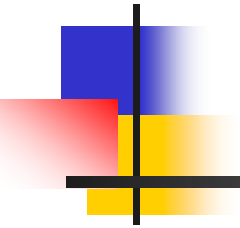

資料庫加密工具

Fred Tseng
玉山科技
02-77128295
http://www.asiapeak.com

產品功能

- 加密資料欄位,以防機密資料被盜取
  - Encrypting data at rest
- 提供加解密演算法API供程式使用
  - 非對稱式加解密:RSA,DSA
  - 對稱式加解密:DES,DES3,AES,RC4
  - Hash Functions: MD5, SHA-1,SHA-256/512
- 應用程式可呼叫這些API, 加上必要之Trigger/Stored Procedure, 來達到欄位資料加密的目標
  - 資料存入DB是自動加密的
  - 資料取出時自動解密
  - 需要修改原有程式碼, 通常改成操作View

產品安裝

- License Activation
- 產品安裝後
  - 增加許多 extended stored procedures (API) ➔xp_****
  - XPCrypt GUI 工具 ➔ 協助第一次整批加密與金鑰管理
  - 文件與API範例

運作原理（使用GUI）一

- 產生金鑰(key)與設定金鑰密碼
- 加密欄位時(如authors.au_lname)
  - 在原table (authors) 增加一加密欄位(enc_au_lname), 將原欄位資料用key加密後放到此加密欄位
  - 產生此table的View (authors.View), 其內容為原table欄位, 除了用加密欄位取代原來欄位外.
  - 在此View上增加Trigger程式(for insert)
- 再將原欄位(au_lname)刪除
- 金鑰/密碼/加密欄位資訊放在DB裡

運作原理（使用GUI）二

- 要存取加密資料時
  - 將程式改為對View操作
  - 必須給key及密碼 (exec master..xp_crypt_set_var ‘keyname',‘password‘)
  - 相關trigger會被執行
  - 原table裡就只有加密過的欄位
- Note: 因 trigger for update 使用狀況不一，須程式設計人員自行撰寫

運作原理(不使用GUI工具)

- 金鑰產生與管理要自己來
- View, Trigger, Subroutine都要自己撰寫與產生
- 可將Key(被保護過)放在檔案/Registry裡
- 請詳讀Tutorial – Advanced Technique

注意事項

- 修改程式
- 效能問題
- 注意金鑰密碼寫死在程式裡的安全考量
  - 例如： exec master..xp_crypt_set_var ‘keyname',‘password‘
  - 可使用Hash 驗證而非比對Password
  - 或用SQLShield將此Store Procedure加密
- 搜尋條件資料若使用加密欄位時的效率考量與作法
  - 將搜尋條件加密後再比較
- 測試再測試（尤其是SQL Statement複雜的AP）