MSSQL EKM 延伸金鑰管理

如何保障金鑰安全 提升資安強度？

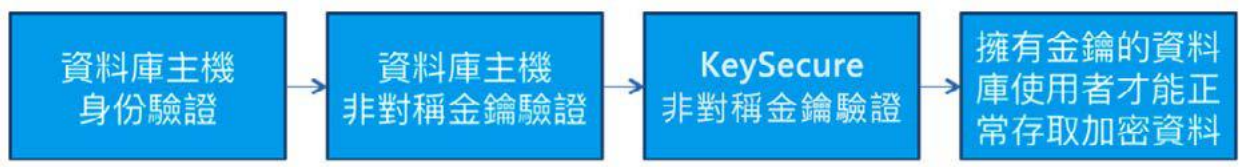
撰稿: 叡揚資訊 資訊安全事業處

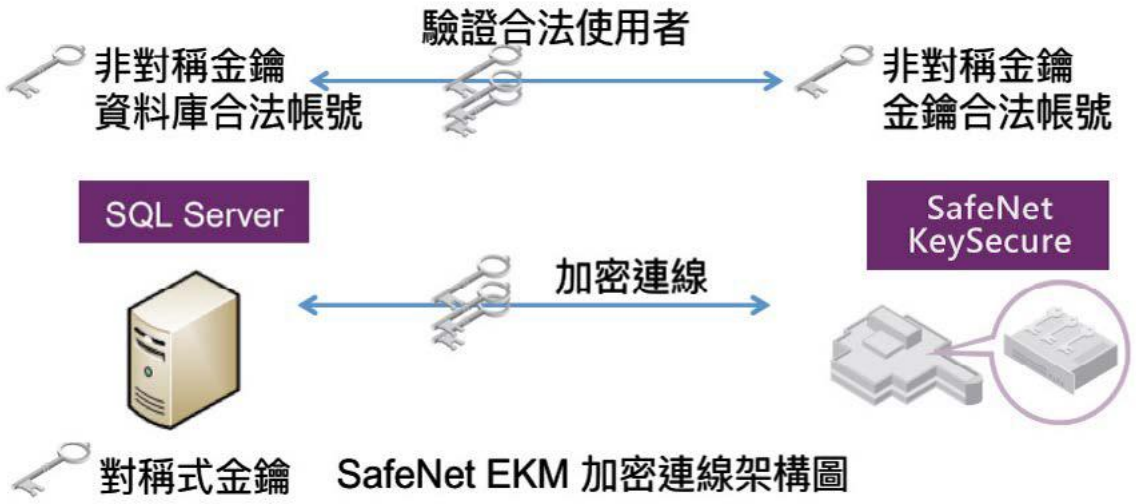
企業常見的資料庫環境安全考量諸如資料庫存放地點是否安全、是否僅限合法使用者存取資料庫、備份機制及保存是否夠安全、備份檔是否加密等，可以透過金鑰管理解決方案，協助企業保護可能導致業務風險的機敏資料 - 不論是信用卡號、個人身分證號碼或是其他任何機敏資訊。對於 MSSQL EKM 更提供了延伸金鑰管理解決方案，將資料庫重要金鑰存放於 Gemalto- SafeNet 經過安全驗證的設備，將可提升資料庫安全等級，並能有效阻絕非法使用者存取資料庫。

SafeNet 企業金鑰管理 KeySecure 提供使用者對應用系統、資料庫、檔案及虛擬主機加解密之功能，可細緻的整合集中金鑰管理的功能，從而提供點對點、簡易且高成本效率的加密解決方案。透過其在網路伺服器、應用伺服器、資料庫伺服器、檔案系統與分散式環境下對機敏資訊執行加密功能。

常見的資料庫安全考量及配套作法

資料庫環境安全性考量	SafeNet MSSQL EKM 如何滿足資料庫延伸金鑰管理
Q: 資料庫資料存放的地點安全嗎？ 人員進出是否有管制？	A: 資料庫合法使用者身份驗證 (KeySecure & SQL Server)
Q: 如何確保只有合法使用者可以存取資料庫主機？誰是正常使用者？	A: 非對稱式金鑰 (KeySecure & SQL Server) 驗證
Q: 資料庫的備份機制及存放位置安全嗎？ 備份檔有無加密？	A: 資料庫加密功能正常啟用
Q: 資料庫的實體檔案容易被複製？	A: 資料庫對稱式金鑰可使用並查閱所加密資料





■ SafeNet MSSQL EKM 延伸金鑰支援演算法全球最大軟體安全顧問公司
RC4、DES、Triple DES、Triple DES 3、AES、RSA

■ SafeNet MSSQL EKM 延伸金鑰支援資料庫版本及作業系統版本

- MSSQL Server 2008 and MSSQL Server 2008 R2：
  - Windows Server 2003 32-bit, 64-bit
  - Windows Server 2008 32-bit SP2, 64-bit SP2
  - Windows Server 2008 R2 64-bit
  - Windows Server 2012 64-bit
- MSSQL Server 2012：
  - Windows Server 2008 32-bit SP2, 64-bit SP2
  - Windows Server 2008 R2 64-bit
  - Windows Server 2012 64-bit

■ SafeNet 資料加密解決方案用途

解決方案	用途
KeySecure 企業金鑰管理	功能：集中管理合法使用者金鑰存取權限，包含建立、修改、刪除、備份。 設計目的：為了整個企業的加密資料提供集中化的金鑰與政策管理，並具備一些先進功能，例如 key rotation 與版本控制，確保安全與簡易使用性。

更多最新資安電子報：請瀏覽 http://www.gss.com.tw/index.php/focus/security