證管理中心網站，例如：GCA 政府憑證管理中心網站→訊息公告及儲存庫→儲存庫→下載 HiCOS 卡片管理工具、安裝手冊(http://gca.nat.gov.tw/02-04.html)。

(3) HiCOS 卡片管理工具之安裝，依作業系統區分，請參考「HiCOS 卡片管理工具 Windows XP 平台安裝手冊」或「HiCOS 卡片管理工具 Windows Vista 平台安裝手冊」。

(4) HiCOS 卡片管理工具所支援的 IC 卡片包括 GCA/XCA/MOEACA/MOICA/GTESTCA 對用戶所發之 1024 位元與 2048 憑證 IC 卡。

2.3 HiSECURE C/C++ API檢測程式

(1) HISECURE_CryptoModule：密碼模組檢測程式

(2) HISECURE_CERTPARSING：憑證及CRL檢測程式

3. 檢測程式使用說明

3.1 密碼模組檢測程式

(1)毋需安裝，請解壓縮後，直接點選exe檔(HISECURE_CryptoModule.exe)執行。

(2)程式執行所需之測試資料(例如：明文檔案)，可以使用data資料夾下的檔案或自備檔案。

(3)提供以下檢測功能：數位簽章Sign與驗證簽章Verify、非對稱式加解密Encrypt Decrypt、對稱式加解密Encrypt&Decrypt、雜湊函式Hash。清除為清除運算結果欄位資料。明文、密文或簽體檔案請使用開啟檔案選擇。

(4)執行上述功能時會將一連串呼叫到的函式名稱和執行結果列出，顯示於運算結果欄位中。若該函式的回傳值為0，則表示功能正常。若有錯誤，則會回傳非0的錯誤代碼。

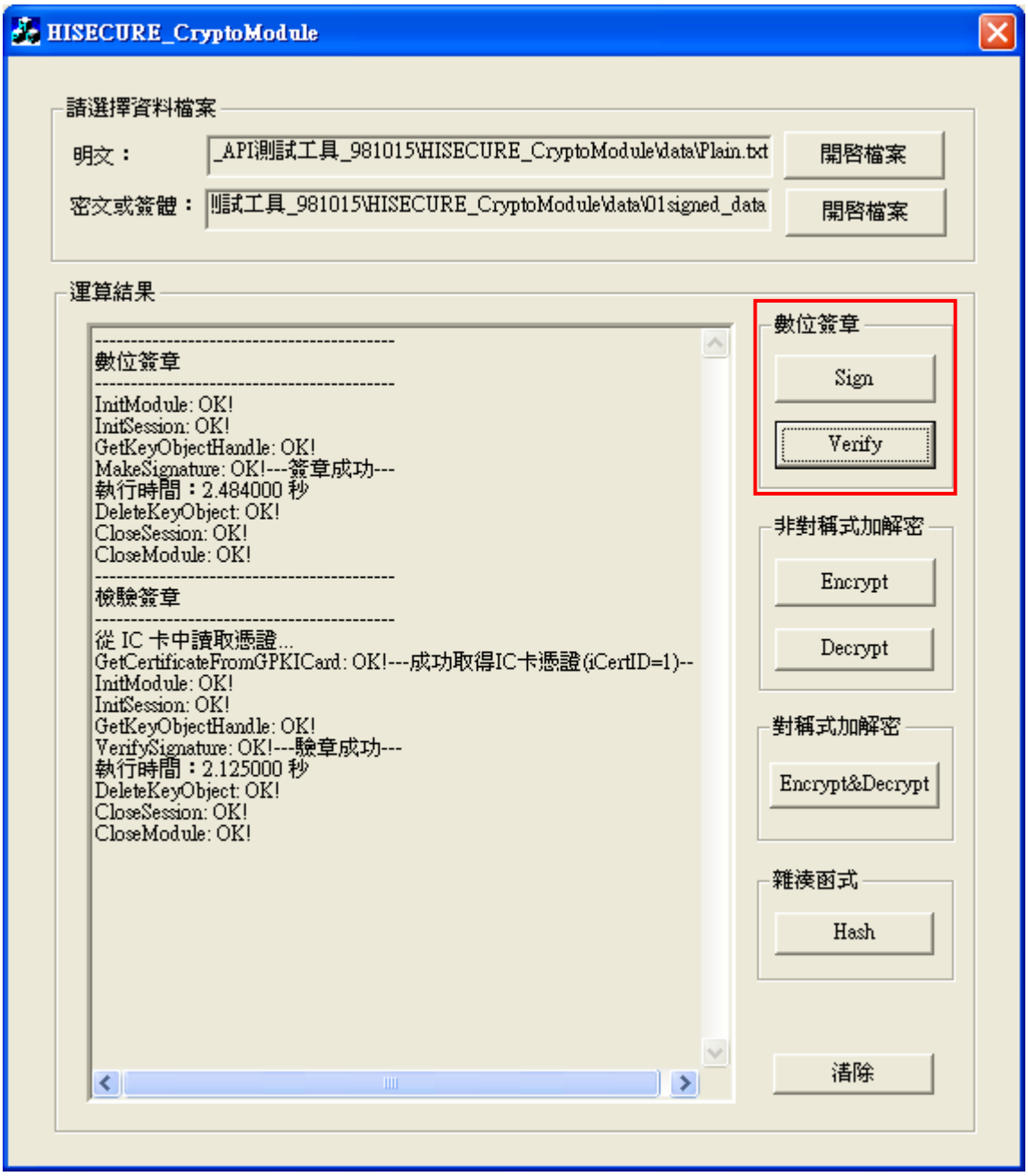
(5)數位簽章Sign與驗證簽章Verify

功能說明：

i. 製作數位簽章時，將使用IC卡內之簽章用私密金鑰對所選取之檔案進行製作數位簽章的動作。請選擇明文檔案後，按下Sign，輸入正確PinCode，簽章完成。接著將出現另存新檔對話方塊，預設儲存檔案為“01signed_data”，此數位簽章檔案名稱可自行修改。

ii. 驗證數位簽章時，將使用IC卡內之簽章用憑證之公開金鑰對所選取之檔案進行簽章驗證的動作。請選擇明文檔案和簽體檔案(例如：上述簽章完成產生之“01signed_data”)後，按下Verify，驗章完成，驗章結果將顯示於運算結果欄位。

執行畫面：



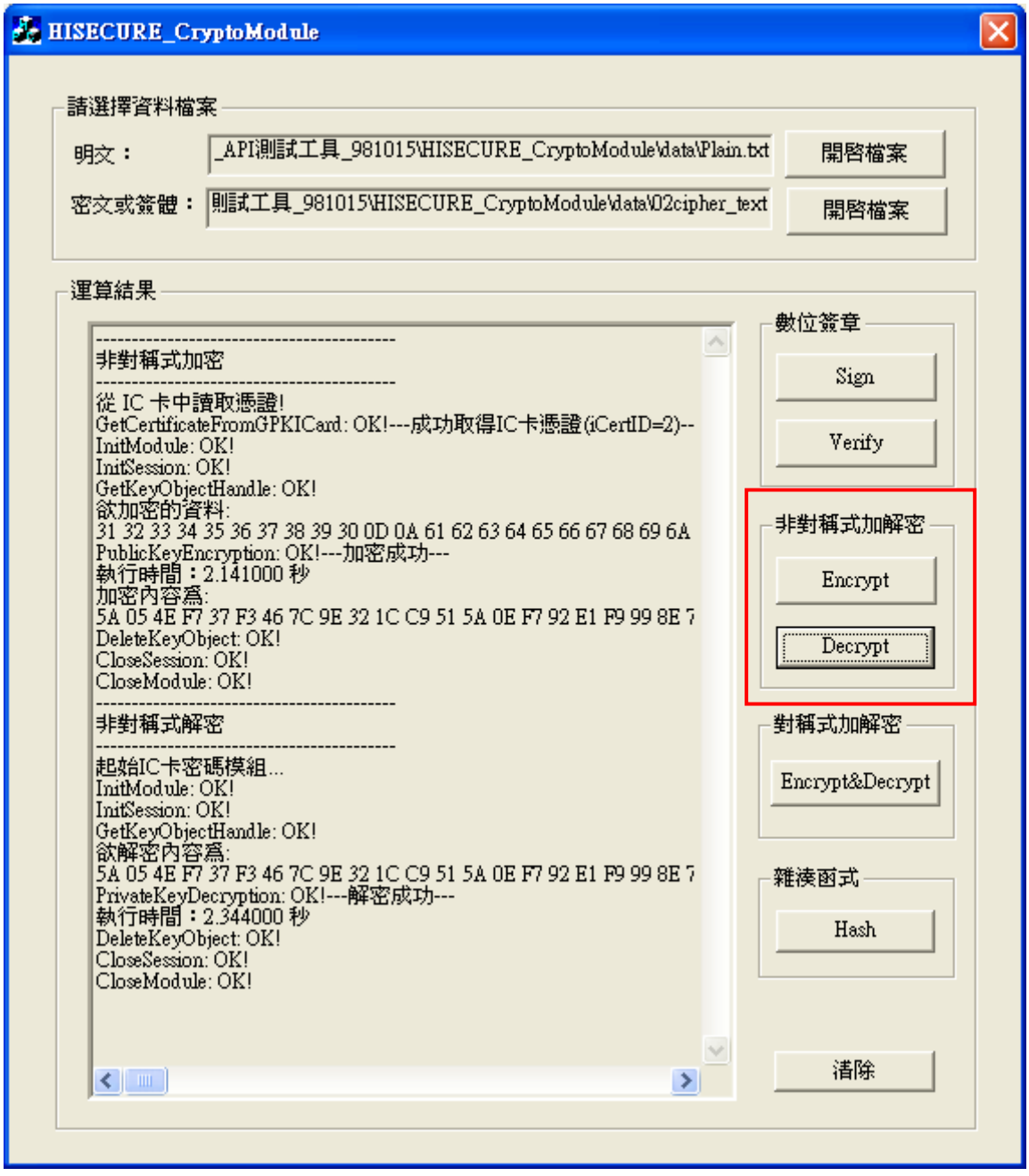
(6)非對稱式加解密 Encrypt Decrypt

功能說明：

i. 加密時，將使用IC卡內之加密用憑證之公開金鑰對所選取之檔案執行RSA加密動作。請選擇明文檔案後，按下Encrypt，非對稱式加密完成，密文產生。接著將出現另存新檔對話方塊，預設儲存檔案為“02cipher_text”，此密文檔案名稱可自行修改。

ii. 解密時，將使用IC卡內之解密用私密金鑰對所選取之檔案執行RSA解密動作。請選擇明文檔案和密文檔案(例如：上述加密完成產生之“02cipher_text”)後，按下Decrypt，非對稱式解密完成，解密結果將顯示於運算結果欄位。接著將出現另存新檔對話方塊，預設儲存檔案為“03decrypt_to_plain.txt”，此檔案名稱可自行修改。此檔案內容應與加密前之明文內容相同。

執行畫面：



(7)對稱式加解密 Encrypt&Decrypt

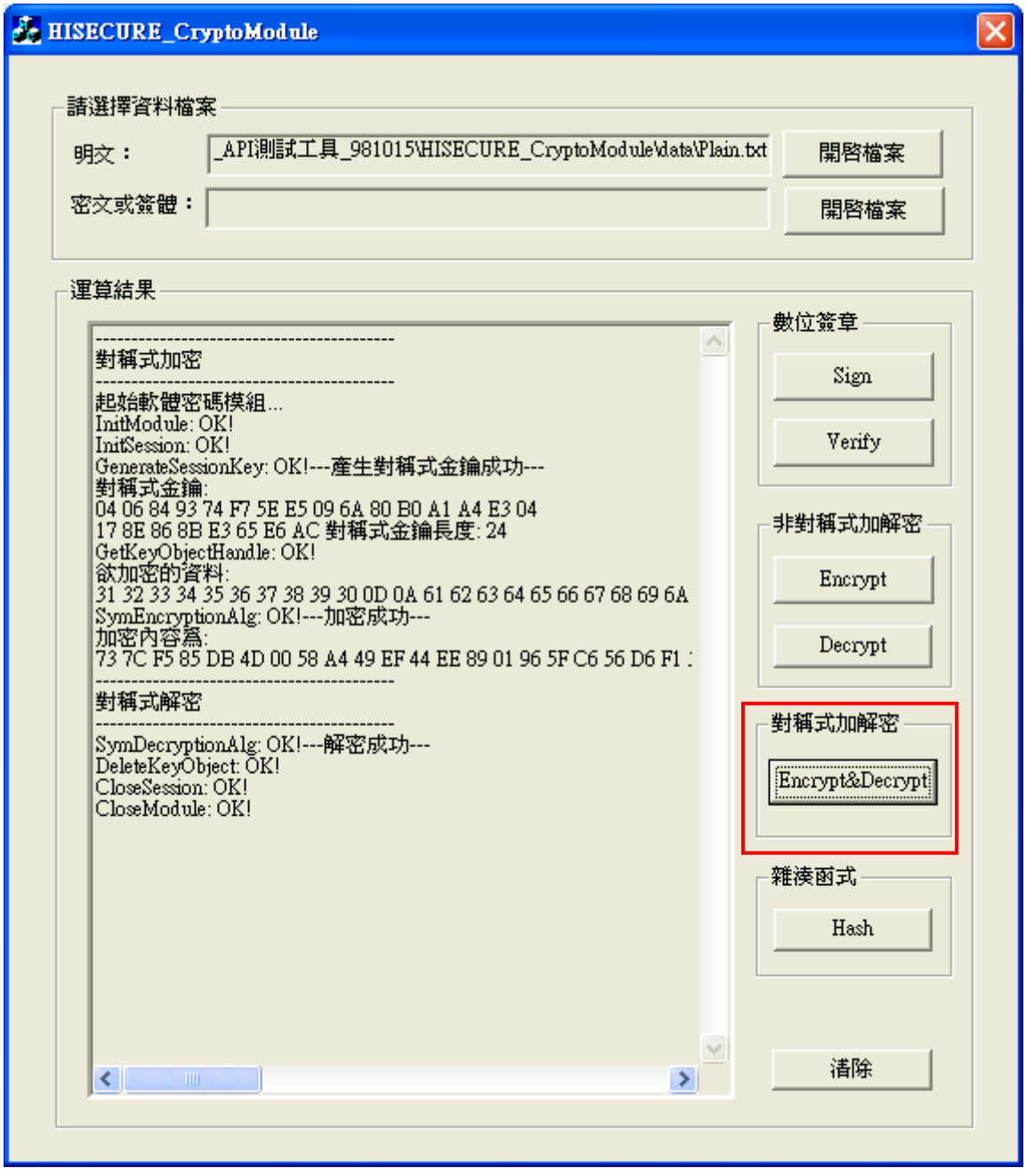
功能說明：

i. 無需使用IC卡。

ii. 加密時，程式自動產生對稱式金鑰對所選取之檔案執行AES加密動作。請選擇明文檔案後，按下Encrypt&Decrypt，對稱式加密完成。接著將出現另存新檔對話方塊，預設儲存檔案為“04sym_enc_cipher_text”，此密文檔案名稱可自行修改。

iii. 解密時，程式直接使用同一把對稱式金鑰對上述之密文內容執行AES解密動作。對稱式解密完成，解密結果將顯示於運算結果欄位。接著將出現另存新檔對話方塊，預設儲存檔案為“05sym_decrypt_to_plain.txt”，此檔案名稱可自行修改。此檔案內容應與加密前之明文內容相同。

執行畫面：



(8)雜湊函式 Hash

功能說明：

i. 無需使用IC卡。

ii. 請選擇明文檔案後，按下Hash，程式將對所選取之檔案執行SHA1雜湊函數演算法。雜湊運算完成，接著將出現另存新檔對話方塊，預設儲存檔案為“06hashvalue.txt”，此檔案名稱可自行修改。此檔案內容即為雜湊值。

執行畫面：

3.2 憑證及CRL檢測程式

(1)毋需安裝，請解壓縮後，直接點選exe檔(HISECURE_CERTPARSING.exe)執行。

(2)程式執行所需之測試資料(例如：憑證、CRL檔案)，可以使用data資料夾下的檔案或自備檔案。

(3)提供以下檢測功能：

憑證解析、取得CRL資料、驗證CRL簽章、憑證廢止狀況查詢(CRL)。

清除為清除運算結果欄位資料。憑證、CRL檔案請使用開啟檔案選擇。

(4)執行上述功能時會將一連串呼叫到的函式名稱和執行結果列出，顯示於運算結果欄位中。若該函式的回傳值為0，則表示功能正常。若有錯誤，則會回傳非0的錯誤代碼。

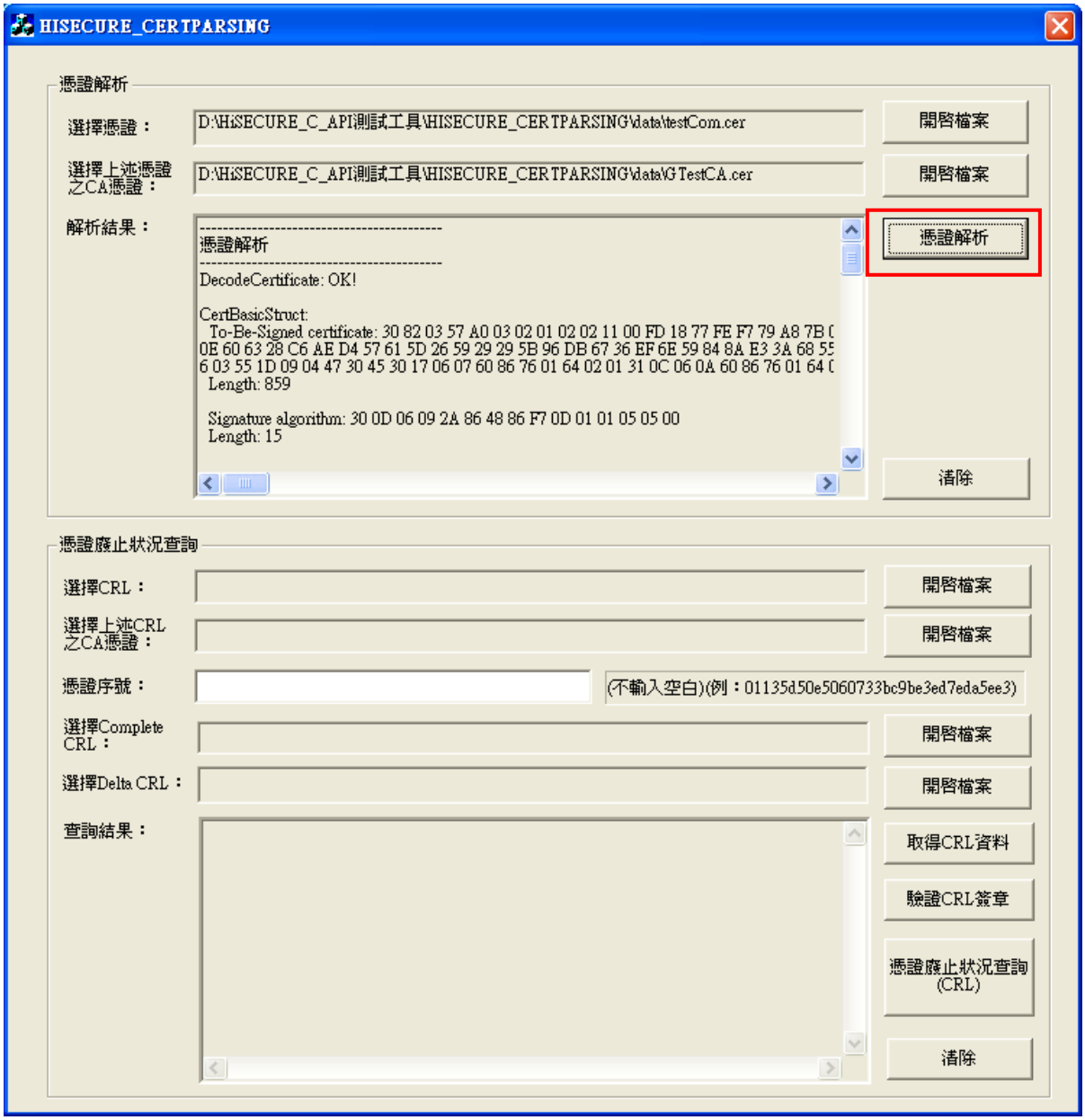
(5)憑證解析

功能說明：

i. 請選擇憑證檔案和簽發該憑證之CA憑證檔案，按下憑證解析。

ii. 當憑證解析完成，解析資訊詳見解析結果欄位。

執行畫面：



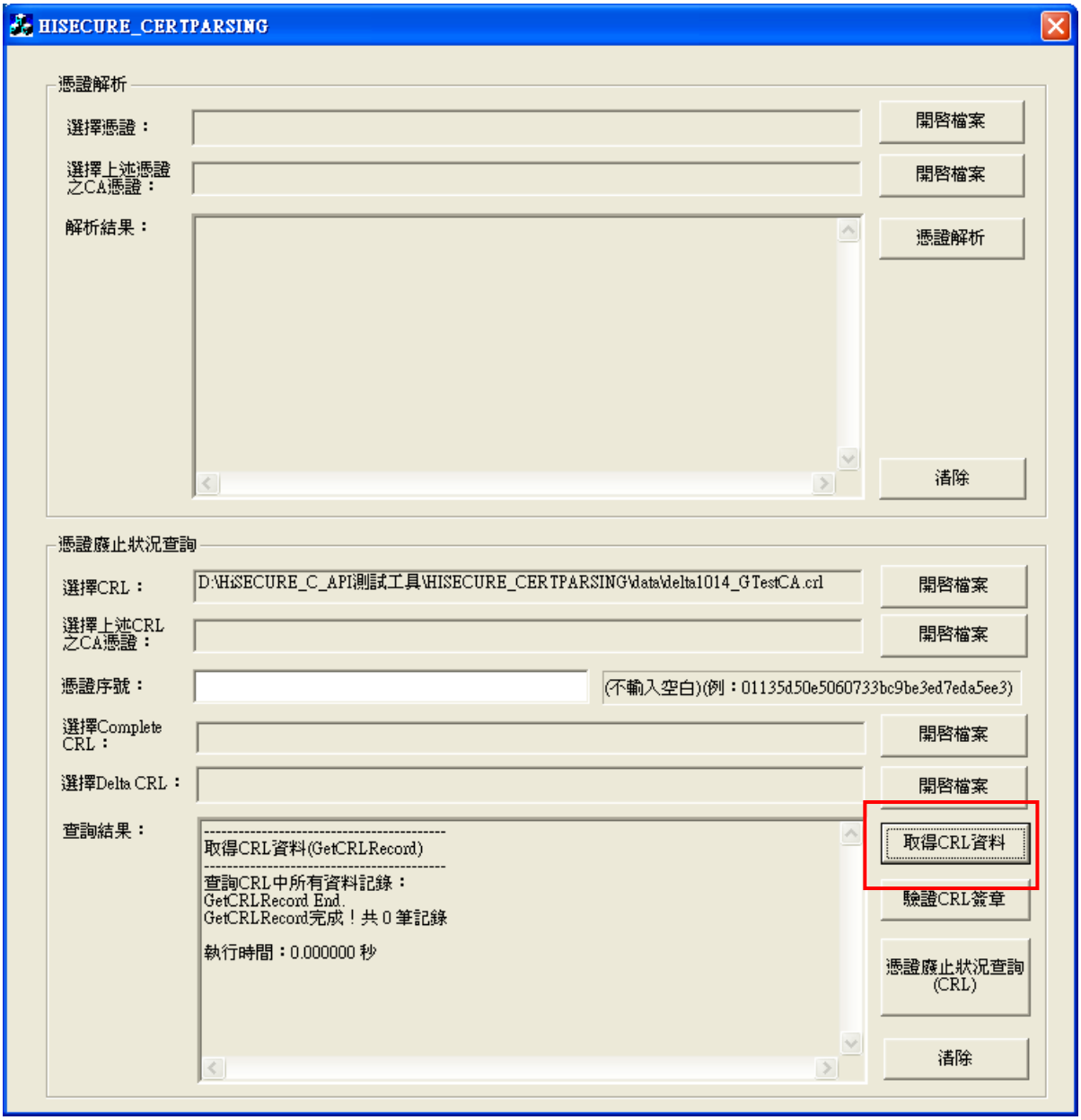
(6)取得CRL資料

功能說明：

i.請選擇CRL檔案，按下取得CRL資料，此動作可能需花費您一些時間(視CRL資料筆數而定)。

ii.當取得CRL資料完成，將於查詢結果欄位顯示每筆CRL資料，以及共有幾筆資料等資訊。

執行畫面：



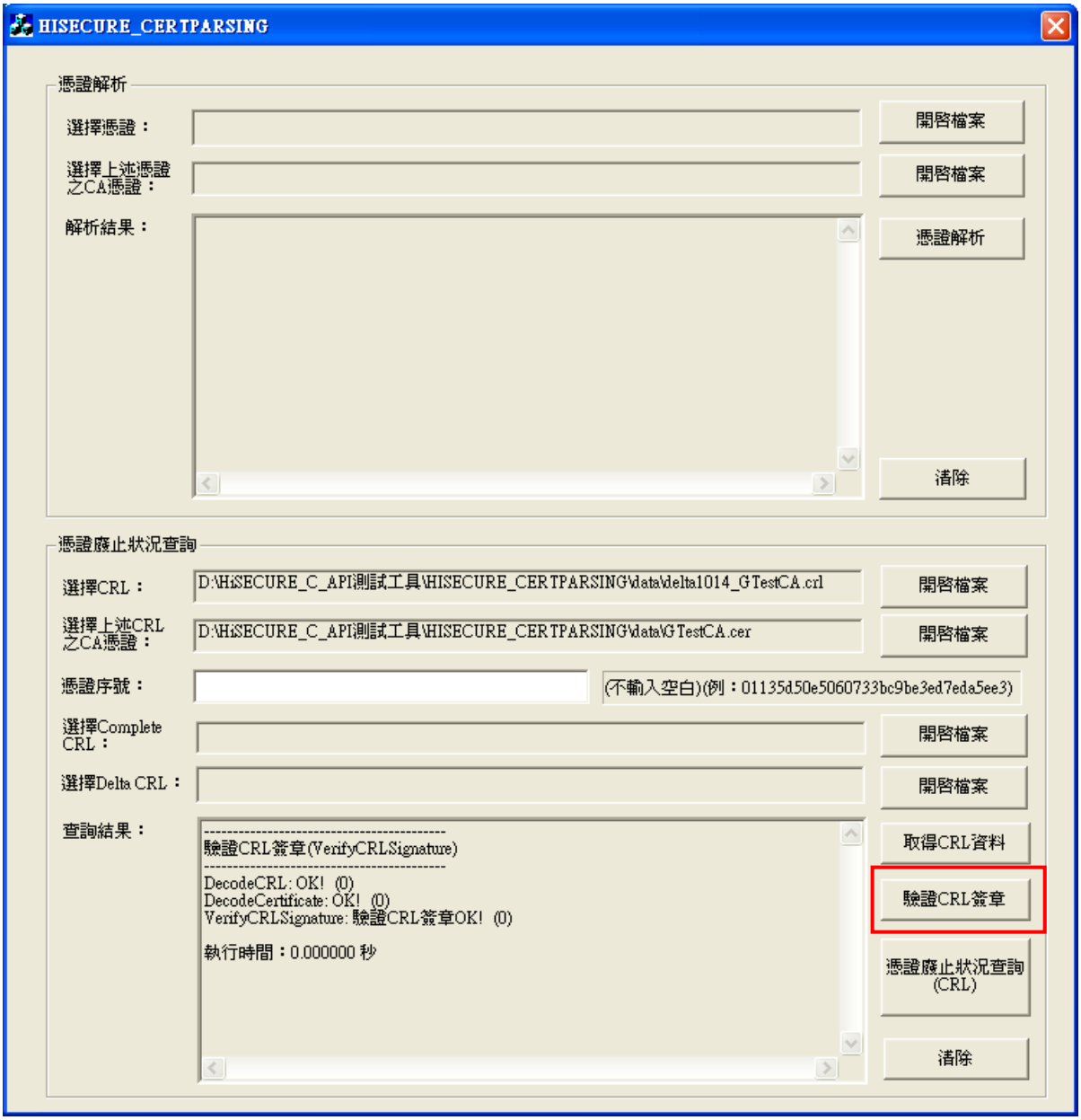
(7)驗證CRL簽章

功能說明：

i. 請選擇CRL檔案和簽發該CRL之CA憑證檔案，按下驗證CRL簽章。

ii. 當驗證CRL簽章完成，驗證結果將於查詢結果欄位顯示。

執行畫面：



(8)憑證廢止狀況查詢(CRL)

功能說明：

i.請輸入欲查詢是否廢止之憑證序號(不輸入空白符號)，並選擇Complete CRL檔案和Delta CRL檔案，按下憑証廢止狀況查詢(CRL)，此動作可能需花費您一些時間(視CRL資料筆數而定)。

ii.當憑證廢止狀況查詢(CRL)完成，查詢結果將於查詢結果欄位顯示。

執行畫面：