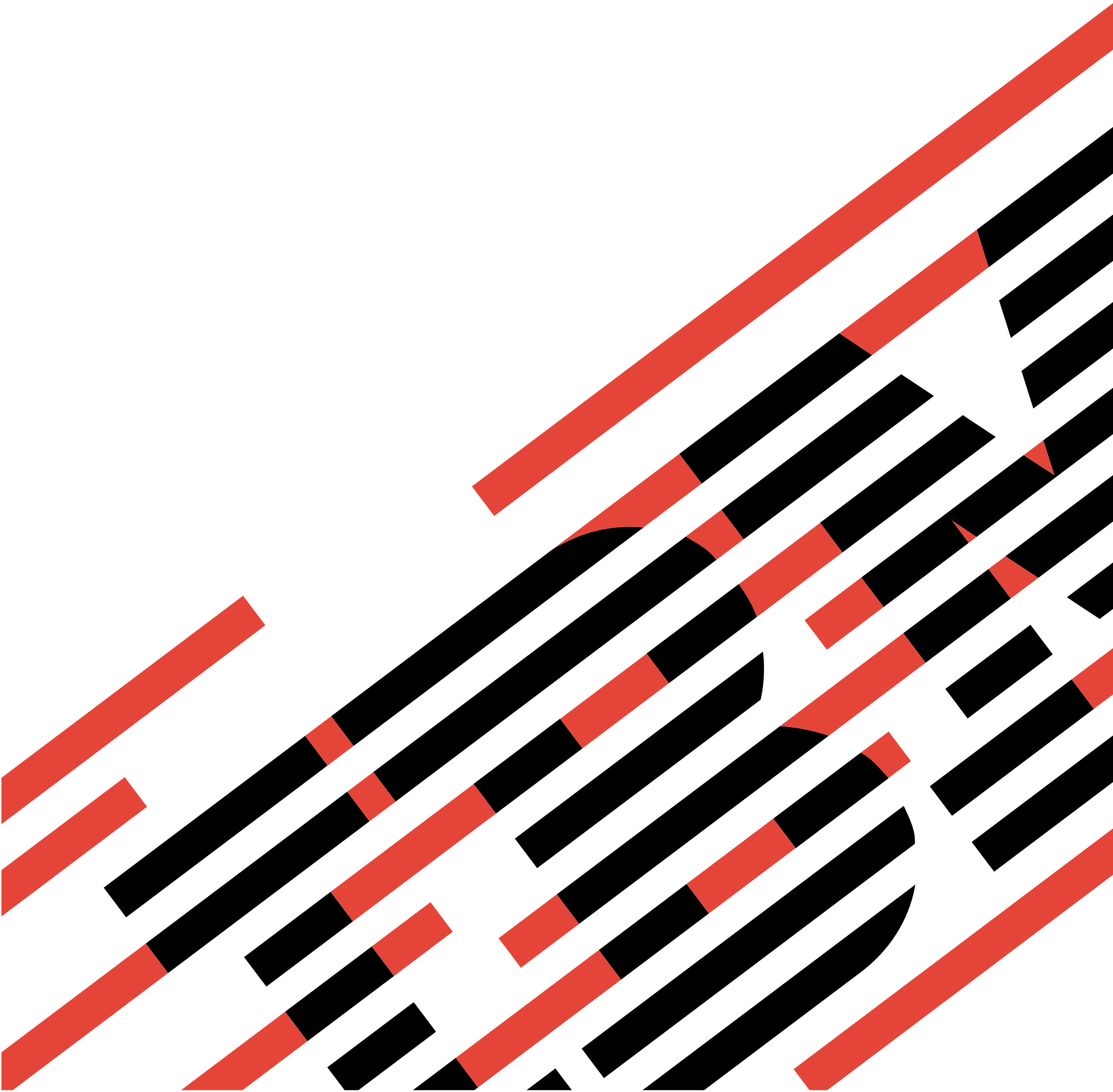
IBM

eserver

iSeries

加密硬體



IBM

@server

iSeries

加密硬體

目錄

第 1 篇 2058 加密加速器

第 1 章 列印此主題

您可檢視或下載這些主題的 PDF 版本：

- 加密硬體 (大約 756 KB 或 292 頁) 包含所有關於 V5R2 上 iSeries™ 伺服器所支援之 IBM® 加密硬體的資訊。
- 2058 加密加速器 (大約 79 KB 或 24 頁) 包含關於 V5R2 上 iSeries 伺服器所支援之「2058 加密加速器」硬體的資訊。

儲存 PDF 檔案

若要在您的工作站上儲存 PDF 以供檢視或列印：

1. 在您的瀏覽器中以滑鼠右鍵按一下 PDF。
2. 按一下**另存目標**。
3. 導覽到您想要儲存 PDF 之處。
4. 按一下**儲存**。

下載 Adobe Acrobat Reader

如果您需要 Adobe Acrobat Reader 來檢視或列印這些 PDF，可從 Adobe 網站 (www.adobe.com/products/acrobat/readstep.html) 下載複本。

第 2 章 V5R2 的新增功能

若您正在尋找關於最新加密硬體之最新資訊，及 iSeries 伺服器之現有加密硬體選項的新增特性，那麼您是來對地方了。

新的加密硬體：IBM 2058 電子商業加密加速器

除了「4758 加密輔助處理器」外，也可用 IBM 2058 電子商業加密加速器 (「硬體特性」碼 4805，此後稱爲「2058 加密加速器」)。透過重新遞送私密金鑰的處理程序 (使它不由系統處理器處理) 的設計，來增進 iSeries 的效能，此硬體選項爲處理高容量 SSL (Secure Sockets Layer) 交易的 iSeries 施行之極好選擇。雖然「2058 加密加速器」是增強 iSeries 伺服器 SSL 效能的極好選擇，並且容易安裝及初始化，但是它並未提供「4758 輔助處理器」所提供的大量配置選項。

請參閱 iSeries 「2058 加密加速器」的相關資訊，此將協助您決定哪一個加密硬體選項爲最佳的 iSeries 伺服器施行。

附加功能：「4758 加密輔助處理器」

「4758 加密輔助處理器」向客戶提供了下列新功能：

- 金融個人識別碼 (PIN) 處理程序：每筆交易唯一金鑰 (UKPT)
- 共同密碼架構 (CCA) 2.4

新的加密硬體實務

爲了向您提供關於如何與 iSeries 伺服器一起使用加密硬體的一些意見，我們已經將下列實務新增至 「iSeries 資訊中心」：

- 加密硬體實務：增強 iSeries SSL 效能

若要尋找此版次中有關新增功能或變更的其它資訊，請參閱使用者備忘錄

。

如何查看新增功能或變更

爲了協助您查看已作過技術變更的地方，此資訊使用：

- 影像標示新增功能或變更資訊開始的地方。
- 影像標示新增功能或變更資訊結束的地方。

第 3 章 概念

加密

加密之於資料保全，不僅是一門技術，也是一種藝術。基本的加密服務必須能夠確保訊息的隱密性、維護訊息的完整性，並鑑別通信各方的身份，以及保證通信方無法否認其曾經傳送過訊息。

您可以利用加密來儲存資訊或與其他方進行通信，並保證未參與的各方無從了解儲存的資訊或通信的內容。加密會將可以理解的文字轉換成無法理解的資料 (密碼文字)。而解密則會將這些無法理解的資料復置成可以理解的文字。兩種處理都和數學公式、演算法及密鑰資料 (金鑰) 有密切的關係。

加密演算法

加碼演算法有下列兩種類型：

1. 使用密鑰或**對稱金鑰演算法**的通信雙方會共用同一只金鑰。加密和解密都必須使用該份金鑰。「資料加密標準 (DES)」與「三重 DES 演算法」皆屬密碼鎖演算法的例子。
2. 公開金鑰或**不對稱金鑰演算法**則是使用一對金鑰。其中的私密金鑰爲單方專用，不會與他人共享。而公開金鑰則不然，會公開與他人共用。資料在使用其中一只金鑰加密之後，便須使用另一只金鑰，才能夠予以解密及回復。上述兩只金鑰雖然都是以數理爲基礎，但實際上絕無可能從公開金鑰推得私密金鑰。RSA 演算法爲公開金鑰演算法一種。

兩種演算法類型都會透過金鑰來決定資料的變更方式。不同的加密處理會依其所要達成的目的而選用適合的演算法。您可以根據您的目的選擇所需的加密處理；例如您可能需要產生訊息鑑別碼 (MAC)，以確保資料的完整性。使用者針對「4758 加密輔助處理器」所撰寫的應用程式，會使用相對應的安全性應用程式設計介面 (SAPI) 來呼叫加密處理。金鑰和加密處理會一起轉換資料。具有 SAPI 授權的使用者將可以存取該項加密處理。由此可知，金鑰控制了資料的存取權限。您必須保護金鑰，才能夠保護資料。您若能夠妥善保管金鑰值而不外洩，便可以保障每一次使用該金鑰演算加密之資料的安全性。

加密

對於欄位層次的加密，使用者應用程式會明確地要求加密服務。使用者應用程式全權控制金鑰的產生、選取及分送。使用者應用程式同時還控制了加密的資料項目，以及應保留爲純文字的資料項目。對於階段作業層次的加密，則系統會要求加密服務，而不是應用程式。您的應用程式可能知道，也可能不知道加密的進行。鏈結層次的加密通常會利用加密專用的硬體，在通信協定堆疊的最底層執行。「4758 輔助處理器」支援欄位層次的加密及 Secure Sockets Layer (SSL) 階段作業建立的加密，但不支援 VPN 或 SNA 階段作業層次的加密。「2058 加密加速器」只支援 SSL 階段作業建立的加密。

資料完整性

要確定資料的可靠與否，您必須了解資料是否出自於授權的來源，且未經變更。亦即資料的正確性及資料的完整性。「4758 輔助處理器」藉建立「訊息鑑別碼 (MAC)」、訊息摘要或數位簽章來確定資料的正確性與整合性。

訊息鑑別碼 (MAC)

MAC 處理是一種保持資料完整的技術，可以讓您定義重要的資料元素。例如，您可以定義資金轉送訊息中的金額部份。重要資料元素、密碼演算法與 MAC 金鑰會產生 MAC。之後 MAC 即成爲訊息的一部份，且與訊息一起遞送。MAC 處理會使用 DES 或「三重 DES 演算法」金鑰。

訊息接收者會使用與傳送者相同的 MAC 金鑰、演算法及程序重新產生 MAC。若接收者的 MAC 與訊息一起傳送的 MAC 相符，便可以原封不動地收下該 MAC。

MAC 處理可協助鑑別收到的訊息；但由於傳輸的資料爲純文字格式，因此無法防堵未經授權的讀取進行。藉使用 MAC 處理進而加密整個訊息，將可以更有效地保障資料的私密性與完整性。

訊息摘要

您可以對資料執行訊息摘要處理，以產生摘要值，作爲加密過程中所產生的總和檢查。資料一經修改，所產生的摘要亦會有所不同。您可以保留訊息摘要的複本加以比較。訊息摘要若是相同，便表示資料未經修改。

數位簽章

數位簽章也可用於驗證正確性及完整性。此處理一共有兩個步驟：

1. 首先產生資料的摘要，然後再使用 RSA 私密金鑰加密摘要。其結果便是數位簽章。您可以使用公開金鑰解密簽章，回復其原始摘要，對簽章進行驗證。
2. 產生另一份資料摘要，與原始摘要進行比較。若兩者相同，便表示通過驗證，可以確信該資料未經任何改變。

「4758 加密輔助處理器」相關的金鑰類型

「4758 輔助處理器」所使用的金鑰類型繁多。但並非所有的 DES 或「三重 DES 演算法」金鑰都適用於全部的對稱金鑰作業。同樣地，也並非所有的公開金鑰演算法 (PKA) 金鑰，都適用於全部的不對稱金鑰作業。以下是「4758 輔助處理器」所使用的金鑰類型清單：

主要金鑰

此爲未加密金鑰，表示其未經其它金鑰的加密。「4758 輔助處理器」利用主要金鑰加密所有的作業金鑰。「4758 輔助處理器」會將主要金鑰存在損害回應模組中。您無法從「4758 輔助處理器」中擷取之。「4758 輔助處理器」會以損毀主要金鑰及其原廠證明的方式回應損害的企圖。4758-023 有兩只主要金鑰：一只用於加密 DES 金鑰，另一只則用於加密 PKA 金鑰。

雙倍長度的加密用的密鎖鑰

「4758 輔助處理器」會使用這種類型的「三重 DES 演算法」金鑰，加密或解密其它的 DES 或「三重 DES 演算法」金鑰。加密用金鑰一般會用於系統之間的金鑰傳輸。但也可以在離線時儲存金鑰以爲備份。若使用加密用金鑰傳輸金鑰，則兩個系統便須共用加密用金鑰本身的清除值。匯出器的加密用金鑰會於匯出作業時使用，並於其間將使用

主要金鑰加密的金鑰解密，接著再以加密用的金鑰予以加密。匯入器的加密用金鑰會在匯入作業時使用，並於其間將使用加密用金鑰加密的金鑰解密，接著再以主要金鑰予以加密。

雙倍長度的 PIN 金鑰

「4758 輔助處理器」會透過此種類型的金鑰產生、驗證、加密及解密金融作業中所使的 PIN。這些屬於「三重 DES 演算法」金鑰。

MAC 金鑰

「4758 輔助處理器」會使用此種類型的金鑰產生「訊息鑑別碼 (MAC)」。這些可以是 DES 或「三重 DES 演算法」金鑰。

密碼金鑰

「4758 輔助處理器」會使用此種類型的金鑰加密或解密資料。這些可以是 DES 或「三重 DES 演算法」金鑰。

單倍長度相容性金鑰

「4758 輔助處理器」會使用此種類型的金鑰加密或解密資料，並產生 MAC。這些是 DES 金鑰，多在加密資料或 MAC 與未施行「共同密碼架構」的系統進行交換時使用。

私密金鑰

「4758 輔助處理器」會利用私密金鑰來產生數位簽章，以及解密由公開金鑰所加密的 DES 或「三重 DES 演算法」金鑰。

公開金鑰

「4758 輔助處理器」會使用公開金鑰來驗證數位簽章、加密 DES 或「三重 DES 演算法」金鑰，以及解密由私密金鑰所加密的資料。

金鑰格式

「4758 輔助處理器」會使用下列四種金鑰格式之一。金鑰格式及金鑰類型決定了加密處理運用該金鑰的方式。這四種格式包括：

清除格式

金鑰的清除值未以任何加密的方法保護。「4758 輔助處理器」不使用未加密金鑰。未加密金鑰必須先匯入安全的模組中，並使用主要金鑰加密，然後後儲存於安全模組之外。

作業格式

以主要金鑰加密的金鑰屬作業格式。「4758 輔助處理器」的加密作業可以直接使用這些金鑰。作業金鑰又稱爲內部金鑰。所有儲存在伺服器金鑰儲存檔中的金鑰都屬於作業金鑰。但您無需將所有的作業金鑰都儲存在金鑰儲存檔中。

匯出格式

以匯出器加密用金鑰加密的金鑰作爲匯出作業結果者皆屬匯出格式。這類金鑰又稱爲外部金鑰。若匯入器加密用金鑰的清除值與匯出器加密用金鑰的清除值相同，則此種匯出格式的金鑰也可以歸類成匯入格式。您可以選擇任意方式將金鑰儲存成匯入格式，但卻不可以將其存入金鑰儲存檔中。

匯入格式

以匯入器加密用金鑰加密的金鑰皆屬匯入格式。只有匯入格式的金鑰才可以用爲匯入作業的來源。這類金鑰又稱爲外部金鑰。若匯出器加密用金鑰的清除值與匯入器加密用金鑰的清除值相同，則此種匯入格

式的金鑰也可以歸類成匯出格式。您可以選擇任意方式將金鑰儲存成匯出格式，但卻不可以將其存入金鑰儲存檔中。

函數控制向量

IBM 提供的數位簽章值稱爲「函數控制向量」。該值將促使「4758 輔助處理器」中的加密應用程式，產生與適用之匯入規則與匯出規則一致的加密服務層次。「函數控制向量」會隨附在您系統上所安裝的 IBM Cryptographic Access Provider (5722-ACx) 產品中。該檔案的路徑名稱爲 /QIBM/ProdData/CAP/FCV.CRT。函數控制向量提供「4758 輔助處理器」產生金鑰所需的金鑰長度資訊。

控制向量

控制向量與函數控制向量不同，是已知的值，與控制下列項目的金鑰相關聯：

- 金鑰類型
- 其它可由此金鑰加密的金鑰
- 「4758 輔助處理器」是否可以匯出此金鑰
- 此金鑰所允許的其它用途

控制向量會以加密的方式鏈結到某只金鑰，若未同時變更此金鑰值，便無法變更此控制向量。

金鑰儲存檔

爲 OS/400® 資料庫檔案，用於儲存以「4758 輔助處理器」之主要金鑰加密的金鑰。

金鑰記號

一種資料結構，內含加密金鑰、控制向量及其它金鑰相關資訊。大部份作用於金鑰上或使用金鑰的 CCA API 動詞都會將金鑰記號用爲參數。

第 4 章 iSeries 的 2058 加密加速器

使用 V5R2 (或更新版本) iSeries 伺服器的客戶可以使用「2058 加密加速器」。客戶不需要「4758 加密輔助處理器」高度安全性，但需要硬體加速器提供的高度加密效能以卸下主處理器「2058 加密加速器」爲這些客戶提供另一種選擇。已設計「2058 加密加速器」來增進那些不需要安全金鑰儲存體的 SSL 應用程式的效能。它沒有像「4758 加密輔助處理器」那樣，提供金鑰的防損害儲存體。您可以在 iSeries 伺服器中最多安裝四個「2058 加密加速器」卡。

「2058 加密加速器」提供一種特殊硬體，可使用長度最長爲 2048 位元的資料金鑰，以最優化 RSA 加密 (模組的乘冪) 。 「2058 加速器」使用多重 RSA (Rivest、Shamir 及 Adleman 演算法) 引擎。請參照 iSeries 效能管理 特定 iSeries 伺服器模型的效能資訊的網站。

如需「2058 加密加速器」的相關資訊，請參照下列頁：

- 「2058 加密加速器」特性
- 加密硬體實務：增強 iSeries SSL 效能
- 「2058 加密加速器」計畫
- 配置「2058 加密加速器」

2058 加密加速器特性

「2058 加密加速器」的部份特性包括：

- 單一卡高效能加密配接卡 (標準 PCI 卡)
- 已爲 RSA 加密設計並最佳化
- 機載硬體式的 RNG (亂數產生器)
- 五個已裝載的 IBM UltraCypher 加密引擎

請參閱下列關於「2058 加密加速器」的資訊：

- 「2058 加密加速器」計畫
- 配置「2058 加密加速器」

加密硬體實務：增強 iSeries SSL 效能

爲使您知道如何在您的 iSeries 伺服器上使用此加密硬體的方法，我們已新增此用法實務。

狀況

公司的 iSeries 伺服器每天要處理幾千個安全的網際網路交易。公司的交易利用 Secure Sockets Layer 與 Transport Layer Security 通信協定 (SSL 與 TLS) - 安全進行網際網路交易的一般方法。此公司的系統管理者 Sue 想爲附加的應用程式處理程序釋放伺服器資源，包括支援更多 SSL 交易的能力。Sue 正在尋找適合這些目標的解決方案：

- 應用程式處理程序增加相當大的可用伺服器資源包括附加的 SSL 交易

- 最小安裝及配置努力
- 最小資源管理基本要求

基於這些目標，Sue 會訂購並安裝 IBM 「2058 電子商業加密加速器」。 (此後簡稱爲「2058 加密加速器」)。「2058 加密加速器」爲 PCI (週邊元件交互連接) 卡，是爲建立 SSL/TLS 階段作業時，加速所需的高度計算密集處理程序而特別設計的。在 iSeries 伺服器上，能藉由訂購硬體特性碼 4805 來取得「2058 加密加速器」。

明細

1. iSeries 伺服器已安裝並配置「2058 加密加速器」。
2. iSeries 伺服器從網路接收大量 SSL 交易要求。
3. 「2058 加密加速器」會在 SSL 交易起始設定中執行加密處理程序，並會快取與 SSL 交易的數位憑證相關的私密金鑰。

先決條件及假設

此實務假設 Sue 已經計畫安裝「2058 加密加速器」，然後再適當地配置卡 (請參閱 2058 加密加速器計畫，及配置 2058 加密加速器)。此實務也假設 Sue 已經設定 SSL 的數位憑證。

配置步驟

Sue 完成下列步驟來增強其公司的 iSeries 伺服器 SSL 效能：

1. 訂購「硬體特性」碼 4805，此提供「2058 加密加速器」。
2. 安裝「2058 加密加速器」。
3. 建立「2058 加密加速器」的裝置說明，並轉接該裝置 (請參閱配置 2058 加密加速器以取得明細)。

「2058 加密加速器」計畫

於安裝並使用「2058 加密加速器」前，伺服器必須符合這些基本要求。

硬體基本要求

IBM 電子商業加密加速器 (可訂購之特性碼 4805，此後稱爲「2058 加密加速器」)。4805 特性爲標準 PCI 卡，並且在下列 iSeries 伺服器模型上得到支援：

- 270
- 810、820、825、830、840、870 和 890
- SB2 和 SB3
- 擴充裝置 5074、5075、5078、5079、5088、5094、5095 和 5294

OS/400 與 SSL 基本要求

「2058 加密加速器」需要 OS/400 V5R2M0 (版本 5 版次 2 修改 0) 軟體。雖然已爲加密作業完全啓用「2058 加密加速器」，也必須將「密碼存取提供者」128-bit 位元 (5722-AC3) 授權程式產品安裝在 iSeries 伺服器上，以啓用 OS/400 中之 SSL 也會使用的加密功能。

配置 2058 加密加速器

您必須建立裝置說明，以使 OS/400 之 SSL 能將 RSA 加密作業指向「2058 加密加速器」。您可藉由使用「建立裝置 Crypto CL」指令來建立裝置說明。

建立裝置說明

若要使用 CL 指令來建立裝置說明，請遵循下列步驟：

1. 在指令行鍵入 CRTDEVCRP。
2. 按提示指定裝置名稱。
3. 接受 PKA 金鑰儲存的預設名稱：*NONE。
4. 接受 DES 金鑰儲存的預設名稱：*NONE。
5. 按提示指定說明。這是可選用的。
6. 一旦您已經建立裝置說明，請使用「轉接配置 (VRYCFG)」或「使用配置狀態 (WRKCFGSTS)」CL 指令來轉接裝置。

對於由軟體產生並儲存在軟體中的數位憑證，一旦轉接裝置， OS/400 SSL 會自動啓動使用「2058 加密加速器」。卸下與 SSL 及 TLS 階段作業建立相關的私密金鑰處理程序至「2058 加密加速器」。當轉斷裝置時，OS/400 SSL 切回建立 SSL 及 TLS 階段作業之軟體型的加密，從而將私密金鑰處理程序載入放回到該伺服器上。

註: 僅當不是由「4758 加密輔助處理器」建立的憑證與私密金鑰，此才爲眞。如果認證是使用「4758 加密輔助處理器」產生的，「4758 加密輔助處理器」必須用於那些使用該特定憑證的 SSL 或 TLS 階段作業。

一旦安裝並轉接了「2058 加密加速器」，加密硬體實務：增強 iSeries SSL 效能頁會提供「2058 加密加速器」的 iSeries 伺服器用法實務。«