資料保護：簡化金鑰的替換機制

安全的金鑰管理是種有效集中保護資料的策略。本文將說明簡化金鑰管理最佳實務的關鍵技術「金鑰版本」。

集中金鑰管理：安全、可靠和可稽核

組織內的整體資料保護方案，要安全地、高效地管理加密金鑰，機制往往是最艱鉅的任務。金鑰管理提供了一個架構，管理金鑰的建立、存儲、分發、替換、歸檔和撤銷的機制，以保護敏感資料是安全、可靠和可稽核。金鑰管理的一個重要的步驟是金鑰替換。經由金鑰定期替換使用，可以將組織長時間繼續使用加密金鑰的風險降到最低。

強制管理員重新輸入所有資料再加密或是使用舊的金鑰在應用程序建立邏輯關聯進行使用金鑰加密成密文，這個過程可以是非常地繁瑣難處理。這兩個選項都沒有特別吸引人，因為重新輸入資料需要幾天，可能需要系統離線才能進行，及現成許多的應用軟體都無法修改與邏輯相關需要的金鑰與加密成密文。

SafeNet的DataSecure解決方案，提供簡單機制來解決這些問題。本文將討論在金鑰替換過程中的關鍵細節，並解釋如何使用金鑰版本的技術，可以簡化整個金鑰替換的程序。

什麼是金鑰替換？

嚴格地定義，金鑰替換的要點是你停止使用一把鑰匙並且開始使用另一把鑰匙。定期執行金鑰替換是安全最佳實踐必要的部分，因此被支付信用狀業數據安全性標準(PCI DSS)所規範。按定期計畫的基礎去執行金鑰替換，對於因應可能入侵的破壞是必要的。雖然金鑰替換和重新輸入金鑰資料是完全單獨的功能，很多組織將這兩個概念合併為一。先使用舊的金鑰將資料加密然後再使用新的金鑰再重新加密它的全部數據。

在替換金鑰時，大多數組織比較不喜歡重新輸入建立新的金鑰資料，在某些狀況下重新建立金鑰資料是無法避免的，例如金鑰已經遭到破壞或是應用系統無法支援同時使用多個金鑰。

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

金鑰替換面臨的挑戰

當組織明確地要遵循PCI法規的規定，導入金鑰替換的最佳實務的作法，會面臨哪些挑戰。

對系統營運時間的影響

大多數情況下，為了維持組織正常的商業運作，針對高度敏感的資料進行加密是很關鍵的因素。因此期望在進行金鑰替換的整個過程當中，存儲系統和應用系統間還是可以繼續連線進行敏感資料的交換。如果您現在金鑰替換過程需要系統採取離線模式作業，將會迫使您的營運業務的停頓和造成潛在的收入損失，那麼你應該考慮，可以在連線模式進行金鑰替換的方案，不會去影響到業務的正常運行時間。

使用多個活躍金鑰存在的問題

組織將要重新輸入他們的資料或修改他們的應用系統程序以允許使用多個金鑰。為了維護多個活躍金鑰，你必須結合金鑰與密文，否則，你將不知道哪個金鑰去於解密文。有些客戶會建立金鑰索引來追蹤哪個金鑰用來加密那段文字。每次建立一個新的金鑰，您還必須更新金鑰的搜尋表，並修改您的應用程序，開始使用新的金鑰進行資料加密和新插入的金鑰的索引表更新。(如參考圖一)

Customer Table

First Name	Last Name	Account Number	Key Index
Ron	Crews	1101111011001010101	1
Hy	Lee	0110111000101001010	1
Mary	Christie	0101101001111010101	2
Krishna	Patel	1111011101100100100	2

Key Lookup

Key Index	Key Name
1	Key 1
2	Key 2

圖一：Data Structure Required to Maintain Multiple Active Keys

金鑰替換需要改變您的資料結構及要更新您的應用系統撰寫方式，以下是一個 Java 程式碼範例,展示如何進行金鑰替換的程序。(如參考圖二)

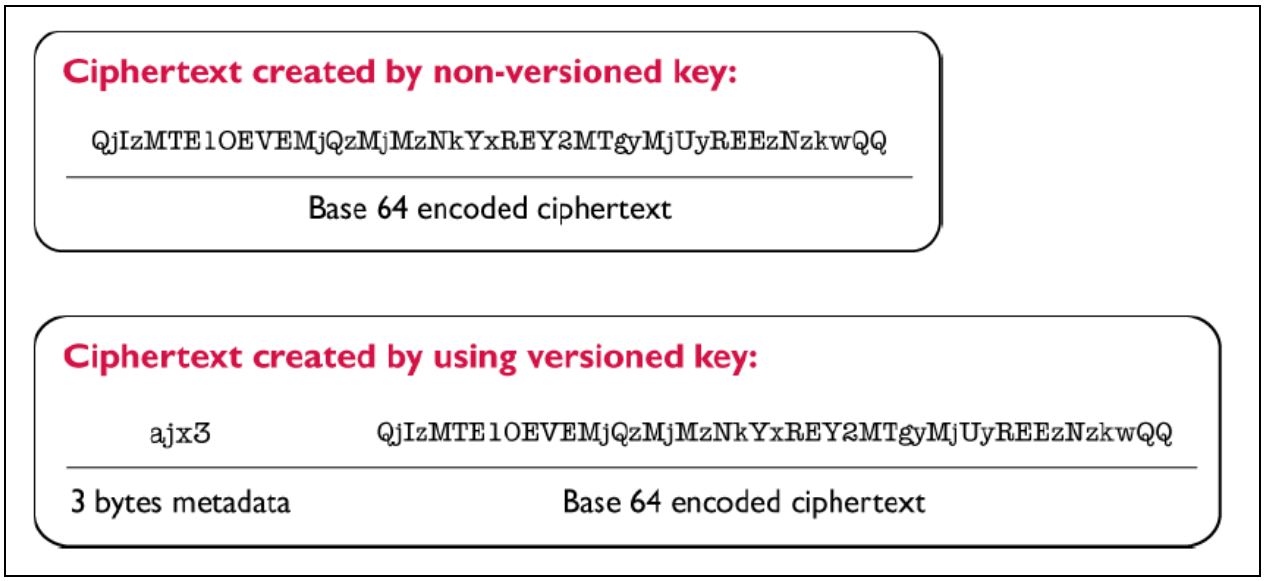
```
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding", "SafeNetProvider");
SecretKey key = NAEKey.getSecretKey("KEY1", session);
cipher.init(Cipher.ENCRYPT_MODE, key, new IvParameterSpec(iv));
byte[ ] ciphertext = cipher.doFinal("Hello World!".getBytes());

Update the key name in line 2 above:

SecretKey key = NAEKey.getSecretKey("KEY2", session);
```

圖二：Code Required to Enable Multiple Active Keys

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

簡化金鑰的替換

SafeNet的DataSecure解決方案可減緩金鑰替換時或建立嚴密規劃時的密文和金鑰間的對應關聯，亦即需要重新輸入資料的問題。這是通過提供支援多版本的金鑰技術。一個版本的金鑰，本質上是一個獨特的金鑰數組可以被引用使用相同的金鑰的名稱。當資料使用版本的金鑰加密，DataSecure 服務主機，會插入3個位元組的中介資料在密文的前面。這使得服務主機可以確定是使用哪個版本的金鑰是用於建立密文的加密。這反過來，允許你發送一個請求到服務主機，解密沒有指定特定版本的關鍵。考慮圖三中的例子。



圖三：Difference between Ciphertext created by non-versioned and versioned key

使用金鑰版本技術，您只要簡單建立一個金鑰版本使用的金鑰，不需要修改任何的程式碼與更新金鑰的索引。

使用 DataSecure 進行金鑰管理

組織要長期地保護敏感的資料數列，可能是一項很繁重的工作。有一個集中的管理工具，如 SafeNet 的 DataSecure 管理控制台所提供的功能，使正確的金鑰和主要版本金鑰的最佳實務做法，將可以減少金鑰替換所要耗費的時間和精力。DataSecure 定義的難易程度，管理員可以配置和部署金鑰管理，以符合企業的需求和安全的政策，建構系統持續營運的基礎。這有很重要的後續影響，不僅涉及到所需要的資源配置系統最初，而且更重要的是，後續持續進行運營和維護的費用。

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

彙總

現在你明白使用金鑰版本技術來簡化金鑰替換的工作所帶來的好處，讓你可以專注於重要的工作，保護組織的敏感數據的安全。通過利用來自SafeNet公司的資料保護解決方案DataSecure，讓您有獨特的能力，可以集中管理金鑰，使用的金鑰版本技術，以消除金鑰替換工作的麻煩，並報告符合法規的任務，如符合 PCI 規範。

下一代的資料保護方案，主動積極的組織利用集中管理金鑰和政策管理，簡化符合法規的規定，確保生產力，並提供最高的安全性衡量機制，保護組織的最敏感的資料和知識產權。這包括結構化資料，常駐在各種資料庫，應用程序和主機，或非結構化的資料，在資料中心的檔案伺服器，以及完整的磁盤保護終端設備，如筆記本電腦，個人電腦，移動設備或移動媒體，或更精細的保護特定的文件。無論您的資料保護需求為何，SafeNet的DataSecure產品系列能夠滿足現今下一代的資料保護方案的安全需要。

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787