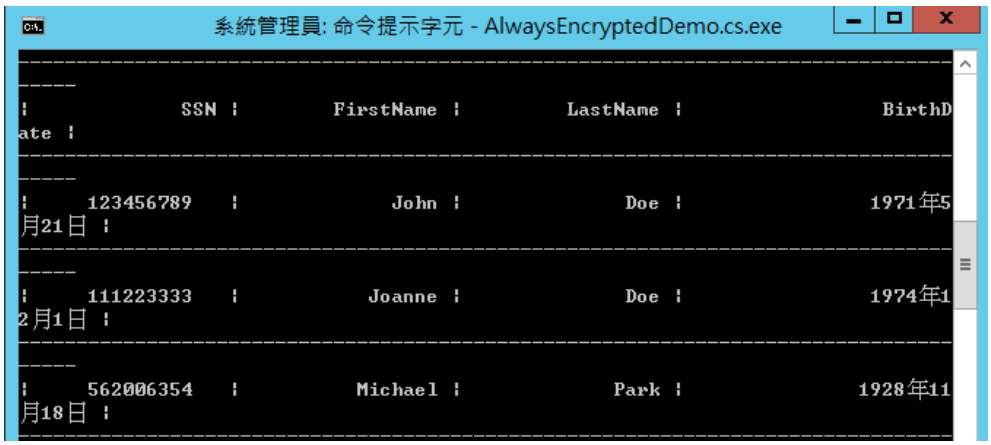
PAYSECURE TECHNOLOGY CO.,LTD. 聯宏科技

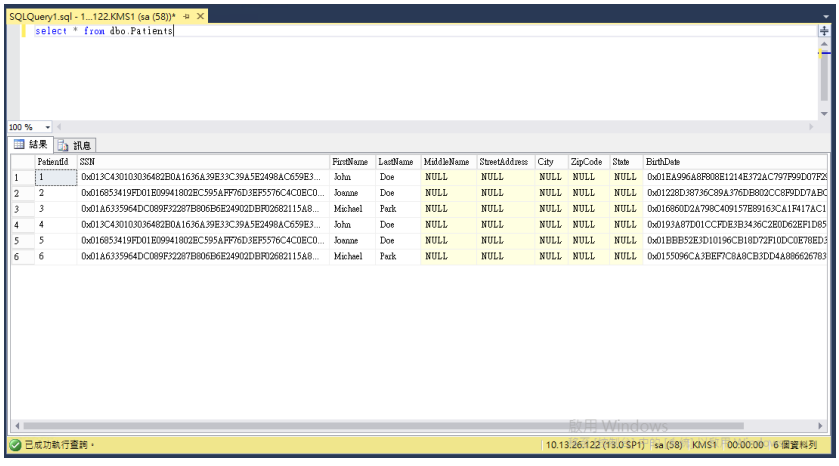
gemalto security to be free

Microsoft SQL 2016 Server
欄位加密安全解決方案

微軟在 SQL Server 2016 新增「Always Encrypted」欄位式加密模組功能，資料在應用程式端傳送到 SQL Server 時，經由擴充 ADO.NET 函式庫將資料加密，主要用來防止開發人員或未經授權的使用者，有意或無意去窺探不該看的資料。而欄位主金鑰(CMK)存放於 Gemalto SafeNet Network HSM 集中管理，就算 AP 遭 Clone 或資料庫被竊取，都無法取得 CMK 解密欄位資料，只有被合法授權存取 HSM 的 AP 應用程式才可存取並解密欄位資料，達到欄位加密防護。



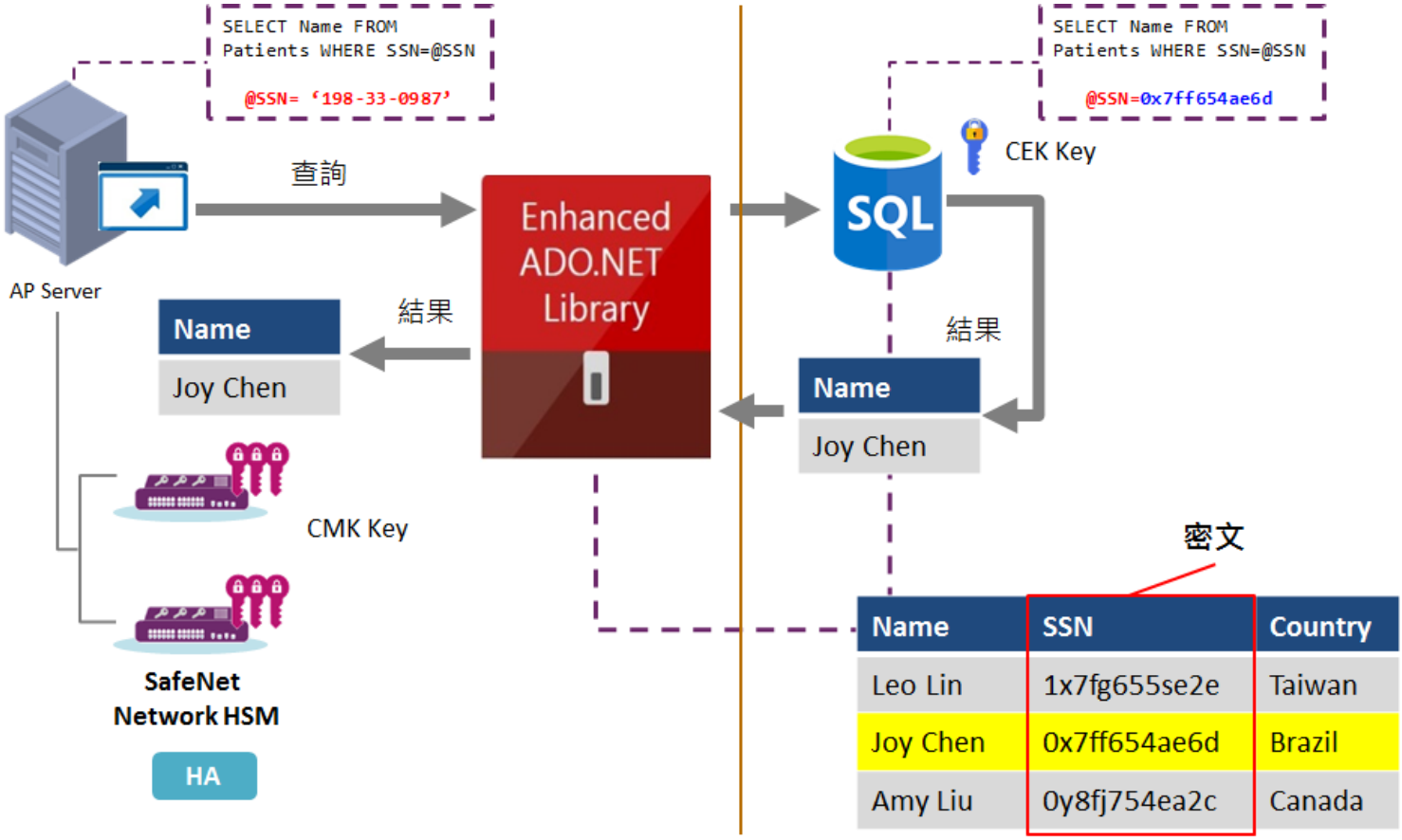
▲ 受信任 AP 程式才可 Select 明文資料



▲ 機敏資料被 HSM 金鑰加密保護

解決方案優點

- 欄位主金鑰(CMK)保存於 HSM 中。
- HSM 通過 FIPS 140-2 Level 3 認證可保護主金鑰。
- 只有受信任的 AP 才可存取 HSM 金鑰並解密資料。
- 支援動態加密(RANDOMIZED)、固定加密(DETERMINISTIC)。
- 支援 MS SQL 2016 欄位加密(Always Encrypted)。
- 插入資料 (Insert Data)時執行加密。
- HSM 連線白名單授權信任 AP 存取金鑰 (NTLS 連線)。



欄位加密 (Always Encrypted)

Always Encrypted 主要使用兩種金鑰做到欄位加密，當資料庫資料的加解密會在 AP 端的 ADO.NET 應用程式執行，資料庫只負責提供被加密的 CEK 以及存取 AP 前端加密後的資料。AP 加密資料時會使用 CEK 對資料進行加密，這把 CEK 會在實際交易前從資料庫取回，且 CEK 是被加密的狀態；接著 AP 端從 Gemalto SafeNet Network HSM 中取得 CMK 並解開 CEK，進行資料的寫入加密、讀取解密。

- 如竊取整個資料庫，**無法取得 CMK 金鑰**來解密 CEK；
- 如 Clone 整個 AP 應用程式伺服器，**少了 HSM 連線白名單授權**，也無法取得 CMK 金鑰。

[支援條件]

使用 Always Encrypted 功能需配合以下條件：

- 資料庫版本需為 MS SQL 2016 SP1
- 必須使用 .NET Framework 4.6 以上版本
- AP 程式連線字串必須加入 Column Encryption Setting=Enabled

PAYSECURE TECHNOLOGY CO.,LTD.
聯 宏 科 技
114台北市內湖區內湖路一段91巷17號10樓之1
10F. -1, No.17, Lane 91, Sec.1, Neihu Rd., Neihu District, Taipei City 114, Taiwan
TEL +886-2-2657-1187 FAX +886-2-2657-1205

Microsoft