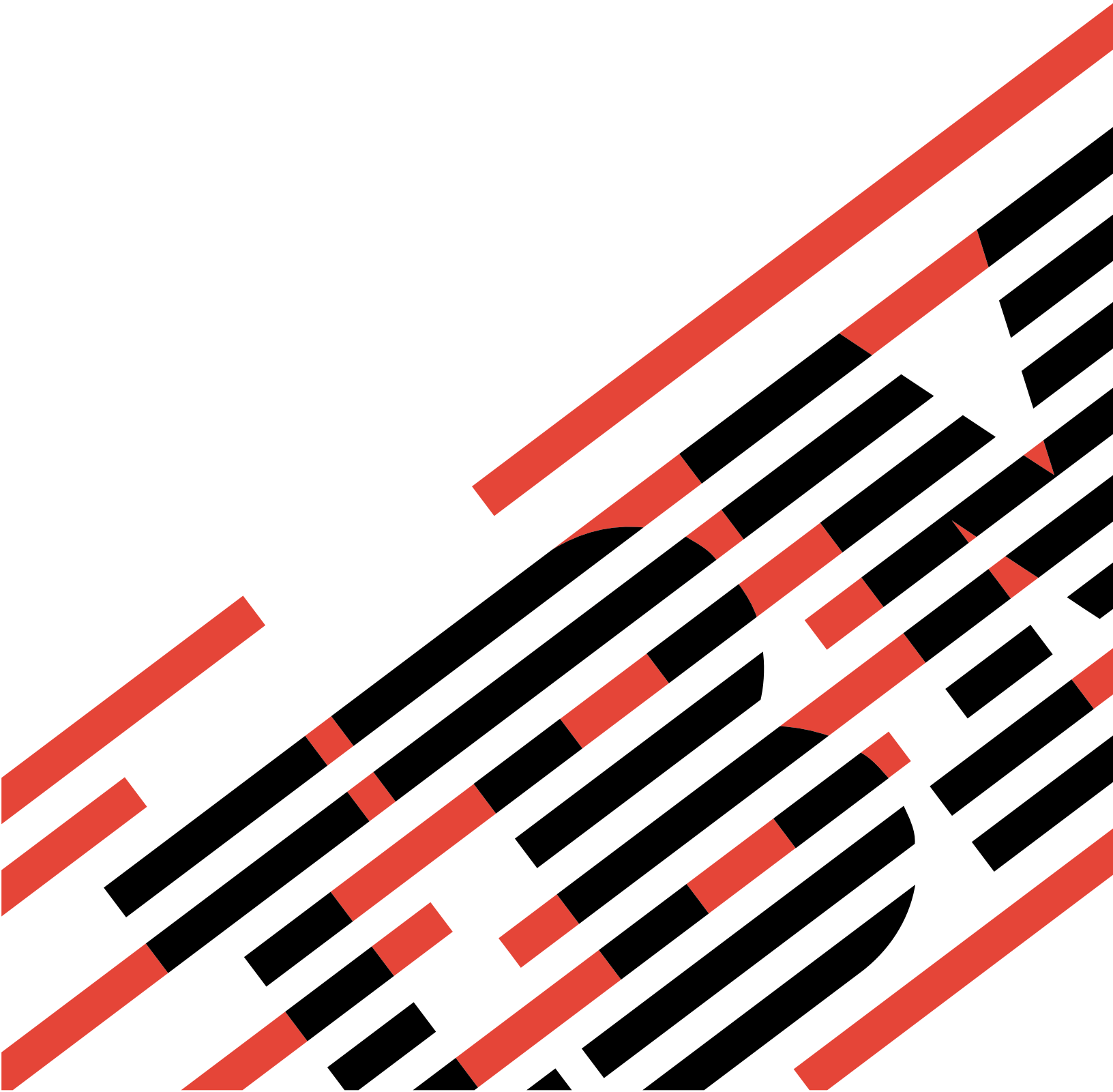
IBM

eserver

iSeries

數位憑證管理程式



IBM

@server

iSeries

數位憑證管理程式

目錄

第 1 篇 數位憑證管理程式

數位憑證是一種電子機密，可以讓您在電子交易中建立身份證明。數位憑證有愈來愈多種用途，可提供強化的網路安全措施。例如，在配置和使用 Secure Sockets Layer (SSL) 方面，數位憑證很重要。在不可靠的網路上，例如網際網路，使用 SSL 可讓您在使用者和伺服器應用程式之間建立安全連線。在網際網路上保護重要資料（例如使用者名稱和密碼）的私密性方面，SSL 是最佳的解決方案之一。許多 iSeries™ 服務和應用程式，例如 FTP、Telnet、HTTP Server for iSeries 等，皆提供 SSL 支援來確保資料私密性。

iSeries 提供大量的數位憑證支援，可讓您在許多安全性應用程式中使用數位憑證當做認證。除了使用憑證來配置 SSL 以外，在 SSL 和虛擬專用網路 (VPN) 交易上，您可以使用憑證當做從屬站鑑別的認證。另外，您可以使用數位憑證及其相關安全金鑰來簽署物件。簽署物件可讓您驗證物件上的簽章，偵測物件內容的變更或可能的破壞，以確保其完整性。

如果您使用「數位憑證管理程式 (DCM)」這個免費的 iSeries 特性來集中管理應用程式的憑證，就可以很容易地利用 iSeries 在憑證方面的支援。 DCM 可讓您管理從任何「認證中心」(CA) 取得的憑證。另外，您可以使用 DCM 來建立和操作自己的「區域 CA」，發出專用憑證給組織內的應用程式和使用者。

適當地規劃和評估是有效使用憑證來增加安全性優勢的關鍵。您應該複查這些主題，以進一步了解憑證如何運作及如何使用 DCM 來管理憑證和使用它們的應用程式：

V5R2 新增功能
請閱讀本資訊來了解關於「數位憑證管理程式」功能的變更，以及本版次的資訊主題的變更。

列印此主題
請閱讀本頁來了解如何將整個主題列印成 PDF 檔案。

從舊版次移轉至 DCM
請閱讀本資訊來了解您必須執行的作業，以及將現有版本的 DCM 移轉至最新版本時的注意事項。

DCM 實務
請閱讀本資訊來複查兩個實務，其中說明典型的憑證施行方法，協助您規劃自己的憑證施行作爲您的 iSeries 安全原則。每一個實務亦提供您在運用上述實務時所必須執行的所有必要配置作業。

數位憑證概念
請使用本概念和參考資料來清楚瞭解什麼是數位憑證及其運作方式。瞭解不同的憑證類型及如何使用它們作爲安全原則的一部份。

DCM 規劃
請使用本資訊來協助您決定如何及何時使用數位憑證以達到您的安全性目標。請使用本資訊來瞭解您需要安裝的必備軟體，以及使用 DCM 之前必須考慮的其他基本要求。

配置 DCM
請使用本資訊來瞭解如何配置所有必要項目，以確保您可以使用 DCM 來管理憑證及其金鑰。

管理 DCM

請使用本資訊來瞭解如何使用 DCM 來管理憑證及使用它們的應用程式。另外，您可以瞭解如何以數位方式簽署物件，以及如何建立和操作您自己的「認證中心」。

DCM 疑難排解

請使用本資訊來瞭解如何解決使用 DCM 時可能發生的一些常見錯誤。

DCM 相關資訊

請使用本頁來取得其他資源的鏈結，以進一步了解數位憑證、公開金鑰基礎設施、「數位憑證管理程式」以及其他相關資訊。

第 1 章 V5R2 的新增功能

V5R2 數位憑證管理程式 (DCM) 和 iSeries 數位憑證功能的加強功能包括：

- **指派憑證功能**
  這項新的 DCM 作業可讓您更快更容易地指派憑證給一或多個應用程式。您可以從**管理憑證**作業清單或從**使用伺服器和憑證**及**使用物件簽署憑證**捷徑頁存取此作業。此功能僅適用於 *SYSTEM 和 *OBJECTSIGNING 憑證庫。
- **簽署指令 (*CMD) 物件**
  現在您可以使用 DCM 在指令 (*CMD) 物件上建立數位簽章，來提供檢查其完整性的方法。同時，您可以選擇 *CMD 物件的簽章範圍；您可以選擇要簽署整個 *CMD 物件，或只簽署 *CMD 物件的基核元件。當您使用 DCM 檢視 *CMD 物件上的簽章時， DCM 會提供關於簽章範圍的資訊。
- **不使用 DCM 而建立由區域 CA 簽署的使用者憑證的 API**
  現在有兩個新的 API，供您以程式設計方式發出由區域認證中心 (CA) 簽署的憑證給非 iSeries 使用者。這些 API 可讓您發出憑證給使用者而不需要 iSeries 使用者設定檔，且使用者不必使用 DCM 個別取得憑證來進行從屬站鑑別。

本主題的新資訊或已強化的資訊包括：

- 兩個新的實務，可用它們來幫助您決定如何善用憑證來實現您的安全性目標。
- 重組過的資訊，方便您快速找到您使用 DCM 時所需要的資訊。

要尋找關於本版次的新增功能或變更功能的其它資訊，請參閱使用者備忘錄 。

第 2 章 列印此主題

若要檢視或下載 PDF 版本，請選取數位憑證管理程式  （檔案大小爲 468 KB 左右，或大約 110 頁）。

若要在工作站上儲存 PDF 以供檢視或列印：
1. 在瀏覽器開啓 PDF（按一下上面的鏈結）。
2. 在瀏覽器的功能表中按一下**檔案**。
3. 按一下**另存新檔**。
4. 導覽您所要儲存 PDF 的目錄。
5. 按一下**儲存**。

您若需使用 Adobe Acrobat Reader 檢視或列印 PDF，可從 Adobe 網站 (www.adobe.com/prodindex/acrobat/readstep.html) 下載複本  。

第 3 章 從舊版 DCM 移轉

從 V4R3 版本的數位憑證管理程式 (DCM) 移轉到 V5R2 時，DCM 會自動升級現有的區域認證中心 (CA) 和系統憑證金鑰環檔案。DCM 升級這些檔案（叫作 default.kyr）到對應的憑證庫檔案（叫作 default.kdb）。DCM 亦移轉與超文字轉送通信協定 (HTTP) 和輕裝備目錄存取通信協定 (LDAP) 伺服器相關聯的金鑰環檔案中的所有有效憑證。 DCM 將有效的憑證移轉到 *SYSTEM 憑證庫 (default.kdb)。

註: 如果您是從 V4R4、V4R5 或 V5R1 版本的 DCM 移轉，則不必執行任何移轉作業，因爲來自這些版本的憑證檔案與 V5R2 版本的 DCM 是相容的。

憑證庫移轉的金鑰環 - V4R3 移轉

在 V5R2 DCM 安裝期間，系統會移轉下列金鑰環檔案：
- DCM 的預設金鑰環檔案。
- HTTP 伺服器配置檔使用的金鑰環。
- LDAP 伺服器配置檔使用的金鑰環。

如果您使用 DCM 未自動升級的 .kyr 檔，當您第一次在 DCM 使用它時， DCM 會將它轉換爲 kyr.kdb 檔。例如，您第一次在 DCM 使用者介面中指定 secure.kyr 檔案時，DCM 將該檔案轉換成新的憑證庫，並使用 secure.kyr.kdb 這個檔名。

註: 金鑰環與憑證庫不同，因此您必須透過 DCM 使用者介面使用它們，來轉換 DCM 未自動升級的金鑰環檔案。若手動變更副檔名爲 .kdb，以後當您要透過 DCM 使用者介面使用那些檔案時會導致錯誤發生。

如果您在使用 DCM 時試圖刪除 secure.kyr 檔，實際上 DCM 會保存它而刪除 secure.kyr.kdb 檔。

預設憑證庫密碼

如果檔案 /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR 存在，系統會將此金鑰環檔案及其它任何合格的金鑰環檔案移轉到 *SYSTEM 憑證庫。與 /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR 檔相關聯的原始密碼將作爲 *SYSTEM 憑證庫的密碼來使用。

如果 /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR 檔案不存在，但有合格的其它金鑰環檔案可以移轉（例如，HTTP 伺服器配置檔使用的金鑰環檔案），系統會以 DEFAULT（全大寫）這個密碼建立 *SYSTEM 憑證庫並完成移轉。

關於檔案移轉程序中所發生錯誤的資訊，以及如何解決錯誤的資訊，請參閱： 移轉錯誤及回復解決方案。

第 4 章 DCM 實務

數位憑證管理程式和您 iSeries 提供的數位憑證支援可讓您使用憑證，以許多不同的方式來增強安全原則。根據您的企業目標和安全性需求，您選擇使用憑證的方式並不相同。

使用數位憑證可幫助您在許多方面增進安全性。數位憑證可讓您使用 Secure Sockets Layer (SSL) 對網站和其它網際網路服務進行安全的存取。您可以使用數位憑證來配置虛擬專用網路 (VPN) 連線。此外，您可以使用憑證的金鑰以數位方式簽署物件，或驗證數位簽章以確定物件的確實性。這種數位簽章確保物件起源的可靠性並保護物件的完整性。

您可以在伺服器和使用者之間使用數位憑證（而非使用者名稱和密碼）來鑑別及授權階段作業，進一步增加系統安全性。而且，您可以使用 DCM 使某使用者的憑證與該使用者的 iSeries 使用者設定檔產生關聯。然後，該憑證與相關聯的設定檔即擁有相同的授權和許可權。

因此，根據各種不同的因素，您選擇使用憑證的方式可能很複雜。本主題提供的實務說明典型企業環境中一些比較一般的數位憑證安全性目標。每一個實務亦說明所有必需的系統和軟體先決條件以及您要實施此實務必須執行的所有配置作業。複查這些實務可幫助您決定如何使用憑證增加安全性才最適合您的需求：

實務：使用憑證來保護公用應用程式和資源的存取
此實務說明何時及如何使用憑證來保護及限制公用使用者存取公用資源或企業外網路資源和應用程式。

實務：使用憑證來保護內部應用程式和資源的存取
此實務說明何時及如何使用憑證來保護及限制內部使用者在您內部伺服器上可以存取哪些資源和應用程式。

實務：使用憑證來保護公用應用程式和資源的存取

狀況

您爲一家保險公司 (MyCo., Inc) 工作，負責維護您公司的 Intranet 和企業外網路網站上不同的應用程式。您所負責的其中一個特別應用程式是費率計算應用程式，它讓數百個獨立的代理人能夠爲客戶計算報價。因爲此應用程式提供的資訊有點機密性，所以您想確定只有已登記的代理人可以使用它。最後您想進一步提供一個比現行使用者名稱和密碼方法更安全的方法，讓使用者存取應用程式。當此資訊透過不可靠的網路傳輸時，您擔心未獲授權的使用者會攫取到此資訊。此外，不同代理人可以彼此共用此資訊而不需要授權。

經過一番研究之後，您覺得使用數位憑證可以提供您所需要的安全性。使用憑證可讓您使用 Secure Sockets Layer (SSL) 來保護費率資料的傳輸。雖然最後您希望所有代理人都能使用憑證來存取此應用程式，但您知道貴公司和您的代理人需要一些時間才能達成此目標。目前，您打算繼續使用現行使用者名稱和密碼鑑別方法，因爲 SSL 保護此機密資料在傳輸時的私密性。

根據應用程式的類型及其使用者和您在使用者憑證鑑別方面的未來目標，您決定使用來自知名認證中心 (CA) 的公用憑證來配置 SSL 給應用程式。

實務優點

此實務有下列幾項優點：

- 使用數位憑證配置 SSL 存取您的費率計算應用程式，可確定伺服器和從屬站之間傳輸的資訊受到保護且有私密性。
- 儘可能地對從屬站鑑別使用數位憑證，可提供更安全的方法來識別授權使用者。即使不可行，利用使用者名稱和密碼的從屬站鑑別也會受到 SSL 階段作業保護並保持私密性，使這種機密資料的交換更加安全。
- 在這些或類似的條件下，使用*公用*數位憑證來限制或允許存取您的應用程式和資料是一個實用的選擇：
  - 資料和應用程式需要不同程度的安全性。
  - 可靠的使用者間的流動率很高。
  - 您提供對應用程式和資料的公用存取，例如網際網路網站或企業外網路應用程式。
  - 您不想操作自己的認證中心 (CA)，因爲有大量使用者存取您的應用程式和資源或因爲管理方面的其它理由。
- 在此實務中使用公用憑證來配置 SSL 的費率計算應用程式會減少使用者要存取應用程式時必須執行的配置數量。大部份從屬站軟體均包含大部份知名 CA 的 CA 憑證。

目標

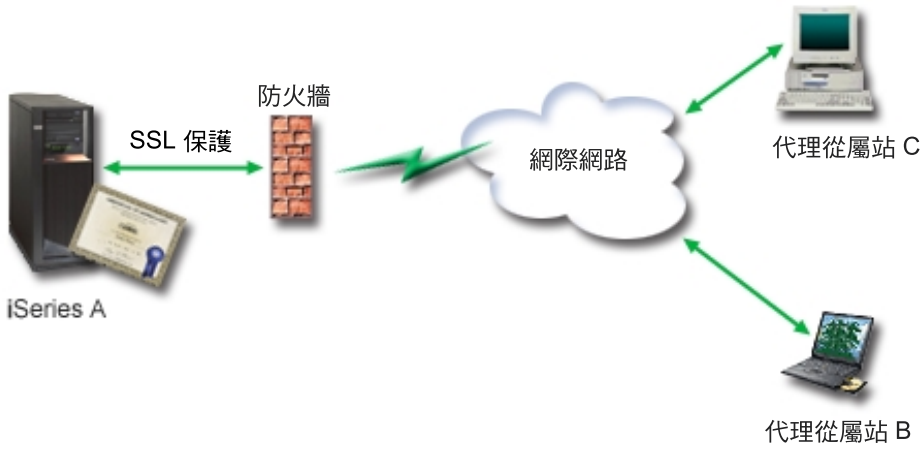
在此實務中，MyCo., Inc. 想使用數位憑證來保護其應用程式提供給獲授權的公用使用者的費率計算資訊。該公司希望有更安全的方法來鑑別那些獲准存取此應用程式的使用者。

此實務的目標如下所示：

- 公司公用費率計算應用程式必須使用 SSL 保護它提供給使用者的資料的私密性。
- 必須以來自知名公用網際網路認證中心 (CA) 的公用憑證完成 SSL 配置。
- 授權使用者必須提供有效的使用者名稱和密碼，在 SSL 模式中存取應用程式。最後，授權使用者必須能夠使用兩種安全鑑別方法的其中一種來授予存取權給應用程式。代理人必須提出一個來自知名認證中心 (CA) 的公用數位憑證，或一個有效的使用者名稱和密碼。

明細

下圖說明此實務的網路配置狀況：



此圖說明關於此實務的狀況的下列資訊：

公司公用伺服器 - iSeries A

- iSeries A 是裝載公司費率計算應用程式的伺服器。
- iSeries A 執行 OS/400® 5.2 版 (V5R2)。
- iSeries A 有安裝密碼存取提供者 (5722-AC3)。
- iSeries A 有安裝及配置數位憑證管理程式 (OS/400 option 34) 和 IBM® HTTP Server for iSeries (5722-DG1)。
- iSeries A 執行費率計算應用程式，它已配置成：
  - 需要 SSL 模式。
  - 在 SSL 配置中使用來自知名認證中心 (CA) 的公用憑證。
  - 需要藉由使用者名稱和密碼進行使用者鑑別。
- 當 Clients B 和 C 存取此應用程式時，iSeries A 提出憑證來起始一個 SSL 階段作業。
- 在起始設定 SSL 階段作業之後，iSeries A 要求 Clients B 和 C 提供有效的使用者名稱和密碼，然後才允許它們存取費率計算應用程式。

代理程式從屬站系統 - Client B 和 Client C

- Clients B 和 C 是獨立的代理程式，他們存取費率計算應用程式。
- Clients B 和 C 有一個知名 CA 憑證的複本，它對安裝在其從屬站軟體中的應用程式發出憑證。
- Clients B 和 C 在 iSeries A 存取費率計算應用程式，iSeries A 對其從屬站軟體提出其憑證，以驗證其識別身份並起始 SSL 階段作業。
- Clients B 和 C 上的從屬站軟體已配置爲接受來自 iSeries A 的憑證，然後 SSL 階段作業開始。
- 在 SSL 階段作業開始之後，在 iSeries A 授予對應用程式的存取權之前，Clients B 和 C 必須提供有效的使用者名稱和密碼。

先決條件和假設

此實務依據下列先決條件和假設而定：

1. iSeries A 上的費率計算應用程式是一個通屬應用程式，可配置爲使用 SSL。大部份應用程式，包括許多 iSeries 應用程式在內，均提供 SSL 支援。各應用程式間的 SSL

配置步驟大不相同。因此，此實務並不提供特定的指示來配置費率計算應用程式使用 SSL。此實務提供配置及管理憑證的指示，任何應用程式要使用 SSL 必須有這些憑證。

2. *選用性地*，費率計算應用程式可提供需要憑證進行從屬站鑑別的能力。此實務提供的指示是關於如何使用數位憑證管理程式 (DCM) 爲那些提供此支援的應用程式配置憑證信任。因爲用於從屬站鑑別的配置步驟在各應用程式之間大不相同，所以此實務並不提供爲費率計算應用程式配置憑證從屬站鑑別的特定指示。
3. iSeries A 符合安裝及使用數位憑證管理程式 (DCM) 的基本要求。
4. 先前沒有人在 iSeries A 配置或使用 DCM。
5. 不論誰在此實務中使用 DCM 執行作業，在其使用者設定檔中都必須擁有 *SECADM 和 *ALLOBJ 特殊權限。
6. iSeries A 沒有安裝 IBM 4758-023 PCI 加密輔助處理器。

作業步驟

要實施此實務，您必須在 iSeries A 執行這些作業：

1. 完成所有先決條件步驟來安裝和配置所有需要的 iSeries 產品。
2. 使用數位憑證管理程式 (DCM) 建立伺服器憑證要求。
3. 配置應用程式使用 Secure Sockets Layer (SSL)。
4. 使用 DCM 匯入和指派已簽署的伺服器或從屬站憑證到您應用程式的應用程式 ID。
5. 必要時，以 SSL 模式啓動應用程式。
6. *可選用的作業*：使用 DCM 定義 CA 信任清單，根據提供此支援的應用程式的憑證來啓用從屬站鑑別。

註： 此實務所說明的狀況並不需要費率計算應用程式使用憑證進行從屬站鑑別。許多應用程式都提供憑證從屬站鑑別支援；您如何配置此支援，各應用程式之間大不相同。提供這項可選用的作業是爲了幫助您了解，如何使用 DCM 啓用從屬站鑑別方面的憑證信任，作爲配置應用程式的憑證從屬站鑑別支援的基礎。

配置明細

完成下列作業步驟以使用憑證來配置對應用程式和資源的受保護公用存取，如此實務所述。

步驟 1：完成先決條件作業來安裝所有需要的 iSeries 產品

在您可以執行特定的配置作業來實施此實務之前，您必須先完成安裝和配置所有需要的 iSeries 產品的所有先決條件作業才行。

步驟 2：建立伺服器或從屬站憑證要求

如此實務所述，要開始使用 Secure Sockets Layer (SSL) 保護應用程式的資料通信時，您必須先向公用認證中心 (CA) 取得數位憑證才行。您使用數位憑證管理程式 (DCM) 建立公用 CA 發出憑證所需的資訊。

要開始取得憑證的程序，請完成下列步驟：

1. 啓動 DCM。

2. 在 DCM 的導覽頁框中，選取**建立新的憑證庫**以啓動引導作業及完成一連串套表。這些套表引導您建立一個憑證庫及您的應用程式可用於 SSL 階段作業的一個憑證。

   註: 如果您對於如何完成本引導作業中的特定套表有問題，請選取問號 (**?**) （位於頁頂端）來存取線上說明。
3. 選取 ***SYSTEM** 作爲要建立的憑證庫並按一下**繼續**。
4. 選取**是**來建立憑證，這是建立 *SYSTEM 憑證庫的一部份，並按一下**繼續**。
5. 選取 **VeriSign 或其它網際網路認證中心 (CA)** 作爲新憑證的簽署者，並按一下**繼續**以顯示一個套表，它可讓您提供新憑證的識別資訊。
6. 完成套表並按一下**繼續**以顯示一確認頁。此確認頁顯示您必須提供給公用認證中心 (CA) 的憑證要求資料，此 CA 將發出您的憑證。憑證簽署要求 (CSR) 資料是由公開金鑰和您爲新憑證指定的其它資訊所組成。
7. 請小心將 CSR 資料複製並貼到憑證申請表或個別檔案中，公用 CA 要求憑證時需要它。您必須使用所有 CSR 資料，包括 Begin 和 End New Certificate Request 這兩行。當您結束本頁時資料會遺失，您無法回復它。
8. 傳送此申請表或檔案給您已選擇要發出及簽署憑證的 CA。
9. 等待 CA 傳回已簽署、已完成的憑證之後，才繼續此實務的下一個作業步驟。

在 CA 傳回已簽署、已完成的憑證之後，您可以配置應用程式使用 SSL、匯入憑證到 *SYSTEM 憑證庫，並指派它給您的應用程式使用於 SSL。

步驟 3：配置應用程式使用 SSL

當您收到公用認證中心 (CA) 傳回的已簽署的憑證時，可以繼續這項程序，亦即爲公用應用程式啓用 Secure Sockets Layer (SSL) 通信。在使用已簽署的憑證之前，您應該配置應用程式使用 SSL。當您配置應用程式使用 SSL 時，有些應用程式如 HTTP Server for iSeries 會產生唯一的應用程式 ID，並向數位憑證管理程式 (DCM) 登記此 ID。您必須知道此應用程式 ID 之後才能使用 DCM 指派已簽署的憑證給它，並完成 SSL 配置程序。

您如何配置應用程式使用 SSL 將因應用程式而異。此實務對於它所說明的費率計算應用程式並不假設特定來源，因爲 MyCo., Inc. 有很多方式可以提供此應用程式給其代理人。

要配置應用程式使用 SSL，請遵循應用程式文件提供的指示。此外，您可以複查資訊中心主題以 SSL 保護應用程式，進一步了解關於配置許多常用的 IBM 應用程式使用 SSL。

步驟 4：匯入和指派已簽署的公用憑證

在配置應用程式使用 SSL 之後，您可以使用數位憑證管理程式 (DCM) 匯入已簽署的憑證並指派它給您的應用程式。

要匯入憑證並指派它給應用程式以完成配置 SSL 的程序，請遵循下列步驟：

1. 啓動 DCM。
2. 在導覽頁框中，按一下**選取憑證庫**並選取 ***SYSTEM** 作爲要開啓的憑證庫。
3. 當「憑證庫和密碼」頁顯示時，請提供您在建立憑證庫時指定給它的密碼並按一下**繼續**。
4. 在導覽頁框重新整理之後，選取**管理憑證**以顯示作業清單。

5. 從作業清單中，選取**匯入憑證**，開始匯入已簽署的憑證到 *SYSTEM 憑證庫的程序。

   註: 如果您對於如何完成本引導作業中的特定套表有問題，請選取問號 (**?**) （位於頁頂端）來存取線上說明。
6. 接下來，從**管理憑證**作業清單中，選取**指派憑證**，以顯示現行憑證庫的憑證清單。
7. 從清單中選取一個憑證並按一下**指派至應用程式**以顯示現行憑證庫的應用程式定義清單。
8. 從清單中選取您的應用程式並按一下**繼續**。會出現一頁顯示您的分派選項的確認訊息，如果發生問題則顯示錯誤訊息。

這些作業完成後，您就可以在 SSL 模式啓動應用程式，開始保護它提供的資料的私密性。

步驟 5：在 SSL 模式啓動應用程式

在完成匯入及指派憑證給應用程式的程序之後，您可能需要結束應用程式，然後在 SSL 模式重新啓動應用程式。有時候這是必需的，因爲當應用程式執行時，應用程式可能無法判斷憑證分派是否存在。請複查應用程式的文件以判斷您是否需要重新啓動應用程式，或取得關於在 SSL 模式啓動應用程式的其它特定資訊。

可選用的步驟 6：為需要憑證進行從屬站鑑別的應用程式定義 CA 信任清單

支援在 Secure Sockets Layer (SSL) 階段作業期間使用憑證來進行從屬站鑑別的應用程式，必須決定是否接受憑證作爲有效的識別證明。應用程式用來鑑別憑證的其中一個準則是，應用程式是否信任發出該憑證的認證中心 (CA)。

此實務所說明的狀況並不需要費率計算應用程式使用憑證進行從屬站鑑別。許多應用程式都提供憑證從屬站鑑別支援；您如何配置此支援，各應用程式之間大不相同。提供這項可選用的作業是爲了幫助您了解，如何使用 DCM 啓用從屬站鑑別方面的憑證信任，作爲配置應用程式使用憑證進行從屬站鑑別的基礎。

在您可以定義應用程式的 CA 信任清單之前，必須符合下列幾項條件：
- 應用程式必須支援使用憑證進行從屬站鑑別。
- 應用程式的 DCM 定義必須指定應用程式使用 CA 信任清單。

如果應用程式的定義指定應用程式使用 CA 信任清單，在應用程式可以順利執行憑證從屬站鑑別之前，您必須定義此清單。這確定應用程式只驗證來自您指定爲可靠的 CA 的那些憑證。如果使用者或從屬站應用程式提出的憑證是來自非 CA 信任清單中指定爲可靠的 CA，則應用程式將不接受它作爲有效鑑別的基礎。

要使用 DCM 爲應用程式定義 CA 信任清單，請完成下列步驟：
1. 啓動 DCM。
2. 在導覽頁框中，按一下**選取憑證庫**並選取 ***SYSTEM** 作爲要開啓的憑證庫。
3. 當「憑證庫和密碼」頁顯示時，請提供您在建立憑證庫時指定給它的密碼並按一下**繼續**。
4. 在導覽頁框重新整理之後，選取**管理憑證**以顯示作業清單。
5. 從作業清單中選取**設定 CRL 狀態**以顯示 CA 憑證清單。

   註: 如果您對於如何完成本引導作業中的特定套表有問題，請選取問號 (**?**) （位於頁頂端）來存取線上說明。

6. 從清單中選取您應用程式信任的 CA 憑證，並按一下**啓用**以顯示使用 CA 信任清單的應用程式清單。
7. 從該清單選取要在其信任清單中新增所選取的 CA 的應用程式，並按一下**確定**。一訊息顯示在頁頂端，指出您選取的應用程式信任該 CA 及它發出的憑證。

現在您可以配置應用程式爲需要以憑證進行從屬站鑑別。遵循應用程式文件提供的指示。

實務：使用憑證來保護內部應用程式和資源的存取

狀況

您是某公司 (MyCo., Inc.) 的網路管理者，該公司的人力資源部門關心記錄的私密性和合法性等問題。公司員工要求能夠線上存取他們個人津貼和保健資訊。公司回應此要求，建立內部網站來提供此資訊給員工。由您負責管理此內部網站。

因爲員工分處兩個不同的辦公室，而且有些員工經常出差，因此您關心此資訊行經網際網路時如何保持私密性。而且，您習慣上以使用使用者名稱和密碼鑑別的方式限制公司資料的存取。因爲此資料的機密性和私密性，所以您了解，靠密碼限制存取是不夠的。畢竟，人們會分享、忘記、甚至竊取密碼。

經過一番研究之後，您覺得使用數位憑證可以提供您所需要的安全性。使用憑證可讓您使用 Secure Sockets Layer (SSL) 來保護資料的傳輸。此外，您可以使用憑證代替密碼，更安全地鑑別使用者並限制他們可以存取的人力資源資訊。

因此，您決定要設定專用區域認證中心 (CA)，並發出憑證給所有員工，讓員工將他們的憑證與他們的 iSeries 使用者設定檔產生關聯。此專用憑證施行類型可讓您更嚴格地控制機密資料的存取，並使用 SSL 來控制資料的私密性。最後，發出憑證給自己，如此即增加資料安全的機率，只有特定人士才能存取您的資料。

實務優點

此實務有下列幾項優點：

- 使用數位憑證配置 SSL 存取您的人力資源 Web 伺服器，可確定伺服器和從屬站之間傳輸的資訊受到保護且有私密性。
- 對從屬站鑑別使用數位憑證，可提供更安全的方法來識別授權使用者。
- 在這些或類似的條件下，使用*專用*數位憑證來限制或允許存取您的應用程式和資料是一個實用的選擇：
  - 尤其在鑑別使用者方面，您需要很高的安全性。
  - 您信任您發出憑證的個人。
  - 使用者已有 iSeries 使用者設定檔來控制對應用程式和資料的存取。
  - 您想要操作自己的認證中心 (CA)。
- 使用專用憑證進行從屬站鑑別可讓您更容易將憑證與授權使用者的 iSeries 使用者設定檔產生關聯。憑證與使用者設定檔的連結可讓 HTTP Server 在鑑別期間判斷憑證擁有者的使用者設定檔。然後 HTTP Server 可切換至它並在該使用者設定檔之下執行，或根據該使用者設定檔中的資訊對該使用者執行動作。

目標

在此實務中，MyCo., Inc. 想使用數位憑證來保護其內部人力資源網站提供給公司員工的機密個人資訊。該公司也希望有更安全的方法來鑑別那些獲准存取此網站的使用者。

此實務的目標如下所示：
- 公司內部人力資源網站必須使用 SSL 保護它提供給使用者的資料的私密性。
- 必須以來自內部區域認證中心 (CA) 的專用憑證完成 SSL 配置。
- 授權使用者必須提供有效憑證才能在 SSL 模式中存取人力資源網站。

明細

下圖說明此實務的網路配置狀況：

此圖說明關於此實務的狀況的下列資訊：

公司人力資源 Web 伺服器 - iSeries A
- iSeries A 是裝載公司網路人力資源應用程式的伺服器。
- iSeries A 執行 OS/400 5.2 版 (V5R2)。
- iSeries A 有安裝密碼存取提供者 (5722-AC3)。
- iSeries A 有安裝及配置數位憑證管理程式 (OS/400 option 34) 和 IBM HTTP Server for iSeries (5722-DG1)。
- iSeries A 執行人力資源應用程式，它已配置成：
  - 需要 SSL 模式。
  - 在 SSL 配置中使用來自區域認證中心 (CA) 的專用憑證。
  - 需要憑證進行從屬站鑑別。
- 當 Clients B、C 和 D 存取此應用程式時，iSeries A 提出它的憑證來起始一個 SSL 階段作業。
- 在起始設定 SSL 階段作業之後，iSeries A 要求 Clients B、C 和 D 提供有效的憑證，然後才允許它們存取人力資源應用程式。這種憑證的交換對 Clients B、C 和 D 的使用者而言是透明化的。

員工從屬站系統 - Client B、Client C 和 Client D
- Client B 是任職於 MyCo 總公司（iSeries A 位於此處）的一名員工。
- Client C 是任職於 MyCo 子公司（與總公司分處兩地）的一名員工。
- Client D 是在遠地工作並經常出差的一名員工，不論身處何處，他必須能夠安全地存取人力資源網站。
- Clients B、C 和 D 都是存取人力資源應用程式的公司員工。

- Clients B、C 和 D 有一個區域 CA 憑證的複本，它對安裝在其從屬站軟體中的應用程式發出憑證。
- Clients B、C 和 D 在 iSeries A 存取人力資源應用程式，iSeries A 對其從屬站軟體提出其憑證，以驗證其識別身份並起始 SSL 階段作業。
- Clients B、C 和 D 上的從屬站軟體已配置爲接受來自 iSeries A 的憑證，然後 SSL 階段作業開始。
- 在 SSL 階段作業開始之後，在 iSeries A 授予對應用程式及其資源的存取權之前，Clients B、C 和 D 必須提供有效的憑證才行。

先決條件和假設

此實務依據下列先決條件和假設而定：

1. IBM HTTP Server for iSeries 在 iSeries A 執行人力資源應用程式。有兩種類型的 HTTP Server for iSeries（原始和 Apache 驅動），還有一個大幅修改的 HTTP Server 版本將在此資訊發行之後問世。因此，此實務並不提供*特定的*指示來配置 HTTP Server 使用 SSL。此實務提供配置及管理憑證的指示，任何應用程式要使用 SSL 必須有這些憑證。
2. HTTP Server 提供需要憑證進行從屬站鑑別的能力。此實務提供的指示是關於如何使用數位憑證管理程式 (DCM) 來配置此實務的憑證管理基本要求。不過，此實務並不提供爲 HTTP Server 配置憑證從屬站鑑別的*特定*配置步驟。
3. 在 iSeries A 上的人力資源 HTTP Server 已使用密碼保護。
4. iSeries A 符合安裝及使用數位憑證管理程式 (DCM) 的基本要求。
5. 先前沒有人在 iSeries A 配置或使用 DCM。
6. 不論誰在此實務中使用 DCM 執行作業，在其使用者設定檔中都必須擁有 *SECADM 和 *ALLOBJ 特殊權限。
7. iSeries A 沒有安裝 IBM 4758-023 PCI 加密輔助處理器。

作業步驟

您必須完成兩組作業才能實施此實務：一組作業可讓您在 iSeries A 設定人力資源應用程式使用 SSL，並需要憑證進行使用者鑑別。另一組作業可讓 Clients B、C 和 D 上的使用者以人力資源應用程式參與 SSL 階段作業並取得憑證進行使用者鑑別。

人力資源 Web 伺服器應用程式作業步驟

要實施此實務，您必須在 iSeries A 執行這些作業：

1. 完成所有先決條件步驟來安裝和配置所有需要的 iSeries 產品。
2. 配置人力資源 HTTP 伺服器使用 SSL 並記下要用於伺服器實例的應用程式 ID。
3. 使用數位憑證管理程式 (DCM) 建立及操作區域 CA，並用它來發出憑證給人力資源 HTTP 伺服器。此引導作業亦確保您指派憑證給 Web 伺服器應用程式，及新增 CA 到應用程式信任的 CA 清單中。
4. 配置人力資源 Web 伺服器爲需要憑證進行從屬站鑑別。
5. 在 SSL 模式啓動人力資源 HTTP Server。

從屬站配置作業步驟

若要實施此實務，要在 iSeries A 上存取人力資源 Web 伺服器的每一個使用者（Clients B、C 和 D）都必須執行下列這些作業：

6. 讓使用者在其瀏覽器軟體中安裝區域 CA 憑證的複本。

7. 向區域 CA 要求憑證。

配置明細

完成下列作業步驟以使用憑證來配置對內部應用程式和資源的受保護存取，如此實務所述。

步驟 1：完成先決條件作業來安裝所有需要的 iSeries 產品

在您可以執行特定的配置作業來實施此實務之前，您必須先完成安裝和配置所有需要的 iSeries 產品的所有先決條件作業才行。

步驟 2：配置人力資源 HTTP Server 使用 SSL

根據您使用原始或 Apache 驅動版本，對 iSeries A 上的人力資源 HTTP Server 的 Secure Sockets Layer (SSL) 配置步驟並不相同。

關於配置 HTTP Server（原始）使用 SSL 的特定資訊，請參閱在 HTTP Server 上配置安全伺服器。

關於配置 HTTP Server（Apache 驅動）使用 SSL 的特定資訊，請參閱實務：JKL 在 HTTP Server（Apache 驅動）上啓用 Secure Sockets Layer (SSL) 保護。此實務提供建立虛擬主電腦和配置它使用 SSL 的所有作業步驟。關於配置 SSL 的特定步驟，請參閱此標頭：「爲虛擬主電腦啓用 SSL」。

關於配置 HTTP Server for iSeries（原始或 Apache 驅動）的現行版本和未來版本的其餘資訊，請參閱 Web 服務主題。

步驟 3：建立和操作區域 CA

在配置人力資源 HTTP Server 使用 Secure Sockets Layer (SSL) 之後，您必須配置憑證供伺服器用來起始 SSL。根據此實務的目標，您選擇要建立和操作區域認證中心 (CA) 發出憑證給伺服器。

當您使用數位憑證管理程式 (DCM) 建立區域 CA 時，它會引導您完成處理，確保您配置所需的一切來爲應用程式啓用 SSL。這包括指派該區域 CA 發給您的 Web 伺服器應用程式的憑證。此外，您會新增區域 CA 到 Web 伺服器應用程式的 CA 信任清單中。讓區域 CA 出現在應用程式的信任清單上，可確定該應用程式能夠辨識及鑑別使用者，他們提出區域 CA 發出的憑證。

要使用數位憑證管理程式 (DCM) 來建立及操作區域 CA 並發出憑證給人力資源伺服器應用程式，請完成下列這些步驟：

1. 啓動 DCM。
2. 在 DCM 的導覽頁框中，選取**建立認證中心 (CA)** 以顯示一連串套表。這些套表引導您建立區域 CA 及完成其它所需的作業，來開始對 SSL、物件簽署及簽章驗證使用數位憑證。

   註: 如果您對於如何完成本引導作業中的特定套表有問題，請選取問號 (**?**) 按鈕（位於頁頂端）來存取線上說明。

3. 完成此引導作業的套表。在使用這些套表來執行所有必要作業以設定工作的區域認證中心 (CA) 時，您必須：
   a. 提供區域 CA 的識別資訊。
   b. 在 PC 上或瀏覽器中安裝區域 CA 憑證，使軟體可以辨識區域 CA 及驗證區域 CA 發出的憑證。
   c. 選擇區域 CA 的原則資料。

      註: 一定要選取區域 CA 可以發出使用者憑證。
   d. 使用新的區域 CA 發出伺服器或從屬站憑證，供您的應用程式使用於 SSL 連線。
   e. 選取可對 SSL 連線使用伺服器或從屬站憑證的應用程式。

      註: 一定要選取人力資源 HTTP Server 的應用程式 ID。
   f. 使用新的區域 CA 發出物件簽署憑證，應用程式使用該憑證來以數位方式簽署物件。此子作業建立 *OBJECTSIGNING 憑證庫；這是您用來管理物件簽署憑證的憑證庫。

      註: 雖然此實務不使用物件簽署憑證，但一定要完成此步驟。如果您在這個時候取消作業，作業會結束，您必須執行個別作業才能完成 SSL 憑證配置。
   g. 選取應該信任區域 CA 的應用程式。

      註: 一定要選取人力資源 HTTP Server 的應用程式 ID 作爲信任區域 CA 的其中一個應用程式。

既然您已完成 Web 伺服器應用程式要使用 SSL 所需要的憑證配置，您就可以配置 Web 伺服器應用程式爲需要以憑證進行使用者鑑別。

步驟 4：配置人力資源 Web 伺服器為需要以憑證進行從屬站鑑別

根據您使用的應用程式是原始或 Apache 驅動版本，對 iSeries A 上的人力資源 HTTP Server 需要以憑證進行從屬站鑑別的 Secure Sockets Layer (SSL) 配置步驟並不相同。

關於配置 HTTP Server（原始）爲需要以憑證進行從屬站鑑別的其它特定資訊，請參閱在 HTTP Server（原始）上建立保護設定。

關於配置 HTTP Server（Apache 驅動）使用憑證進行從屬站鑑別的特定資訊，請參閱實務：JKL 在 HTTP Server（Apache 驅動）上啓用 Secure Sockets Layer (SSL) 保護。此 HTTP Server 實務提供建立虛擬主電腦和配置它使用 SSL 及憑證進行從屬站鑑別的所有作業步驟。關於配置 SSL 及憑證進行從屬站鑑別的特定步驟，請參閱此標頭：「爲虛擬主電腦啓用 SSL」。

關於配置 HTTP Server for iSeries（原始或 Apache 驅動）的現行版本和未來版本的其餘資訊，請參閱 Web 服務主題。

步驟 5：在 SSL 模式啓動人力資源 Web 伺服器

您可能需要停止並重新啓動 HTTP Server，以確定該伺服器能夠判斷憑證分派是否存在並用它來起始 SSL 階段作業。

要停止及啓動 HTTP Server（原始），請使用「配置與管理」套表並遵循下列步驟：
1. 按一下**管理**。

2. 按一下**管理 HTTP 伺服器**。
3. 選取該伺服器。
4. 在套表上所提供的欄位中輸入可選用的啓動參數。
5. 按一下**啓動**。

註: 當您進行憑證分派時如果該伺服器在執行中，您應該先停止再啓動該伺服器。按一下**重新啓動**不一定確保伺服器能夠在執行時判斷所發生的憑證變更。

要停止及啓動 HTTP Server（Apache 驅動），請使用「配置與管理」套表並遵循下列步驟：

1. 按一下**管理**。
2. 在左邊的功能表上，按一下**一般伺服器管理**之下**管理 HTTP Servers**。
3. 選取您要使用的伺服器，然後按一下**啓動**或**停止**。關於啓動參數的其餘資訊，請參照線上說明。

關於管理 HTTP Server for iSeries（原始或 Apache 驅動）的現行版本和未來版本的其餘資訊，請參閱 Web 服務主題。

這些作業完成後，您就可以在 SSL 模式啓動人力資源應用程式，開始保護它提供的資料的私密性。

步驟 6：讓使用者在其瀏覽器軟體中安裝區域 CA 憑證的複本。

當使用者存取一個提供 Secure Sockets Layer (SSL) 連線的伺服器時，該伺服器提出憑證給使用者的從屬站軟體作爲其識別身份的證明。因此在伺服器可以建立階段作業之前，從屬站軟體必須驗證該伺服器的憑證。若要驗證伺服器憑證，針對發出該伺服器憑證的認證中心 (CA)，從屬站軟體必須能夠存取在本端儲存的憑證複本。如果伺服器提出的憑證是來自公用網際網路 CA，則該使用者的瀏覽器或其它從屬站軟體應該已具有該 CA 憑證的複本。如果像此實務一樣，伺服器提出的憑證是來自專用區域 CA，則每一個使用者必須使用數位憑證管理程式 (DCM) 來安裝區域 CA 憑證的複本。

每一個使用者（Clients B、C 和 D）必須完成下列這些步驟才能取得區域 CA 憑證的複本：

1. 啓動 DCM。
2. 在導覽頁框中，選取**在 PC 上安裝區域 CA 憑證**以顯示一頁畫面，它可讓您下載區域 CA 憑證到瀏覽器中或將它儲存在系統上的一個檔案中。
3. 選取要安裝憑證的選項。本選項下載區域 CA 憑證作爲瀏覽器中的最高授信使用者。這可確定瀏覽器可以與 Web 伺服器（它們使用來自此 CA 的憑證）之間建立安全通信階段作業。瀏覽器將顯示一連串視窗幫助您完成安裝。
4. 按一下**確定**回到數位憑證管理程式首頁。

步驟 7：讓每一個使用者向區域 CA 要求憑證

在前面的步驟中，您配置人力資源 Web 伺服器爲需要以憑證進行使用者鑑別。現在使用者必須提出一個來自區域 CA 的有效憑證，才能獲准存取 Web 伺服器。每一個使用者必須使用數位憑證管理程式 (DCM)，利用**建立憑證**作業取得一個憑證。爲了從區域 CA 取得憑證，區域 CA 原則必須允許 CA 發出使用者憑證。

每一個使用者（Clients B、C 和 D）必須完成下列這些步驟才能取得憑證：

1. 啓動 DCM。

2. 在導覽頁框中，選取**建立憑證**。
3. 選取**使用者憑證**作爲要建立的憑證類型。會顯示一個套表，供您提供憑證的識別資訊。
4. 完成套表並按一下**繼續**。

   註: 如果您對於如何完成本引導作業中的特定套表有問題，請選取問號 (**?**) （位於頁頂端）來存取線上說明。
5. 此時，DCM 使用瀏覽器建立憑證的私密金鑰和公開金鑰。瀏覽器可能顯示一些視窗來引導您完成此程序。請遵循瀏覽器的指示來完成這些作業。在瀏覽器產生金鑰之後，會顯示一確認頁指出 DCM 已建立憑證。
6. 在瀏覽器軟體中安裝新的憑證。瀏覽器可能顯示一些視窗來引導您完成此程序。遵循瀏覽器提供的指示來完成此作業。
7. 按一下**確定**以完成作業。

在處理程序中，數位憑證管理程式會自動使憑證與 iSeries 使用者設定檔產生關聯。

第 5 章 數位憑證概念

在開始使用數位憑證來增強系統和網路安全原則之前，您應該先瞭解它們是什麼以及它們提供什麼樣的安全性優點。

數位憑證是一種數位證明，它驗證憑證擁有者的身份，就像護照一樣。可靠的一方叫作認證中心 (CA)，它發出數位憑證給使用者和伺服器或從屬站應用程式。對 CA 的信任是信任憑證爲有效憑證的基礎。

要了解更多關於數位憑證概念，請複查這些主題：

識別名稱
閱讀本資訊以了解更多有關數位憑證的識別性質。

數位簽章
閱讀本資訊以了解什麼是數位簽章，以及如何運用數位簽章以確定物件完整性。

公開-私密金鑰對
閱讀本資訊以進一步了解與數位憑證相關的安全金鑰。

認證中心 (CA)
閱讀本資訊以進一步了解發出數位憑證的實體：CA。

CRL 位置
閱讀本資訊以了解什麼是憑證廢止清冊 (CRL) 以及它們如何使用於驗證和鑑別憑證的程序中。

憑證庫
閱讀本資訊以了解什麼是憑證庫以及如何使用數位憑證管理程式 (DCM) 來使用它們和它們所包含的憑證。

加密
閱讀本資訊以了解什麼是加密，以及數位憑證如何使用加密功能來提供安全性。

Secure Sockets Layer (SSL)
閱讀本資訊以取得 SSL 的簡短說明。

識別名稱

每一個 CA 都有一個原則來決定 CA 需要什麼識別資訊來發出憑證。有些公用網際網路認證中心可能需要很少資訊，例如名稱和電子郵件位址。其它公用 CA 在發出憑證之前可能需要更多資訊以及需要該識別資訊更嚴格的證明。例如，支援 Public Key Infrastructure Exchange (PKIX) 標準的 CA 可能需要要求端在發出憑證之前透過註冊管理中心 (RA) 驗證識別資訊。因此，如果您打算接受及使用憑證作爲證明，應複查 CA 的識別基本要求，以判斷其基本要求是否適合您的安全性需求。

識別名稱 (DN) 這個術語說明憑證擁有者的識別資訊，是憑證本身的一部份。根據發出憑證的 CA 的識別原則，DN 可包括各種不同資訊。您可以使用數位憑證管理程式 (DCM) 來操作專用認證中心及發出專用憑證。您也可以使用 DCM 來產生憑證的 DN 資訊和金鑰對，公用網際網路 CA 爲您組織發出這些憑證。您可以提供給任一憑證類型的 DN 資訊包括：

- 憑證擁有者的一般名稱
- 組織

- 組織單位
- 城市
- 省/縣
- 國家

當您使用 DCM 發出專用憑證時，可提供該憑證的其它 DN 資訊，包括：
- 版本 4 IP 位址
- 完整網域名稱
- 電子郵件位址

如果您打算使用憑證來配置虛擬專用網路 (VPN) 連線，則此附加資訊非常有用。

數位簽章

電子文件或其它物件上的數位簽章是使用加密形式建立，它相當於書面文件上的個人簽章。數位簽章提供物件起源的證明，並提供一種方法來驗證物件的完整性。數位憑證擁有者使用憑證的私密金鑰來「簽署」物件。物件的接受者使用該憑證的對應公開金鑰來解密簽章，它驗證已簽章物件的完整性並驗證傳送者確實爲來源。

認證中心 (CA) 簽署它發出的憑證。此簽章是由一個資料字串所組成，該字串以認證中心的私密金鑰加密。因此使用者可以使用認證中心的公開金鑰來解密簽章，以驗證憑證上的簽章。

數位簽章是一個電子簽章，這是您或應用程式使用數位憑證的私密金鑰在物件上所建立。物件上的數位簽章提供簽署者（已簽署金鑰的擁有者）的識別與物件起源的唯一電子連結。當您存取包含數位簽章的物件時，可以驗證該物件上的簽章，來驗證物件的來源確實有效（例如，您下載的應用程式確實來自一個獲授權的來源，例如 IBM）。此驗證程序也可讓您判斷該物件在簽署之後是否有任何未獲授權的變更。

數位簽章的運作範例

軟體程式開發者建立了 iSeries 應用程式，他想要透過網際網路分送此應用程式，爲客戶提供一個便利而具成本效益的方式。不過，他知道客戶擔心透過網際網路下載程式有問題是情有可原的，因爲物件僞裝爲合法程式，實際上卻包含有害的程式（例如病毒），像這類的問題越來越多。

因此，他決定以數位方式簽署應用程式，使客戶可以驗證他的公司爲應用程式的合法來源。他使用他從知名公用認證中心取得的數位憑證的私密金鑰來簽署應用程式。然後提供給客戶下載。在下載套裝軟體中他併入用來簽署物件的數位憑證的複本。當客戶下載應用程式套裝軟體時，可使用該憑證的公開金鑰來驗證應用程式上的簽章。此程序可讓客戶識別及驗證應用程式，以及確定應用程式物件的內容在簽署之後未曾改變。

公開-私密金鑰對

每一個數位憑證都有一對相關聯的加密金鑰。這一對金鑰是由一個私密金鑰和一個公開金鑰所組成。（簽章驗證憑證是此規則的一個例外，它們只有相關聯的公開金鑰）。

公開金鑰是擁有者數位憑證的一部份，任何人都可以使用。不過，私密金鑰受金鑰擁有者的保護，而且只有該擁有者可以使用。這項限制存取可確保使用此金鑰的通信的安全。

憑證擁有者可使用這些金鑰來利用金鑰提供的加密安全特性的優點。例如，憑證擁有者可使用憑證的私密金鑰來「簽署」及加密在使用者和伺服器之間傳送的資料，例如訊息、文件和程式碼物件。然後已簽署物件的接受者可使用簽署者的憑證中所包含的公開金鑰來解密簽章。這種數位簽章確保物件起源的可靠性並提供一種方法來檢查物件的完整性。

認證中心 (CA)

「認證中心」(CA) 是一個可靠的的中央管理實體，可以發出數位憑證給使用者和伺服器。CA 的公信力是憑證被視爲有效證明的信任基礎。 CA 使用其私密金鑰在它發出的憑證上建立數位簽章，來驗證憑證的來源。其他人可以使用 CA 憑證的公開金鑰來驗證 CA 發出和簽署的憑證的確實性。

CA 可以是一個公開的商業實體，例如 VeriSign，或是組織內部操作的一個專用實體。有數種行業提供商用「認證中心」服務供網際網路使用者使用。「數位憑證管理程式」(DCM) 可讓您管理來自公用和專用 CA 的憑證。

另外，您可以使用 DCM 來操作自己的專用 CA，以發出專用憑證給系統和使用者。當 CA 發出使用者憑證時，DCM 會自動結合憑證和使用者的 iSeries 系統使用者設定檔。這確保憑證的存取權和授權與擁有者的使用者設定檔相同。

最高授信使用者狀態

最高授信使用者是指給予「認證中心」憑證的一種特殊稱呼。此最高授信使用者稱呼可讓瀏覽器或其他應用程式鑑別和接受此「認證中心」(CA) 所發出的憑證。

當您下載一個「認證中心」的憑證到瀏覽器時，瀏覽器可讓您指定它做爲最高授信使用者。其他支援使用憑證的應用程式也必須先配置爲信任 CA，才能鑑別和信任特定 CA 所發出的憑證。

您可以使用 DCM 來啓用或停用憑證庫中一個「認證中心」(CA) 憑證的信任狀態。當您啓用 CA 憑證時，您可以指定應用程式可使用此憑證來鑑別和接受此 CA 發出的憑證。當您停用 CA 憑證時，您無法指定應用程式可使用此憑證來鑑別和接受此 CA 發出的憑證。

認證中心原則資料

當您使用「數位憑證管理程式」來建立「認證中心」(CA) 時，您可以指定 CA 的原則資料。CA 的原則資料說明其具備的簽署權。原則資料決定：

- CA 是否可以發出和簽署使用者憑證。
- CA 發出的憑證的有效期限。

憑證廢止清冊 (CRL) 位置

憑證廢止清冊 (CRL) 是一個檔案，它列示特定的認證中心 (CA) 的所有無效及撤回的憑證。 CA 定期更新其 CRL 並使它們可供其他人公佈在輕裝備目錄存取通信協定 (LDAP) 目錄中。少數 CA（例如芬蘭的 SSH）自己在 LDAP 目錄中公佈 CRL 供您直接存取。如果 CA 公佈自己的 CRL，則該憑證會以 Uniform Resource Identifier (URI) 形式併入一個 CRL 分送點副檔名來表示。

數位憑證管理程式 (DCM) 可讓您定義及管理 CRL 位置資訊以確定對您使用的或您從其他人接受的憑證進行更嚴格的鑑別。 CRL 位置定義說明儲存 CRL 的輕裝備目錄存取通信協定 (LDAP) 伺服器的位置及存取資訊。

執行憑證鑑別的應用程式爲特定的 CA 存取 CRL 位置（如果有定義它的話），以確定該 CA 未撤回特定憑證。 DCM 可讓您定義及管理 CRL 位置資訊，應用程式在憑證鑑別期間執行 CRL 處理程序時需要此資訊。可能執行 CRL 處理程序的應用程式和程序範例包括：虛擬專用網路 (VPN) 網際網路金鑰資料交換 (IKE) 伺服器、Secure Sockets Layer (SSL) 型應用程式以及物件簽署程序。此外，當您定義 CRL 位置並使它與 CA 憑證產生關聯時， DCM 會執行 CRL 處理程序，這是爲指定的 CA 發出的憑證驗證程序的一部份。

憑證庫

憑證庫是一個特殊金鑰資料庫檔案，數位憑證管理程式 (DCM) 使用它來儲存數位憑證。除非您選擇使用 4758 加密輔助處理器來儲存金鑰，否則憑證庫亦包含憑證的私密金鑰。 DCM 可讓您建立及管理數種類型的憑證庫。 DCM 透過密碼以及構成憑證庫的 IFS 目錄和 IFS 檔案的存取控制來控制憑證庫的存取。

憑證庫基於它們包含的憑證類型加以分類。您可以爲每一個憑證庫執行的管理作業因憑證庫包含的憑證類型而異。 DCM 提供下列預先定義的憑證庫供您建立和管理：

區域認證中心 (CA)
如果您建立區域 CA，DCM 將使用此憑證庫來儲存區域 CA 憑證及其私密金鑰。您可以使用此憑證庫中的憑證來簽署您使用區域 CA 發出的憑證。當區域 CA 發出憑證時，DCM 會在適當的憑證庫（例如 *SYSTEM）放置一份 CA 憑證的複本（不含私密金鑰）作爲鑑別用途。應用程式使用 CA 憑證來驗證它們必須驗證的憑證的起源，這是對資源授權的 SSL 協議的一部份。

***SYSTEM**
DCM 提供此憑證庫來管理伺服器或從屬站憑證，應用程式使用這些憑證來參與 Secure Sockets Layer (SSL) 通信階段作業。 IBM iSeries 應用程式（以及許多其它軟體程式開發者的應用程式）被撰寫成僅使用 *SYSTEM 憑證庫中的憑證。當您使用 DCM 建立區域 CA 時，DCM 會建立此憑證庫，這是該程序的一部份。當您選擇從公用 CA（例如 VeriSign）取得憑證供伺服器或從屬站應用程式使用時，必須建立此憑證庫。

***OBJECTSIGNING**
DCM 提供此憑證庫來管理您用來以數位方式簽署物件的憑證。此外，此憑證庫中的作業可讓您在物件上建立數位簽章以及檢視和驗證物件上的簽章。當您使用 DCM 建立區域 CA 時，DCM 會建立此憑證庫，這是該程序的一部份。當您選擇從公用 CA（例如 VeriSign）取得憑證來簽署物件時，必須建立此憑證庫。

***SIGNATUREVERIFICATION**

DCM 提供此憑證庫來管理您用以驗證物件上的數位簽章確實性的憑證。若要驗證數位簽章，此憑證庫必須包含簽署該物件的憑證複本。憑證庫也必須包含發出物件簽署憑證的 CA 的 CA 憑證的複本。您取得這些憑證的方式是在現行系統上匯出物件簽署憑證，或匯入您從物件簽署者接收的憑證。

其它系統憑證庫

此憑證庫提供替代儲存體位置，來儲存您使用於 SSL 階段作業的伺服器或從屬站憑證。其它系統憑證庫是使用者定義來儲存 SSL 憑證的次要憑證庫。其它系統憑證庫選項可讓您管理您或其他人撰寫的應用程式的憑證，這些應用程式使用 SSL_Init API，以程式設計方式存取及使用憑證來建立 SSL 階段作業。此 API 可讓應用程式使用憑證庫的預設憑證，而不是您特別識別的憑證。通常，您從舊版 DCM 移轉憑證時會使用此憑證庫，或建立特殊憑證子集供 SSL 使用。

註: 如果您在 iSeries 伺服器上安裝了 4758 PCI 加密輔助處理器，您可以爲憑證選擇其它的私密金鑰儲存體選項（但物件簽署憑證例外）。您可以選擇將私密金鑰儲存在輔助處理器本身，或使用輔助處理器加密私密金鑰，並將它儲存在特殊金鑰檔而非儲存在憑證庫中。

DCM 透過密碼控制憑證庫的存取。 DCM 亦維護構成憑證庫的整合檔案系統目錄及檔案的存取控制。區域認證中心 (CA)、*SYSTEM、 *OBJECTSIGNING 和 *SIGNATUREVERIFICATION 憑證庫必須位於整合檔案系統內的特定路徑上，其它系統憑證庫可位於整合檔案系統的任何地方。

加密

加密是保護資料安全的一種專門技巧。加密可讓您在儲存資訊或與其他人通信時，防止未參與的第三者瞭解儲存的資訊或通信內容。加密將可瞭解的文字轉換成難以理解的資料（密碼文字）。解密將無法理解的資料回復成可瞭解的文字。這兩種程序涉及數學公式或演算法，以及一連串機密資料（金鑰）。

加密有兩種類型：

- 在**共用或密碼鎖（對稱的）**加密中，金鑰是通信雙方之間的共用密鑰。加密和解密都使用相同的金鑰。
- 在**公開金鑰（不對稱）**加密中，加密和解密各使用不同的金鑰。一方有一對金鑰，由一個公開金鑰和一個私密金鑰組成。公開金鑰可自由分送，通常放在數位憑證內，而私密金鑰則由擁有者私下保存。這兩個金鑰在數學運算上有其相關性，但實際上不可能從公開金鑰導出私密金鑰。以某人的公開金鑰來加密的物件，例如一則訊息，只能使用相關的私密金鑰來解密。另外，伺服器或使用者可以使用私密金鑰來「簽署」物件，接收者可以使用對應的公開金鑰來解密數位簽章，以驗證物件的來源和完整性。

Secure Sockets Layer (SSL)

由 Netscape 開發的 Secure Sockets Layer (SSL) 是從屬站和伺服器之間的階段作業加密的業界標準。 SSL 使用不對稱或公開金鑰加密來加密伺服器和從屬站之間的階段作業。從屬站和伺服器應用程式在交換數位憑證期間，協調此階段作業金鑰。金鑰會在 24 小時之後自動到期，SSL 處理程序會爲每一個伺服器連線和每一個從屬站建立不同的金鑰。因此，即使未授權的使用者截取並解密階段作業金鑰（不太可能），仍然無法使用它來竊聽後來的階段作業。

第 6 章 DCM 的規劃

若要使用「數位憑證管理程式」(DCM) 來有效管理公司的數位憑證，則對於您在安全原則中將如何使用數位憑證方面，您必須有一個全盤的規劃。

關於如何規劃使用 DCM 及深入瞭解數位憑證如何配合您的安全原則，請複查這些主題：

使用 DCM 的基本要求
請閱讀本資訊來瞭解您必須安裝的軟體，以及設定您的系統來使用 DCM 的其他必要資訊。

數位憑證的類型
請閱讀本資訊來瞭解您可以使用 DCM 來管理的不同憑證類型。

公用憑證與專用憑證
一旦您決定如何使用憑證來發揮其提供的附加安全性，請閱讀本資訊來瞭解如何決定最符合企業需求的憑證類型。您可以使用來自於公用 CA 的憑證，或建立和操作一個專用 CA 來發出憑證。您選擇取得憑證的方式是根據您規劃的用途而定。

Secure Sockets Layer (SSL) 通信的數位憑證
請閱讀本資訊來瞭解如何使用憑證，使您的應用程式能夠建立安全通信階段作業。

使用者鑑別的數位憑證
請閱讀本資訊來瞭解如何使用憑證來對存取 iSeries 伺服器資源的使用者提供一種更強化的鑑別方法。

鑑別虛擬專用網路 (VPN) 連線的數位憑證
請閱讀本資訊來瞭解如何在配置虛擬專用網路 (VPN) 連線時使用憑證。

簽署物件的數位憑證
請閱讀本資訊來瞭解如何使用憑證來確保物件的完整性，或驗證物件的數位簽章以驗證其確實性。

驗證物件簽章的數位憑證
請閱讀本資訊來瞭解如何使用憑證來驗證物件的數位簽章，以驗證其確實性。

DCM 設定基本要求

數位憑證管理程式 (DCM) 是一個免費的 iSeries 特性，可讓您集中管理應用程式的數位憑證。要順利使用 DCM，請確定您有執行下列步驟：

- 安裝密碼存取提供者授權程式 (5722-AC3)。此加密產品基於進出口規定，決定密碼演算法所允許的最大金鑰長度。在建立憑證之前，您必須安裝此產品。
- 安裝 OS/400 的選項 34。這是瀏覽器型 DCM 特性。
- 安裝 IBM HTTP Server for iSeries (5722-DG1) 並啓動 *ADMIN 伺服器實例。
- 確定系統上已配置 TCP，使您可以使用 Web 瀏覽器和 HTTP Server *ADMIN 案例來存取 DCM 特性。

註: 除非您安裝所有必要的產品，否則無法建立憑證。如果未安裝必要的產品，DCM 會顯示錯誤訊息，指示您安裝缺少的元件。

數位憑證的類型

數位憑證分成幾類。這些分類說明憑證的用途。您可以使用「數位憑證管理程式」(DCM) 來管理下列憑證類型：

認證中心 (CA) 憑證

「認證中心」憑證是一種數位證明，用來驗證擁有憑證的「認證中心」的身份。「認證中心」的憑證包含「認證中心」的識別資訊及其公開金鑰。其他人可以使用 CA 憑證的公開金鑰來驗證 CA 發出和簽署的憑證的確實性。「認證中心」憑證可以由另一個 CA 來簽署，例如 VeriSign，如果是獨立的實體，則可以自己簽署。您在「數位憑證管理程式」中建立的 CA 是一個獨立的實體。其他人可以使用 CA 憑證的公開金鑰來驗證 CA 發出和簽署的憑證的確實性。若要在 SSL 上使用憑證、用來簽署物件或驗證物件簽章，則對於發出憑證的 CA，您必須有一份此 CA 的 CA 憑證複本。

伺服器憑證或從屬站憑證

伺服器或從屬站憑證是一種數位證明，用來識別在安全通信上使用憑證的伺服器或從屬站應用程式的身份。伺服器或從屬站憑證包含擁有此應用程式之組織的識別資訊，例如系統的識別名稱。憑證亦包含系統的公開金鑰。伺服器必須具有數位憑證，才能在安全通信上使用 Secure Sockets Layer (SSL)。支援數位憑證的應用程式可以檢查伺服器的憑證，在從屬站存取伺服器時驗證伺服器的身份。然後，應用程式可以使用憑證的鑑別，當做在從屬站和伺服器之間起始一個 SSL 加密階段作業的基礎。您只能從 *SYSTEM 憑證庫來管理這些憑證類型。

物件簽署憑證

物件簽署憑證是您以數位方式來「簽署」物件所用的一種憑證。經由簽署物件，您提供一種方法來驗證物件的完整性和物件的來源或所有權。您可以使用憑證來簽署各種物件，包括「整合檔案系統」 (IFS) 中的大部份物件和 *CMD 物件。您可以在「物件簽署」和「簽章驗證」主題中找到完整的可簽署物件清單。當您使用物件的簽署憑證的私密金鑰來簽署物件時，物件的接收者必須有權限來存取一份對應的簽章驗證憑證，才能適當地鑑別物件簽章。您只可以從 *OBJECTSIGNING 憑證庫來管理這些憑證類型。

簽章驗證憑證

簽章驗證憑證是一份不含憑證私密金鑰的物件簽署憑證。您可使用簽章驗證憑證的公開金鑰來鑑別以物件簽署憑證所建立的數位簽章。驗證簽章可讓您判斷物件的來源，以及物件在簽署之後是否遭到改變。您只可以從 *SIGNATUREVERIFICATION 憑證庫來管理這些憑證類型。

使用者憑證

使用者憑證是一種數位證明，用來驗證擁有憑證的從屬站或使用者的身份。許多應用程式現在都支援讓您使用憑證來鑑別資源的使用者，以代替使用者名稱和密碼。「數位憑證管理程式」(DCM) 會自動使您的專用 CA 發出的使用者憑證與使用者的iSeries 使用者設定檔產生關聯。您也可以使用 DCM 來使其他「認證中心」發出的使用者憑證與使用者的 iSeries 使用者設定檔產生關聯。

當您使用「數位憑證管理程式」(DCM) 來管理憑證時， DCM 會按照這些分類來組織憑證，並且將憑證及其相關的私密金鑰放入憑證庫中。

註: 如果您已安裝一個 IBM 4758 PCI 加密輔助處理器在 iSeries 伺服器上，則您可以爲憑證選擇其他私密金鑰儲存選項（物件簽署憑證除外）。您可以選擇將私密金鑰儲存在輔助處理器本身。或者，您可以使用輔助處理器來加密私密金鑰，並儲存在特殊金鑰檔中，而不要放入憑證庫中。不過，使用者憑證及其私密金鑰是儲存在使用者系統上的瀏覽器軟體或檔案中，供其他從屬站套裝軟體使用。

公用憑證與專用憑證

一旦您決定使用憑證，就應該選擇最適合您安全性需求的憑證施行類型。您取得憑證的選擇有：

- 向公用網際網路認證中心 (CA) 購買憑證。
- 操作自己的 CA 來發出專用憑證給使用者和應用程式。
- 使用來自公用網際網路 CA 與您自己的 CA 的憑證組合。

要選擇哪一個施行選項取決於一些因素，其中最重要的一個因素是使用憑證的環境。以下一些資訊可幫助您決定哪一個施行選項最適合您的企業和安全性需求。

使用公用憑證

公用網際網路 CA 發出憑證給有給付必要款項的每一個人。不過，在發出憑證之前網際網路 CA 仍需要一些識別證明。但根據 CA 的識別原則，此證明等級並不相同。在決定要向 CA 取得憑證或信任它發出的憑證之前，您應該評估 CA 的識別原則的嚴格性是否適合您的安全性需求。隨著 Public Key Infrastructure for X.509 (PKIX) 標準發展出來後，現在有一些較新的公用 CA 在發出憑證方面提供更嚴格的識別標準。由於向這類 PKIX CA 取得憑證的程序越來越複雜，CA 發出的憑證能提供更多保證，來保護特定使用者對應用程式的存取。數位憑證管理程式 (DCM) 可讓您使用及管理來自 PKIX CA 的憑證，它們使用這些新的憑證標準。

您也必須考慮使用公用 CA 發出憑證的相關成本。如果您需要將憑證發出給數量有限的伺服器或從屬站應用程式和使用者，則成本對您而言可能不是一項重要因素。不過，如果您有大量的私密使用者需要公用憑證來進行從屬站鑑別，則成本顯得特別重要。在此案例中，要將伺服器應用程式配置爲只接受公用 CA 發出的特定憑證子集，其所需的管理和程式設計成本也應考慮在內。

使用來自公用 CA 的憑證可節省您的時間和資源，因爲許多伺服器、從屬站和使用者應用程式都配置成能夠辨識大部份知名的公用 CA。而且，和您專用 CA 發出的憑證相比，其它公司和使用者可能比較能夠辨識和信任知名公用 CA 發出的憑證。

使用專用憑證

如果您建立自己的區域 CA，則可以發出憑證給有限定範圍的系統和使用者，例如在您公司或組織之內。建立和維護您自己的 CA 可讓您只發出憑證給本身是您群組的可靠成員的那些使用者。這提供更佳的安全性，因爲您可以更嚴格地控制誰擁有憑證，以及誰可以存取您的資源。維護您自己的區域 CA 可能有一個缺點，就是您必須投資時間和資源。不過，數位憑證管理程式 (DCM) 幫您簡化此程序。

當您使用區域 CA 發出憑證給使用者以進行從屬站鑑別時，您應該決定是否讓使用者的憑證與 iSeries 使用者設定檔產生關聯。如果您想要讓使用者的憑證與 iSeries 使用者設定檔產生關聯，您可以讓使用者透過 DCM 從區域 CA 取得其憑證。或者，從 V5R2 開始，您可以使用 API 以程式設計方式發出憑證給非 iSeries 使用者，讓這些使用者不必擁有 iSeries 使用者設定檔就可以使用專用憑證來進行從屬站鑑別。

註: 不論您使用哪一個 CA 發出憑證，系統管理者都會控制其系統上的應用程式應該信任哪些 CA。如果可在您瀏覽器上找到某知名 CA 的憑證複本，則您的瀏覽器可設定爲信任該 CA 發出的伺服器憑證。不過，如果該 CA 憑證不在 *SYSTEM 憑證庫，則您的伺服器無法信任該 CA 發出的使用者或從屬站憑證。要信任 CA 發出

的使用者憑證，您必須向該 CA 取得 CA 憑證複本。它必須是正確的檔案格式，而且您必須將該憑證加入自己的 DCM 憑證庫中。

您也許會發現，複查一些常用的憑證使用實務非常有用，因爲它們可幫助您選擇使用公用或專用憑證才是最適合您的企業和安全性需求。

相關作業

在決定您要如何使用憑證以及要使用的類型之後，請複查這些程序，進一步了解如何使用數位憑證管理程式將您的計劃付諸實現：

- 建立和操作專用 CA，說明萬一您選擇操作 CA 來發出專用憑證時所必須執行的作業。
- 管理來自公用網際網路 CA 的憑證，說明您要使用來自知名公用 CA（包括 PKIX CA）的憑證時必須執行的作業。
- 在其它 iSeries 伺服器上使用區域 CA，說明如果您想要在不止一個系統上使用來自專用 CA 的憑證時必須執行的作業。

用於 SSL 安全通信的數位憑證

您可以使用數位憑證，配置應用程式使用 Secure Sockets Layer (SSL) 來進行安全通信階段作業。爲了建立 SSL 階段作業，伺服器一律提供其憑證複本給要求連線的從屬站驗證。使用 SSL 連線：

- 向從屬站或一般使用者保證您的網站是可靠的。
- 提供加密通信階段作業以確定透過連線傳送的資料保有私密性。

伺服器和從屬站應用程式以下列方式共同運作，確保資料安全：

1. 伺服器應用程式提供憑證給從屬站（使用者）應用程式作爲伺服器識別身份的證明。
2. 從屬站應用程式根據發出的認證中心憑證複本來驗證伺服器的識別身份。（從屬站應用程式對於本端儲存的相關 CA 憑證複本必須有存取權限。）
3. 伺服器和從屬站應用程式對於加密的對稱金鑰取得一致意見，並使用它來加密通信階段作業。
4. 選用性地，在容許存取所要求的資源之前，現在伺服器可以要求從屬站提供識別證明。要使用憑證作爲識別證明，通信應用程式必須支援使用憑證進行使用者鑑別。

SSL 在 SSL 交握式處理程序中使用不對稱金鑰（公開金鑰）演算法來協議一個對稱金鑰，該特定 SSL 階段作業後續將用它來加密和解密應用程式的資料。這表示伺服器和從屬站對每一個連線使用不同的階段作業金鑰，它在一段指定時間之後會自動到期。萬一（不太可能發生）有人截取及解密某特定階段作業金鑰，該階段作業金鑰就無法用來推論任何未來的金鑰。

用於使用者鑑別的數位憑證

傳統上，使用者是基於其使用者名稱和密碼，從應用程式或系統接收對資源的存取權限。您可以在許多伺服器應用程式和使用者之間使用數位憑證（而非使用者名稱和密碼）來鑑別及授權階段作業，進一步增加系統安全性。而且，您可以使用數位憑證管理程式 (DCM)，使某使用者的憑證與該使用者的 iSeries 使用者設定檔產生關聯。然後，該憑證與相關聯的設定檔即擁有相同的授權和許可權。從 V5R2 開始，您可以使用 API

以程式設計方式使用專用區域認證中心發出憑證給非 iSeries 使用者。當您不希望使用者擁有 iSeries 使用者設定檔時，這些 API 提供您能力發出專用憑證給這些使用者。

數位憑證是一種電子證明，它驗證提出它的人的眞實身份。就這點而言，憑證類似護照。兩者均建立個人識別身份，包含識別用的唯一號碼，而且有一個被認可的發行中心來驗證此證明非假冒。就憑證而言，認證中心 (CA) 是作爲可靠的第三者，它發出憑證並驗證它爲非假冒的證明。

憑證利用公開金鑰和相關的私密金鑰來進行鑑別。發出憑證的 CA 連結這些金鑰以及其它關於憑證擁有者的資訊與憑證本身來進行識別。

現在有越來越多的應用程式支援在 SSL 階段作業期間使用憑證來進行從屬站鑑別。目前，這些 iSeries 應用程式提供從屬站鑑別憑證支援：

- Telnet 伺服器
- IBM HTTP 伺服器（原始和 Apache 驅動）
- 目錄服務 (LDAP)
- 管理中心
- Client Access Express（包括 iSeries 領航員）
- FTP 伺服器

假以時日，其它的應用程式可能提供從屬站鑑別憑證支援；請複查特定應用程式的文件以判斷它們是否提供此支援。

憑證可以提供更強大的方法來鑑別使用者，其原因如下：

- 個人可能會忘記他或她的密碼。因此，使用者必須背下或記下他們的使用者名稱和密碼以確定他們不會忘記。所以，未獲授權的使用者可能更容易向授權使用者取得使用者名稱和密碼。因爲憑證是儲存在檔案或其它電子位置，所以由從屬站應用程式（而非使用者）處理存取及提供憑證來鑑別。這可確保使用者較不可能與未獲授權的使用者共用憑證，除非未獲授權的使用者對使用者的系統有存取權限。同時，憑證可以安裝在智慧型卡片上，作爲另一種保護方法，避免憑證被未獲授權者使用。
- 憑證包含的私密金鑰在識別時絕不會隨憑證一起傳送。相反地，在加密和解密處理程序中，系統會使用此金鑰。其他人可以使用憑證的對應公開金鑰來驗證以該私密金鑰簽署的物件的傳送者的識別身份。
- 許多系統需要長度在 8 字元以內的密碼，這使得這些密碼更容易被猜到。憑證的加密金鑰長達數百個字元。此長度以及它們的隨機性質，使加密金鑰比密碼更難被猜到。
- 數位憑證金鑰提供密碼無法提供的數種可能用法，例如資料完整性和私密性。您可以使用憑證及其相關金鑰來：
  - 偵測資料的變更以確保資料完整性。
  - 證明確實執行某特定動作。這稱爲無可否認性。
  - 確定資料轉送的私密性，使用 Secure Sockets Layer (SSL) 來加密通信階段作業。

要進一步了解關於配置 iSeries 伺服器應用程式使用憑證，以便在 SSL 階段作業期間進行從屬站鑑別，請參閱以 SSL 保護應用程式。

用於 VPN 連線的數位憑證

您可以使用數位憑證作爲建立 iSeries 虛擬專用網路 (VPN) 連線的一種方法。在啓動連線之前，動態虛擬專用網路 (VPN) 連線的兩端點都必須能夠鑑別對方。端點鑑別是由網際網路金鑰資料交換 (IKE) 伺服器在每一端完成。順利完成鑑別之後，IKE 伺服器會協議加密法及演算法來保護虛擬專用網路 (VPN) 連線。

在 V5R1 之前，IKE 伺服器只能透過預先共用的金鑰來鑑別對方。使用預先共用金鑰比較不安全，因爲您必須手動地將此金鑰傳遞給 VPN 另一端點的管理者。因此，在傳遞金鑰的過程中，該金鑰有可能外曝給其他人知道。

您可以使用數位憑證鑑別端點代替使用預先共用金鑰來避開此風險。 IKE 伺服器可以鑑別另一個伺服器的憑證，建立連線來協議加密法和演算法，讓伺服器用來保護連線。

您可以使用數位憑證管理程式 (DCM) 來管理 IKE 伺服器用來建立動態虛擬專用網路 (VPN) 連線的憑證。您必須先決定是否要對 IKE 伺服器使用公用憑證與發出專用憑證。

有些虛擬專用網路 (VPN) 需要憑證除了標準識別名稱資訊之外還包含替代的主旨名稱資訊，例如網域名稱或電子郵件位址。當您使用 DCM 公用程式的專用 CA 發出憑證時，您可以指定該憑證的替代主旨名稱資訊。指定此資訊可確定 iSeries 虛擬專用網路 (VPN) 連線與需要它來鑑別的其它 VPN 施行相容。

要進一步了解如何管理虛擬專用網路 (VPN) 連線的憑證，請複查這些資源：

- 如果您以前未曾使用過 DCM 來管理憑證，則這些主題可幫助您入門：
  - 建立及操作區域、專用 CA，說明如何使用 DCM 發出應用程式的專用憑證。
  - 從公用網際網路 CA 管理憑證，說明如何使用 DCM 來處理來自公用 CA 的憑證。
- 如果您目前使用 DCM 管理其它應用程式的憑證，請複查這些資源，以了解如何指定應用程式使用現有的憑證以及應用程式可接受及鑑別哪些憑證：
  - 管理應用程式的憑證分派，說明如何使用 DCM 指派現有的憑證給應用程式，例如 IKE 伺服器。
  - 定義應用程式的 CA 信任清單，說明當應用程式接受用於從屬站（或 VPN）鑑別的憑證時如何指定應用程式可以信任的 CA。

用於簽署物件的數位憑證

從 V5R1 開始，OS/400 支援使用憑證以數位方式「簽署」物件。以數位方式簽署物件提供一種方法驗證物件內容及其原始來源的完整性。物件簽署支援加強傳統 iSeries 系統工具，來控制誰可以變更物件。當物件透過網際網路或其它不可靠的網路傳輸時，或當物件儲存在非 iSeries 系統上時，傳統控制無法保護物件使它免遭未獲授權者擅改。此外，傳統控制無法每次都判斷出物件是否遭到未獲授權者變更或擅改。在物件上使用數位簽章能提供一個可靠的方法，來偵測已簽署物件的變更。

在物件上加上數位簽章是使用憑證的私密金鑰在物件中加入資料的加密算術總和。簽章保護資料免遭未獲授權者變更。物件及其內容並未加密，且由數位簽章保持其私密性；不過，總和本身有加密以防止未獲授權者變更它。若有人想要確定該物件在傳輸時未被變更以及該物件是來自一個被接受的合法來源，他可以使用簽署憑證的公開金鑰來驗證原始數位簽章。如果簽章不再相符，表示資料已被改變。在這種情況下，接受者可避免使用該物件，並聯絡簽章者以取得已簽署物件的另一個複本。

如果您覺得使用數位簽章適合您的安全性需求和原則，您應該評估是否要使用公用憑證與發出專用憑證。如果您想要分送物件給一般大眾的使用者，您應考慮使用來自知名公用認證中心 (CA) 的憑證來簽署物件。使用公用憑證確保他人能輕易且花費不多地驗證您對分送給他們的物件上所加的簽章。不過，如果您打算只在組織內分送物件，可使用數位憑證管理程式 (DCM) 操作您自己的區域 CA 來發出憑證給簽署物件。使用來自區域 CA 的專用憑證簽署物件比購買來自知名公用 CA 的憑證更便宜。

物件上的簽章代表簽署該物件的系統，而不是該系統上的特定使用者（不過該使用者必須有適當的權限才能對簽署物件使用憑證）。您使用數位憑證管理程式 (DCM) 來管理您用來簽署物件及驗證物件簽章的憑證。您也可以使用 DCM 簽署物件及驗證物件簽章。

驗證物件簽章的數位憑證

從 V5R1 開始，iSeries 支援使用憑證來驗證物件的數位簽章。任何人如果想要確保已簽署的物件在傳送期間未遭到改變，且物件來自於一個可接受的合法來源，皆可以使用簽署憑證的公開金鑰來驗證原始數位簽章。如果簽章不相符，則表示資料可能已被改變。在此情況下，接受者可以避免使用此物件，並可連絡簽署者來取得另一份已簽署的物件複本。

物件上的簽章代表簽署此物件的系統，並不是該系統上的特定使用者。在驗證數位簽章的過程中，您必須決定您信任的「認證中心」以及您信任用來簽署物件的憑證。當您選擇信任某個 CA 時，您可以選擇是否信任某人以此 CA 所發出的憑證來建立的簽章。當您選擇不信任某個 CA 時，也就是不信任此 CA 發出的憑證或某人以這些憑證所建立的簽章。

驗證物件復置 (QVFYOBJRST) 系統值

如果您決定執行簽章驗證，您必須做的其中一個重要決定就是決定簽章對於要復置到系統中的物件有多麼重要。您可以使用系統值 QVFYOBJRST 來控制。此系統值的預設設定允許復置未簽署的物件，但確保唯有當物件具備有效簽章時才可以復置已簽署的物件。只有當物件具備您的系統所信任的簽章時，系統才會將物件定義成已簽署；系統會忽略物件上的其他「不信任」簽章，將物件視爲尚未簽署。

有數個值適用於 QVFYOBJRST 系統值上，範圍從忽略全部簽章到對於系統復置的全部物件都要求有效簽章。此系統值只影響要復置的可執行物件，不影響儲存檔或 IFS 檔案。關於使用此值和其他系統值的詳細資訊，請參閱「資訊中心」的系統值搜尋器。

您可以使用「數位憑證管理程式」(DCM) 來實作您的憑證和 CA 信任決策，以及管理您用來驗證物件簽章的憑證。您也可以使用 DCM 來簽署物件和驗證物件簽章。

第 7 章 配置 DCM

「數位憑證管理程式」(DCM) 提供一個瀏覽器使用者介面，可讓您用來管理應用程式和使用者的數位憑證。使用者介面分爲兩個主要頁框：導覽頁框和作業頁框。

您可以使用導覽頁框來選取管理憑證的作業或使用憑證的應用程式。有些個別作業會直接出現在主要導覽頁框中，導覽頁框內的大部份作業會分類。例如，**管理憑證**就是一個作業種類，包含各種個別引導作業，例如「檢視憑證」、「更新憑證」、「匯入憑證」等。如果導覽頁框中有一個項目是種類，且包含一個以上的作業，則其左邊會顯示一個箭頭。箭頭表示當您選取此種類鏈結時，將顯示一個展開的作業清單，讓您選擇想要執行的作業。

除了**捷徑**種類以外，導覽頁框中的每一個作業皆爲引導作業，可讓您經由一連串步驟，快速簡單地完成作業。「捷徑」種類提供一組憑證和應用程式管理功能，可讓有經驗的 DCM 使用者快速地從集中頁存取各種相關作業。

導覽頁框中可用的作業視您使用的憑證庫而定。您在導覽頁框中看到的種類和作業數，也是根據您的 iSeries 使用者設定檔具備的授權而定。至於操作 CA、管理應用程式使用的憑證等所有作業以及其他系統層次作業，只有 iSeries 安全主管或管理者才能夠使用。安全主管或管理者必須具備 *SECADM 和 *ALLOBJ 特殊權限，才能夠檢視和使用這些作業。沒有這些特殊權限的使用者只能存取使用者憑證功能。

要了解如何配置 DCM 及開始使用它來管理憑證，請複查這些主題：

啓動 DCM
請閱讀本資訊來瞭解如何存取 iSeries 提供的「數位憑證管理程式」功能。

第一次設定憑證
請閱讀本資訊來瞭解如何開始使用 DCM 來設定首次使用憑證時所需的一切。瞭解如何開始管理來自於公用網際網路「認證中心」(CA) 的憑證，或如何建立和操作專用「區域」CA 來發出憑證。

如果您想知道更多關於在網際網路環境中使用數位憑證來強化系統和網路安全性的資訊，VeriSign 網站是一個相當不錯的資源。VeriSign 網站在數位憑證方面提供豐富的檔案庫，也提供其他許多關於網際網路安全性的主題。

您可以存取其 VeriSign 說明平台  上的檔案庫。

啓動數位憑證管理程式

在您可以使用它的任何功能之前，您需要先啓動數位憑證管理程式 (DCM)。請完成這些作業以確定您可以順利啓動 DCM：

1. 安裝 5722 SS1 選項 34。這就是數位憑證管理程式 (DCM)。

   安裝 5722 DG1。這是 IBM HTTP Server for iSeries。

   安裝 5722 AC3。這是 V5R2 DCM 用來產生憑證的公開-私密金鑰對的加密產品，來加密匯出的憑證檔及解密匯入的憑證檔。
2. 使用 iSeries 領航員啓動 HTTP Server *ADMIN 案例：
   a. 啓動 **iSeries 領航員**。

b. 在主要樹狀檢視畫面上連按兩下 iSeries 伺服器。
c. 連按兩下**網路**。
d. 連按兩下**伺服器**。
e. 連按兩下 **TCP/IP**。
f. 以滑鼠右鍵按一下 **HTTP 管理**。
g. 按一下**啓動**。

3. 啓動 Web 瀏覽器。
4. 使用瀏覽器移到系統上的 iSeries 作業頁，網址是 http://*your_system_name*:2001。
5. 從 iSeries 作業頁的產品清單中選取**數位憑證管理程式**來存取 DCM 功能。

如果您是從舊版 DCM 移轉，此頁將提供您升級系統所需的明細。

第一次設定憑證

「數位憑證管理程式」(DCM) 的左邊頁框是作業導覽頁框。您可以使用此頁框來選取許多不同的作業，以管理憑證及用到這些憑證的應用程式。可用的作業視您已開啓的憑證庫及您的使用者設定檔權限而定。大部份作業只有在您具備 *ALLOBJ 和 *SECADM 特殊權限時才可以使用。

當您第一次使用「數位憑證管理程式」(DCM) 時，不存在任何憑證庫（除非您已移轉自前一版的 DCM）。因此，當您具備必要的權限時，導覽頁框只會顯示這些作業：

- 管理使用者憑證。
- 建立新的憑證庫。
- 建立「認證中心」(CA)。（註：在您使用此作業來建立專用 CA 之後，此作業就不會再出現於清單中。）
- 管理 CRL 位置。
- 管理 PKIX 要求位置。

即使您的系統上已存在憑證庫（例如，您移轉自舊版的 DCM）， DCM 在左邊導覽頁框中只會顯示有限的作業或作業種類。您必須先存取適當的憑證庫，才能開始使用大部份憑證和應用程式管理作業。若要開啓特定的憑證庫，請按一下導覽頁框中的**選取憑證庫**。

DCM 的導覽頁框亦提供一個**安全連線**按鈕。您可以使用此按鈕來顯示第二個瀏覽器視窗，使用 Secure Sockets Layer (SSL) 來起始一個安全連線。若要順利使用此功能，您必須先配置 IBM HTTP Server for iSeries 於安全模式下使用 SSL。然後，您必須以安全模式啓動 HTTP Server。如果您尚未配置和啓動 HTTP Server 供 SSL 作業，則會出現錯誤訊息，您的瀏覽器將不會啓動安全階段作業。

入門

雖然您會想要使用憑證來達成許多安全性方面的目標，但您的第一個動作將視您如何規劃來取得憑證而定。第一次使用 DCM 時，根據您想要使用 公用憑證與發出專用憑證而定，有兩個可採行的主要途徑：

建立和操作「區域」CA 來發出憑證給您的應用程式。

管理來自於公用網際網路 CA 的憑證，供您的應用程式使用。

建立及操作區域 CA

在仔細複查安全性需求及原則之後，您已決定操作區域認證中心 (CA) 來發出應用程式的專用憑證。您可以使用數位憑證管理程式 (DCM) 來建立及操作您自己的區域 CA。DCM 提供引導的作業路徑，引導您建立 CA 和使用它來發出憑證給應用程式。引導的作業路徑確保您已備妥一切，可以開始使用數位憑證來配置應用程式使用 SSL 及簽署物件和驗證物件簽章。

註: 若要在 IBM HTTP Server for iSeries 中使用憑證，在使用 DCM 之前您應該先建立和配置 Web 伺服器。在配置 Web 伺服器使用 SSL 時，會產生伺服器的應用程式 ID。您必須記下此應用程式 ID，以便使用 DCM 指定此應用程式要用於 SSL 的憑證。

在使用 DCM 指派憑證給伺服器之前，請勿結束及重新啓動伺服器。如果您在指派憑證給伺服器之前結束及重新啓動 Web 伺服器的 *ADMIN 案例，該伺服器將不會啓動，而且您將無法使用 DCM 指派憑證給伺服器。

若要使用 DCM 建立及操作區域 CA，請遵循下列步驟：

1. 啓動 DCM。
2. 在 DCM 的導覽頁框中，選取**建立認證中心 (CA)** 以顯示一連串套表。這些套表引導您建立區域 CA 及完成其它所需的作業，來開始對 SSL、物件簽署及簽章驗證使用數位憑證。

   註: 如果您對於如何完成本引導作業中的特定套表有問題，請選取問號 (**?**) 按鈕（位於頁頂端）來存取線上說明。
3. 完成此引導作業的所有套表。在使用這些套表來執行所有必要作業以設定工作的區域認證中心 (CA) 時，您必須：
   a. 選擇如何儲存區域 CA 憑證的私密金鑰。（唯有已將 IBM 4758-023 PCI 加密輔助處理器安裝在 iSeries 系統上，才會併入此步驟。如果您系統上沒有加密輔助處理器， DCM 會自動將憑證及其私密金鑰儲存在區域認證中心 (CA) 憑證庫中。）
   b. 提供區域 CA 的識別資訊。
   c. 在 PC 上或瀏覽器中安裝區域 CA 憑證，使軟體可以辨識區域 CA 及驗證 CA 發出的憑證。
   d. 選擇區域 CA 的原則資料。
   e. 使用新的區域 CA 發出伺服器或從屬站憑證，供您的應用程式使用於 SSL 連線。（如果已安裝 iSeries 有IBM 4758-023 PCI 加密輔助處理器，此步驟可讓您選取如何儲存伺服器或從屬站憑證的私密金鑰。如果您系統上沒有輔助處理器， DCM 會自動將憑證及其私密金鑰儲存在 *SYSTEM 憑證庫中。DCM 會建立 *SYSTEM 憑證庫，這是子作業的一部份。）
   f. 選取可對 SSL 連線使用伺服器或從屬站憑證的應用程式。

      註: 如果您先前已使用 DCM 建立 *SYSTEM 憑證庫來管理來自公用網際網路 CA 的 SSL 憑證，則不需執行此步驟或前一步驟。
   g. 使用新的區域 CA 發出物件簽署憑證，應用程式使用該憑證來以數位方式簽署物件。此子作業建立 *OBJECTSIGNING 憑證庫；這是您用來管理物件簽署憑證的憑證庫。
   h. 選取可使用物件簽署憑證在物件上加入數位簽章的應用程式。

註: 如果您先前已使用 DCM 建立 *OBJECTSIGNING 憑證庫來管理來自公用網際網路 CA 的物件簽署憑證，則不需執行此步驟或前一步驟。

i. 選取信任區域 CA 的應用程式。

當您完成引導作業時，即已備妥一切，可以開始配置應用程式使用 SSL 來進行安全通信。

在配置應用程式之後，透過 SSL 連線存取應用程式的使用者必須使用 DCM 取得區域 CA 憑證的複本。每一個使用者必須有憑證的複本，讓使用者的從屬站軟體能夠使用它來鑑別伺服器的識別身份，這是 SSL 協議程序的一部份。使用者可使用 DCM 複製區域 CA 憑證到檔案中，或將憑證下載到他們的瀏覽器上。使用者如何儲存區域 CA 憑證，視他們用來建立應用程式 SSL 連線的從屬站軟體而定。

此外，您可以使用此區域 CA 來發出憑證給網路上其它 iSeries 系統上的應用程式。

要進一步了解如何使用 DCM 管理使用者憑證以及使用者如何取得區域 CA 憑證的複本來鑑別區域 CA 發出的憑證，請複查這些主題：

管理使用者憑證
了解使用者如何使用 DCM 取得憑證或使現有的憑證與其 iSeries 使用者設定檔產生關聯。

使用 API 以程式設計方式發出憑證給非 iSeries 使用者
了解如何使用區域 CA 發出專用憑證給使用者，而不必使該憑證與 iSeries 使用者設定檔產生關聯。

取得一份專用 CA 憑證
了解如何取得一份專用 CA 憑證，並將它安裝在您的 PC 上，以便鑑別該 CA 發出的任何伺服器憑證。

管理使用者憑證

您和使用者可以使用「數位憑證管理程式」(DCM) 來管理使用者參與 Secure Sockets Layer (SSL) 階段作業所需的憑證。

如果使用者透過 SSL 連線來存取您的公用或內部伺服器，他們必須擁有發出伺服器憑證的「認證中心」(CA) 憑證的複本。使用者必須具有 CA 憑證，其從屬站軟體才能夠驗證伺服器憑證的確實性以建立連線。如果您的伺服器使用一個來自公用 CA 的憑證，則使用者的軟體應該已擁有一份 CA 憑證複本。因此，不論身爲 DCM 管理者的您或您的使用者，皆不需要執行任何動作，即可參與 SSL 階段作業。不過，如果您的伺服器使用一個來自於專用「區域」CA 的憑證，則您的使用者必須取得一份「區域」CA 憑證的複本，才能夠與伺服器建立 SSL 階段作業。

此外，如果伺服器應用程式支援和需要透過憑證的從屬站鑑別，則使用者必須提供可接受的使用者憑證，才能存取伺服器提供的資源。根據您的安全性需求，使用者可以提供來自於公用網際網路 CA 的憑證，或從您操作的「區域」CA 取得憑證。對於目前有iSeries 使用者設定檔的內部使用者，如果您的伺服器應用程式提供資源的存取權限，則您可以使用 DCM 將其憑證加入其使用者設定檔中。當使用者提出憑證時，這種連結關係可確定使用者對資源的存取權和限制，與其使用者設定檔授予或拒絕的權限相同。

「數位憑證管理程式」(DCM) 可讓您管理已分派到 iSeries 使用者設定檔的憑證。如果您的使用者設定檔具有 *SECADM 和 *ALLOBJ 特殊權限，則可以爲您自己或其他人管理使用者設定檔憑證分派。當沒有開啓憑證庫或有「區域認證中心」(CA) 憑證庫開啓

時，您可以在導覽頁框中選取**管理使用者憑證**來存取適當的作業。如果開啓不同的憑證庫，則使用者憑證作業會整合到**管理憑證**之下的作業。

不具 *SECADM 和 *ALLOBJ 使用者設定檔特殊權限的使用者，只可管理自己的憑證分派。他們可以選取**管理使用者憑證**來存取作業，容許他們檢視其使用者設定檔相關的憑證、從使用者設定檔中移除憑證或從不同的 CA 指派憑證給其使用者設定檔。不論是否具有使用者設定檔的特殊權限，使用者皆可以在主要導覽頁框中選取**建立憑證**作業，從「區域 CA」取得使用者憑證。

關於如何使用 DCM 來管理和建立使用者憑證，請複查這些主題：

建立使用者憑證
請閱讀本資訊來瞭解使用者如何使用「區域 CA」來發出用於從屬站鑑別的憑證。

指派使用者憑證
請閱讀本資訊來瞭解如何使您擁有的憑證與您的使用者設定檔產生關聯。憑證可能來自於另一個系統的專用「區域 CA」或一個知名的網際網路 CA。在您能夠指派憑證給使用者設定檔之前，伺服器必須信任發出憑證的 CA，且憑證不可以已經與該系統上的使用者設定檔產生關聯。

建立使用者憑證: 如果您要使用數位憑證來進行使用者鑑別，則使用者必須具有憑證。如果您使用「數位憑證管理程式」(DCM) 來操作一個專用「區域認證中心」(CA)，則您可以使用此「區域 CA」來發出憑證給每一位使用者。每一位使用者必須存取 DCM，使用**建立憑證**作業來取得憑證。爲了從「區域 CA」取得憑證，CA 原則必須容許 CA 發出使用者憑證。

若要從「區域 CA」取得憑證，請完成這些步驟：
1. 啓動 DCM。
2. 在導覽頁框中，選取**建立憑證**。
3. 選取**使用者憑證**當做要建立的憑證類型。這時會顯示一個套表，讓您提供憑證的識別資訊。
4. 完成此套表，按一下**繼續**。

   註: 如果您對於在此引導作業中完成特定的套表有問題，請選取頁頂端的問號 (**?**) 來存取線上說明。
5. 此時，DCM 會使用您的瀏覽器來建立憑證的專用和公開金鑰。您的瀏覽器可能顯示視窗來引導您完成此程序。請遵循瀏覽器的指示來完成這些作業。瀏覽器產生金鑰之後會出現一個確認頁，表示 DCM 已建立憑證。
6. 請在瀏覽器軟體中安裝新的憑證。您的瀏覽器可能顯示視窗來引導您完成此程序。請遵循瀏覽器提供的指示來完成此作業。
7. 按一下**確定**完成作業。

在處理期間，「數位憑證管理程式」會自動使憑證與您的 iSeries 使用者設定檔產生關聯。

當使用者提出另一個 CA 的憑證來進行從屬站鑑別時，如果您要讓此憑證的權限與其使用者設定檔相同，則使用者可以使用 DCM 來指派憑證給其使用者設定檔。

指派使用者憑證: 如果您要使用數位憑證來進行使用者鑑別，則使用者必須具有憑證。如果您的使用者必須提出公用網際網路「認證中心」(CA) 的憑證，則他們可以使用「數位憑證管理程式」(DCM) 來指派這些憑證給其使用者設定檔。這可讓您及使用者使用 DCM 來管理這些憑證。

若要使用**指派使用者憑證**作業，您必須與 HTTP Server 建立一個安全階段作業，透過此階段作業來存取「數位憑證管理程式」(DCM)。您是否建立安全階段作業，可從您用來存取 DCM 的 URL 中的埠號來判斷。如果您使用存取 DCM 的預設埠 2001，則沒有建立安全階段作業。另外，也必須配置 HTTP Server 來使用 SSL，才可以切換到安全階段作業。

當您選取此作業時會顯示一個新的瀏覽器視窗。如果您沒有安全階段作業， DCM 會提示您按一下**指派使用者憑證**來啓動一個安全階段作業。然後 DCM 會與您的瀏覽器起始 Secure Sockets Layer (SSL) 協議。

在這些協議當中，瀏覽器可能詢問您是否信任發出憑證來識別 HTTP Server 的「認證中心」(CA)。瀏覽器也可能詢問您是否接受伺服器憑證本身。

在容許瀏覽器信任 CA 和接受伺服器憑證之後，伺服器可能會要求您提出憑證來進行從屬站鑑別。根據瀏覽器的配置設定值，瀏覽器可能提示您選取憑證來進行鑑別。如果您的瀏覽器提出的憑證是來自於系統信任的 CA，則 DCM 會在另一個視窗中顯示憑證資訊。如果您未提出可接受的憑證，則在容許您存取之前，伺服器會提示您輸入使用者名稱和密碼來進行鑑別。

一旦建立一個安全階段作業，DCM 會嘗試從您的瀏覽器擷取適當的憑證，使它可以與您的使用者設定檔產生關聯。如果 DCM 順利擷取一或多個憑證，則您可以檢視憑證資訊，並選擇使憑證與您的使用者設定檔產生關聯。

如果 DCM 未顯示憑證的資訊，則表示您未提供可讓 DCM 指派給使用者設定檔的憑證。在幾個使用者憑證問題當中有一個問題很重要。例如，瀏覽器包含的憑證已與您的使用者設定檔產生關聯。

如果您偏好使用「區域 CA」來發出憑證給使用者，則使用者必須建立使用者憑證。

使用 API 以程式設計方式發出憑證給非 iSeries 使用者

從 V5R2 開始有提供兩個新的 API，供您以程式設計方式發出憑證給非 iSeries 使用者。在前版次，當您使用區域認證中心 (CA) 發出憑證給使用者時，這些憑證會自動與其 iSeries 使用者設定檔產生關聯。因此，要使用區域 CA 發出憑證給使用者進行從屬站鑑別時，您必須提供使用者一個 iSeries 使用者設定檔。此外，當使用者需要從區域 CA 憑證來進行從屬站鑑別時，每一個使用者必須使用數位憑證管理程式 (DCM) 來建立所需的憑證。因此，每一個使用者必須在裝載 DCM 的 iSeries 伺服器上有一個使用者設定檔，而且能夠有效登入該 iSeries 伺服器。

使憑證與使用者設定檔產生關聯有它的好處，尤其是考慮到內部使用者。不過，這些限制和基本要求在使用區域 CA 發出使用者憑證給大量使用者時比較不切實際，尤其當您不希望那些使用者擁有 iSeries 使用者設定檔時。如果您要求自己的應用程式需要有憑證來進行使用者鑑別的話，爲了避免提供使用者設定檔給這些使用者，您可能會要求使用者要付款給知名 CA 發出的憑證。

這兩個新 API 提供的支援，可讓您爲任何使用者名稱提供介面，來建立由區域 CA 憑證簽署的使用者憑證。此憑證不會與使用者設定檔產生關聯。使用者不需要存在於裝載 DCM 的 iSeries 伺服器上，且使用者不需要使用 DCM 來建立憑證。

有兩個 API，分別針對兩大主要瀏覽器程式，當您使用 Net.Data® 建立程式來發出憑證給使用者時可以呼叫此 API。您建立的應用程式必須提供所需的圖形式使用者介面 (GUI) 程式碼，來建立使用者憑證及呼叫其中一個適當的 API 來使用區域 CA 以簽署憑證。

關於使用這些 API 的詳細資訊，請參閱這幾頁：
- 建立及簽署使用者憑證要求 (QYCUGSUC) API。
- 簽署使用者憑證要求 (QYCUSUC) API。

取得一份專用 CA 憑證

當您存取一個使用 Secure Sockets Layer (SSL) 連線的伺服器時，伺服器會提供憑證給您的從屬站軟體，做爲其身份的證明。然後，您的從屬站軟體必須驗證伺服器的憑證，伺服器才可以建立階段作業。若要驗證伺服器憑證，則對於發出伺服器憑證的「認證中心」(CA) ，您的從屬站軟體必須有權限來存取本端儲存的憑證複本。如果伺服器提供的憑證是來自於公用網際網路 CA，則您的瀏覽器或其他從屬站軟體應該已有一份 CA 憑證複本。不過，如果伺服器提出的憑證是來自於專用「區域 CA」，則您必須使用「數位憑證管理程式」(DCM) 來取得一份「區域 CA」憑證複本。

您可以使用 DCM 來直接下載「區域 CA」憑證到您的瀏覽器，或將「區域 CA」憑證複製到一個檔案，供其他從屬站軟體來存取和使用。如果您同時使用瀏覽器和其他應用程式來進行安全通信，則可能需要使用兩種方法來安裝「區域 CA」憑證。如果使用兩種方法，請先在瀏覽器安裝憑證，再將它複製和貼到檔案中。

如果伺服器應用程式要求您提供來自於「區域 CA」的憑證來鑑別自己，則您應該先下載「區域 CA」憑證到瀏覽器，再從「區域 CA」要求使用者憑證。

若要使用 DCM 來取得一份「區域 CA」憑證複本，請完成這些步驟：
1. 啓動 DCM。
2. 在導覽頁框中，選取**在您的 CA 上安裝區域 CA 憑證**來顯示一頁，它可讓您下載「區域 CA」憑證到瀏覽器中，或儲存成系統中的一個檔案。
3. 選取一種方法來取得「區域 CA」憑證。
   a. 選取**安裝憑證**來下載「區域 CA」憑證，做爲瀏覽器的一個最高授信使用者。這確保您的瀏覽器可以與使用此 CA 之憑證的伺服器建立安全通信階段作業。您的瀏覽器將顯示一連串視窗來協助您完成安裝作業。
   b. 選取**複製和貼上憑證**來顯示一頁，其中包含一份特殊編碼的「區域 CA」憑證。將頁上顯示的文字物件複製到剪貼簿。稍後您必須將此資訊貼到一個檔案中。此檔案由一個 PC 公用程式（例如 MKKF 或 IKEYMAN）用來儲存憑證，供 PC 上的從屬站程式使用。在您的從屬站應用程式能夠辨識和使用「區域 CA」憑證來進行鑑別之前，您必須配置應用程式將此憑證視爲一個最高授信使用者。請遵循這些應用程式提供的指示來使用此檔案。
4. 按一下**確定**來返回「數位憑證管理程式」首頁。

從公用網際網路 CA 管理憑證

在仔細複查安全性需求及原則之後，您已決定要使用來自公用網際網路認證中心 (CA) 的憑證，例如 VeriSign。比方說，您操作一個公用網站，並且想要對安全通信階段作業使

用 Secure Sockets Layer (SSL)，以確定特定資訊交易的私密性。因爲網站可供一般大眾存取，所以您想要使用大部份 Web 瀏覽器可輕易辨識的憑證。

或者，您爲外部客戶開發應用程式，並且想要使用公用憑證，以數位化方式簽署應用程式套裝軟體。藉由簽署應用程式套裝軟體，您的客戶可以確定該套裝軟體是來自您公司，且未獲授權的一方未改變傳輸中的程式碼。您想要使用公用憑證，使客戶可以輕易且花費不多地驗證套裝軟體上的數位簽章。您也可以在傳送套裝軟體給客戶之前使用此憑證來驗證簽章。

您可以使用數位憑證管理程式 (DCM) 中的引導作業，集中管理這些公用憑證及使用它們的應用程式，來建立 SSL 連線、簽署物件或驗證物件上的數位簽章的確實性。

管理公用憑證

當您使用 DCM 來管理公用網際網路 CA 的憑證時，您必須先建立憑證庫。憑證庫是一個特殊金鑰資料庫檔案，DCM 使用它來儲存數位憑證及其相關聯的私密金鑰。根據憑證庫包含的憑證類型，DCM 可讓您建立及管理數種類型的憑證庫。

您建立的憑證庫類型以及您在管理憑證及使用它們的應用程式時必須執行的後續作業，取決於您如何規劃使用憑證。要了解如何使用 DCM 爲應用程式建立適當的憑證庫及管理公用網際網路憑證，請複查這些主題：

- 管理公用網際網路憑證以進行SSL通信階段作業。
- 管理公用網際網路憑證來簽署物件。
- 管理網際網路憑證來驗證物件簽章。

DCM 也可讓您管理憑證 (自 Public Key Infrastructure for X.509 (PKIX) 憑證中心取得的憑證)。

管理 SSL 通信階段作業的公用網際網路憑證

您可以使用「數位憑證管理程式」(DCM) 來管理公用網際網路憑證，讓您的應用程式能夠以 Secure Sockets Layer (SSL) 來建立安全通信階段作業。如果您不使用 DCM 來操作自己的區域「認證中心」(CA)，則必須先建立適當的憑證庫來管理您在 SSL 上使用的公用憑證。此爲 *SYSTEM 憑證庫。當您建立憑證庫時， DCM 會引導您建立憑證要求資訊，您必須提供此資訊給公用 CA 才能取得憑證。

若要使用 DCM 來管理和使用公用網際網路憑證，使您的應用程式能夠建立 SSL 通信階段作業，請遵循下列步驟：

1. 啓動 DCM。
2. 在 DCM 的導覽頁框中，選取**建立新的憑證庫**來啓動引導作業，並完成一連串套表。這些套表會引導您建立憑證庫和憑證，供您的應用程式在 SSL 階段作業中使用。

   註: 如果您對於在此引導作業中完成特定套表有問題，請選取頁頂端的問號 (**?**) 來存取線上說明。
3. 選取 ***SYSTEM** 做爲要建立的憑證庫，按一下**繼續**。
4. 選取**是**，在建立 *SYSTEM 憑證庫期間建立一個憑證，按一下**繼續**。
5. 選取**VeriSign 或其他網際網路認證中心 (CA)** 當做新憑證的簽署者，按一下**繼續**來顯示一個套表，讓您提供新憑證的識別資訊。

註: 如果您的 iSeries 已安裝 IBM 4758-023 PCI 加密輔助處理器， DCM 可讓您選擇如何儲存憑證的私密金鑰，這是下一個要處理的作業。如果您的系統沒有輔助處理器，DCM 會自動將私密金鑰放入 *SYSTEM 憑證庫中。如果您需要選取私密金鑰如何儲存的說明，請參閱 DCM 的線上說明。

6. 完成此套表，按一下**繼續**來顯示確認頁。此確認頁顯示您必須提供給公用「認證中心」(CA) 的憑證要求資料，此 CA 將發出您的憑證。「憑證簽署要求」(CSR) 資料由公開金鑰及您爲新憑證指定的其他資訊所組成。
7. 請小心將 CSR 資料複製並貼到憑證申請表或個別檔案中，公用 CA 在要求憑證時需要它。您必須使用所有 CSR 資料，包括 Begin New Certificate Request 和 End New Certificate Request 兩行。當您結束此頁時，資料會失去且無法回復。將申請表或檔案傳送到您選擇要發出和簽署憑證的 CA。

   註: 您必須等待 CA 傳回已簽署完成的憑證，才算完成此程序。

   註: 若要對 HTTP Server for iSeries 使用憑證，您應該先建立和配置 Web 伺服器，再利用 DCM 來使用已簽署完成的憑證。當您配置 Web 伺服器去使用 SSL 時，將爲伺服器產生一個應用程式 ID。您必須記下此應用程式 ID，以便使用 DCM 來指定此應用程式在 SSL 上應該使用的憑證。

   在使用 DCM 來指派簽署完成的憑證給伺服器之前，請勿結束和重新啓動伺服器。如果您在指派憑證給伺服器之前就先結束和重新啓動 Web 伺服器的 *ADMIN 案例，則伺服器將不會啓動，且您將無法使用 DCM 來指派憑證給伺服器。
8. 在公用 CA 傳回您簽署的憑證之後，請啓動 DCM。
9. 在導覽頁框中，按一下**選取憑證庫**，再選取 ***SYSTEM** 做爲要開啓的憑證庫。
10. 顯示「憑證庫和密碼」頁時，請提供您在建立憑證庫時所指定的密碼，按一下**繼續**。
11. 在導覽頁框重新整理之後，請選取**管理憑證**來顯示作業清單。
12. 在作業清單中，選取**匯入憑證**，開始將簽署的憑證匯入 *SYSTEM 憑證庫中。在完成匯入憑證之後，您可以指定在 SSL 通信上要使用此憑證的應用程式。
13. 在導覽頁框中，選取**管理應用程式**來顯示作業清單。
14. 在作業清單中，選取**更新憑證分派**以顯示可讓您指派憑證的 SSL 型應用程式清單。
15. 從清單中選取一個應用程式，按一下**更新憑證分派**。
16. 選取您匯入的憑證，按一下**指派新的憑證**。 DCM 會顯示訊息來確認您爲應用程式所選取的憑證。

    註: 根據憑證，部份 SSL 型應用程式支援從屬站鑑別。如果要讓具備此支援的應用程式能夠在提供資源存取權限之前先鑑別憑證，您必須爲應用程式定義 CA 信任清單。這確保應用程式只驗證您信任的 CA 所發出的憑證。如果使用者或從屬站應用程式提供的憑證不是來自於 CA 信任清單中的 CA，則應用程式不會接受此憑證做爲有效鑑別的基礎。

當您完成引導的作業時，就可以開始爲安全通信配置您的應用程式使用 SSL。在使用者能夠透過 SSL 階段作業來存取這些應用程式之前，對於發出伺服器憑證的 CA，使用者必須先有一份此 CA 的 CA 憑證複本。如果您的憑證是來自於知名的網際網路 CA，則使用者的從屬站軟體可能已有一份必要的 CA 憑證複本。如果使用者需要取得 CA 憑證，則應該存取 CA 的網站，依照網站提供的指示來進行。

管理公用網際網路憑證來簽署物件

您可以使用「數位憑證管理程式」(DCM) 來管理公用網際網路憑證，以數位方式簽署物件。如果您不使用 DCM 來操作自己的「認證中心」(CA)，則必須先建立適當的憑證庫來管理您用來簽署物件的公用憑證。此爲 *OBJECTSIGNING 憑證庫。當您建立憑證庫時， DCM 會引導您建立憑證要求資訊，您必須提供此資訊給公用網際網路 CA 來取得憑證。

另外，若要使用憑證來簽署物件，您必須定義應用程式 ID。此應用程式 ID 控制某人使用特定憑證來簽署物件時需要多少權限，並且提供超越 DCM 的另一個層次的存取控制。依預設，應用程式定義要求使用者要備具 *ALLOBJ 特殊權限，才能使用憑證供應用程式簽署物件。（不過，您可以使用iSeries 領航員來變更應用程式 ID 所需的權限。）

若要使用 DCM 來管理和使用公用網際網路憑證來簽署物件，請完成下列作業：

1. 啓動 DCM。
2. 在 DCM 左邊的導覽頁框中，選取**建立新的憑證庫**來啓動引導作業，並完成一連串套表。這些套表會引導您建立憑證庫和憑證，讓您用來簽署物件。

   註: 如果您對於在此引導作業中完成特定套表有問題，請選取頁頂端的問號 (**?**) 按鈕來存取線上說明。
3. 選取 ***OBJECTSIGNING** 做爲要建立的憑證庫，按一下**繼續**。
4. 選取**是**，在建立憑證庫期間建立一個憑證，按一下**繼續**。
5. 選取**VeriSign 或其他網際網路認證中心 (CA)** 當做新憑證的簽署者，按一下**繼續**。這會顯示一個套表，可讓您提供新憑證的識別資訊。
6. 完成此套表，按一下**繼續**來顯示確認頁。此確認頁顯示您必須提供給公用「認證中心」(CA) 的憑證要求資料，此 CA 將發出您的憑證。「憑證簽署要求」(CSR) 資料由公開金鑰及您爲新憑證指定的其他資訊所組成。
7. 將小心將 CSR 資料複製並貼到憑證申請表或個別檔案中，公用 CA 要求憑證時需要它。您必須使用所有 CSR 資料，包括 Begin 和 End New Certificate Request 兩行。當您結束此頁時，資料會失去且無法回復。將申請表或檔案傳送到您選擇要發出和簽署憑證的 CA。

   註: 您必須等待 CA 傳回已簽署完成的憑證，才算完成此程序。
8. 在公用 CA 將簽署的憑證傳給您之後，請啓動 DCM。
9. 在左邊導覽頁框中，按一下**選取憑證庫**，再選取 ***OBJECTSIGNING** 做爲要開啓的憑證庫。
10. 顯示「憑證庫和密碼」頁時，請提供您在建立憑證庫時所指定的密碼，按一下**繼續**。
11. 在導覽頁框中，選取**管理憑證**來顯示作業清單。
12. 在作業清單中，選取**匯入憑證**，開始將簽署的憑證匯入 *OBJECTSIGNING 憑證庫中。在完成匯入憑證之後，您可以建立應用程式定義，以便使用憑證來簽署物件。
13. 在左邊導覽頁框重新整理之後，請選取**管理應用程式**來顯示作業清單。
14. 在作業清單中，選取**新增應用程式**來開始建立物件簽署應用程式定義，以便使用憑證來簽署物件。

15. 完成套表來定義您的物件簽署應用程式，按一下**新增**。此應用程式定義不說明實際的應用程式，而是說明您計畫以特定憑證來簽署的物件類型。請閱讀線上說明來決定如何完成套表。
16. 按一下**確定**來認可應用程式定義確認訊息，並且顯示「管理應用程式」作業清單。
17. 在作業清單中，選取**更新憑證分派**，按一下**繼續**來顯示可讓您指派憑證的物件簽署應用程式 ID 清單。
18. 從清單中選取一個應用程式 ID，按一下**更新憑證分派**。
19. 選取您匯入的憑證，按一下**指派新的憑證**。

當您完成這些作業時，就可以開始簽署物件來確保其完整性。

當您分送已簽署的物件時，收到物件的人必須使用 V5R1 或更高版本的 DCM 來驗證物件的簽章，以確定資料沒有變更並驗證傳送者的身份。若要驗證簽章，接收者必須有一份簽章驗證憑證的複本。您應該在已簽署的物件套件中提供這個憑證的複本。

對於發出憑證讓您用來簽署物件的 CA，接收者也必須有一份此 CA 的 CA 憑證複本。如果您使用知名網際網路 CA 的憑證來簽署物件，則接收者的 DCM 版本應該已經有一份必要的 CA 憑證複本。不過，如果您認爲接收者可能沒有這一份 CA 憑證複本，則應該隨同簽署的物件提供此複本。例如，如果您使用專用「區域 CA」的憑證來簽署物件，則應該提供一份「區域 CA」憑證複本。基於安全性考量，您應該在分開的套件中提供 CA 憑證，或公開提供 CA 憑證供需要的人索取。

管理憑證來驗證物件簽章

您可以使用「數位憑證管理程式」(DCM) 來管理您用來驗證物件之數位簽章的簽章驗證憑證。若要簽署物件，您可以使用憑證的私密金鑰來建立簽章。當您傳送已簽署的物件給其他人時，您必須包含一份用來簽署此物件的憑證複本。您可以使用 DCM 來匯出物件簽署憑證（不含憑證的私密金鑰）當做簽章驗證憑證。您可以將簽章驗證憑證匯出到一個檔案，然後再分送給其他人。或者，如果要驗證您所建立的簽章，您可以將簽章驗證憑證匯出到 *SIGNATUREVERIFICATION 憑證庫。

若要驗證物件的簽章，您必須有一個用來簽署物件的憑證。您可以使用簽署憑證中的公開金鑰來檢查和驗證以對應的私密金鑰所建立的簽章。因此，在您能夠驗證物件的簽章之前，您必須從提供簽署物件的一方取得一份簽署憑證的複本。

對於發出憑證來簽署物件的 CA，您也必須具有一份此 CA 的「認證中心」(CA) 憑證複本。您可以使用 CA 憑證來驗證用以簽署物件的憑證確實性。 DCM 提供大部份知名 CA 的 CA 憑證複本。不過，如果物件是以另一個公用 CA 或專用「區域 CA」來簽署，則您必須先取得一份 CA 憑證複本，才能驗證物件簽章。

若要使用 DCM 來驗證物件簽章，首先您必須建立適當的憑證庫來管理必要的簽章驗證憑證；此爲 *SIGNATUREVERIFICATION 憑證庫。當您建立此憑證庫時， DCM 會自動匯入大部份知名的公用 CA 憑證複本。

註： 如果您要使用自己的物件簽署憑證來驗證簽章，則必須建立 *SIGNATUREVERIFICATION 憑證庫，並且將 *OBJECTSIGNING 憑證庫中的憑證複製過來。即使您計畫在 *OBJECTSIGNING 憑證庫內執行簽章驗證，仍然要執行這項動作。

若要使用 DCM 來管理您的簽章驗證憑證，請完成下列作業：

1. 啓動 DCM。
2. 在 DCM 左邊的導覽頁框中，選取**建立新的憑證庫**來啓動引導作業，並完成一連串套表。

   註: 如果您對於在此引導作業中完成特定套表有問題，請選取頁頂端的問號 (**?**) 按鈕來存取線上說明。
3. 選取 ***SIGNATUREVERIFICATION** 做爲要建立的憑證庫，按一下**繼續**。

   註: 如果 *OBJECTSIGNING 憑證庫已存在，則此時 DCM 會提示您是否將物件簽署憑證複製到新的憑證庫中，當做簽章驗證憑證。如果您要使用現有的物件簽署憑證來驗證簽章，請選取**是**，然後按一下**繼續**。您必須知道 *OBJECTSIGNING 憑證庫的密碼，才能複製其中的憑證。
4. 請指定新憑證庫的密碼，按一下**繼續**來建立憑證庫。此時會顯示一個確認頁，指出已順利建立憑證庫。現在，您可以使用此憑證庫來管理和使用憑證來驗證物件簽章。

   註: 如果您已建立此憑證庫，且可以驗證您所簽署之物件的簽章，則可以就此停止。當您建立新的物件簽署憑證時，您應該將憑證從 *OBJECTSIGNING 憑證庫匯出到此憑證庫中。如果您不匯出，則無法驗證您所建立的簽章。

   註: 如果您已建立此憑證庫來驗證您從其他來源收到之物件的簽章，則應該繼續此程序，以便將所需的憑證匯入憑證庫中。
5. 在導覽頁框中，按一下**選取憑證庫**，再選取 ***SIGNATUREVERIFICATION** 做爲要開啓的憑證庫。
6. 顯示「憑證庫和密碼」頁時，請提供您在建立憑證庫時所指定的密碼，按一下**繼續**。
7. 在導覽頁框重新整理之後，請選取**管理憑證**來顯示作業清單。
8. 在作業清單中選取**匯入憑證**。此引導作業可引導您將所需的憑證匯入憑證庫中，讓您能夠驗證所收到之物件的簽章。
9. 選取您要匯入的憑證類型。選取**簽章驗證**來匯入您在簽署的物件上收到的憑證，並完成匯入作業。

   註: 對於發出簽章驗證憑證的 CA，如果憑證庫不含一份此 CA 的 CA 憑證複本，則您必須先匯入 CA 憑證。如果您在匯入簽章驗證憑證之前未匯入 CA 憑證，則匯入簽章驗證憑證時可能會發生錯誤。

您現在可以使用這些憑證來驗證物件簽章。

第 8 章 管理 DCM

在配置數位憑證管理程式 (DCM) 之後，您必須執行一些憑證管理作業。要了解如何使用 DCM 管理數位憑證，請複查這些主題：

使用區域 CA 發出憑證給其它 iSeries 系統
了解如何在一個系統上使用專用區域 CA 發出憑證供其它 iSeries 系統使用。

在 DCM 中管理應用程式
了解如何針對 SSL 型應用程式或物件簽署應用程式使用 DCM 來處理應用程式定義。此主題提供關於建立應用程式定義以及如何管理應用程式的憑證分派的資訊。您會學到關於定義 CA 信任清單，應用程式根據此清單來接受憑證進行從屬站鑑別。

驗證憑證和應用程式
了解在應用程式使用或接受憑證之前您如何驗證特定憑證的確實性。

指派憑證
了解如何快速指派憑證給一或多個應用程式使用於安全功能。

管理 CRL 位置，了解如何定義及使用憑證廢止清冊 (CRL) 位置，應用程式可用來驗證它們接受的憑證是否有效。

在 IBM 4758 加密輔助處理器上儲存憑證金鑰
了解如何使用已安裝的輔助處理器爲憑證的私密金鑰提供更安全的儲存。

管理 PKIX CA 的要求位置
了解如何使用 DCM 管理您從公用網際網路 CA 取得的憑證，這些 CA 是根據 Public Key Infrastructure for X.509 (PKIX) 標準發出憑證。

簽署物件
了解如何使用 DCM 來管理您用來以數位方式簽署物件的憑證，以確定其完整性。

驗證物件簽章
了解如何使用 DCM 驗證物件上的數位簽章的確實性。

使用區域 CA 發出憑證給其它 iSeries 系統

您可能已在您網路的 iSeries 系統上使用專用區域認證中心 (CA)。現在，您要在網路中的另一個 iSeries 系統上延伸使用這個區域 CA。例如，您要現行區域 CA 發出伺服器或從屬站憑證給另一個 iSeries 系統上的應用程式，來用於 SSL 通信階段作業。或者，您要使用來自一個系統上的區域 CA 的憑證來簽署您儲存於另一個 iSeries 伺服器上的物件。

您可以使用「數位憑證管理程式 (DCM)」來達成這個目標。您可以在操作「區域 CA」所在的 iSeries 上執行一些作業，而在裝載您要對其發出憑證的應用程式所在的第二個 iSeries 系統上執行其它作業。這第二個系統稱爲目標系統。您在目標系統上必須執行的作業視系統版次而定。

註: 如果您操作區域 CA 所在的 iSeries 系統使用密碼存取提供者產品，它提供比目標系統更強的加密，您可能會遇到問題。（若是 V5R2，唯一可用的密碼存取提供者爲 5722-AC3，它是目前功能最強的產品。不過，在之前的版次中，您可能安裝其它功能較弱的密碼存取提供者產品（5722-AC1 或 5722-AC2），其提供的加密功能層次較低。）當您匯出憑證（及其私密金鑰）時，系統會加密檔案以保護其內容。

如果系統使用的加密產品比目標系統更強，則目標系統無法在匯入程序中將檔案解密。因此，匯入可能失敗或憑證可能無法用於建立 SSL 階段作業。即使您對新憑證使用適合目標系統上的加密產品的金鑰大小，情況還是一樣。

您可以使用區域 CA 發出憑證給其它系統，然後用於簽署物件或讓應用程式用於建立 SSL 階段作業。當您使用區域 CA 建立憑證在另一個 iSeries 系統上使用時，DCM 建立的檔案含有區域 CA 憑證的複本，以及許多公用網際網路 CA 憑證的複本。

根據您區域 CA 發出的憑證類型，以及目標系統的版次和狀況，您在 DCM 中必須執行的作業稍有不同。

發出專用憑證以使用於另一個 V5R2 或 V5R1 iSeries 系統

若要使用區域 CA 發出憑證來使用於另一個 V5R2 或 V5R1 iSeries 系統，請在裝載區域 CA 的系統上執行下列這些步驟：

1. 啓動 DCM。

   註: 如果您對於如何完成本引導作業中的特定套表有問題，請選取問號 (**?**) （位於頁頂端）來存取線上說明。
2. 在導覽頁框中，選取**建立憑證**來顯示可使用區域 CA 建立的憑證類型清單。

   您不需要開啓憑證庫來完成此作業。這些指示假設您不是在特定憑證庫內工作，或假設您在區域認證中心 (CA) 憑證庫內工作。此系統上必須有區域 CA，您才可以執行這些作業。
3. 選取您要區域 CA 發出的憑證類型，然後按一下**繼續**，開始引導作業並完成一連串套表。選擇**對另一個 iSeries** 建立伺服器或從屬站憑證（用於 SSL 階段作業），或對**另一個 iSeries** 建立物件簽署憑證（用於另一個系統）。

   註: 如果您建立物件簽署憑證供另一個系統使用，該系統必須執行 V5R1 或更新版的 OS/400，才能使用建立的憑證。由於目標系統必須是 V5R1 或更新版本，主電腦系統上的 DCM 不會提示您爲新物件簽署憑證選擇目標版次格式。
4. 如果您要建立伺服器或從屬站憑證，請選取您對其建立憑證的 iSeries 系統版次。按一下**繼續**，顯示一個套表，它可讓您提供新憑證的識別資訊。

   註: 您選取的版次可判定 DCM 用來建立新憑證的格式。識別資訊的數量和類型視您所選取的版次而有不同。這可確保憑證檔案與使用憑證的 iSeries 系統相容。
5. 完成套表並按一下**繼續**以顯示一確認頁。

   註: 如果目標系統上已有 *OBJECTSIGNING 或 *SYSTEM 憑證庫，請務必爲憑證指定唯一的憑證標籤及檔名。指定唯一的憑證標籤及檔名可讓您輕易匯入憑證到目標系統上現有的憑證庫中。

   此確認頁顯示 DCM 爲您建立來轉送至目標系統的檔案名稱。DCM 根據您指定的目標系統版次來建立這些檔案。DCM 會自動將區域 CA 憑證複本放入這些檔案中。

   註: DCM 會在其本身的憑證庫中建立新憑證並產生供您轉送的兩個檔案：一個是憑證庫檔案（副檔名爲 .KDB），另一個是要求檔（副檔名爲 .RDB)。
6. 使用二進位「檔案轉送通信協定 (FTP)」或另一個方法，將檔案轉送到目標系統。

發出專用憑證以使用於 V4R4 或 V4R5 iSeries 系統

若要使用區域 CA 發出憑證來於 V4R4 或 V4R5 iSeries 系統上使用，請在裝載 V5R2 區域 CA 的系統上執行下列這些步驟：

1. 啓動 DCM。

   註: 如果您對於如何完成本引導作業中的特定套表有問題，請選取問號 (**?**) （位於頁頂端）來存取線上說明。

2. 在導覽頁框中，選取**建立憑證**來顯示可使用區域 CA 建立的憑證類型清單。

   您不需要開啓憑證庫來完成此作業。這些指示假設您不是在特定憑證庫內工作，或假設您在區域 CA 憑證庫內工作。此系統上必須有區域 CA，您才可以執行這些作業。

3. 選取您要區域 CA 發出的憑證類型，然後按一下**繼續**，開始引導作業並完成一連串套表。

   註: 由於您要建立這個憑證來於 V4R4 或 V4R5 iSeries 系統上使用，所以必須**為另一個 iSeries** 選擇伺服器或從屬站憑證。V5R1 之前版次的目標系統無法使用物件簽署憑證。

4. 選取您要對其建立憑證的 iSeries 版次。按一下**繼續**，顯示一個套表，它可讓您提供新憑證的識別資訊。

   註: 您選取的版次可判定 DCM 用來建立新憑證的格式。識別資訊的數量和類型視您所選取的版次而有不同。這可確保憑證檔案與使用憑證的 iSeries 系統相容。

5. 完成套表並按一下**繼續**以顯示一確認頁。

   註: 如果目標系統上已有 *SYSTEM 憑證庫，請務必爲憑證指定唯一的憑證標籤及檔名。指定唯一的憑證標籤及檔名可讓您輕易匯入憑證到目標系統上現有的憑證庫中。

   此確認頁顯示 DCM 爲您建立來轉送至目標系統的檔案名稱。DCM 根據您指定的目標系統版次來建立這些檔案。DCM 會自動將區域 CA 憑證複本放入這些檔案中。

   註: DCM 會在其本身的憑證庫中建立新憑證並產生供您轉送的兩個檔案：一個是憑證庫檔案（副檔名爲 .KDB），另一個是要求檔（副檔名爲 .RDB)。

註: 如果您打算使用 V4R4 或 V4R5 目標系統上現有的 *SYSTEM 憑證庫內這些檔案中的憑證，則不能直接從 .KDB 及 .RDB 檔匯入區域 CA 憑證。因爲 CA 憑證格式不是 DCM 匯入功能可辨識及使用的格式。所以，您必須使用主電腦系統將區域 CA 憑證複本匯出至個別檔案，以確保 CA 憑證格式可供舊版的匯入功能使用。

6. 在導覽頁框中，按一下**選取憑證庫**並選取 ***SYSTEM** 作爲要開啓的憑證庫。
7. 當顯示「憑證庫與密碼」頁時，提供您在主電腦系統上建立憑證庫時所指定的密碼，然後按一下**繼續**。
8. 在導覽頁框中，選取**管理憑證**來顯示作業清單。
9. 從作業清單中，選取**匯出憑證**。
10. 選取**認證中心 (CA)** 爲匯出的憑證類型，然後按一下**繼續**來顯示 CA 憑證清單。
11. 從憑證清單中，選取區域 CA 憑證（例如， LOCAL_CERTIFICATE_AUTHORITY）。按一下**匯出**，顯示一個套表，它可讓您選擇 CA 憑證的目的地。
12. 選取**檔案**，然後按一下**繼續**。
13. 指定匯出檔的完整路徑和檔名，然後按一下**繼續**。顯示一確認頁，指示 DCM 順利匯出檔案。

註: 請確定所指定的檔名和副檔名是唯一的。例如，您可以將檔案命名爲 mycafile.exp。爲檔案命名時，請勿使用下列其中一個副檔名：.TXT、.KDB、.RDB 或 .KYR。若使用其中一個副檔名類型，則在目標系統上匯入檔案時可能會有問題。

14. 使用二進位「檔案轉送通信協定 (FTP)」或另一個方法，將您建立的憑證庫檔案（.KDB 和 .RDB）轉送到 V4R4 或 V5R5 目標系統。使用 ASCII FTP 模式來轉送含有匯出的區域 CA 憑證之檔案。

使用目標系統上轉送的檔案

轉送檔案之後，可透過目標系統上的 DCM 來使用轉送的憑證檔。您必須執行的 DCM 作業視目標系統版次及目標系統上存在的憑證庫而有不同。另外，您在主電腦系統上建立的憑證類型也會影響到您在目標系統上必須執行的作業。若要瞭解如何透過目標系統上的 DCM 來使用轉送的憑證檔，請參考下列主題：

- 將專用憑證用於 V5R2 目標系統上的 SSL 階段作業。
- 將專用憑證用於 V5R1 目標系統上的 SSL 階段作業。
- 將專用憑證用於 V5R2 或 V5R1 目標系統上的物件簽署。
- 將專用憑證用於 V4R5 或 V4R4 目標系統上的 SSL 階段作業。

將專用憑證用於 V5R2 目標系統上的 SSL 階段作業

您可以從「數位憑證管理程式 (DCM)」的 *SYSTEM 憑證庫中，管理您應用程式用於 SSL 階段作業的憑證。如果您從未使用 V5R2 目標系統上的 DCM 來管理 SSL 的憑證，則這個憑證庫不應存在於目標系統上。使用您在區域 CA 主電腦系統上所建立轉送的憑證庫檔案之作業，視 *SYSTEM 憑證庫是否存在而有不同。如果 *SYSTEM 憑證庫不存在，您可以使用轉送的憑證檔作爲建立 *SYSTEM 憑證庫的方法。如果 *SYSTEM 憑證庫存在於 V5R2 目標系統上，您可以藉由下列兩方法之一來使用轉送的憑證檔：

- 將轉送的檔案當作其它系統憑證庫。
- 將轉送的檔案匯入現有的 *SYSTEM 憑證庫中。

*SYSTEM 憑證庫不存在

如果 *SYSTEM 憑證庫不存在於您要使用轉送的憑證庫檔案之 V5R2 系統上，您可以將轉送的憑證檔當作 *SYSTEM 憑證庫。若要在 V5R2 目標系統上建立 *SYSTEM 憑證庫及使用憑證檔，請遵循下列步驟：

1. 請確定您在管理區域 CA 的系統上所建立的憑證庫檔案（兩個檔案：一個具有 .KDB 副檔名，另一個具有 .RDB 副檔名）位於 /QIBM/USERDATA/ICSS/CERT/SERVER 目錄中。
2. 一旦轉送的憑證檔位於 /QIBM/USERDATA/ICSS/CERT/SERVER 目錄中，請將這些檔案更名爲 DEFAULT.KDB 及 DEFAULT.RDB。藉由在適當目錄中更名這些檔案，您可以建立包含目標系統的 *SYSTEM 憑證庫之元件。憑證庫檔案已包含許多公用網際網路 CA 的憑證複本。DCM 會將這些複本及區域 CA 憑證的複本新增到您所建立的憑證庫檔案中。

   注意: 如果您目標系統的 /QIBM/USERDATA/ICSS/CERT/SERVER 目錄中已有 DEFAULT.KDB 和 DEFAULT.RDB 檔，表示 *SYSTEM 憑證庫目前存在於這個目標系統上。所以，建議不要將轉送的檔案更名。改寫預設檔案會在使用 DCM、轉送的憑證庫及其內容時產生問題。所以，您應該確定它們有唯一

的名稱，而且應將轉送的憑證庫當作**其它系統憑證庫**。如果您將檔案當作「其它系統憑證庫」，則無法使用 DCM 來指定哪些應用程式應使用憑證。

3. 啓動 DCM。現在，您必須將更名轉送的檔案所建立的 *SYSTEM 憑證庫密碼變更。變更密碼可讓 DCM 儲存新密碼，以便您使用憑證庫上所有 DCM 憑證管理功能。
4. 在導覽頁框中，按一下**選取憑證庫**並選取 ***SYSTEM** 作爲要開啓的憑證庫。
5. 當顯示「憑證庫與密碼」頁時，提供您對 V5R2 目標系統建立憑證時，在*主電腦*系統上對憑證庫指定的密碼，然後按一下**繼續**。
6. 在導覽頁框中，選取**管理憑證庫**，再從作業清單中選取**變更密碼**。完成套表來變更憑證庫密碼。變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。接著，您可以指定哪些應用程式應對 SSL 階段作業使用憑證。
7. 在導覽頁框中，按一下**選取憑證庫**並選取 ***SYSTEM** 作爲要開啓的憑證庫。
8. 當顯示「憑證庫與密碼」頁時，提供新密碼，然後按一下**繼續**。
9. 在導覽頁框重新整理之後，選取導覽頁框中的**管理憑證**來顯示作業清單。
10. 從作業清單中，選取**指派憑證**來顯示現行憑證庫中的憑證清單。
11. 選取您在*主電腦*系統上所建立的憑證，然後按一下**指派給應用程式**，以顯示您可將憑證指派至其中的 SSL 型應用程式清單。
12. 選取應對 SSL 階段作業使用憑證的應用程式，然後按一下**繼續**。 DCM 顯示一則訊息來確認您對應用程式選擇的憑證。

    註: 某些 SSL 型應用程式根據憑證來支援從屬站鑑別。具備這種支援的應用程式必須能夠鑑別憑證，才能提供資源存取權。因此，您必須爲應用程式 定義 CA 信任清單。這確定應用程式只驗證來自您指定爲可靠的 CA 的那些憑證。如果使用者或從屬站應用程式提出的憑證是來自非 CA 信任清單中指定爲可靠的 CA，則應用程式將不接受它作爲有效鑑別的基礎。

完成這些作業後，目標系統上的應用程式可使用另一個 iSeries 上區域 CA 所發出的憑證。不過，在開始對這些應用程式使用 SSL 之前，您必須配置應用程式使用 SSL。

使用者在透過 SSL 連線存取選定的應用程式之前，必須使用 DCM 來從主電腦系統中取得區域 CA 憑證的複本。根據 SSL 型應用程式的基本要求，區域 CA 憑證必須複製到使用者 PC 上的檔案，或下載到使用者瀏覽器中。

*SYSTEM 憑證庫存在 -- 將檔案當作「其它系統憑證庫」

如果 V5R2 目標系統已有 *SYSTEM 憑證庫，您必須決定如何使用憑證檔案。您可以選擇將轉送的憑證檔當作**其它系統憑證庫**。或者，選擇匯入專用憑證及其對應的區域 CA 憑證到現有的 *SYSTEM 憑證庫中。

其它系統憑證庫是使用者定義來儲存 SSL 憑證的次要憑證庫。您可以建立並使用它們來提供憑證給使用者撰寫的 SSL 型應用程式，這些應用程式不透過 DCM API 來使用 DCM 功能登記應用程式 ID。其它系統憑證庫選項可讓您管理您或其他人撰寫的應用程式的憑證，這些應用程式使用 SSL_Init API，以程式設計方式存取及使用憑證來建立 SSL 階段作業。此 API 可讓應用程式使用憑證庫的預設憑證，而不是您特別識別的憑證。

IBM iSeries 應用程式（以及許多其它軟體程式開發者的應用程式）被撰寫成僅使用 *SYSTEM 憑證庫中的憑證。如果您選擇使用轉送的檔案作爲「其它系統憑證庫」，則無法使用 DCM 來指定哪些應用程式應對 SSL 階段作業使用憑證。因此，您無法配置

標準 iSeries SSL 型應用程式來使用此憑證。如果您要將憑證用於 iSeries 應用程式，您必須將憑證從轉送的憑證庫檔案匯入 *SYSTEM 憑證庫中。

若存取及使用轉送的憑證檔案作爲「其它系統憑證庫」，請遵循下列步驟：

1. 啓動 DCM。
2. 在導覽頁框中，按一下**選取憑證庫**，然後選取**其它系統憑證庫**作爲要開啓的憑證庫。
3. 當顯示「憑證庫與密碼」頁時，提供您從主電腦系統轉送的憑證庫檔案（副檔名爲 .KDB 的檔案）之完整路徑和檔名。同時提供您對 V5R2 目標系統建立憑證時，在*主電腦*系統上對憑證庫指定的密碼，然後按一下**繼續**。
4. 在導覽頁框中，選取**管理憑證庫**，再從作業清單中選取**變更密碼**。完成套表來變更憑證庫密碼。

   註: 當變更憑證庫密碼時，請務必選取**自動登入**選項。使用此選項可讓 DCM 儲存新密碼，以便您使用新憑證庫上所有 DCM 憑證管理功能。

   變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。接著，您可以指定此憑證庫中的憑證作爲預設憑證。
5. 在導覽頁框中，按一下**選取憑證庫**，然後選取**其它系統憑證庫**作爲要開啓的憑證庫。
6. 當顯示「憑證庫與密碼」頁時，提供憑證庫檔案的完整路徑和檔名、提供新密碼，然後按一下**繼續**。
7. 在導覽頁框重新整理之後，選取**管理憑證庫**，再從作業清單中選取**設定預設憑證**。

現在您已建立及配置「其它系統憑證庫」了，任何使用 SSL_Init API 的應用程式皆可使用其中的憑證來建立 SSL 階段作業。

*SYSTEM 憑證庫存在 -- 使用現有的 *SYSTEM 憑證庫中的憑證

您可以使用 V5R2 系統上現有的 *SYSTEM 憑證庫內轉送的憑證庫檔案中的憑證。若要這麼做，您必須將憑證庫檔案中的憑證匯入現有的 *SYSTEM 憑證庫中。不過，您無法直接從 .KDB 及 .RDB 檔案匯入憑證，因爲它們的格式不是 DCM 匯入功能可辨識及使用的格式。若要使用現有的 *SYSTEM 憑證庫中轉送的憑證，您必須將檔案開啓爲「其它系統憑證庫」，然後將它們匯出到 *SYSTEM 憑證庫。

若要將憑證庫檔案中的憑證匯出到 *SYSTEM 憑證庫，請在 V5R2 目標系統上完成下列步驟：

1. 啓動 DCM。
2. 在導覽頁框中，按一下**選取憑證庫**，然後指定**其它系統憑證庫**作爲要開啓的憑證庫。
3. 當顯示「憑證庫與密碼」頁時，提供您從主電腦系統轉送的憑證庫檔案（副檔名爲 .KDB 的檔案）之完整路徑和檔名。同時提供您對 V5R2 目標系統建立憑證時，在*主電腦*系統上對憑證庫指定的密碼，然後按一下**繼續**。
4. 在導覽頁框中，選取**管理憑證庫**，再從作業清單中選取**變更密碼**。完成套表來變更憑證庫密碼。

   註: 當變更憑證庫密碼時，請務必選取**自動登入**選項。使用此選項可讓 DCM 儲存新密碼，以便您使用新憑證庫上所有 DCM 憑證管理功能。如果您沒有變更密碼但選取「自動登入」選項，則將此憑證庫中的憑證匯出到 *SYSTEM 憑證庫

時，可能發生錯誤。

變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。

5. 在導覽頁框中，按一下**選取憑證庫**，然後選取**其它系統憑證庫**作爲要開啓的憑證庫。
6. 當顯示「憑證庫與密碼」頁時，提供憑證庫檔案的完整路徑和檔名、提供新密碼，然後按一下**繼續**。
7. 在導覽頁框重新整理之後，選取導覽頁框中的**管理憑證**來顯示作業清單，然後選取**匯出憑證**。
8. 選取**認證中心 (CA)** 爲匯出的憑證類型，然後按一下**繼續**。

   註: 將伺服器或從屬站憑證匯出到憑證庫之前，您應該先將區域 CA 憑證匯出到憑證庫。如果您先匯出伺服器或從屬站憑證，則可能發生錯誤，因爲區域 CA 憑證不存在於憑證庫中。
9. 選取要匯出的區域 CA 憑證，然後按一下**匯出**。
10. 選取**憑證庫**爲匯出的憑證目的地，然後按一下**繼續**。
11. 輸入 *SYSTEM 爲目標憑證庫，輸入 *SYSTEM 憑證庫密碼，然後按一下**繼續**。會顯示訊息指出憑證順利匯出，如果匯出程序失敗則提供錯誤資訊。
12. 現在，您可以將伺服器或從屬站憑證匯出到 *SYSTEM 憑證庫。重新選取**匯出憑證**作業。
13. 選取**伺服器或從屬站**爲匯出的憑證類型，然後按一下**繼續**。
14. 選取要匯出的適當伺服器或從屬站憑證，然後按一下**匯出**。
15. 選取**憑證庫**爲匯出的憑證目的地，然後按一下**繼續**。
16. 輸入 *SYSTEM 爲目標憑證庫，輸入 *SYSTEM 憑證庫密碼，然後按一下**繼續**。會顯示訊息指出憑證順利匯出，如果匯出程序失敗則提供錯誤資訊。
17. 現在，您可以將憑證指派給用於 SSL 的應用程式。在導覽頁框中，按一下**選取憑證庫**，然後選取 ***SYSTEM** 爲要開啓的憑證庫。
18. 當顯示「憑證庫與密碼」頁時，提供 *SYSTEM 憑證庫密碼，然後按一下**繼續**。
19. 在導覽頁框重新整理之後，選取**管理憑證**以顯示作業清單。
20. 從作業清單中，選取**指派憑證**來顯示現行憑證庫中的憑證清單。
21. 選取您在*主電腦*系統上所建立的憑證，然後按一下**指派給應用程式**，以顯示您可將憑證指派至的 SSL 型應用程式清單。
22. 選取應對 SSL 階段作業使用憑證的應用程式，然後按一下**繼續**。DCM 顯示一則訊息來確認您對應用程式選擇的憑證。

    註: 某些 SSL 型應用程式根據憑證來支援從屬站鑑別。具備這種支援的應用程式必須能夠鑑別憑證，才能提供資源存取權。因此，您必須爲應用程式 定義 CA 信任清單。這確定應用程式只驗證來自您指定爲可靠的 CA 的那些憑證。如果使用者或從屬站應用程式提出的憑證是來自非 CA 信任清單中指定爲可靠的 CA，則應用程式將不接受它作爲有效鑑別的基礎。

完成這些作業後，目標系統上的應用程式可使用另一個 iSeries 上區域 CA 所發出的憑證。不過，在開始對這些應用程式使用 SSL 之前，您必須配置應用程式使用 SSL。

使用者在透過 SSL 連線存取選定的應用程式之前，必須使用 DCM 來從主電腦系統中取得區域 CA 憑證的複本。根據 SSL 型應用程式的基本要求，區域 CA 憑證必須複製到使用者 PC 上的檔案，或下載到使用者瀏覽器中。

將專用憑證用於 V5R1 目標系統上的 SSL 階段作業

您可以從「數位憑證管理程式 (DCM)」的 *SYSTEM 憑證庫中，管理您應用程式用於 SSL 階段作業的憑證。如果您從未使用 V5R1 目標系統上的 DCM 來管理 SSL 的憑證，則這個憑證庫不應存在於目標系統上。使用您在區域 CA 主電腦系統上所建立轉送的憑證庫檔案之作業，視 *SYSTEM 憑證庫是否存在而有不同。如果 *SYSTEM 憑證庫 不存在，您可以使用轉送的憑證檔作爲建立 *SYSTEM 憑證庫的方法。如果 *SYSTEM 憑證庫存在於 V5R1 目標系統上，您可以藉由下列兩方法之一來使用轉送的憑證檔：

- 將轉送的檔案當作其它系統憑證庫。
- 將轉送的檔案匯入現有的 *SYSTEM 憑證庫中。

*SYSTEM 憑證庫不存在

如果 *SYSTEM 憑證庫不存在於您要使用轉送的憑證庫檔案之 V5R1 系統上，您可以將轉送的憑證檔當作 *SYSTEM 憑證庫。若要使用 V5R1 目標系統上的憑證檔，請遵循下列步驟：

1. 請確定您在管理區域 CA 的系統上所建立的憑證庫檔案（兩個檔案：一個具有 .KDB 副檔名，另一個具有 .RDB 副檔名）位於 /QIBM/USERDATA/ICSS/CERT/SERVER 目錄中。
2. 一旦轉送的憑證檔位於 /QIBM/USERDATA/ICSS/CERT/SERVER 目錄中，請將這些檔案更名爲 DEFAULT.KDB 及 DEFAULT.RDB。藉由在適當目錄中更名這些檔案，您可以建立包含目標系統的 *SYSTEM 憑證庫之元件。憑證庫檔案已包含許多公用網際網路 CA 的憑證複本。DCM 會將這些複本及區域 CA 憑證的複本新增到您所建立的憑證庫檔案中。

   注意: 如果您目標系統的 /QIBM/USERDATA/ICSS/CERT/SERVER 目錄中已有 DEFAULT.KDB 和 DEFAULT.RDB 檔，表示 *SYSTEM 憑證庫目前存在於這個目標系統上。所以，建議不要將轉送的檔案更名。改寫預設檔案會在使用 DCM、轉送的憑證庫及其內容時產生問題。所以，您應該確定它們有唯一的名稱，而且應將轉送的憑證庫當作 **其它系統憑證庫**。如果您將檔案當作「其它系統憑證庫」，則無法使用 DCM 來指定哪些應用程式應使用憑證。
3. 啓動 DCM。現在，您必須變更 *SYSTEM 憑證庫的密碼，這是您以更名轉送的檔案的方式所建立的憑證庫。變更密碼可讓 DCM 儲存新密碼，以便您使用憑證庫上所有 DCM 憑證管理功能。
4. 在導覽頁框中，按一下**選取憑證庫**並選取 ***SYSTEM** 作爲要開啓的憑證庫。
5. 當顯示「憑證庫與密碼」頁時，提供您對 V5R1 目標系統建立憑證時，在*主電腦*系統上對憑證庫指定的密碼，然後按一下**繼續**。
6. 在導覽頁框中，選取**管理憑證庫**，再從作業清單中選取**變更密碼**。完成套表來變更憑證庫密碼。變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。接著，您可以指定哪些應用程式應對 SSL 階段作業使用憑證。
7. 在導覽頁框中，按一下**選取憑證庫**並選取 ***SYSTEM** 作爲要開啓的憑證庫。
8. 當顯示「憑證庫與密碼」頁時，提供新密碼，然後按一下**繼續**。
9. 在導覽頁框重新整理之後，選取導覽頁框中的**管理應用程式**來顯示作業清單。
10. 從作業清單中，選取**更新憑證分派**來顯示您可對其指派憑證的 SSL 型應用程式清單。
11. 從清單中選取應用程式，然後按一下**更新憑證分派**。
12. 選取*主電腦*系統上區域 CA 發出的憑證，然後按一下**指派新的憑證**。 DCM 顯示一則訊息來確認您對應用程式選擇的憑證。

註: 某些 SSL 型應用程式根據憑證來支援從屬站鑑別。具備這種支援的應用程式必須能夠鑑別憑證，才能提供資源存取權。因此，您必須爲應用程式定義 CA 信任清單。這確定應用程式只驗證來自您指定爲可靠的 CA 的那些憑證。如果使用者或從屬站應用程式提出的憑證是來自非 CA 信任清單中指定爲可靠的 CA，則應用程式將不接受它作爲有效鑑別的基礎。

完成這些作業後，目標系統上的應用程式可使用另一個 iSeries 上區域 CA 所發出的憑證。不過，在開始對這些應用程式使用 SSL 之前，您必須配置應用程式使用 SSL。

使用者在透過 SSL 連線存取選定的應用程式之前，必須使用 DCM 來從主電腦系統中取得區域 CA 憑證的複本。根據 SSL 型應用程式的基本要求，CA 憑證必須複製到使用者 PC 上的檔案，或下載到使用者瀏覽器中。

*SYSTEM 憑證庫存在 -- 將檔案當作「其它系統憑證庫」

如果 V5R1 目標系統已有 *SYSTEM 憑證庫，您必須決定如何使用憑證檔案。您可以選擇將轉送的憑證檔當作**其它系統憑證庫**。或者，選擇匯入專用憑證及其對應的區域 CA 憑證到現有的 *SYSTEM 憑證庫中。

其它系統憑證庫是使用者定義來儲存 SSL 憑證的次要憑證庫。您可以建立並使用它們來提供憑證給使用者撰寫的 SSL 型應用程式，這些應用程式不透過 DCM API 來使用 DCM 公用程式登記應用程式 ID。其它系統憑證庫選項可讓您管理您或其他人撰寫的應用程式的憑證，這些應用程式使用 SSL_Init API，以程式設計方式存取及使用憑證來建立 SSL 階段作業。此 API 可讓應用程式使用憑證庫的預設憑證，而不是您特別識別的憑證。

IBM iSeries 應用程式（以及許多其它軟體程式開發者的應用程式）被撰寫成僅使用 *SYSTEM 憑證庫中的憑證。如果您選擇使用轉送的檔案作爲「其它系統憑證庫」，則無法使用 DCM 來指定哪些應用程式應對 SSL 階段作業使用憑證。因此，您無法配置標準 iSeries SSL 型應用程式來使用此憑證。如果您要將憑證用於 iSeries 應用程式，您必須將憑證從轉送的憑證庫檔案匯入 *SYSTEM 憑證庫中。

若要存取及使用轉送的憑證檔案作爲「其它系統憑證庫」，請遵循下列步驟：

1. 啓動 DCM。
2. 在導覽頁框中，按一下**選取憑證庫**，然後選取**其它系統憑證庫**作爲要開啓的憑證庫。
3. 當顯示「憑證庫與密碼」頁時，提供您從主電腦系統轉送的憑證庫檔案（副檔名爲 .KDB 的檔案）之完整路徑和檔名。同時提供您對 V5R1 目標系統建立憑證時，在*主電腦*系統上對憑證庫指定的密碼，然後按一下**繼續**。
4. 在導覽頁框中，選取**管理憑證庫**，再從作業清單中選取**變更密碼**。完成套表來變更憑證庫密碼。

   註: 當變更憑證庫密碼時，請務必選取**自動登入**選項。使用此選項可讓 DCM 儲存新密碼，以便您使用新憑證庫上所有 DCM 憑證管理功能。

   變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。接著，您可以指定此憑證庫中的憑證作爲預設憑證。
5. 在導覽頁框中，按一下**選取憑證庫**，然後選取**其它系統憑證庫**作爲要開啓的憑證庫。
6. 當顯示「憑證庫與密碼」頁時，提供憑證庫檔案的完整路徑和檔名、提供新密碼，然後按一下**繼續**。

7. 在導覽頁框重新整理之後，選取**管理憑證庫**，再從作業清單中選取**設定預設憑證**。

現在您已建立及配置「其它系統憑證庫」了，任何使用 SSL_Init API 的應用程式皆可使用其中的憑證來建立 SSL 階段作業。

*SYSTEM 憑證庫存在 -- 使用現有的 *SYSTEM 憑證庫中的憑證

您可以使用 V5R1 系統上現有的 *SYSTEM 憑證庫內轉送的憑證庫檔案中的憑證。若要這麼做，您必須將憑證庫檔案中的憑證匯入現有的 *SYSTEM 憑證庫中。不過，您無法直接從 .KDB 及 .RDB 檔案匯入憑證，因爲它們的格式不是 DCM 匯入功能可辨識及使用的格式。若要使用現有的 *SYSTEM 憑證庫中轉送的憑證，您必須將檔案開啓爲「其它系統憑證庫」，然後將它們匯出到 *SYSTEM 憑證庫。

註: 此程序說明如何使用目標系統上的「其它系統憑證庫」，將原始憑證庫中的憑證匯出到 *SYSTEM 憑證庫。當目標系統使用的密碼存取提供者產品（例如 5722-AC2）比主電腦系統的功能還要弱時，使用此方法將憑證新增至 *SYSTEM 憑證庫，可協助您避免發生可能的問題。

若要將憑證庫檔案中的憑證匯出到 *SYSTEM 憑證庫，請在 V5R1 目標系統上完成下列步驟：

1. 啓動 DCM。
2. 在導覽頁框中，按一下**選取憑證庫**，然後指定**其它系統憑證庫**作爲要開啓的憑證庫。
3. 當顯示「憑證庫與密碼」頁時，提供您從主電腦系統轉送的憑證庫檔案（副檔名爲 .KDB 的檔案）之完整路徑和檔名。同時提供您對 V5R1 目標系統建立憑證時，在*主電腦*系統上對憑證庫指定的密碼，然後按一下**繼續**。
4. 在導覽頁框中，選取**管理憑證庫**，再從作業清單中選取**變更密碼**。完成套表來變更憑證庫密碼。

   註: 當變更憑證庫密碼時，請務必選取**自動登入**選項。使用此選項可讓 DCM 儲存新密碼，以便您使用新憑證庫上所有 DCM 憑證管理功能。如果您沒有變更密碼但選取「自動登入」選項，則將此憑證庫中的憑證匯出到 *SYSTEM 憑證庫時，可能發生錯誤。

   變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。
5. 在導覽頁框中，按一下**選取憑證庫**，然後選取**其它系統憑證庫**作爲要開啓的憑證庫。
6. 當顯示「憑證庫與密碼」頁時，提供憑證庫檔案的完整路徑和檔名、提供新密碼，然後按一下**繼續**。
7. 在導覽頁框重新整理之後，選取導覽頁框中的**管理憑證**來顯示作業清單，然後選取**匯出憑證**。
8. 選取**認證中心 (CA)** 爲匯出的憑證類型，然後按一下**繼續**。

   註: 將伺服器或從屬站憑證匯出到憑證庫之前，您應該先將區域 CA 憑證匯出到憑證庫。如果您先匯出伺服器或從屬站憑證，則可能發生錯誤，因爲區域 CA 憑證不存在於憑證庫中。
9. 選取要匯出的區域 CA 憑證，然後按一下**匯出**。
10. 選取**憑證庫**爲匯出的憑證目的地，然後按一下**繼續**。
11. 輸入 *SYSTEM 爲目標憑證庫，輸入 *SYSTEM 憑證庫密碼，然後按一下**繼續**。

12. 現在，您可以將伺服器或從屬站憑證匯出到 *SYSTEM 憑證庫。重新選取**匯出憑證**作業。
13. 選取**伺服器或從屬站**爲匯出的憑證類型，然後按一下**繼續**。
14. 選取要匯出的適當伺服器或從屬站憑證，然後按一下**匯出**。
15. 選取**憑證庫**爲匯出的憑證目的地，然後按一下**繼續**。
16. 輸入 *SYSTEM 爲目標憑證庫，輸入 *SYSTEM 憑證庫密碼，然後按一下**繼續**。會顯示訊息指出憑證順利匯出，如果匯出程序失敗則提供錯誤資訊。
17. 現在，您可以將憑證指派給用於 SSL 的應用程式。在導覽頁框中，按一下**選取憑證庫**，然後選取 ***SYSTEM*** 爲要開啓的憑證庫。
18. 當顯示「憑證庫與密碼」頁時，提供 *SYSTEM 憑證庫密碼，然後按一下**繼續**。
19. 在導覽頁框重新整理之後，選取**管理憑證**以顯示作業清單。
20. 從作業清單中，選取**更新憑證分派**來顯示您可對其指派憑證的 SSL 型應用程式清單。
21. 從清單中選取應用程式，然後按一下**更新憑證分派**。
22. 選取*主電腦*系統上區域 CA 發出的憑證，然後按一下**指派新的憑證**。 DCM 顯示一則訊息來確認您對應用程式選擇的憑證。

    註: 某些 SSL 型應用程式根據憑證來支援從屬站鑑別。具備這種支援的應用程式必須能夠鑑別憑證，才能提供資源存取權。因此，您必須爲應用程式 定義 CA 信任清單。這確定應用程式只驗證來自您指定爲可靠的 CA 的那些憑證。如果使用者或從屬站應用程式提出的憑證是來自非 CA 信任清單中指定爲可靠的 CA，則應用程式將不接受它作爲有效鑑別的基礎。

完成這些作業後，目標系統上的應用程式可使用另一個 iSeries 上區域 CA 所發出的憑證。不過，在開始對這些應用程式使用 SSL 之前，您必須配置應用程式使用 SSL。

使用者在透過 SSL 連線存取選定的應用程式之前，必須使用 DCM 來從主電腦系統中取得區域 CA 憑證的複本。根據 SSL 型應用程式的基本要求，CA 憑證必須複製到使用者 PC 上的檔案，或下載到使用者瀏覽器中。

將專用憑證用於 V5R2 或 V5R1 目標系統上的簽署物件

您可以從「數位憑證管理程式 (DCM)」的 *OBJECTSIGNING 憑證庫中，管理您用於簽署物件的憑證。如果您從未使用目標系統上的 DCM 來管理物件簽署憑證，則這個憑證庫不應存在於目標系統上。若要使用您在區域 CA 主電腦系統上所建立的轉送憑證庫檔案，您必須執行的作業將視 *OBJECTSIGNING 憑證庫是否存在而有不同。如果 *OBJECTSIGNING 憑證庫不存在，您可以使用轉送的憑證檔作爲建立 *OBJECTSIGNING 憑證庫的方法。如果 *OBJECTSIGNING 憑證庫存在於目標系統上，您必須將轉送的憑證匯入其中。

*OBJECTSIGNING 憑證庫不存在

若要使用您在區域 CA 主電腦系統上所建立的憑證庫檔案，您所執行的作業視您是否曾在目標系統上使用 DCM 來管理物件簽署憑證而有不同。

如果 *OBJECTSIGNING 憑證庫不存在於具有轉送的憑證庫檔案之 V5R2 或 V5R1 目標系統上，請遵循下列步驟：

1. 請確定您在裝載區域 CA 的系統上所建立的憑證庫檔案（兩個檔案：一個具有 .KDB 副檔名，另一個具有 .RDB 副檔名）位於 /QIBM/USERDATA/ICSS/CERT/SIGNING 目錄中。

2. 一旦轉送的憑證檔位於 /QIBM/USERDATA/ICSS/CERT/SIGNING 目錄中，必要時，請將憑證檔更名爲 SGNOBJ.KDB 及 SGNOBJ.RDB。藉由更名這些檔案，您可以建立包含目標系統的 *OBJECTSIGNING 憑證庫之元件。憑證庫檔案已包含許多公用網際網路 CA 的憑證複本。DCM 會將這些複本及區域 CA 憑證的複本新增到您所建立的憑證庫檔案中。

   注意: 如果您目標系統的 /QIBM/USERDATA/ICSS/CERT/SIGNING 目錄中已有 SGNOBJ.KDB 和 SGNOBJ.RDB 檔，表示 *OBJECTSIGNING 憑證庫目前存在於這個目標系統上。所以，建議不要將轉送的檔案更名。改寫預設物件簽署檔案會在使用 DCM、轉送的憑證庫及其內容時產生問題。您可以使用下列兩方法之一，從這些檔案中取得憑證來匯入現有的 *OBJECTSIGNING 憑證庫中。您可以將這個檔案中的憑證匯出到一組純文字檔，從其中將憑證匯入現有的 *OBJECTSIGNING 憑證庫中。或者，您可以將轉送的檔案開啓爲「其它系統憑證庫」，然後將憑證直接匯出至 *OBJECTSIGNING 憑證庫中，如本資料中詳述。無論哪一種情況，如果您想要管理應用程式，如本程序描述地來使用它們，則必須將憑證匯入至 *OBJECTSIGNING 憑證庫中。
3. 啓動 DCM。現在，您必須變更 *OBJECTSIGNING 憑證庫密碼。變更密碼可讓 DCM 儲存新密碼，以便您使用憑證庫上所有 DCM 憑證管理功能。
4. 在導覽頁框中，按一下**選取憑證庫**並選取 ***OBJECTSIGNING** 作爲要開啓的憑證庫。
5. 當顯示密碼頁時，提供您在主電腦系統上建立憑證庫時所指定的密碼，然後按一下**繼續**。
6. 在導覽頁框中，選取**管理憑證庫**，再從作業清單中選取**變更密碼**。完成套表來變更憑證庫密碼。變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。接著，您可以建立應用程式定義，使用憑證來簽署物件。
7. 在重新開啓憑證庫之後，選取導覽頁框中的**管理應用程式** 來顯示作業清單。
8. 從作業清單中，選取**新增應用程式**，開始建立物件簽署應用程式定義的程序，以使用憑證來簽署物件。
9. 完成套表來定義您的物件簽署應用程式，然後按一下**新增**。此應用程式定義並未描述一個實際的應用程式，而是說明您打算使用特定憑證來簽署的物件類型。使用線上說明來瞭解如何完成套表。
10. 按一下**確定**以認可應用程式定義確認訊息，並顯示**管理應用程式**作業清單。
11. 從作業清單中，選取**更新憑證分派**來顯示您可對其指派憑證的物件簽署應用程式 ID 清單。
12. 從清單中選取您的應用程式 ID，然後按一下**更新憑證分派**。
13. 選取主電腦系統上區域 CA 建立的憑證，然後按一下**指派新的憑證**。

完成這些作業後，您就可以開始簽署物件來確保其完整性。

當您分送簽署的物件時，物件接收者必須使用 V5R2 或 V5R1 版本 DCM 來對物件驗證簽章，以確保資料沒有變更並驗證傳送者的身份。若要驗證簽章，接收者必須有簽章驗證憑證複本。您應該提供此憑證的複本作爲已簽署物件的封裝組件之一。

接收者也必須擁有發出您用來簽署物件的憑證之 CA 的 CA 憑證複本。如果您簽署的物件具有來自知名網際網路 CA 的憑證，接收者的 DCM 版本應已有必要的 CA 憑證複本。不過必要時您應該連同簽署的物件，以個別套件提供 CA 憑證的複本。例如，如果您簽署的物件具有來自區域 CA 的憑證，您應該提供區域 CA 憑證的複本。基於安全考量，您應該以個別套件提供 CA 憑證，或基於需求者的要求公開提供 CA 憑證。

*OBJECTSIGNING 憑證庫存在

您可以使用 V5R1 或 V5R2 系統上現有的 *OBJECTSIGNING 憑證庫內轉送的憑證庫檔案中的憑證。若要這麼做，您必須將憑證庫檔案中的憑證匯入現有的 *OBJECTSIGNING 憑證庫中。不過，您無法直接從 .KDB 及 .RDB 檔案匯入憑證，因爲它們的格式不是 DCM 匯入功能可辨識及使用的格式。您可以藉由在 V5R2 或 V5R1 目標系統上將轉送的檔案開啓爲「其它系統憑證庫」，來將憑證新增至現有的 *OBJECTSIGNING 憑證庫中。然後，您可以將憑證直接匯出到 *OBJECTSIGNING 憑證庫。您必須從轉送的檔案匯出物件簽署憑證本身及區域 CA 憑證兩者的複本。

若要將憑證庫檔案中的憑證直接匯出到 *OBJECTSIGNING 憑證庫，請在 V5R2 或 V5R1 目標系統上完成下列步驟：

1. 啓動 DCM。
2. 在導覽頁框中，按一下**選取憑證庫**，然後指定**其它系統憑證庫**作爲要開啓的憑證庫。
3. 當顯示「憑證庫與密碼」頁時，提供憑證庫檔案的完整路徑和檔名。同時提供您在主電腦系統上建立憑證庫時所使用的密碼，然後按一下**繼續**。
4. 在導覽頁框中，選取**管理憑證庫**，再從作業清單中選取**變更密碼**。完成套表來變更憑證庫密碼。

   註: 當變更憑證庫密碼時，請務必選取**自動登入**選項。使用此選項可讓 DCM 儲存新密碼，以便您使用新憑證庫上所有 DCM 憑證管理功能。如果您沒有變更密碼但選取「自動登入」選項，則將此憑證庫中的憑證匯出到 *OBJECTSIGNING 憑證庫時，可能發生錯誤。

   變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。
5. 在導覽頁框中，按一下**選取憑證庫**，然後選取**其它系統憑證庫**作爲要開啓的憑證庫。
6. 當顯示「憑證庫與密碼」頁時，提供憑證庫檔案的完整路徑和檔名、提供新密碼，然後按一下**繼續**。
7. 在導覽頁框重新整理之後，選取導覽頁框中的**管理憑證**來顯示作業清單，然後選取**匯出憑證**。
8. 選取**認證中心 (CA)** 爲匯出的憑證類型，然後按一下**繼續**。

   註: 此作業的用語假設您使用「其它系統憑證庫」時是使用伺服器或從屬站憑證。這是因爲此類型憑證庫係設計來作爲 *SYSTEM 憑證庫的次要憑證庫。不過，在這個憑證庫中使用匯出作業，是將轉送的檔案中憑證新增到現有的 *OBJECTSIGNING 憑證庫的最簡單方法。
9. 選取要匯出的區域 CA 憑證，然後按一下**匯出**。

   註: 將物件簽署憑證匯出到憑證庫之前，您應該先將區域 CA 憑證匯出到憑證庫。如果您先匯出物件簽署憑證，則可能發生錯誤，因爲區域 CA 憑證不存在於憑證庫中。
10. 選取**憑證庫**爲匯出的憑證目的地，然後按一下**繼續**。
11. 輸入 *OBJECTSIGNING 爲目標憑證庫，輸入憑證庫密碼，然後按一下**繼續**。
12. 現在，您可以將物件簽署憑證匯出到 *OBJECTSIGNING 憑證庫。重新選取**匯出憑證**作業。
13. 選取**伺服器或從屬站**爲匯出的憑證類型，然後按一下**繼續**。
14. 選取要匯出的適當憑證，然後按一下**匯出**。
15. 選取**憑證庫**爲匯出的憑證目的地，然後按一下**繼續**。

16. 輸入 *OBJECTSIGNING 爲目標憑證庫，輸入 *OBJECTSIGNING 憑證庫密碼，然後按一下**繼續**。會顯示訊息指出憑證順利匯出，如果匯出程序失敗則提供錯誤資訊。

    註: 若要使用此憑證來簽署物件，您必須立即指派憑證給物件簽署應用程式。

將專用憑證用於 V4R5 或 V4R4 目標系統上的 SSL 階段作業

您可以從「數位憑證管理程式 (DCM)」的 *SYSTEM 憑證庫中，管理您應用程式用於 SSL 階段作業的憑證。如果您從未使用 V4R5 或 V4R4 目標系統上的 DCM 來管理 SSL 的憑證，則這個憑證庫不應存在於目標系統上。您在區域 CA 主電腦系統上所建立的已轉送憑證庫檔案中含有兩個憑證。這些檔案是您建立的伺服器或從屬站憑證，以及您用來簽署的專用區域 CA 憑證。

您必須使用轉送的憑證庫檔案來執行的作業，視 *SYSTEM 憑證庫是否存在而有不同。如果 *SYSTEM 憑證庫 不存在 ，您可以使用轉送的憑證檔作爲建立 *SYSTEM 憑證庫的方法。如果 *SYSTEM 憑證庫存在於目標系統上，您可以藉由下列兩方法之一來使用轉送的憑證檔：

- 將轉送的檔案當作其它系統憑證庫。
- 將轉送的檔案匯入現有的 *SYSTEM 憑證庫中。

*SYSTEM 憑證庫不存在

如果 *SYSTEM 憑證庫不存在於您要使用轉送的憑證庫檔案所在的 V4R5 或 V4R4 系統上，請遵循下列步驟：

1. 請確定您在裝載區域 CA 的系統上所建立的憑證庫檔案（兩個檔案：一個具有 .KDB 副檔名，另一個具有 .RDB 副檔名）位於 /QIBM/USERDATA/ICSS/CERT/SERVER 目錄中。
2. 一旦轉送的憑證檔位於 /QIBM/USERDATA/ICSS/CERT/SERVER 目錄中，請將這些檔案更名爲 DEFAULT.KDB 及 DEFAULT.RDB。藉由在適當目錄中更名這些檔案，您可以建立包含目標系統的 *SYSTEM 憑證庫之元件。憑證庫檔案已包含許多公用網際網路 CA 的憑證複本。DCM 會將這些複本及區域 CA 憑證的複本新增到您所建立的憑證庫檔案中。

   注意: 如果您目標系統的 /QIBM/USERDATA/ICSS/CERT/SERVER 目錄中已有 DEFAULT.KDB 和 DEFAULT.RDB 檔，表示 *SYSTEM 憑證庫目前存在於這個目標系統上。所以，建議不要將轉送的檔案更名。改寫預設檔案會在使用 DCM、轉送的憑證庫及其內容時產生問題。所以，您應該確定它們有唯一的名稱，而且應將轉送的憑證庫檔案當作**其它**憑證庫。如果您將檔案當作「其它」憑證庫，則無法使用 DCM 來指定哪些應用程式應使用憑證。
3. 啓動 DCM。現在，您必須變更 *SYSTEM 憑證庫密碼。變更密碼可讓 DCM 儲存新密碼，以便您使用憑證庫上所有 DCM 憑證管理功能。
4. 在導覽頁框中，確定 *SYSTEM 顯示爲下拉清單方塊中的憑證庫，然後選取**系統憑證**來顯示可用的作業清單。即顯示**憑證庫與密碼**視窗。
5. 在適當的欄位中，輸入 *SYSTEM 表示要開啓的憑證庫，以及輸入使用主電腦系統上的區域 CA 建立檔案時使用的密碼。現在，您可以變更憑證庫的密碼。
6. 從導覽頁框的作業清單中，選取**變更密碼**。完成套表來變更憑證庫密碼。變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。
7. 在重新開啓 *SYSTEM 憑證庫之後，從作業清單中選取**使用安全應用程式**來顯示一頁，它可讓您管理與特定應用程式相關的憑證。

8. 從應用程式清單中，選取應在 SSL 階段作業使用轉送的專用憑證之應用程式。
9. 按一下**使用系統憑證**，然後選取主電腦系統上區域 CA 發出的憑證。
10. 按一下**指派新的憑證**，讓指定的應用程式使用選取的憑證。

註: 某些 SSL 型應用程式根據憑證來支援從屬站鑑別。將憑證用於從屬站鑑別，確保應用程式存取其控制的資源之前接收有效的憑證。具備這種支援的應用程式在鑑別特定 CA 發出的憑證之前，必須設定爲信任 CA。使用**使用認證中心**頁來確定 CA 憑證在憑證庫爲信任的狀態。然後，使用**使用安全應用程式**頁來確定使用憑證的應用程式信任發出憑證的區域 CA。這確定應用程式只驗證來自您指定爲可靠的 CA 的那些憑證。如果使用者或從屬站應用程式提出來自某個 CA 的憑證，而該 CA 不是指定爲信任的 CA，則應用程式不接受它作爲有效鑑別的基礎。

完成這些作業後，V4R5 或 V4R4 目標系統上的應用程式可使用另一個 iSeries 上的 V5R2 區域 CA 發出的憑證。不過，在開始對這些應用程式使用 SSL 之前，您必須配置應用程式使用 SSL。

使用者在透過 SSL 連線存取選定的應用程式之前，必須使用 DCM 來從主電腦系統中取得區域 CA 憑證的複本。根據 SSL 型應用程式的基本要求，CA 憑證必須複製到使用者 PC 上的檔案，或下載到使用者瀏覽器中。

*SYSTEM 憑證庫存在 -- 將檔案當作「其它系統憑證庫」

如果 V4R5 或 V4R4 目標系統已有 *SYSTEM 憑證庫，您必須決定如何使用憑證檔案。轉送的憑證庫檔案含有兩個憑證：一個是您所建立的伺服器或從屬站憑證，另一個是您用來簽署的專用區域 CA 憑證。您可以選擇將轉送的憑證檔當作**其它**系統憑證庫。或者，選擇匯入專用憑證及其對應 CA 憑證到現有的 *SYSTEM 憑證庫中。

如果您選擇將轉送的檔案當作**其它**系統憑證庫，則無法使用 DCM 來指定哪些應用程式應對 SSL 階段作業使用憑證。不過，您可以將這個憑證庫中的憑證指定爲憑證庫的預設憑證。「其它系統憑證庫」選項可讓您管理自己或其他人撰寫的應用程式憑證，使用 SSL_Init API 以程式設計方式存取及使用憑證來建立 SSL 階段作業。此 API 允許應用程式使用憑證庫的預設憑證，而非特定的憑證。

如果 *SYSTEM 憑證庫存在於您要使用轉送的憑證庫檔案所在的 V4R5 或 V4R4 系統上，請遵循下列步驟：

1. 啓動 DCM。現在，您必須變更轉送的憑證庫密碼。變更密碼可讓 DCM 儲存新密碼，以便您使用憑證庫上所有 DCM 憑證管理功能。
2. 在導覽頁框中，確定 OTHER 顯示爲下拉清單方塊中的憑證庫，然後選取**系統憑證**來顯示可用的作業清單。即顯示**憑證庫與密碼**視窗。
3. 在適當的欄位中，輸入您從區域 CA 主電腦系統轉送的憑證庫（副檔名爲 .KDB）之完整路徑和檔名。輸入您在*主電腦*系統上建立檔案時使用的密碼。現在，您可以變更憑證庫的密碼。
4. 在導覽頁框中，從「系統憑證」作業清單中選取**變更密碼**。完成套表來變更憑證庫密碼。

註: 變更憑證庫密碼時，請務必選取**自動登入**選項。使用此選項可讓 DCM 儲存新密碼，以便您使用新憑證庫上所有 DCM 憑證管理功能。

變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。接著，您可以指定此憑證庫中的憑證作爲預設憑證。

5. 在導覽頁框中，選取**使用憑證**來顯示一頁，它可讓您執行一些憑證管理作業。
6. 從憑證清單中，選取要作爲現行憑證庫預設憑證的憑證，然後按一下**設為預設值**。

現在您已建立及配置「其它」系統憑證庫，任何使用 SSL_Init API 的應用程式皆可使用其中的憑證來建立 SSL 階段作業。

*SYSTEM 憑證庫存在 -- 將檔案匯入現有的 *SYSTEM 憑證庫中

將憑證匯入 V4R5 或 V4R4 目標系統的 *SYSTEM 中之前，您必須先將所建立憑證庫中的憑證匯出到不同的檔案格式。然後，您可以將新檔案中的憑證匯入 *SYSTEM 憑證庫中。轉送的憑證庫檔案含有兩個憑證：一個是您所建立的伺服器或從屬站憑證，另一個是您用來簽署的專用區域 CA 憑證。您必須將建立的伺服器或從屬站憑證及專用區域 CA 憑證匯入 *SYSTEM 憑證庫中。

註: V4R5 和 V4R4 版 DCM 中可用的匯出功能不像 V5R2 版發展得那麼好，所以您在使用目標系統來匯出專用區域 CA 憑證時可能會遇到一些問題。因此，您應該使用 V5R2 主電腦系統將區域 CA 憑證的*其它*複本匯出到個別檔案，而非使用 V4R4 或 V4R5 目標系統來匯出。匯出 V5R2 主電腦系統上的區域 CA 憑證後，您可以手動將區域 CA 憑證匯出檔轉送到 V4R4 或 V4R5 目標系統，然後遵循此程序接下來提供的步驟，將區域 CA 憑證匯入 *SYSTEM 憑證庫中。在匯入使用區域 CA 建立的專用憑證*之前*，您必須先匯入區域 CA 憑證。如果您先匯入專用憑證，則可能發生錯誤，因爲區域 CA 憑證不存在於憑證庫中。

若要將憑證庫檔案中的憑證匯出，請在 V4R4 或 V4R5 目標系統上完成下列步驟：

1. 啓動 DCM。
2. 在導覽頁框中，確定 OTHER 顯示爲下拉清單方塊中的憑證庫，然後選取**系統憑證**來顯示可用的作業清單。即顯示**憑證庫與密碼**視窗。
3. 指定轉送的憑證庫檔案之完整路徑和檔名，提供您在*主電腦*系統上建立它們時使用的密碼，然後按一下**確定**。現在，您可以變更憑證庫的密碼。
4. 在導覽頁框中，從「系統憑證」作業清單中選取**變更密碼**。完成套表來變更憑證庫密碼。

   註: 當變更憑證庫密碼時，請務必選取**自動登入**選項。使用此選項可讓 DCM 儲存新密碼，以便您使用新憑證庫上所有 DCM 憑證管理功能。如果您沒有變更密碼並選取「自動登入」選項，則將此憑證庫中的憑證匯出時，可能發生錯誤。

   變更密碼之後，您必須重新開啓憑證庫，之後才能使用其中的憑證。
5. 在導覽頁框中，選取**使用憑證**來顯示憑證清單。
6. 從清單中選取專用憑證，然後按一下**匯出**來顯示「匯出憑證」頁。
7. 完成「匯出憑證」套表。

   註: 請確定所指定的檔名和副檔名是唯一的。例如，您可以將檔案命名爲 myfile.exp。爲檔案命名時，請勿使用下列其中一個副檔名： .TXT、.KDB、.RDB 或 .KYR，因爲使用這些其中一個副檔名可能會導致您匯入檔案中的憑證時發生錯誤。請選取將使用此憑證的目標系統的適當版次。選取的版次會影響匯出的憑證格式。
8. 按一下**確定**。頁頂端顯示一則訊息，指示 DCM 已將憑證匯出到您指定的檔案。

因此，您應該使用原始 V5R2 主電腦系統上的 DCM 來匯出區域 CA 憑證的額外複本，並手動將它轉送到 V4R4 或 V5R5 目標系統。您也應該使用此目標系統上的 DCM 將專用伺服器或從屬站憑證匯出到檔案。現在，您可以將這些憑證匯入 *SYSTEM 憑證庫

中。在匯入使用區域 CA 建立的專用憑證*之前*，您必須先匯入區域 CA 憑證。如果您先匯入專用憑證，則可能發生錯誤，因爲區域 CA 憑證不存在於憑證庫中。

若要匯入這些匯出檔案中的憑證及指定 SSL 型應用程式使用它們，請在 V4R4 或 V4R5 目標系統上完成下列步驟：

1. 啓動 DCM。
2. 在導覽頁框中，確定 *SYSTEM 顯示爲下拉清單方塊中的憑證庫，然後選取**系統憑證**來顯示可用的作業清單。即顯示**憑證庫與密碼**視窗。
3. 指定 *SYSTEM 爲要開啓的憑證庫，提供密碼，然後按一下**繼續**。
4. 現在，您必須從 V5R2 主電腦系統上所建立的匯出檔案中匯入區域 CA 憑證。在導覽頁框中，選取**接收 CA 憑證**來顯示套表。
5. 完成此套表，然後按一下**確定**來顯示「接收憑證順利完成」頁。當您使用 *SYSTEM 憑證庫時，此頁顯示您可設定爲信任匯入的 CA 憑證之應用程式清單。

   註: 某些 SSL 型應用程式根據憑證來支援從屬站鑑別。將憑證用於從屬站鑑別，確保應用程式存取其控制的資源之前接收有效的憑證。具備這種支援的應用程式在鑑別特定 CA 發出的憑證之前，必須設定爲信任 CA。這確定應用程式只驗證來自您指定爲可靠的 CA 的那些憑證。如果使用者或從屬站應用程式提出來自某個 CA 的憑證，而該 CA 不是指定爲信任的 CA，則應用程式不接受它作爲有效鑑別的基礎。
6. 選取應信任 CA 憑證的應用程式，然後按一下**確定**。顯示「安全應用程式狀態」頁，確認選取的應用程式設定爲信任新憑證。
7. 現在，您可以匯入伺服器憑證。在導覽頁框中，選取**使用憑證**來顯示憑證清單。
8. 按一下**匯入**來顯示「匯入憑證」頁。
9. 完成「匯入憑證」套表，然後按一下**確定**來返回「使用憑證」頁。請確定提供的檔名含有匯出的伺服器或從屬站憑證，並且確定所指定的目標版次符合您先前匯出憑證時所指定的版次。頁頂端顯示一則訊息，指示 DCM 已將憑證新增至現行憑證庫中。您匯入的憑證應該也出現在憑證清單中。
10. 現在，您必須指定哪些應用程式應對 SSL 使用匯入的專用憑證。在導覽頁框中，選取**使用安全應用程式**來顯示一頁，它可讓您管理與特定應用程式相關的憑證。
11. 從清單中選取應用程式，然後按一下**使用系統憑證**，以顯示可指定選取的應用程式用於建立 SSL 階段作業的憑證清單。
12. 從清單中選取憑證，然後按一下**指派新的憑證**，將選取的憑證指派給指定的應用程式。頁頂端顯示一則指示憑證選項的確認訊息。

完成這些作業後，V4R4 或 V4R5 目標系統上的應用程式可使用另一個 iSeries 上的區域 CA 所發出的憑證。不過，在開始對這些應用程式使用 SSL 之前，您必須 配置應用程式使用 SSL。

使用者在透過 SSL 連線存取選定的應用程式之前，必須使用 DCM 來從主電腦系統中取得區域 CA 憑證的複本。根據 SSL 型應用程式的基本要求，CA 憑證必須複製到使用者 PC 上的檔案，或下載到使用者瀏覽器中。

在 DCM 中管理應用程式

您可以使用「數位憑證管理程式」(DCM)，對 SSL 型應用程式和物件簽署應用程式執行各種管理作業。例如，您可以爲 Secure Sockets Layer (SSL) 通信階段作業來管理應用程式所用的憑證。您可以執行的應用程式管理作業視您使用的應用程式類型和憑證庫而定。您只能管理 *SYSTEM 或 *OBJECTSIGNING 憑證庫內的應用程式。

雖然 DCM 提供的大部份應用程式管理作業都很簡單，但有一些作業可能是您不熟悉的。關於這些作業的詳細資訊，請複查下列主題：

建立應用程式定義說明您可以定義和使用的應用程式類型。

管理憑證分派說明如何指派或變更應用程式在建立 SSL 階段作業或簽署物件時所用的憑證。

定義 CA 信任清單說明何時您可以和應該定義應用程式在驗證和接收憑證時可信任的「認證中心」。

您可以在線上說明中找到有關其他 DCM 作業的資訊。

建立應用程式定義

您在 DCM 中有兩種可以使用的應用程式定義類型：伺服器或從屬站應用程式的應用程式定義，應用程式使用 SSL 和您用來簽署物件的應用程式定義。

若要使用 DCM 來處理 SSL 應用程式定義及其憑證，應用程式首先必須向 DCM 登記成應用程式定義，使之具有唯一的應用程式 ID。應用程式開發者使用一個 API (QSYRGAP, QsyRegisterAppForCertUse) 在 DCM 中自動建立應用程式 ID，以登記 SSL 型應用程式。所有 IBM iSeries SSL 型應用程式皆向 DCM 登記，所以您可以輕易地使用 DCM 來指派憑證給應用程式，使之能夠建立 SSL 階段作業。另外，對於您撰寫或購買的應用程式，您可以建立應用程式定義並在 DCM 本身之內建立其應用程式 ID。您必須使用 *SYSTEM 憑證庫，才能爲從屬站應用程式或伺服器應用程式建立 SSL 應用程式定義。

若要使用憑證來簽署物件，您必須先定義一個讓憑證使用的應用程式。不同於 SSL 應用程式定義，物件簽署應用程式不說明實際的應用程式。相反地，您建立的應用程式定義應該說明您想要簽署的物件類型或群組。您必須使用 *OBJECTSIGNING 憑證庫，才能建立物件簽署應用程式定義。

若要建立應用程式定義，請遵循下列步驟：

1. 啓動 DCM。
2. 按一下**選取憑證庫**，選取適當的憑證庫。（此爲 *SYSTEM 憑證庫或 *OBJECTSIGNING 憑證庫，視您要建立的應用程式定義類型而定。）

   註: 如果您對於在此引導作業中完成特定套表有問題，請選取頁頂端的問號 (**?**) 來存取線上說明。
3. 顯示「憑證庫和密碼」頁時，請指定您在建立憑證庫時所指定的密碼，按一下**繼續**。
4. 在導覽頁框中，選取**管理應用程式**來顯示作業清單。
5. 從作業清單中選取**新增應用程式**來顯示一個定義應用程式的套表。

   註: 如果您使用 *SYSTEM 憑證庫，DCM 將提示您選擇新增伺服器應用程式定義，或從屬站應用程式定義。
6. 完成套表，按一下**新增**。您爲應用程式定義可指定的資訊視您要定義的應用程式類型而定。如果您要定義伺服器應用程式，則也可以指定應用程式是否可使用憑證來進行從屬站鑑別，以及是否應該要求從屬站鑑別。您也可以指定應用程式必須使用 CA 信任清單來鑑別憑證。

管理應用程式的憑證分派

您必須先使用「數位憑證管理程式」(DCM) 來指派憑證給應用程式，應用程式才能夠執行安全性功能，例如建立 Secure Sockets Layer (SSL) 階段作業或簽署物件。若要指派憑證給應用程式，或變更應用程式的憑證分派，請遵循下列步驟：

1. 啓動 DCM。
2. 按一下**選取憑證庫**，選取適當的憑證庫。（此爲 *SYSTEM 憑證庫或 *OBJECTSIGNING 憑證庫，視您指派憑證的應用程式類型而定。）

   註: 如果您對於在此引導作業中完成特定套表有問題，請選取頁頂端的問號 (**?**) 來存取線上說明。
3. 顯示「憑證庫和密碼」頁時，請指定您在建立憑證庫時所指定的密碼，按一下**繼續**。
4. 在導覽頁框中，選取**管理應用程式**來顯示作業清單。
5. 如果您使用 *SYSTEM 憑證庫，請選取要管理的應用程式類型。（適當地選取**伺服器**或**從屬站**應用程式。）
6. 在作業清單中，選取**更新憑證分派**來顯示可讓您指派憑證的應用程式清單。
7. 從清單中選取一個應用程式，按一下**更新憑證分派**來顯示您可指派給應用程式的憑證清單。
8. 從清單中選取憑證，按一下**指派新的憑證**。 DCM 會顯示訊息來確認您爲應用程式所選取的憑證。

   註: 如果您指派憑證給 SSL 型應用程式，且應用程式支援使用憑證來進行從屬站鑑別，則您必須爲應用程式定義 CA 信任清單。這確保應用程式只驗證您信任的 CA 所發出的憑證。如果使用者或從屬站應用程式提供的憑證不是來自於 CA 信任清單中的 CA，則應用程式不會接受此憑證做爲有效鑑別的基礎。

當您變更或移除應用程式的憑證時，如果應用程式正在執行中，則不一定會知道這項變更。例如，Client Access Express 伺服器將自動套用任何的憑證變更。不過，您可能需要停止再啓動 Telnet 伺服器、IBM HTTP Server for iSeries 或其他應用程式，才能使這些應用程式套用您的憑證變更。

從 V5R2 開始，當您想要一次指派一個憑證給數個應用程式時，您可以使用指派憑證作業。

定義應用程式的 CA 信任清單

支援在 Secure Sockets Layer (SSL) 階段作業期間使用憑證來進行從屬站鑑別的應用程式，必須決定是否接受憑證當做身份的有效證明。應用程式用來鑑別憑證的其中一個準則就是應用程式是否信任發出此憑證的「認證中心」(CA)。

您可以使用「數位憑證管理程式」(DCM) 來定義應用程式在執行憑證的從屬站鑑別時可以信任的 CA。您透過 CA 信任清單來管理應用程式所信任的 CA。

在定義應用程式的 CA 信任清單之前，必須先符合幾項條件：

- 應用程式必須支援使用憑證來進行從屬站鑑別。
- 應用程式的定義必須指定應用程式去使用 CA 信任清單。

如果應用程式的定義指定應用程式去使用 CA 信任清單，則您必須先定義此清單，應用程式才能夠順利執行憑證從屬站鑑別。這確保應用程式只驗證您信任的 CA 所發出的憑證。如果使用者或從屬站應用程式提供的憑證不是來自於 CA 信任清單中的 CA，則應用程式不會接受此憑證做爲有效鑑別的基礎。

當您新增一個 CA 到應用程式的信任清單時，您也必須確定此 CA 已啓用。

若要定義應用程式的 CA 信任清單，請遵循下列步驟：

1. 啓動 DCM。
2. 按一下**選取憑證庫**，選取 *SYSTEM 當做要開啓的憑證庫。

   註: 如果您對於在此引導作業中完成特定套表有問題，請選取頁頂端的問號 (**?**) 來存取線上說明。
3. 顯示「憑證庫和密碼」頁時，請指定您在建立憑證庫時所指定的密碼，按一下**繼續**。
4. 在導覽頁框中，選取**管理應用程式**來顯示作業清單。
5. 在作業清單中選取**定義 CA 信任清單**。
6. 選取您要定義清單的應用程式類型（伺服器或從屬站），按一下**繼續**。
7. 從清單中選取一個應用程式，按一下**繼續**，顯示您用來定義信任清單的 CA 憑證清單。
8. 選取應用程式應該信任的 CA，按一下**確定**。 DCM 會顯示訊息來確認您選擇的信任清單。

   註: 您可以從清單中選取個別的 CA，或指定應用程式應該信任清單中的所有 CA 或都不信任。在信任清單中新增 CA 憑證之前，您也可以先檢視或驗證 CA 憑證。

驗證憑證和應用程式

您可以使用數位憑證管理程式 (DCM) 來驗證個別憑證或使用它們的應用程式。根據您要驗證憑證或應用程式，DCM 檢查的項目清單稍有不同。

應用程式驗證

使用 DCM 驗證應用程式定義有助於防止應用程式在執行需要憑證的功能時發生憑證問題。這類問題會防止應用程式順利參與 Secure Sockets Layer (SSL) 階段作業或順利簽署物件。

當您驗證應用程式後，DCM 會驗證應用程式有一個憑證分派，並確定所指派的憑證有效。此外，如果應用程式配置爲使用認證中心 (CA) 信任清單，則 DCM 確定該信任清單至少包含一個 CA 憑證。然後 DCM 會驗證在該應用程式 CA 信任清單中的 CA 憑證是有效的。而且，如果應用程式定義指定憑證廢止清冊 (CRL) 處理程序發生，且 CA 有一個已定義的 CRL 位置，則 DCM 會檢查 CRL，這是驗證程序的一部份。

憑證驗證

當您驗證憑證後，DCM 會驗證專屬於該憑證的一些項目，以確定該憑證的確實性和有效性。驗證憑證可確定爲了安全通信或簽署物件而使用該憑證的應用程式在使用憑證時不太可能會遇到問題。

DCM 會檢查所選取的憑證是否未過期，這是驗證程序的一部份。如果發出憑證的 CA 有一個 CRL 位置存在，則 DCM 也會檢查該憑證在憑證廢止清冊 (CRL) 中是否未列爲撤回。此外，DCM 還會檢查發出的 CA 的 CA 憑證是在現行憑證庫內，而且已啓用該 CA 憑證，因此它是可靠的。如果憑證有私密金鑰（例如，伺服器、從屬站和物件簽署憑證），則 DCM 也會驗證公開-私密金鑰對，以確定公開-私密金鑰對相符。換句話說，DCM 會以公開金鑰加密資料，然後確定該資料可以用私密金鑰解密。

指派憑證給應用程式

從 V5R2 開始，新的數位憑證管理程式 (DCM) 加強功能可讓您快速而容易地指派憑證給多個應用程式。您只能從 *SYSTEM 或 *OBJECTSIGNING 憑證庫中指派憑證給多個應用程式。

要對一或多個應用程式進行憑證分派，請遵循下列步驟：

1. 啓動 DCM。

   註: 如果您對於如何使用 DCM 完成特定套表有問題，請選取問號 (**?**) （位於頁頂端）來存取線上說明。
2. 在導覽頁框中，按一下**選取憑證庫**並選取 ***OBJECTSIGNING** 或 ***SYSTEM** 作爲要開啓的憑證庫。
3. 輸入憑證庫的密碼並按一下**繼續**。
4. 在導覽頁框重新整理之後，選取**管理憑證**以顯示作業清單。
5. 從作業清單中，選取**指派憑證**以顯示現行憑證庫的憑證清單。
6. 從清單中選取一個憑證並按一下**指派至應用程式**以顯示現行憑證庫的應用程式定義清單。
7. 從清單中選取一或多個應用程式並按一下**繼續**。會出現一頁顯示您的分派選項的確認訊息，如果發生問題則顯示錯誤訊息。

管理 CRL 位置

數位憑證管理程式 (DCM) 可讓您定義及管理憑證廢止清冊 (CRL) 位置資訊，供特定的認證中心 (CA) 在憑證驗證程序中使用。 DCM 或需要 CRL 處理程序的應用程式，可使用 CRL 來判斷發出特定憑證的 CA 尚未撤回憑證。當您定義特定 CA 的 CRL 位置時，支援使用憑證來進行從屬站鑑別的應用程式可存取此 CRL。

支援使用憑證來進行從屬站鑑別的應用程式可執行 CRL 處理程序，以確保對它們所接受的有效識別證明的憑證做更嚴格的鑑別。在應用程式可以在憑證驗證程序中使用已定義的 CRL 之前，DCM 應用程式定義必須要求該應用程式執行 CRL 處理程序。

CRL 處理程序如何運作

當您使用 DCM 驗證憑證或應用程式時，在預設狀況下，DCM 會在驗證程序中執行 CRL 處理程序。如果沒有對發出您要驗證的憑證的 CA 定義 CRL 位置，則 DCM 無法執行 CRL 檢查。不過，DCM 可嘗試驗證其它關於憑證的重要資訊，例如，特定憑證上的 CA 簽章是否有效，發出該憑證的 CA 是否可靠。

定義 CRL 位置

若要定義特定 CA 的 CRL 位置，請遵循下列步驟：

1. 啓動 DCM。
2. 在導覽頁框中，選取**管理 CRL 位置**以顯示作業清單。
3. 從作業清單中選取**新增 CRL 位置**以顯示一個套表，您可以用它來說明 CRL 位置，以及 DCM 或應用程式應該如何存取該位置。
4. 完成套表後按一下**確定**。您必須提供 CRL 位置一個唯一名稱，識別裝載 CRL 的 LDAP 伺服器，並提供說明如何存取 LDAP 伺服器的連接資訊。

註: 如果您對於如何完成本引導作業中的特定套表有問題，請選取問號 (**?**) （位於頁頂端）來存取線上說明。

現在您必須使 CRL 位置定義與特定的 CA 產生關聯。

5. 在導覽頁框中，選取**管理憑證**以顯示作業清單。
6. 從作業清單中選取**更新 CRL 位置分派**以顯示 CA 憑證清單。
7. 從清單中選取 CA 憑證，您要把所建立的 CRL 位置定義指派到此憑證，並按一下**更新 CRL 位置分派**。會顯示 CRL 位置清單。
8. 從清單中選取您要與 CA 產生關聯的 CRL 位置，並按一下**更新分派**。一訊息顯示在頁頂端，指出該 CRL 位置已指派至認證中心 (CA) 憑證。

爲特定的 CA 定義 CRL 的位置之後，在執行 CRL 處理程序時，DCM 或其它應用程式就可以使用它。不過，在 CRL 處理程序可以運作之前，Directory Services 伺服器必須包含適當的 CRL。而且，您必須配置 Directory Services 伺服器和從屬站應用程式均使用 SSL，並指派憑證給 DCM 中的應用程式。

要進一步了解關於配置和使用 iSeries Directory Services (LDAP) 伺服器，請複查這些資訊中心主題：

- 目錄服務 (LDAP)
  本主題告訴您關於配置和使用 iSeries Directory Services (LDAP) 伺服器時所需知道的一切。
- 在 LDAP 目錄伺服器中使用 Secure Sockets Layer (SSL) 安全性
  本主題說明您在配置 LDAP 伺服器使用 SSL 進行安全通信時需要執行的動作。

在 IBM 4758 加密輔助處理器上儲存憑證金鑰

如果您已在 iSeries 上安裝 IBM 4758-023 PCI 加密輔助處理器，您可以使用此輔助處理器爲憑證的私密金鑰提供更安全的儲存。您可以使用輔助處理器儲存伺服器憑證、從屬站憑證或區域認證中心 (CA) 憑證的私密金鑰。不過，您不能使用輔助處理器來儲存使用者憑證私密金鑰，因爲此金鑰必須儲存在使用者的系統上。而且，目前您不能使用輔助處理器儲存物件簽署憑證的私密金鑰。

您可以利用下列兩種方式之一來使用輔助處理器儲存憑證私密金鑰：

- 直接在輔助處理器本身儲存憑證私密金鑰。
- 使用輔助處理器主要金鑰來加密憑證私密金鑰以儲存於特殊金鑰檔內。

您可以選取此金鑰儲存選項，作爲建立或更新憑證的程序的一部份。而且，如果您使用輔助處理器儲存憑證的私密金鑰，您可以變更該金鑰的輔助處理器裝置分派。

要使用輔助處理器來儲存私密金鑰，在使用數位憑證管理程式 (DCM) 之前，您必須確定該輔助處理器已轉接。否則，DCM 不會提供頁面供您選取儲存選項，作爲憑證建立或更新程序的一部份。

如果您要建立或更新伺服器或從屬站憑證，您可以在選取簽署現行憑證的 CA 類型之後選取私密金鑰儲存選項。如果您要建立或更新區域 CA，您可以選取私密金鑰儲存選項作爲此程序的第一步。

直接在輔助處理器上儲存憑證私密金鑰

若要加強保護憑證私密金鑰的存取和使用，您可以選擇將金鑰直接儲存在 IBM 4758-023 PCI 加密輔助處理器上。您可以選取此金鑰儲存選項，作爲在數位憑證管理程式 (DCM) 建立或更新憑證的一部份。

請遵循**選取金鑰儲存位置**頁的下列步驟，將憑證的私密金鑰直接儲存在輔助處理器上：

1. 選取**硬體**作爲儲存選項。
2. 按一下**繼續**。這會顯示**選取密碼裝置說明**頁。
3. 從裝置清單中，選取您要用來儲存憑證私密金鑰的裝置。
4. 按一下**繼續**。DCM 會針對您要完成的作業繼續顯示一些頁，例如識別您要建立或更新的憑證的資訊。

使用輔助處理器主要金鑰來加密憑證私密金鑰

若要加強保護憑證私密金鑰的存取和使用，您可以使用 IBM 4758-023 PCI 加密輔助處理器的主要金鑰來加密私密金鑰，並將該金鑰儲存在特殊金鑰檔內。您可以選取此金鑰儲存選項，作爲在數位憑證管理程式 (DCM) 建立或更新憑證的一部份。

在順利使用此選項之前，您必須使用 IBM 4758-023 PCI 加密輔助處理器配置 Web 介面來建立適當的金鑰庫檔案。同時，您必須使用輔助處理器配置 Web 介面，使金鑰庫檔案與您要使用的輔助處理器裝置說明產生關聯。您可以從 iSeries 作業頁存取輔助處理器配置 Web 介面。

如果系統上所安裝及轉接的輔助處理器裝置不止一個，您可以選擇在多個裝置之間共用憑證的私密金鑰。爲了使裝置說明共用私密金鑰，所有裝置必須有相同的主要金鑰。分送相同主要金鑰給多個裝置的程序叫作*複製*。在裝置之間共用金鑰可讓您使用 Secure Sockets Layer (SSL) 平衡資料流量，來改進安全階段作業的效能。

請遵循**選取金鑰儲存位置**頁的下列步驟來使用輔助處理器主要金鑰，加密憑證的私密金鑰並將它儲存在特殊金鑰庫檔案中：

1. 選取**硬體加密**作爲儲存選項。
2. 按一下**繼續**。這會顯示**選取密碼裝置說明**頁。
3. 從裝置清單中，選取您要用來加密憑證私密金鑰的裝置。
4. 按一下**繼續**。如果您已安裝及轉接的輔助處理器裝置不止一個，**選取其它的密碼裝置說明**頁會顯示。

   註: 如果您沒有多個輔助處理器裝置可用，DCM 會針對您要完成的作業繼續顯示一些頁，例如識別您要建立或更新的憑證的資訊。
5. 從裝置清單中，選取您要共用憑證私密金鑰的一或多個裝置說明的名稱。

   註: 您選取的裝置說明必須與前一頁上選取的裝置具有相同的主要金鑰。要驗證主要金鑰與裝置上的相同，請使用 4758 加密輔助處理器配置 Web 介面上的「主要金鑰驗證」作業。您可以從 iSeries 作業頁存取輔助處理器配置 Web 介面。
6. 按一下**繼續**。DCM 會針對您要完成的作業繼續顯示一些頁，例如識別您要建立或更新的憑證的資訊。

管理 PKIX CA 的要求位置

Public Key Infrastructure for X.509 (PKIX) 認證中心 (CA) 是一個基於最新網際網路 x.509 標準發出憑證的 CA，用來實施公開金鑰基礎架構。PKIX 標準概述於 Request For Comments (RFC) 2560。

PKIX CA 在發出憑證之前要求更嚴格的識別；通常它會要求應徵者透過註冊中心 (RA) 提供識別證明。在應徵者提供 RA 需要的識別證明之後，RA 即證實應徵者的識別。根據 CA 所建立的程序，由 RA 或應徵者提出認證過的申請給相關聯的 CA。隨著這些標準被廣泛採用後，符合 PKIX 規格的 CA 變得越來越普遍。如果您的安全性需求需要對於 SSL 型應用程式提供給使用者的資源實施嚴格的存取控制，則您應該使用符合 PKIX 規格的 CA 來調查。例如，Lotus® Domino™ 提供 PKIX CA 供大眾使用。

如果您選擇由 PKIX CA 發出憑證給應用程式使用，您可以使用數位憑證管理程式 (DCM) 管理這些憑證。您使用 DCM 爲 PKIX CA 配置 URL。這麼做會配置數位憑證管理程式 (DCM) 提供 PKIX CA 作爲取得已簽署憑證的一個選項。

若要使用 DCM 管理來自 PKIX CA 的憑證，您必須遵循下列步驟，配置 DCM 來針對 CA 使用此位置：

1. 啓動 DCM。
2. 在導覽頁框中，選取**管理 PKIX 要求位置**以顯示一個套表，它可讓您指定 PKIX CA 或其相關 RA 的 URL。
3. 針對您要用來要求憑證的 PKIX CA 輸入完整的 URL，
   例如 `http://www.thawte.com`，並按一下**新增**。新增 URL 會配置 DCM 新增 PKIX CA 作爲取得已簽署憑證的一個選項。

在新增 PKIX CA 要求位置之後，DCM 會新增 PKIX CA 作爲指定 CA 類型的一個選項，當您使用**建立憑證**作業時，您可以選擇該 CA 來發出憑證。

簽署物件

有三個方法可用來簽署物件。您可以撰寫程式來呼叫簽署物件 API。您可以使用數位憑證管理程式 (DCM) 簽署物件。或者，從 V5R2 開始，您可以使用 iSeries 領航員的簽署物件的管理中心特性，將它們封裝並分送到其它 iSeries 系統。

您可以使用您在 DCM 管理的憑證來簽署任何您儲存在該系統的整合檔案系統中的物件，但儲存在檔案庫中的物件除外。您只能簽署儲存在 QSYS.LIB 檔案系統中的這些物件：*PGM、*SRVPGM、*MODULE、*SQLPKG 和 *FILE（僅儲存檔案）。您也可以簽署指令 (*CMD) 物件，這是 V5R2 的新功能。您不能簽署那些儲存在其它 iSeries 伺服器上的物件。

您可以用您向公用網際網路認證中心 (CA) 購買的憑證或您在 DCM 中以專用區域 CA 建立的憑證來簽署物件。不論您使用公用或專用憑證，簽署憑證的程序皆相同。

物件簽署先決條件

在您使用 DCM（或簽署物件 API）簽署物件之前，您必須確定有符合某些先決條件：

- 您必須已建立 *OBJECTSIGNING 憑證庫，這可以是建立區域 CA 的程序的一部份，或是從公用網際網路 CA 管理物件簽署憑證的程序的一部份。
- *OBJECTSIGNING 憑證庫必須包含至少一個憑證，它可以是您使用區域 CA 建立的憑證，也可以是您從公用網際網路 CA 取得的憑證。

- 您必須已建立物件簽署應用程式定義來簽署物件。
- 您必須已指派憑證給您打算用來簽署物件的物件簽署應用程式。

使用 DCM 簽署物件

要使用 DCM 簽署一或多個物件，請遵循下列步驟：

1. 啓動 DCM。

   註: 如果您對於如何使用 DCM 完成特定套表有問號 (**?**) （位於頁頂端）來存取線上說明。
2. 在導覽頁框中，按一下**選取憑證庫**並選取 ***OBJECTSIGNING** 作爲要開啓的憑證庫。
3. 輸入 *OBJECTSIGNING 憑證庫的密碼並按一下**繼續**。
4. 在導覽頁框重新整理之後，選取**管理可簽署物件**以顯示作業清單。
5. 從作業清單中，選取**簽署物件**以顯示您用於簽署物件的應用程式定義清單。
6. 選取應用程式並按一下**簽署物件**來檢視套表，以指定您要簽署的物件的位置。

   註: 如果您選取的應用程式沒有被指派任何憑證，則您不能用它來簽署物件。您必須先使用**管理應用程式**之下的**更新憑證分派**作業來指派憑證給應用程式定義。
7. 在提供的欄位中，輸入您要簽署的物件或物件目錄的完整路徑和檔案名稱，並按一下**繼續**。或者，輸入一個目錄位置，並按一下**瀏覽**來檢視目錄內容以選取要簽署的物件。

   註: 您必須用前置斜線作爲物件名稱開頭，否則會發生錯誤。您也可以使用特定萬用字元來說明您要簽署的目錄的那個部份。這些萬用字元是星號 (*****)（指定「任何數目的字元」）及問號 (**?**)（指定「任何單一字元」）。例如，要簽署特定目錄中的所有物件，您可以輸入 `/mydirectory/*`；要簽署特定程式庫中的所有程式，可輸入 `/QSYS.LIB/QGPL.LIB/*.PGM`。您只能在路徑名稱的最後部份使用這些萬用字元；例如， `/mydirectory*/filename` 會導致錯誤訊息出現。如果您想要使用瀏覽功能查看檔案庫或目錄內容的清單，在按一下**瀏覽**之前應輸入萬用字元作爲路徑名稱的一部份。
8. 選取您要用來簽署所選取物件的處理程序選項，並按一下**繼續**。

   註: 如果您選擇等待工作結果，結果檔會直接顯示在瀏覽器中。現行工作的結果會附加到結果檔的結尾。因此，除了現行工作的結果之外，該檔案可能包含來自任何先前工作的結果。您可以使用檔案中的日期欄位來決定檔案中哪幾行套用至現行工作。日期欄位是 YYYYMMDD 格式。檔案中的第一個欄位可以是訊息 ID（如果在處理物件時發生錯誤）或是日期欄位（指出處理工作的日期）。
9. 指定在物件簽署作業中要用來儲存工作結果的完整路徑和檔案名稱並按一下**繼續**。或者，輸入一個目錄位置，並按一下**瀏覽**來檢視目錄內容以選取用來儲存工作結果的檔案。會顯示一訊息，指出已提出該工作來簽署物件。要檢視工作結果，請參閱工作日誌中的 **QOBJSGNBAT** 工作。

驗證物件簽章

您可以使用數位憑證管理程式 (DCM) 來驗證物件上的數位簽章的確實性。當您驗證簽章後，即確定物件中的資料自物件擁有者簽署該物件之後未曾變更過。

簽章驗證先決條件

在您使用 DCM 驗證物件上的簽章之前，您必須確定有符合某些先決條件：

- 您必須已建立 *SIGNATUREVERIFICATION 憑證庫來管理簽章驗證憑證。

  註: 在 *OBJECTSIGNING 憑證庫內工作時，如果您要驗證簽章的物件是在相同系統上簽署，您可執行簽章驗證。您在 DCM 驗證簽章時所執行的步驟在任一憑證庫都一樣。不過， *SIGNATUREVERIFICATION 憑證庫必須存在，且必須包含簽署該物件的憑證複本，即使您在 *OBJECTSIGNING 憑證庫內工作時執行簽章驗證也是一樣。
- *SIGNATUREVERIFICATION 憑證庫必須包含簽署物件的憑證複本。
- *SIGNATUREVERIFICATION 憑證庫必須包含發出憑證來簽署物件的 CA 憑證的複本。

使用 DCM to 驗證物件上的簽章

要使用 DCM 驗證物件簽章，請遵循下列步驟：

1. 啓動 DCM。

   註: 如果您對於如何使用 DCM 完成特定套表有問題，請選取問號 (**?**) （位於頁頂端）來存取線上說明。
2. 在導覽頁框中，按一下**選取憑證庫**並選取 ***SIGNATUREVERIFICATION** 作爲要開啓的憑證庫。
3. 輸入 *SIGNATUREVERIFICATION 憑證庫的密碼並按一下**繼續**。
4. 在導覽頁框重新整理之後，選取**管理可簽署物件**以顯示作業清單。
5. 從作業清單中選取**驗證物件簽章**，以指定您要驗證其簽章的物件的位置。
6. 在提供的欄位中，輸入您要驗證其簽章的物件或物件目錄的完整路徑和檔案名稱，並按一下**繼續**。或者，輸入一個目錄位置，並按一下**瀏覽**來檢視目錄內容以選取用於簽章驗證的物件。

   註: 您也可以使用特定萬用字元來說明您要驗證的目錄的那個部份。這些萬用字元是星號 (*****)（指定「任何數目的字元」）及問號 (**?**)（指定「任何單一字元」）。例如，要簽署特定目錄中的所有物件，您可以輸入 `/mydirectory/*`；要簽署特定程式庫中的所有程式，可輸入 `/QSYS.LIB/QGPL.LIB/*.PGM`。您只能在路徑名稱的最後部份使用這些萬用字元；例如， `/mydirectory*/filename` 會導致錯誤訊息出現。如果您想要使用瀏覽功能查看檔案庫或目錄內容的清單，在按一下**瀏覽**之前應輸入萬用字元作爲路徑名稱的一部份。
7. 選取您要用來驗證所選取物件的簽章的處理程序選項，並按一下**繼續**。

   註: 如果您選擇等待工作結果，結果檔會直接顯示在瀏覽器中。現行工作的結果會附加到結果檔的結尾。因此，除了現行工作的結果之外，該檔案可能包含來自任何先前工作的結果。您可以使用檔案中的日期欄位來決定檔案中哪幾行套用至現行工作。日期欄位是 YYYYMMDD 格式。檔案中的第一個欄位可以是訊息 ID（如果在處理物件時發生錯誤）或是日期欄位（指出處理工作的日期）。
8. 指定在簽章驗證作業中要用來儲存工作結果的完整路徑和檔案名稱並按一下**繼續**。或者，輸入一個目錄位置，並按一下**瀏覽**來檢視目錄內容以選取用來儲存工作結果的檔案。會顯示一訊息，指出已提出該工作來驗證物件簽章。要檢視工作結果，請參閱工作日誌中的 **QOBJSGNBAT** 工作。

您也可以使用 DCM 來檢視關於簽署物件的憑證的資訊。在您使用該物件之前，這可讓您判斷該物件是否來自您信任的來源。

第 9 章 DCM 疑難排解

您可以使用這幾頁來尋找有用的資訊，幫助您解決您在使用數位憑證管理程式 (DCM) 時可能會遇到的一些較常見的問題。

關於問題及其可能的解決方案的資訊，請複查這幾頁：

密碼和一般問題的疑難排解
使用此資訊來了解您可能遇到的常見的 DCM 使用者介面問題，以及您如何解決它們。

憑證庫和金鑰資料庫問題的疑難排解
使用此資訊來了解您可能遇到的常見的憑證庫和金鑰資料庫問題，以及您如何解決它們。

瀏覽器問題的疑難排解
使用此資訊來了解您在使用瀏覽器存取 DCM 時可能遇到的常見問題，以及您如何解決它們。

HTTP Server for iSeries 問題的疑難排解
使用此資訊來了解您可能遇到的常見的 HTTP 伺服器問題，以及您如何解決它們。

移轉錯誤和回復解決方案
使用此資訊來了解您從前版次移轉 DCM 時可能遇到的常見問題，以及您如何解決它們。

指派使用者憑證的疑難排解
使用此資訊來了解您使用 DCM 登記使用者憑證時可能遇到的常見問題，以及您如何解決它們。

密碼和一般問題的疑難排解

使用下表來尋找有用的資訊，幫助您解決您在使用數位憑證管理程式 (DCM) 時可能會遇到的一些較常見的密碼問題和其它一般問題。

問題	可能的解決方案
您找不到 DCM 的其它說明。	在 DCM，按一下 "**?**" 說明圖示。您也可以在網際網路上搜尋資訊中心及外部網站。
當您嘗試開啓憑證庫時接收到 NET.DATA 錯誤。	當您**選取憑證庫**時，請使用滑鼠選取**繼續**按鈕而非使用鍵盤上的 **Enter** 鍵。
區域認證中心 (CA) 的密碼和 *SYSTEM 憑證庫無效。	密碼要區分大小寫。確定大寫鍵與您指派的密碼是相同的。
當您使用「選取憑證庫作業」時試圖重設密碼，但失敗。	唯有當 DCM 已儲存該密碼時，重設功能才有效。當您建立憑證庫時 DCM 會自動儲存密碼。不過，如果您爲「其它系統憑證庫」變更（或重設）密碼，則必須選取**自動登入**選項，使 DCM 得以繼續隱藏密碼。

問題	可能的解決方案
	此外，如果您將憑證庫從一個系統移到另一個系統，必須在新系統上變更憑證庫的密碼，以確定 DCM 會自動隱藏它。若要變更密碼，當您在新系統上開啓憑證庫時必須提供憑證庫的原始密碼。要等到您以原始密碼開啓憑證庫並變更密碼來隱藏它之後，您才能使用重設密碼選項。如果密碼沒有變更及隱藏，當各種功能需要密碼時，DCM 和 SSL 不能自動回復密碼。如果您移動一個要作爲「其它系統憑證庫」的憑證庫，當您變更密碼時必須選取**自動登入**選項，以確定 DCM 隱藏此憑證庫類型的新密碼。
	檢查已指派給「系統服務工具 (SST)」的「使用系統安全」選項下的「允許新的數位憑證」屬性的值。如果此屬性設爲 2（否）的值，則無法重設憑證庫密碼。您可以使用 STRSST 指令並輸入服務工具使用者 ID 和密碼，來檢視或變更此屬性的值。然後選擇「使用系統安全」選項。此服務工具使用者 ID 可能是 QSECOFR 使用者 ID。
您找不到 CA 憑證的來源來將它接收到 iSeries 系統。	有些 CA 不輕易提供其 CA 憑證。如果您無法從 CA 取得 CA 憑證，請聯絡 VAR，因爲 VAR 可能與 CA 之間有特殊的或金錢上的安排。
您找不到 *SYSTEM 憑證庫。	*SYSTEM 憑證的檔案位置必須是 `/qibm/userdata/icss/cert/server/default.kdb`。如果該憑證庫不存在，您必須使用 DCM 來建立憑證庫。請使用**建立新的憑證庫**作業。
您從 DCM 收到一項錯誤，在您更正它之後，該錯誤繼續出現。	請清除瀏覽器快取。將快取記憶體大小設爲 0，並結束瀏覽器後再重新啓動。
您有 LDAP 伺服器問題，例如在指派憑證之後立即顯示關於安全應用程式的資訊時並未顯示憑證分派。使用 iSeries 領航員來開啓 Netscape Communications 瀏覽器時，經常發生此問題。您瀏覽器快取的喜好設定是設定爲「每一個階段作業一次」，來比較快取中的文件與網路上的文件。	變更預設喜好設定，變成每次檢查快取。
當您使用 DCM 來匯入由外部 CA（例如 Entrust）簽署的憑證時，會收到錯誤訊息，說有效期間不包含今天，或不在其發行者的有效期間內。	系統對有效期間使用廣義時間格式。等一天後重試。並且，驗證 iSeries 有正確的 UTC 偏移值 (`dspsysval qutcoffset`)。如果您採用日光節約時間，則您可能未正確設定偏移。
在嘗試匯入 Entrust 憑證時您收到一個基本 64 錯誤。	此憑證被列爲特定的格式，例如 PEM 格式。如果瀏覽器的複製功能效果不佳，您可能會複製到不屬於憑證的額外資料，例如每一行前面的空格。如果是這樣，當您要在 iSeries 上使用憑證時，憑證的格式可能不正確。有些網頁設計會造成此問題。有些網頁在設計上會避免此問題。請務必比較原始憑證的外觀和貼上的結果，因爲貼上的資訊看起來應該一樣。
從 V4R3 版本的 DCM 移轉到 V5R2 版本時，移轉作業並未考慮到過期的系統憑證。	過期的系統憑證現在已損壞，無法進入 *SYSTEM 憑證庫。在移轉之前請從 V4R3 移除或更名舊金鑰環檔案，忽略移轉失敗指示符，或重新嘗試移轉。
您找不到關於將憑證加入驗證清單的程式碼範例。	尚無此程式碼範例。

憑證庫和金鑰資料庫問題的疑難排解

使用下表來尋找有用的資訊，幫助您解決您在使用數位憑證管理程式 (DCM) 時可能會遇到的一些較常見的憑證庫和金鑰資料庫問題。

問題	可能的解決方案
系統找不到金鑰資料庫，或發現它無效。	檢查密碼和檔名是否拼錯。確定檔名中有包含路徑，包括前面的斜線在內。
金鑰資料庫建立失敗。	檢查檔名是否衝突。若與您所要求的檔案不同，則可能有衝突。
系統不接受以二進位模式從另一個系統轉送而來的 CA 文字檔。它不接受以美國國家資訊交換標準碼 (ASCII) 轉送的檔案。	金鑰環和金鑰資料庫是二進位，因此不同。您必須對 CA 文字檔使用 ASCII 模式的檔案轉送通信協定 (FTP)，對二進位檔使用二進位模式的 FTP，例如有這些副檔名的檔案： .kdb、.kyr、.sth、.rdb...等等。
您不能變更金鑰資料庫的密碼。金鑰資料庫中的憑證不再有效。	在驗證不正確密碼已不是問題之後，請在憑證庫中尋找並刪除無效憑證，然後試著變更密碼。如果您的憑證庫中有過期的憑證，則該過期憑證不再有效。由於憑證無效，憑證庫的密碼變更功能可能不允許密碼變更，且加密程序不會加密過期憑證的私密金鑰。這防止密碼發生變更，且系統會報告憑證庫毀損是原因之一。您必須從憑證庫中移除無效（過期）憑證。
您必須對網際網路使用者使用憑證，因此需要使用驗證清單，但 DCM 不提供驗證清單的功能。	撰寫應用程式使用驗證清單的企業夥伴，必須將他們的程式碼撰寫成使驗證清單與其應用程式如預期地產生關聯。他們也必須撰寫程式碼來決定何時適當地驗證網際網路使用者的識別身份，使憑證得以新增至驗證清單中。請複查資訊中心主題中的 QsyAddVldlCertificate API。請參閱《版主手冊》中關於配置安全伺服器實例使用驗證清單的說明。

瀏覽器問題的疑難排解

使用下表來尋找有用的資訊，幫助您解決您在使用數位憑證管理程式 (DCM) 時可能會遇到的一些較常見的瀏覽器相關問題。

問題	可能的解決方案
Microsoft® Internet Explorer 要等到您啓動新的瀏覽器階段作業時才讓您選取不同的憑證。	爲 Internet Explorer 開始一個新的瀏覽器階段作業。
Internet Explorer 不顯示瀏覽器選項清單中所有可選取的從屬站/使用者憑證。 Internet Explorer 只顯示由可靠的 CA 發出的憑證，您可以在安全網站上使用這些憑證。	金鑰資料庫中的 CA 必須是可靠的，而且可被安全應用程式所信任。確定您以同於在瀏覽器放入使用者憑證的使用者名稱登入 PC 的 Internet Explorer 瀏覽器。從您要存取的系統中取得另一個使用者憑證。系統管理者應確定憑證庫（金鑰資料庫）仍然信任簽署使用者和系統憑證的 CA。
Internet Explorer 5 接收 CA 憑證，但無法開啓檔案或找不到您儲存憑證的磁碟。	這是針對 Internet Explorer 瀏覽器尚未信任的憑證而提供的一個新瀏覽器特性。您可以在 PC 上選擇此位置。
您收到瀏覽器警告，說系統名稱和系統憑證不符。	有些瀏覽器在系統名稱的大小寫符合方面有不同的作法。請依照系統憑證顯示的大小寫鍵入 URL。或者，以符合大部份使用者使用的大小寫來建立系統憑證。除非您知道自己在做什麼，否則最好將伺服器名稱或系統名稱保持原狀。您也應該檢查網域名稱伺服器是否正確設定。

問題	可能的解決方案
您以 HTTPS 而非 HTTP 來啓動 Internet Explorer，並且收到警告，說您把安全和非安全階段作業混合在一起。	請選擇接受並忽略警告； Internet Explorer 的未來版次會解決此問題。
Netscape Communicator 4.04 for Windows® 將波蘭文字碼頁上的十六進位值 A1 和 B1 轉換成 B2 和 9A。	這是一項瀏覽器錯誤，會影響 NLS。請使用不同的瀏覽器，或在不同平台上使用此瀏覽器的相同版本，例如， Netscape Communicator 4.04 for AIX®。
在使用者設定檔中，Netscape Communicator for 4.04 能正確顯示大寫使用者憑證 NLS 字元，但錯誤顯示小寫字元。	有些以一個字元正確輸入的國家語言字元，在後來顯示時卻不是相同字元。例如，在 Windows 版本的 Netscape Communicator 4.04，波蘭文字碼頁上的十六進位值 A1 和 B1 被轉換成 B2 和 9A，而導致顯示不同的 NLS 字元。
瀏覽器繼續告訴一般使用者，該 CA 還不可靠。	使用 DCM 設定 **CA 狀態**爲已啓用，將 CA 標示爲可靠的。
Internet Explorer 要求拒絕 HTTPS 連線。	這是瀏覽器功能或其配置的問題。當系統憑證是自我簽署或基於其它理由而無效時，瀏覽器選擇不連接使用該系統憑證的網站。
Netscape Communicator 瀏覽器和伺服器產品運用公司的主要憑證（包括但不限於 VeriSign），作爲 SSL 通信的一項啓用特性 -- 尤其是鑑別方面。所有主要憑證會定期到期。有些 Netscape 瀏覽器和伺服器主要憑證在 1999 年 12 月 25 日到 1999 年 12 月 31 日之間到期。如果您在 1999 年 12 月 14 日那天之前未解決此問題，您會收到錯誤訊息。	瀏覽器的舊版本（Netscape Communicator 4.05 或更舊的版本）有到期的憑證。您需要將瀏覽器升級成最新 Netscape Communicator 版本。許多網站有提供瀏覽器主要憑證上的資訊，包括 `http://home.netscape.com/security/` 和 `http://www.verisign.com/server/cus/rootcert/webmaster.html`。您可以到 `http://www.netcenter.com` 免費下載瀏覽器。

HTTP Server for iSeries 問題的疑難排解

使用下表來尋找有用的資訊，幫助您解決您在使用數位憑證管理程式 (DCM) 時可能會遇到的一些較常見的 HTTP Server for iSeries 問題。

問題	可能的解決方案
超本文傳送通信協定 (HTTPS) 無效。	確定 HTTP Server 有正確配置來使用 SSL。在 V5R1 或以上的版本中，配置檔必須已使用 HTTP Server 的圖形式使用者介面 (GUI) 設定 **SSLAppName**。此外，此配置中必須配置使用 SSL 埠的虛擬主電腦，並在虛擬主電腦內有 **SSLEnable**。也必須有兩個 Listen 指引來指定兩個不同的埠，一個給 SSL，另一個不是給 SSL。確定有建立伺服器實例，且有簽署伺服器憑證。
以安全應用程式登記 HTTP Server 實例的程序需要澄清。	在 iSeries 系統上，到 HTTP Server 的 Web 介面設定 HTTP Server 的配置。首先您必須定義一個虛擬主電腦來啓用 SSL。這是在「環境管理」螢幕上完成。虛擬主電腦必須定義爲使用先前在 Listen 指引上定義的 SSL 埠。接下來，您必須使用「SSL 一般設定」螢幕，在先前配置的虛擬主電腦上開啓 SSL。所有變更必須套用至配置檔。注意，登記實例並不會自動選擇該實例應使用的憑證。在您嘗試先結束再重新啓動伺服器實例之前，您必須使用 DCM 指派一個特定憑證給應用程式。
您在驗證清單及可選用的從屬站鑑別方面設置 HTTP Server 時遇到困難。	請參閱 HTTP Server 《版主手冊》中關於設置實例的選項。資訊中心的 Web 服務主題也有提供此資訊。
Netscape Communicator 等待 HTTP Server 程式碼中的配置指引到期，然後它才可讓您選取不同的憑證。	大的憑證值會使得登記第二個憑證比較困難，因爲瀏覽器仍在使用第一個憑證。

問題	可能的解決方案
您嘗試使瀏覽器對 HTTP Server 顯示 X.509 憑證，使您可以使用該憑證作爲 QsyAddVldlCertificate API 的輸入。	您必須使用 **SSLEnable** 和 **SSLClientAuth ON** 才能使 HTTP Server 載入 HTTPS_CLIENT_CERTIFICATE 環境變數。您可以在資訊中心的 OS/400 API 主題中找到這些 API。您或許也想要查看這些驗證清單或與憑證相關的 API： • QsyListVldlCertificates 和 QSYLSTVC • QsyRemoveVldlCertificate 和 QRMVVC • QsyCheckVldlCertificate 和 QSYCHKVC • QsyParseCertificate 和 QSYPARSC...等等。
您找不到在安裝 HTTP Server 時建立的要求檔案。系統使用此檔案指出在它目錄下的配置檔中的 KEYFILE 指引上找到的有效金鑰環檔案。	如需詳細資訊，請參閱從舊版次移轉到 DCM。在 HTTP Server 方面，正確檔案是 `/qibm/userdata/httpsvr/keyring/keymreq.crt`。 在 LDAP 方面，正確檔案是 `/qibm/userdata/os400/dirsrv/qdirsrv.crt`。
如果您要求驗證清單中的憑證清單，但是超過 10,000 個項目，則 HTTP Server 傳回的時間太久或逾時。	建立批次作業來尋找及刪除符合特定準則的憑證，例如所有已過期或來自特定 CA 的那些憑證。
在 V4R3 版次上安裝 V5R2 之後，您發現憑證庫有問題，且現在 `/qibm/userdata/httpsvr/keyring/keymreq.crt` 或 `/qibm/usedata/os400/dirsrv/qdirsrv.crt` 檔案存在。系統無法完成自動金鑰環到金鑰資料庫移轉。	指定舊金鑰環檔案作爲憑證庫，並在呼叫 `qicss/qyepmgrt` 重試移轉之前，從金鑰環檔案中尋找及刪除無效憑證。或者，如果移轉活動已移動所有重要憑證，則忽略或刪除 `.crt` 檔。
若設定 **SSLEnable**，則 HTTP Server 將無法順利啓動，且錯誤訊息 `HTP8351` 會出現在工作日誌中。當 HTTP Server 失敗時，*ADMIN 伺服器的錯誤日誌顯示 SSL 起始設定作業失敗的錯誤，並含有回覆碼錯誤 `107`。	錯誤 `107` 表示憑證過期。如果伺服器實例是 *ADMIN 伺服器，請暫時設定 **SSLDisable**，使您可以在 *ADMIN 伺服器上使用 DCM。使用 DCM 指派不同的憑證給應用程式；例如，如果伺服器實例是 *ADMIN 伺服器， 則指派 QIBM_HTTP_SERVER_ADMIN。

移轉錯誤和回復解決方案

錯誤和錯誤回復

下列指示符警告您在移轉期間可能發生的錯誤：

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
在您順利安裝選項 34 和 5722-DB1 之後若出現此指示符，表示 5722-DG1 所嘗試的金鑰環移轉並未成功。您可能需要在 *SYSTEM 憑證庫中執行金鑰環移轉。

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT
在您順利安裝選項 34 之後若出現此指示符，表示 LDAP 伺服器的金鑰環移轉並未成功。

除了指示的錯誤之外，可能還有系統未指示的移轉錯誤。例如，當系統發現它需要移轉到 *SYSTEM 憑證庫的金鑰環檔案時，它可能也會發現與現有的整合檔案系統使用者資料檔相衝突。在這種實例中，即使您已順利完成安裝，系統可能未完成金鑰環檔案移轉。

在罕見的實務中，在錯誤防止移轉完成之前，有可能只完成部份系統憑證分派而使金鑰環檔案移轉。當您啓動 IBM HTTP Server *ADMIN 案例時如果 SSLMODE 爲 ON，則這樣做會導致錯誤。可能的解釋是：

- 移轉金鑰環檔案設定了不正確的系統憑證作爲它的預設值。

- DCM 結束移轉以保留已存在於機要檔案名稱中的使用者資料。
- 在移轉程式碼中發生無法預期的錯誤。

您可以啓動 IBM HTTP Server 而不將 SSLMODE 設爲 ON，方法是在啓動 *ADMIN 案例之前先針對 *ADMIN 案例將 SSLMODE 設爲 OFF。這可讓您使用 DCM 來調查憑證庫，並在結束 *ADMIN 案例之前解決問題。在您結束 *ADMIN 案例之後，就可以將 SSLMODE 設回 ON 並啓動 *ADMIN 案例，正確地起始設定 SSL。

在選項 34 移轉之後，在使用憑證庫的正常 DCM 要求期間可能發生錯誤。這些錯誤發生於瀏覽器。以下是這類錯誤的範例：

資料庫錯誤
資料庫讀取錯誤
資料庫寫入錯誤
資料庫毀損
資料庫表格毀損

另外，系統有一個叫作 default.kdb 的無效憑證庫檔案出現在與 /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR 或 /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR 相同的目錄中。在這種情況下，在使用 DCM 建立新憑證之前，您需要完成下列手動移轉：

註: 如果您選擇不要移轉金鑰環檔案，而要建立新的 CA 和系統憑證，請略過下列手動移轉程序。

- 如果您打算安裝 HTTP Server for iSeries (5722-DG1)，請立即安裝它，然後再繼續。

  註:

  1. 在您安裝選項 34 之後，5722-SS1 選項 34 安裝程式碼不會重新嘗試移轉。只重新安裝選項 34 於事無補。
  2. 適當的檔案位於以 PUBLIC *EXCLUDE 權限建立的使用者資料目錄中。請確定您對它們有正確授權。
- 檢查下列檔案是否存在：
  - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

  如果它們存在，請使用 WRKLNK 指令更名它們並建立備份。
- 從具有 *ALLOBJ 權限的使用者設定檔，在指令行上呼叫程式 QICSS/QYEPMGRT，如下所示：

  ```
  CALL QICSS/QYEPMGRT
  ```

  如果結果順利完成，請確定下列檔案都不在您的系統上：
  - /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
  - /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

如果您用來儲存使用者資料的檔案名稱與 DCM 使用的檔名相衝突，DCM 通常會保留使用者資料的備份。如果下列檔案不存在：

- /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
- /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR

但下列檔案存在：

- /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH

- /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH

則系統嘗試將它們更名並附加 .OLD 副檔名。如果那些檔案也已存在，則系統不建立任何備份。相反地，它會直接改寫現有的 .STH 檔。

雜項

如果您嘗試建立 CA 且系統憑證因爲檔名衝突而繼續失效，則您可能是遇到下列其中一種情形：

- **不同檔名衝突** - DCM 嘗試保護它建立的目錄中的使用者資料，即使那些檔案使 DCM 無法在它需要時順利建立檔案。解決方式是將所有衝突的檔案全部複製到不同目錄，可能的話，使用 DCM 功能來刪除對應的檔案。如果您無法使用 DCM 完成此動作，請從與 DCM 相衝突的整合檔案系統目錄中手動刪除檔案。確定您有正確記錄移動了哪些檔案以及移到哪裡。如果您發現仍然需要這些檔案，複本可讓您回復檔案。在移動下列檔案之後，您必須建立新的 CA：

  ```
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.KDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.RDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH .OLD
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POL
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.BAK
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STHBAK
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.STH
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TXT
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.BAK
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TMP
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLTMP
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLBAK
  /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CACRT
  /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CATMP
  /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CABAK
  /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CLIENT/*.USRCRT
  ```

  在移動下列檔案之後，您必須建立新的 *SYSTEM 憑證庫和系統憑證：

  ```
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.BAK
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.RDB
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH.OLD
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STHBAK
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TMP
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TEMP.STH
  /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TMP
  /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.BAK
  /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TXT
  /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.SGN
  /QIBM/USERDATA/ICSS/CERT/SERVER/SGN.TMP
  /QIBM/USERDATA/ICSS/CERT/SERVER/SGN.BAK
  /QIBM/USERDATA/ICSS/CERT/SERVER/EXPSRV.TMP
  /QIBM/USERDATA/ICSS/CERT/SERVER/EXPSGN.TMP
  ```

- **缺少必備項目** - 確定您已正確安裝必備的授權程式 (LPP)。
- **程式碼問題** - 聯絡客戶服務代表。

指派使用者憑證之疑難排解

當您使用**指派使用者憑證**作業時，「數位憑證管理程式」(DCM) 會先顯示憑證資訊讓您審核之後再登記憑證。如果 DCM 無法顯示憑證，可能是下列其中一項狀況導致此問題：

1. 您的瀏覽器未要求您選取憑證來提出給伺服器。如果瀏覽器快取前一個憑證（在存取不同的伺服器時），就可能發生此問題。請嘗試清除瀏覽器的快取，再重新執行作業。瀏覽器應該提示您選取憑證。
2. 您要登記的憑證已透過 DCM 登記。
3. 系統上未指定發出憑證的「認證中心」當做一個最高授信使用者。因此，您提出的憑證無效。請連絡系統管理者來決定發出憑證的 CA 是否正確。如果 CA 正確，則系統管理者可能需要將 CA **匯入** *SYSTEM 憑證庫中。或者，管理者可能需要使用**使用 CA 憑證**作業，讓 CA 成爲系統上的一個最高授信使用者，以解決問題。
4. 您沒有憑證可以登記。您可以在瀏覽器中檢查使用者憑證，判斷是否是這個問題。
5. 您嘗試登記的憑證已過期或不完整。您必須更新憑證或連絡 CA 來發出憑證，以解決問題。
6. IBM HTTP Server for iSeries 未正確設定來使用 SSL 執行憑證登記，以及在安全 *ADMIN 伺服器實例上執行從屬站鑑別。如果前述疑難排解秘訣都無法解決問題，請向系統管理者報告問題。

若要**指派使用者憑證**，您必須使用 SSL 階段作業來連接「數位憑證管理程式」(DCM)。如果您選取**指派使用者憑證**作業時不是使用 SSL， DCM 會顯示訊息表示您必須使用 SSL。此訊息有一個按鈕可讓您使用 SSL 來連接到 DCM。如果訊息中未提供按鈕，請向系統管理者通知此問題。可能需要重新啓動 Web 伺服器，以確保使用 SSL 的配置指引生效。

第 10 章 DCM 的相關資訊

隨著數位憑證的使用越來越普遍，資訊資源也變得越來越多。以下這張簡短的清單列出一些其它資源，您可以複查它以進一步了解數位憑證以及您如何使用它們來增強 iSeries 安全原則：

- **VeriSign 說明平台網站**
  VeriSign 網站提供有關數位憑證主題以及其它網際網路安全性主題的一個大題庫。
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  此 IBM 紅皮書的焦點放在 V5R1 網路安全性加強功能。此紅皮書涵蓋許多主題，包括如何使用 iSeries 物件簽署功能、數位憑證管理程式 (DCM)、SSL 的 4758 加密輔助處理器支援...等等。
- **AS/400® Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)**
  此紅皮書說明數位憑證在 iSeries 伺服器上的用途。它說明如何設定各種伺服器和從屬站去使用憑證。另外，它還提供資訊和程式碼範例，說明如何在使用者應用程式中使用 OS/400 API 來管理及使用數位憑證。
- **RFC 索引搜尋**
  此網站提供一個可搜尋的 Request for Comments (RFC) 儲存庫。 RFC 說明網際網路通信協定標準，例如 SSL、PKIX 以及與使用數位憑證相關的其它通信協定標準。