關於 RSA 金鑰產生脆弱性的應對措施

USRM3-1262-00 2022-03 zh

目錄

前言

前言

您必須更新韌體並執行本文件所述的附加程序，才能升級使用易受攻擊之加密庫建立的 RSA 金鑰。

首先請檢查本機的機型和版本。
如果在此頁面上有找到本機的機型和版本，請更新韌體，然後執行本文件所述的附加程序。 **檢查您是否必須執行附加程序 (P. 4)**
如需關於更新韌體的資訊，請參閱您獲得本文件的網站。

檢查本機的版本

遵循以下程序檢查本機的版本。

1 啟動遠端使用者介面。

2 按一下入口網站頁面的 [狀態確認/取消]。

3 按一下 [裝置資訊] ▶ 檢查 [Main Controller] 中的 [版本資訊]。

需要執行附加程序的機型和版本

機型	版本
- iR C3222L	版本 01.16 至版本 02.05
- LBP631Cw - LBP632Cdw / LBP633Cdw	版本 01.22
- MF651Cw / MF652Cw - MF653Cdw / MF654Cdw / MF655Cdw / MF656Cdw / MF657Cdw	版本 01.22
- LBP233dw / LBP236dw / LBP237dw - LBP1238 II - 1238P II / 1238Pr II	版本 01.22 至版本 01.26
- 1238 II - MF1238 II - MF451dw / MF452dw / MF453dw / MF455dw	版本 01.22 至版本 01.26

註釋

- 本文件中使用的螢幕截圖，視您機器的機型而定，可能與您實際看到的情況不同。如需關於螢幕截圖的詳細資訊，請到線上手冊網站參閱本機的手冊。

  https://oip.manual.canon/

檢查您是否必須執行附加程序

檢查您是否必須執行附加程序

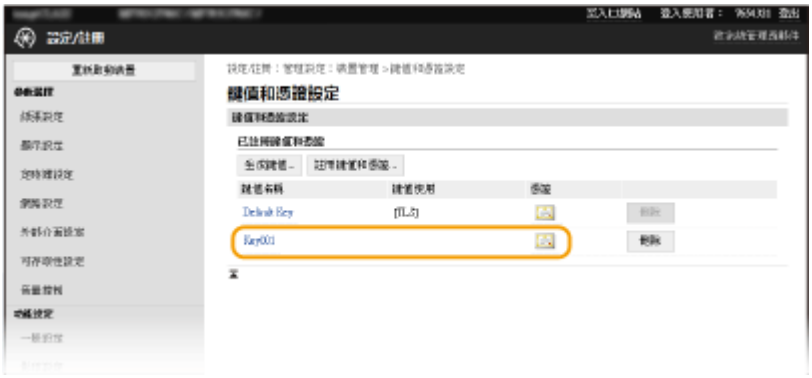
根據本機的設定檢查 RSA 金鑰並執行所需的程序。
如果在本機中註冊的金鑰顯示為「Default Key」，則不需要檢查 RSA 金鑰。

註釋

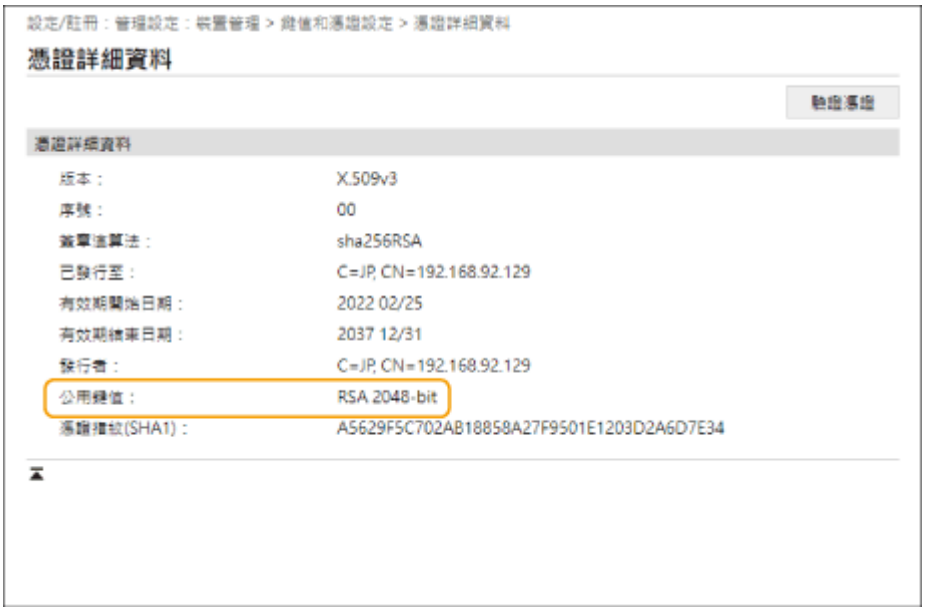
- 本文件中使用的螢幕截圖僅為示範用途。視機器的機型而定，其可能與您實際看到的畫面不同。

1 **啟動遠端使用者介面 ▶ 按一下 [設定/註冊] ▶ [裝置管理] ▶ [鍵值和憑證設定]。**

2 **檢查 [Default Key] 以外的金鑰。**



3 **檢查 [公用鍵值]。**



對於 RSA 以外的憑證

您不需要執行附加程序。

對於 RSA 憑證

按一下畫面上方的 [鍵值和憑證設定] ▶ 檢查金鑰用途。

- 依照這裡顯示的說明執行附加程序。 **RSA 金鑰用途和附加程序(P. 7)**
- 如果金鑰是外部產生且在本機中註冊的 RSA 金鑰，則不需要執行附加程序。
- 如果您必須執行附加程序，則可能需要憑證資訊來停用憑證。請在刪除金鑰/憑證之前記下所需的資訊。向核發憑證的憑證授權單位詢問所需資訊。

RSA 金鑰用途和附加程序

RSA 金鑰用途和附加程序

請參閱「附加程序」並根據金鑰用途加以執行。

RSA 金鑰用途	條件	附加程序
[TLS]	在任何情況下您都必須執行附加程序。	**TLS 的程序(P. 8)**
[IEEE 802.1X]	如果 IEEE 802.1X 認證方法設定為 TLS，您必須執行附加程序。	**IEEE 802.1X 的程序(P. 18)**
[IPSec]	如果 IKE 認證方法設定為數位簽章方法，您必須執行附加程序。	**IPSec 的程序(P. 30)**
[裝置簽章]	在下列情況下，您必須執行附加程序： • 使用裝置簽章的金鑰將數位簽章新增到已傳送的檔案時	**裝置簽章的程序(P. 41)**

註釋

- 本文件中使用的螢幕截圖僅為示範用途。視機器的機型而定，其可能與您實際看到的畫面不同。

TLS 的程序

步驟 1：重新產生金鑰和憑證 (TLS)

您可以為機器產生的金鑰產生兩種類型的憑證：自我簽章憑證和 CSR 憑證。程序會依憑證類型而有不同。

對於自我簽章憑證(P. 9)
對於 CSR 憑證(P. 10)

對於自我簽章憑證

1 **啟動遠端使用者介面。**

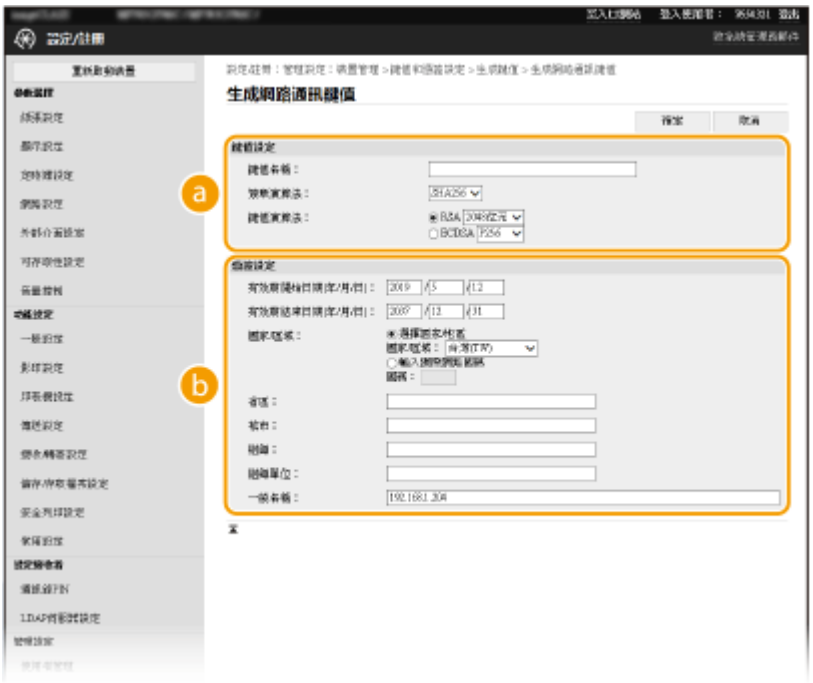
2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **按一下[生成鍵值]。**

5 **選擇 [網路通訊] ▶ 按一下 [確定]。**

6 **指定金鑰和憑證設定。**



a [鍵值設定]

[鍵值名稱]

使用英數字元輸入金鑰名稱。請輸入可在清單中輕鬆找到的名稱。

[簽章演算法]
從下拉式清單中選擇金鑰演算法。

[鍵值演算法]
選擇 [RSA] 或 [ECDSA] 作為金鑰產生演算法 ▶ 從下拉清單中選擇金鑰長度。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

註釋:

- 如果您對 [簽章演算法] 選擇 [SHA384] 或 [SHA512]，則當對 [鍵值演算法] 選擇 [RSA] 時，不能將金鑰長度設定為 [512 位元]。

[憑證設定]

[有效期開始日期(年/月/日)]
輸入憑證有效期的開始日期和結束日期。

[有效期結束日期(年/月/日)]
輸入憑證有效期的結束日期。您不能設定早於 [有效期開始日期(年/月/日)] 中的日期。

[國家/區域]
按一下 [選擇國家/地區]，然後從下拉清單中選擇國家/地區。或者，按一下 [輸入網際網路國碼]，然後輸入國碼，例如「US」代表美國。

[省區]/[城市]
視需要使用英數字元輸入位置。

[組織]/[組織單位]
視需要使用英數字元輸入組織名稱。

[一般名稱]
視需要使用英數字元輸入憑證的一般名稱。「一般名稱」通常縮寫為「CN」。

7 按一下[確定]。

- 金鑰和憑證的產生可能要花一點時間。
- 產生的金鑰和憑證會自動註冊到本機。

對於 CSR 憑證

在本機上產生金鑰和 CSR。使用畫面上顯示的 CSR 資料或輸出為檔案以要求憑證授權單位核發憑證。然後為金鑰註冊核發的憑證。

■1. 產生金鑰和 CSR

1 啟動遠端使用者介面。

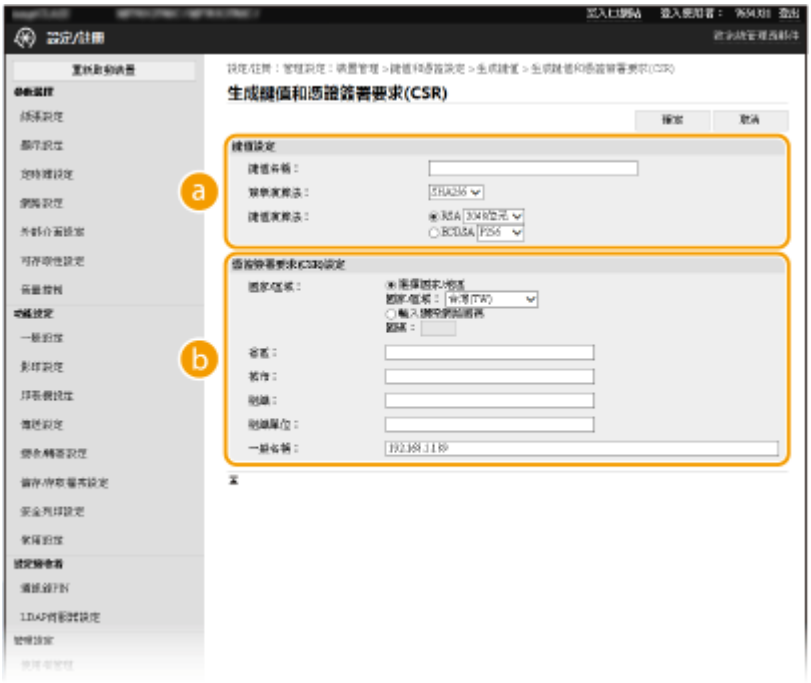
2 按一下入口網站頁面的 [設定/註冊]。

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **按一下[生成鍵值]。**

5 **選擇 [鍵值和憑證簽署要求(CSR)] ▶ 按一下 [確定]。**

6 **指定金鑰和 CSR 設定。**



a [鍵值設定]

[鍵值名稱]
使用英數字元輸入金鑰名稱。請輸入可在清單中輕鬆找到的名稱。

[簽章演算法]
從下拉式清單中選擇金鑰演算法。

[鍵值演算法]
選擇 [RSA] 或 [ECDSA] 作為金鑰產生演算法 ▶ 從下拉清單中選擇金鑰長度。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

註釋:

- 如果您對 [簽章演算法] 選擇 [SHA384] 或 [SHA512]，則當對 [鍵值演算法] 選擇 [RSA] 時，不能將金鑰長度設定為 [512 位元]。

b [憑證簽署要求(CSR)設定]

[國家/區域]
按一下 [選擇國家/地區]，然後從下拉清單中選擇國家/地區。或者，按一下 [輸入網際網路國碼]，然後輸入國碼，例如「US」代表美國。

[省區]/[城市]
視需要使用英數字元輸入位置。

[組織]/[組織單位]
視需要使用英數字元輸入組織名稱。

[一般名稱]
視需要使用英數字元輸入憑證的一般名稱。「一般名稱」通常縮寫為「CN」。

7 按一下[確定]。

- 金鑰和 CSR 的產生可能要花一點時間。

8 按一下[儲存在檔案中]。

- 顯示儲存檔案的對話方塊時，選擇要儲存檔案的目的地 ▶ 按一下 [存檔]。

  ➠ CSR 檔案即會儲存到電腦上。

9 附加儲存的檔案，然後向憑證授權單位提出申請。

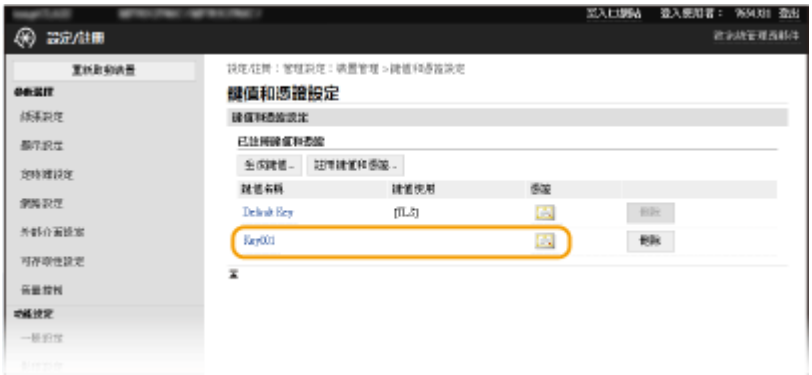
■2. 將核發的憑證註冊到金鑰

1 啟動遠端使用者介面，並以系統管理員的身分登入。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 對於要註冊的憑證按一下 [鍵值名稱] 或 [憑證]。



5 按一下[註冊憑證]。

6 **按一下 [瀏覽] ▶ 指定您要求的憑證檔案 ▶ 按一下 [註冊]。**

步驟 2：重設金鑰和憑證 (TLS)

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [網路] ▶ [TLS 設定]。**

4 **按一下[鍵值和憑證]。**

5 **在要使用的金鑰和憑證右側，按一下 [註冊預設鍵值]。**

- 如果要使用預先安裝的金鑰和憑證，請選擇 [Default Key]。

6 **按一下[確定]。**

7 **重新啟動本機。**

➠ 本機重新啟動，然後套用設定。

步驟 3：刪除過去產生的金鑰/憑證 (TLS)

註釋

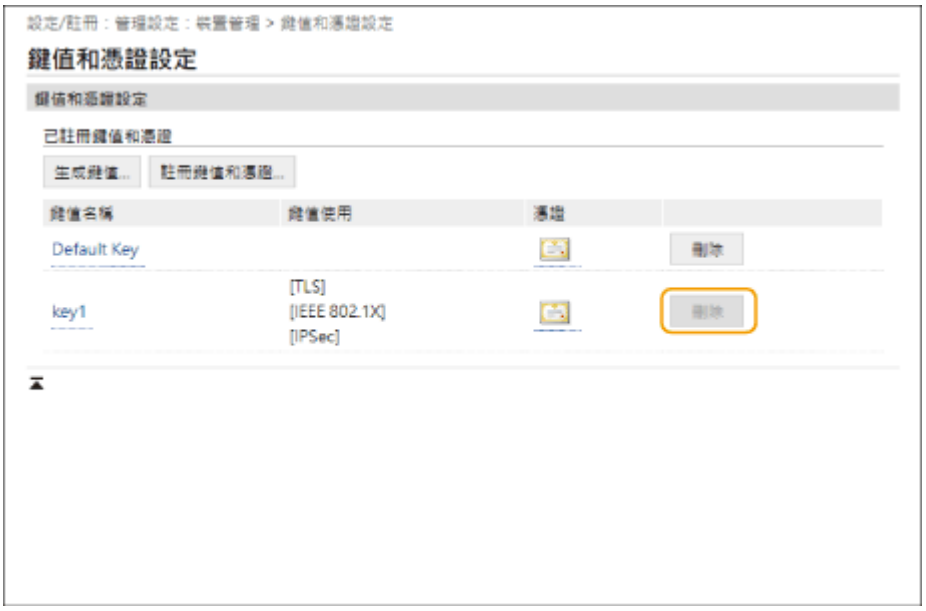
- 停用憑證時，您可能需要向憑證授權單位傳達資訊。請參閱 **檢查您是否必須執行附加程序(P. 4)** ，並在刪除金鑰/憑證之前記下所需資訊。

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **選擇金鑰和憑證 ▶ 按一下 [刪除] ▶ [確定]。**



註釋

- 使用中的金鑰和憑證會顯示其用途，例如 [TLS] 或 [IEEE 802.1X]，且不能刪除。請在停用相應功能或變更為其他金鑰或憑證後，再將其刪除。

步驟 4：停用憑證 (TLS)

停用過去產生的憑證。程序會依憑證類型而有不同。

■對於自我簽章憑證

如果在電腦或網頁瀏覽器中將包含需要附加程序之金鑰的憑證註冊為可信任憑證，請刪除已註冊的憑證。

■對於 CSR 憑證

要求核發憑證的憑證授權單位撤銷憑證。請參閱憑證中的 [發行者] 以瞭解要求的憑證授權單位。

註釋

- 如果在與機器通訊的電腦或網頁瀏覽器中使用 CRL 檢查憑證撤銷，請在撤銷憑證後將更新的 CRL 註冊到電腦或網頁瀏覽器。
- 如果您使用 CRL 以外的方法（例如 OCSP）來檢查憑證撤銷，請執行該方法的程序。

步驟 5：啟用新憑證 (TLS)

啟用機器上新產生的憑證。

■對於自我簽章憑證

在電腦或網頁瀏覽器中將新憑證註冊為可信任憑證。

■對於 CSR 憑證

您不需要執行附加程序。

IEEE 802.1X 的程序

步驟 1：檢查認證方法 (IEEE 802.1X)

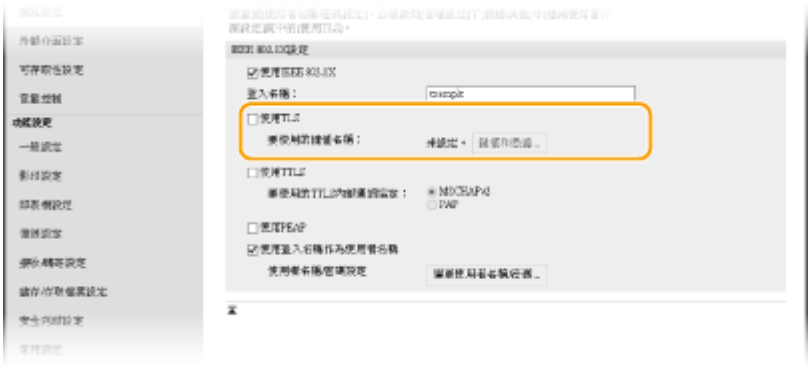
如果 IEEE 802.1X 認證方法設定為 TLS，您必須執行後續程序。
遵循以下程序檢查認證方法。

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [網路] ▶ [IEEE 802.1X 設定] ▶ [編輯]。**

4 **檢查 [使用 TLS]。**



- 如果選擇了 [使用 TLS] 並且顯示金鑰名稱，請執行後續程序。
- 如果取消選擇 [使用 TLS]，您不需要執行後續程序。

步驟 2：重新產生金鑰和憑證 (IEEE 802.1X)

您可以為機器產生的金鑰產生兩種類型的憑證：自我簽章憑證和 CSR 憑證。程序會依憑證類型而有不同。

對於自我簽章憑證(P. 20)
對於 CSR 憑證(P. 21)

對於自我簽章憑證

1 **啟動遠端使用者介面。**

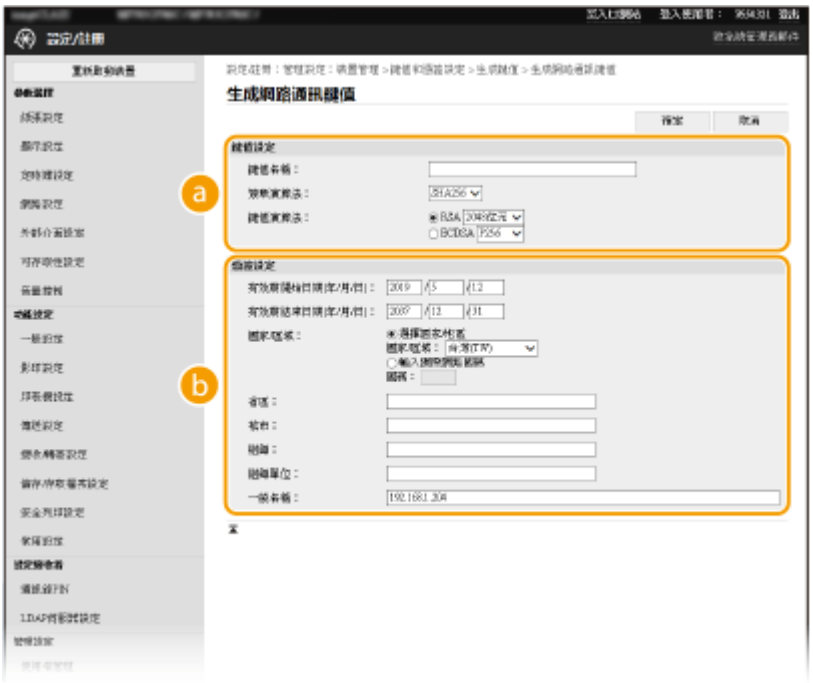
2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **按一下[生成鍵值]。**

5 **選擇 [網路通訊] ▶ 按一下 [確定]。**

6 **指定金鑰和憑證設定。**



a [鍵值設定]

[鍵值名稱]

使用英數字元輸入金鑰名稱。請輸入可在清單中輕鬆找到的名稱。

[簽章演算法]
從下拉式清單中選擇金鑰演算法。

[鍵值演算法]
選擇 [RSA] 或 [ECDSA] 作為金鑰產生演算法 ▶ 從下拉清單中選擇金鑰長度。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

註釋:

- 如果您對 [簽章演算法] 選擇 [SHA384] 或 [SHA512]，則當對 [鍵值演算法] 選擇 [RSA] 時，不能將金鑰長度設定為 [512 位元]。

[憑證設定]

[有效期開始日期(年/月/日)]
輸入憑證有效期的開始日期和結束日期。

[有效期結束日期(年/月/日)]
輸入憑證有效期的結束日期。您不能設定早於 [有效期開始日期(年/月/日)] 中的日期。

[國家/區域]
按一下 [選擇國家/地區]，然後從下拉清單中選擇國家/地區。或者，按一下 [輸入網際網路國碼]，然後輸入國碼，例如「US」代表美國。

[省區]/[城市]
視需要使用英數字元輸入位置。

[組織]/[組織單位]
視需要使用英數字元輸入組織名稱。

[一般名稱]
視需要使用英數字元輸入憑證的一般名稱。「一般名稱」通常縮寫為「CN」。

7 按一下[確定]。

- 金鑰和憑證的產生可能要花一點時間。
- 產生的金鑰和憑證會自動註冊到本機。

對於 CSR 憑證

在本機上產生金鑰和 CSR。使用畫面上顯示的 CSR 資料或輸出為檔案以要求憑證授權單位核發憑證。然後為金鑰註冊核發的憑證。

■1. 產生金鑰和 CSR

1 啟動遠端使用者介面。

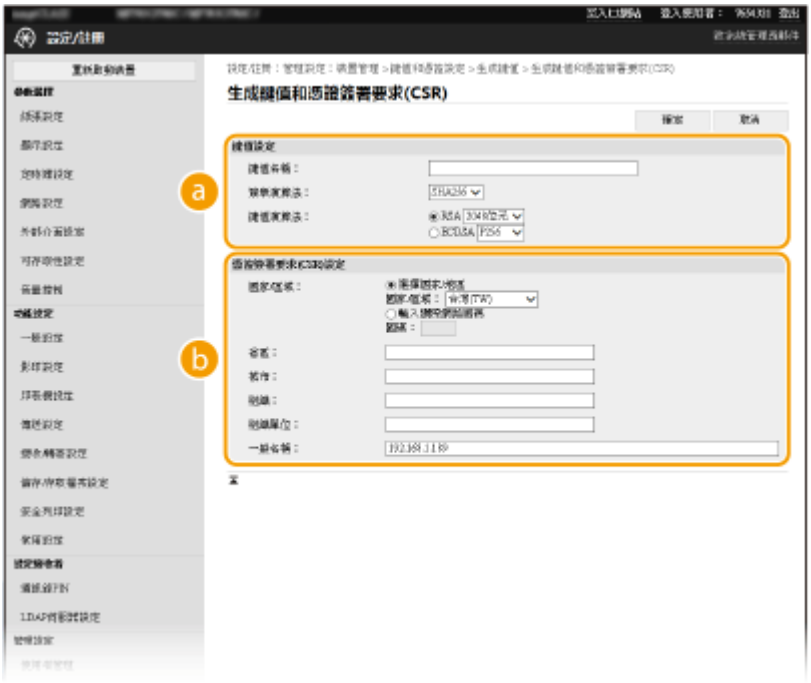
2 按一下入口網站頁面的 [設定/註冊]。

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **按一下[生成鍵值]。**

5 **選擇 [鍵值和憑證簽署要求(CSR)] ▶ 按一下 [確定]。**

6 **指定金鑰和 CSR 設定。**



a [鍵值設定]

[鍵值名稱]
使用英數字元輸入金鑰名稱。請輸入可在清單中輕鬆找到的名稱。

[簽章演算法]
從下拉式清單中選擇金鑰演算法。

[鍵值演算法]
選擇 [RSA] 或 [ECDSA] 作為金鑰產生演算法 ▶ 從下拉清單中選擇金鑰長度。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

註釋:

- 如果您對 [簽章演算法] 選擇 [SHA384] 或 [SHA512]，則當對 [鍵值演算法] 選擇 [RSA] 時，不能將金鑰長度設定為 [512 位元]。

b [憑證簽署要求(CSR)設定]

[國家/區域]
按一下 [選擇國家/地區]，然後從下拉清單中選擇國家/地區。或者，按一下 [輸入網際網路國碼]，然後輸入國碼，例如「US」代表美國。

[省區]/[城市]
視需要使用英數字元輸入位置。

[組織]/[組織單位]
視需要使用英數字元輸入組織名稱。

[一般名稱]
視需要使用英數字元輸入憑證的一般名稱。「一般名稱」通常縮寫為「CN」。

7 按一下[確定]。

- 金鑰和 CSR 的產生可能要花一點時間。

8 按一下[儲存在檔案中]。

- 顯示儲存檔案的對話方塊時，選擇要儲存檔案的目的地 ▶ 按一下 [存檔]。

  ➠ CSR 檔案即會儲存到電腦上。

9 附加儲存的檔案，然後向憑證授權單位提出申請。

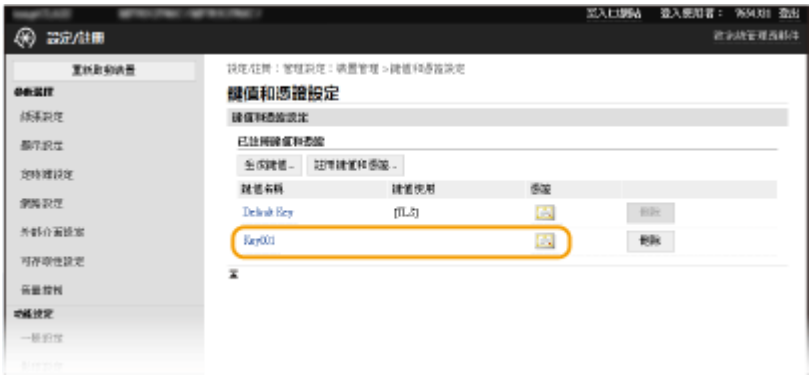
■2. 將核發的憑證註冊到金鑰

1 啟動遠端使用者介面，並以系統管理員的身分登入。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 對於要註冊的憑證按一下 [鍵值名稱] 或 [憑證]。



5 按一下[註冊憑證]。

6 **按一下 [瀏覽] ▶ 指定您要求的憑證檔案 ▶ 按一下 [註冊]。**

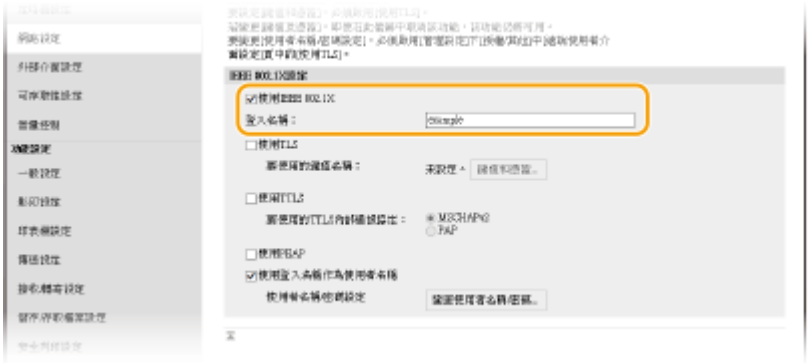
步驟 3：重設金鑰和憑證 (IEEE 802.1X)

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [網路] ▶ [IEEE 802.1X 設定] ▶ [編輯]。**

4 **選擇 [使用 IEEE 802.1X] ▶ 在 [登入名稱] 中輸入登入名稱。**



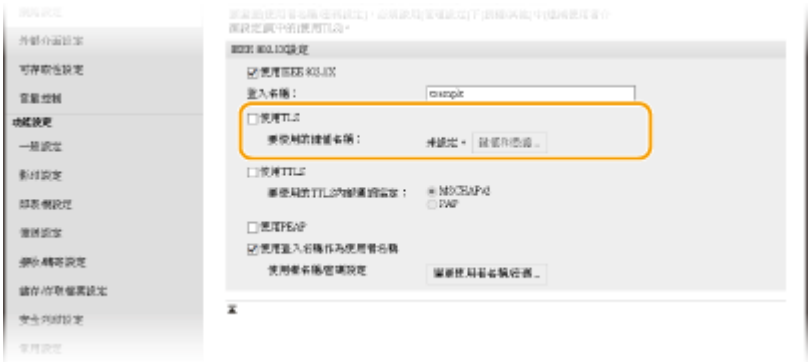
[使用 IEEE 802.1X]

選擇此項以使用 IEEE 802.1X 認證。

[登入名稱]

使用英數字元輸入用於識別使用者的名稱 (EAP 身分)。

5 **選擇 [使用 TLS] ▶ 按一下 [鍵值和憑證]。**



6 **在要使用的金鑰和憑證右側，按一下 [註冊預設鍵值]。**

7 **按一下[確定]。**

8 重新啟動本機。

➠ 本機重新啟動，然後套用設定。

步驟 4：刪除過去產生的金鑰/憑證 (IEEE 802.1X)

註釋

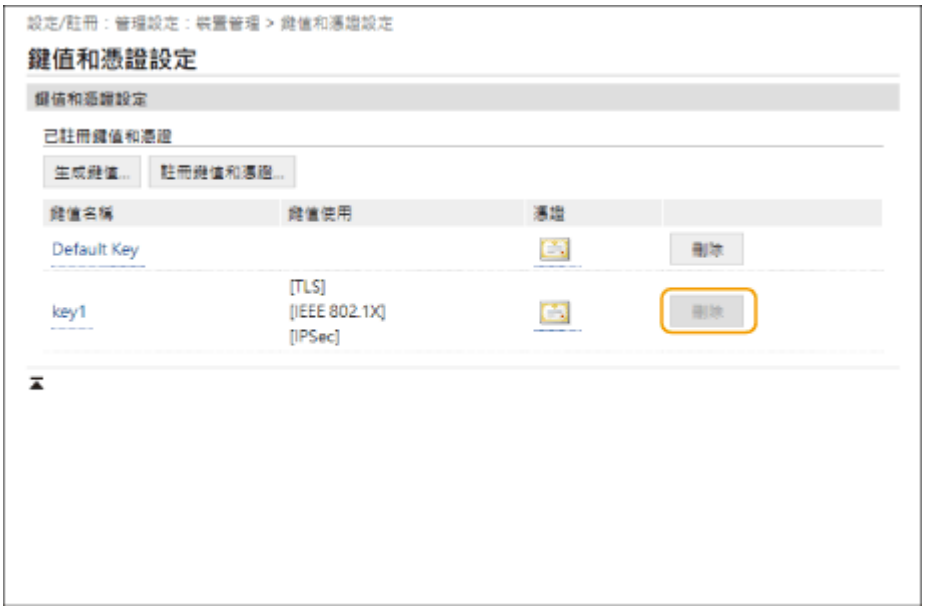
- 停用憑證時，您可能需要向憑證授權單位傳達資訊。請參閱 **檢查您是否必須執行附加程序(P. 4)** ，並在刪除金鑰/憑證之前記下所需資訊。

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **選擇金鑰和憑證 ▶ 按一下 [刪除] ▶ [確定]。**



註釋

- 使用中的金鑰和憑證會顯示其用途，例如 [TLS] 或 [IEEE 802.1X]，且不能刪除。請在停用相應功能或變更為其他金鑰或憑證後，再將其刪除。

步驟 5：停用憑證 (IEEE 802.1X)

停用過去產生的憑證。程序會依憑證類型而有不同。

■對於自我簽章憑證

如果在 IEEE 802.1X 認證伺服器中將包含需要附加程序之金鑰的憑證註冊為可信任憑證，請刪除已註冊的憑證。

■對於 CSR 憑證

要求核發憑證的憑證授權單位撤銷憑證。請參閱憑證中的 [發行者] 以瞭解要求的憑證授權單位。

註釋

- 如果在 IEEE 802.1X 認證伺服器中使用 CRL 檢查憑證撤銷，請在撤銷憑證後將更新的 CRL 註冊到電腦或網頁瀏覽器。
- 如果您使用 CRL 以外的方法（例如 OCSP）來檢查憑證撤銷，請執行該方法的程序。

步驟 6：啟用新憑證 (IEEE 802.1X)

啟用憑證。

■對於自我簽章憑證

在 IEEE 802.1X 認證伺服器中將新憑證註冊為可信任憑證。

■對於 CSR 憑證

您不需要執行附加程序。

IPSec 的程序

步驟 1：檢查認證方法 (IPSec)

如果 IPSec 中的 IKE 設定設為 [數位簽章方法]，您必須執行後續程序。
遵循以下程序檢查認證方法。

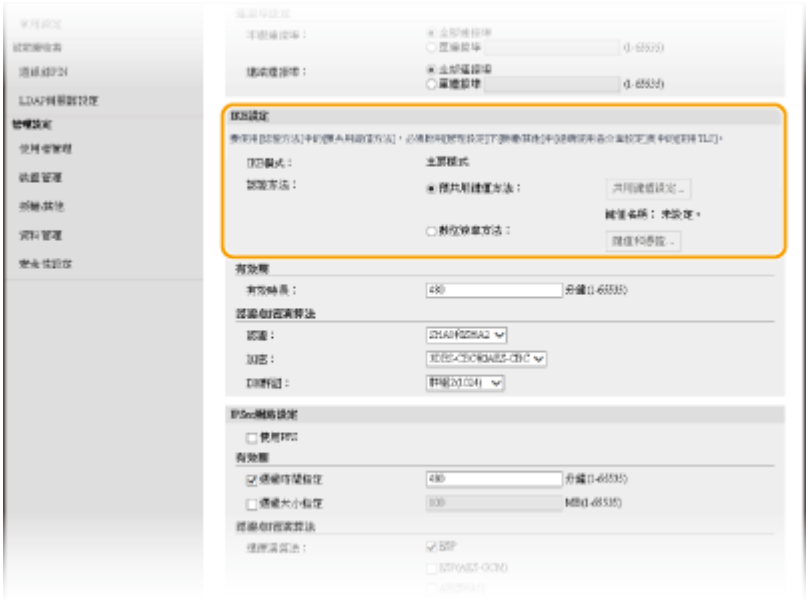
1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [網路] ▶ [IPSec 設定]。**

4 **按一下 [已註冊 IPSec 策略] 中的策略。**

5 **檢查 [IKE 設定] 中的 [認證方法]。**



- 如果 [認證方法] 設為 [數位簽章方法] 並顯示金鑰名稱，請執行後續程序。
- 如果 [認證方法] 設為 [預共用鍵值方法]，您不需要執行後續程序。

步驟 2：重新產生金鑰和憑證 (IPSec)

您可以為機器產生的金鑰產生兩種類型的憑證：自我簽章憑證和 CSR 憑證。程序會依憑證類型而有不同。

對於自我簽章憑證(P. 32)
對於 CSR 憑證(P. 33)

對於自我簽章憑證

1 **啟動遠端使用者介面。**

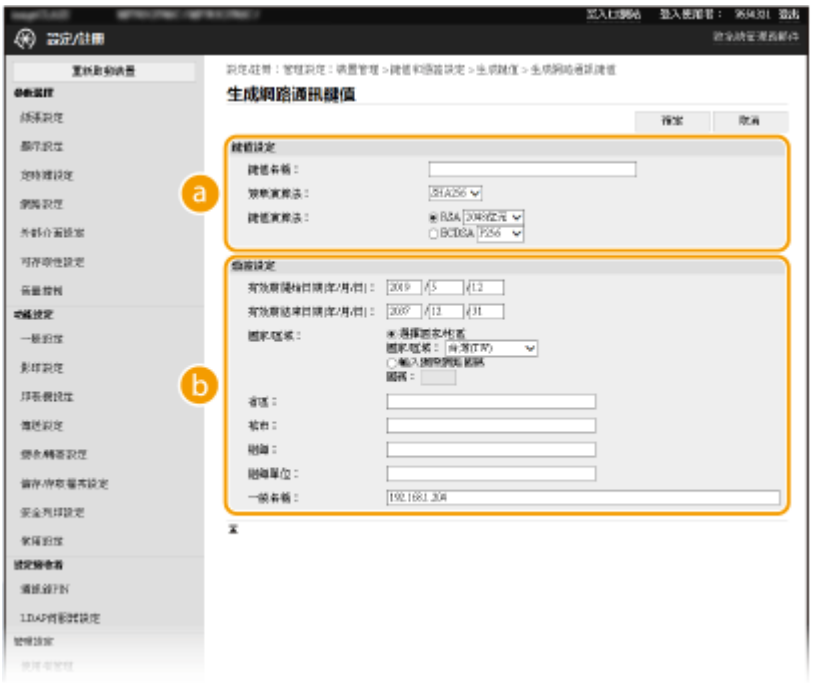
2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **按一下[生成鍵值]。**

5 **選擇 [網路通訊] ▶ 按一下 [確定]。**

6 **指定金鑰和憑證設定。**



a [鍵值設定]

[鍵值名稱]

使用英數字元輸入金鑰名稱。請輸入可在清單中輕鬆找到的名稱。

[簽章演算法]
從下拉式清單中選擇金鑰演算法。

[鍵值演算法]
選擇 [RSA] 或 [ECDSA] 作為金鑰產生演算法 ▶ 從下拉清單中選擇金鑰長度。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

註釋:

- 如果您對 [簽章演算法] 選擇 [SHA384] 或 [SHA512]，則當對 [鍵值演算法] 選擇 [RSA] 時，不能將金鑰長度設定為 [512 位元]。

[憑證設定]

[有效期開始日期(年/月/日)]
輸入憑證有效期的開始日期和結束日期。

[有效期結束日期(年/月/日)]
輸入憑證有效期的結束日期。您不能設定早於 [有效期開始日期(年/月/日)] 中的日期。

[國家/區域]
按一下 [選擇國家/地區]，然後從下拉清單中選擇國家/地區。或者，按一下 [輸入網際網路國碼]，然後輸入國碼，例如「US」代表美國。

[省區]/[城市]
視需要使用英數字元輸入位置。

[組織]/[組織單位]
視需要使用英數字元輸入組織名稱。

[一般名稱]
視需要使用英數字元輸入憑證的一般名稱。「一般名稱」通常縮寫為「CN」。

7 按一下[確定]。

- 金鑰和憑證的產生可能要花一點時間。
- 產生的金鑰和憑證會自動註冊到本機。

對於 CSR 憑證

在本機上產生金鑰和 CSR。使用畫面上顯示的 CSR 資料或輸出為檔案以要求憑證授權單位核發憑證。然後為金鑰註冊核發的憑證。

■1. 產生金鑰和 CSR

1 啟動遠端使用者介面。

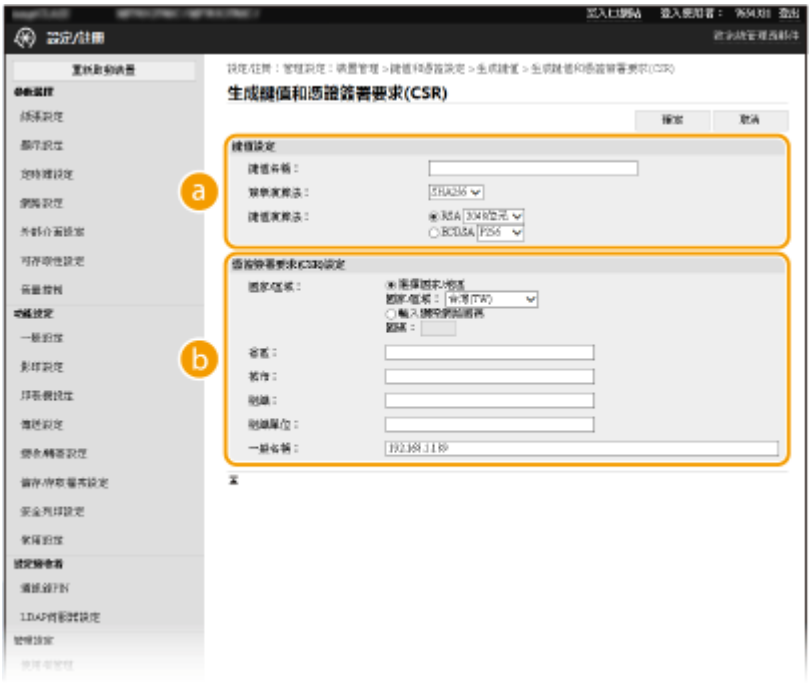
2 按一下入口網站頁面的 [設定/註冊]。

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **按一下[生成鍵值]。**

5 **選擇 [鍵值和憑證簽署要求(CSR)] ▶ 按一下 [確定]。**

6 **指定金鑰和 CSR 設定。**



a [鍵值設定]

[鍵值名稱]
使用英數字元輸入金鑰名稱。請輸入可在清單中輕鬆找到的名稱。

[簽章演算法]
從下拉式清單中選擇金鑰演算法。

[鍵值演算法]
選擇 [RSA] 或 [ECDSA] 作為金鑰產生演算法 ▶ 從下拉清單中選擇金鑰長度。在兩種情況中，較高的值提供較好的安全性但會降低通訊處理速度。

註釋:

- 如果您對 [簽章演算法] 選擇 [SHA384] 或 [SHA512]，則當對 [鍵值演算法] 選擇 [RSA] 時，不能將金鑰長度設定為 [512 位元]。

b [憑證簽署要求(CSR)設定]

[國家/區域]
按一下 [選擇國家/地區]，然後從下拉清單中選擇國家/地區。或者，按一下 [輸入網際網路國碼]，然後輸入國碼，例如「US」代表美國。

[省區]/[城市]
視需要使用英數字元輸入位置。

[組織]/[組織單位]
視需要使用英數字元輸入組織名稱。

[一般名稱]
視需要使用英數字元輸入憑證的一般名稱。「一般名稱」通常縮寫為「CN」。

7 按一下[確定]。

- 金鑰和 CSR 的產生可能要花一點時間。

8 按一下[儲存在檔案中]。

- 顯示儲存檔案的對話方塊時，選擇要儲存檔案的目的地 ▶ 按一下 [存檔]。

  ➠ CSR 檔案即會儲存到電腦上。

9 附加儲存的檔案，然後向憑證授權單位提出申請。

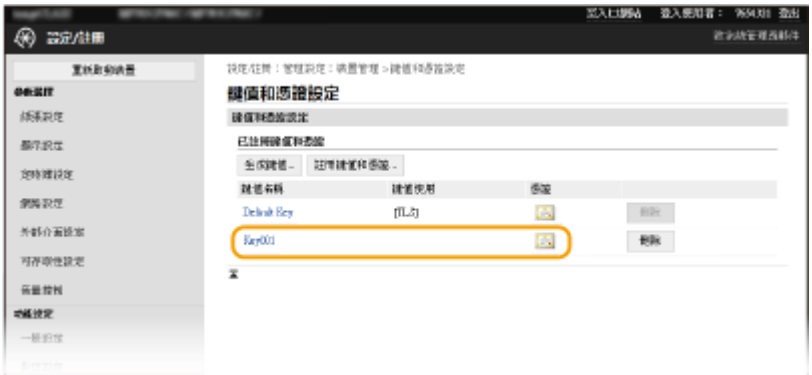
■2. 將核發的憑證註冊到金鑰

1 啟動遠端使用者介面，並以系統管理員的身分登入。

2 按一下入口網站頁面的 [設定/註冊]。

3 按一下 [裝置管理] ▶ [鍵值和憑證設定]。

4 對於要註冊的憑證按一下 [鍵值名稱] 或 [憑證]。



5 按一下[註冊憑證]。

6 **按一下 [瀏覽] ▶ 指定您要求的憑證檔案 ▶ 按一下 [註冊]。**

步驟 3：重設金鑰和憑證 (IPSec)

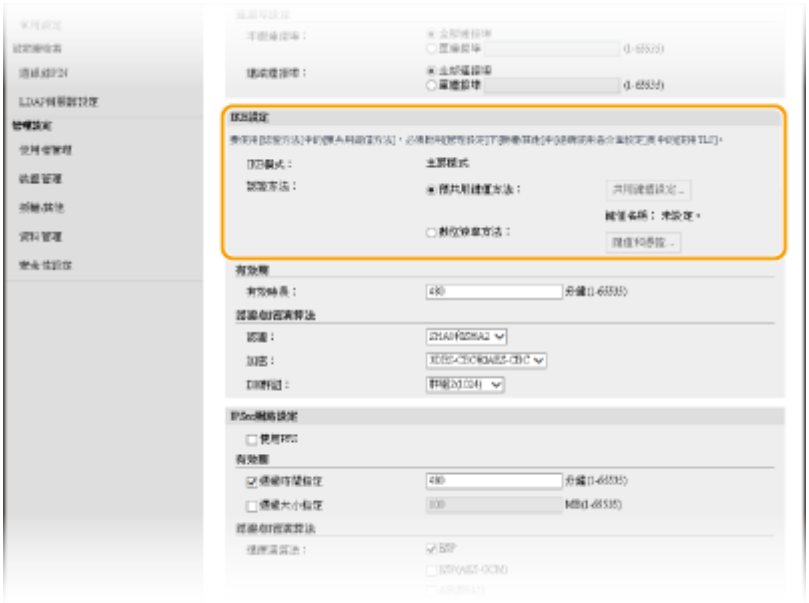
1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [網路] ▶ [IPSec 設定]。**

4 **在 [已註冊 IPSec 策略] 中按一下重設金鑰和憑證的策略。**

5 **指定 [IKE 設定]。**



6 **選擇 [認證方法] 中的 [數位簽章方法] ▶ 按一下 [鍵值和憑證]。**

7 **在要使用的金鑰和憑證右側，按一下 [註冊預設鍵值]。**

8 **按一下[確定]。**

9 **重新啟動本機。**

➠ 本機重新啟動，然後套用設定。

步驟 4：刪除過去產生的金鑰/憑證 (IPSec)

註釋

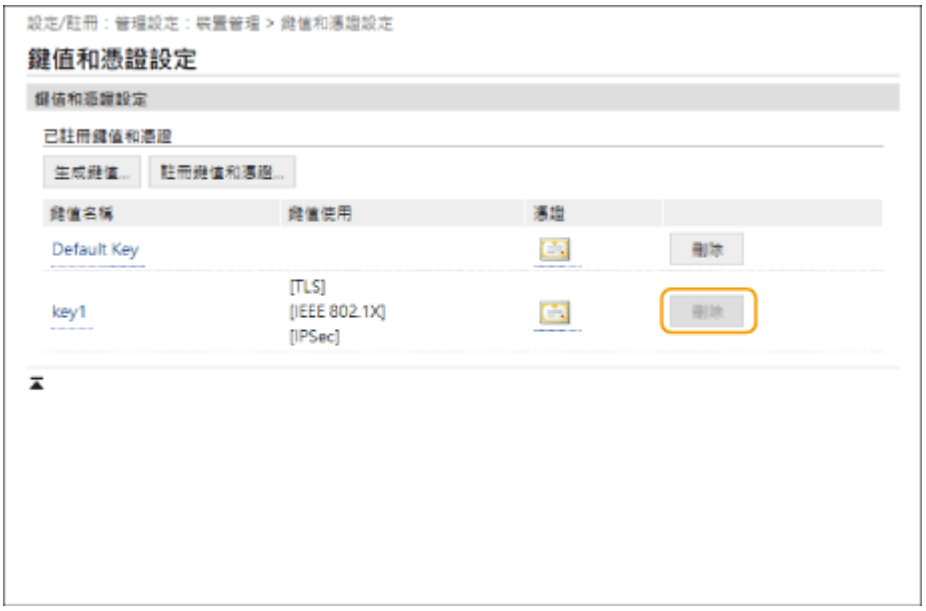
- 停用憑證時，您可能需要向憑證授權單位傳達資訊。請參閱 **檢查您是否必須執行附加程序(P. 4)** ，並在刪除金鑰/憑證之前記下所需資訊。

1 **啟動遠端使用者介面。**

2 **按一下入口網站頁面的 [設定/註冊]。**

3 **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**

4 **選擇金鑰和憑證 ▶ 按一下 [刪除] ▶ [確定]。**



註釋

- 使用中的金鑰和憑證會顯示其用途，例如 [TLS] 或 [IEEE 802.1X]，且不能刪除。請在停用相應功能或變更為其他金鑰或憑證後，再將其刪除。

步驟 5：停用憑證 (IPSec)

停用過去產生的憑證。程序會依憑證類型而有不同。

■對於自我簽章憑證

如果在透過 IPSec 通訊的裝置中將包含需要附加程序之金鑰的憑證註冊為可信任憑證，請刪除已註冊的憑證。刪除已註冊的憑證後，請註冊重新產生之金鑰的憑證。

■對於 CSR 憑證

要求核發憑證的憑證授權單位撤銷憑證。請參閱憑證中的 [發行者] 以瞭解要求的憑證授權單位。

註釋

- 如果在透過 IPSec 通訊的裝置中使用 CRL 檢查憑證撤銷，請在撤銷憑證後將更新的 CRL 註冊到電腦或網頁瀏覽器。
- 如果您使用 CRL 以外的方法（例如 OCSP）來檢查憑證撤銷，請執行該方法的程序。

步驟 6：啟用新憑證 (IPSec)

啟用憑證。

■對於自我簽章憑證

在透過 IPSec 通訊的裝置中將新憑證註冊為可信任憑證。

■對於 CSR 憑證

您不需要執行附加程序。

裝置簽章的程序

步驟 1：重新產生金鑰和憑證 (裝置簽章)(P. 42)
步驟 2：停用憑證 (裝置簽章)(P. 43)
步驟 3：啟用新憑證 (裝置簽章)(P. 44)

步驟 1：重新產生金鑰和憑證 (裝置簽章)

1. **啟動遠端使用者介面。**
2. **按一下入口網站頁面的 [設定/註冊]。**
3. **按一下 [裝置管理] ▶ [鍵值和憑證設定]。**
4. **在要裝置簽章的金鑰和憑證右側，按一下 [更新]。**
5. **按一下[確定]。**

步驟 2：停用憑證 (裝置簽章)

停用過去產生憑證。

■如果裝置簽章的憑證已註冊到 Acrobat

如果已在 Acrobat 中註冊裝置簽章的憑證，請刪除已註冊的憑證。

步驟 3：啟用新憑證 (裝置簽章)

啟用憑證。

■如果裝置簽章的憑證已註冊到 Acrobat

如果已在 Acrobat 中註冊裝置簽章的憑證，請在從本機傳送的 PDF 文件中註冊憑證，並將裝置簽章附加到 Acrobat。

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at: http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION
This license becomes null and void if any of the above conditions are not met.

DISCLAIMER
THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.