

目錄

TPM 晶片設定與使用流程	2
1. BIOS 設定	2
2. Infineon TPM 驅動程式及技嘉 Ultra TPM 程式安裝	3
3. TPM 晶片初始化設定	4
3.1. Easy Mode 簡易設定模式	4
3.2. Advanced Mode 進階設定模式	6
4. 技嘉 Ultra TPM 設定與使用	16

TPM 晶片設定與使用流程

若要啟動 TPM 晶片功能，請依序完成下列設定：

- 1. BIOS 設定
- 2. Infineon TPM 驅動程式及技嘉 Ultra TPM 程式安裝
- 3. TPM 晶片初始化設定
- 4. 技嘉 Ultra TPM 設定與使用

1. BIOS 設定

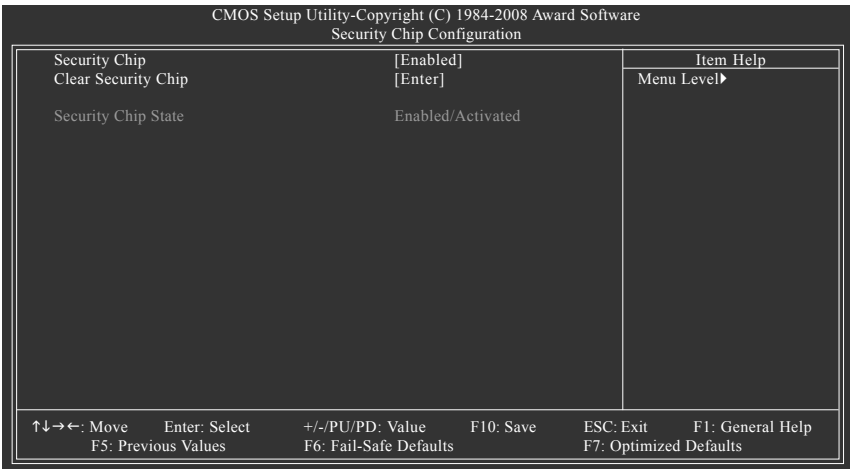
啟動 TPM 晶片功能前需先至 BIOS 設定程式啟動 TPM 晶片。

步驟一：

開機進入 BIOS 設定程式後，選擇「Security Chip Configuration」即會出現以下畫面，將「Security Chip」選項變更為「Enabled」即可啟動 TPM 晶片功能。建議您再進入「Clear Security Chip」選項清除 TPM 晶片內的所有設定。



清除 TPM 晶片內容後，若有已設定完成的加密檔案將無法再讀取，因此清除前請先備份。



步驟二：

完成設定後，按<F10>儲存 BIOS 設定並重新開機。

2. Infineon TPM 驅動程式及技嘉 Ultra TPM 程式安裝

若要啟動技嘉 Ultra TPM 功能，請確認您的系統已經安裝 Infineon TPM 驅動程式及技嘉 Ultra TPM 程式。

方法一：

放入技嘉主機板驅動程式光碟片後，「Xpress Install」會自動掃描您的系統並列出建議安裝的驅動程式。您可以按下「Xpress Install 完整安裝」鍵，「Xpress Install」將會安裝所有勾選的驅動程式，包含 Infineon TPM 驅動程式及技嘉 Ultra TPM 程式。



方法二：

若要單獨安裝 Infineon TPM 驅動程式及技嘉 Ultra TPM 程式，請點選「單點安裝」頁面，並分別在「Infineon TPM Driver」及「GIGABYTE Ultra TPM」按下「安裝」鍵進行安裝。



安裝 Infineon TPM 驅動程式。



安裝 Ultra TPM 程式。

3. TPM 晶片初始化設定

確認已完成 BIOS 設定及驅動程式的安裝並重新啟動系統後，在常駐程式列會出現 Infineon Security Platform 的小圖示 (此圖示顯示 Infineon Security Platform 尚未初始化)，雙擊此圖示即可進入「Easy Mode」簡易設定模式(請參考 3.1 章節的說明)或是選擇「Advanced Mode」進階設定模式(請參考 3.2 章節的說明)，並開始進行 Infineon Security Platform 初始化與設定。

3.1. Easy Mode 簡易設定模式

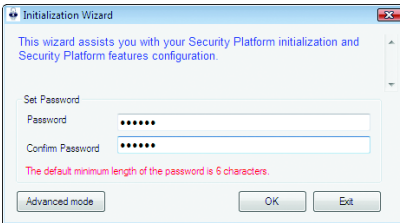
雙擊常駐程式列的 Infineon Security Platform 圖示 即可開啟技嘉「Initialization Wizard」，此為「Easy Mode」簡易設定模式。「Easy Mode」提供您簡易的 Infineon Security Platform 初始化介面，讓您輕易地進行 TPM 晶片初始化及設定 Personal Secure Drive (PSD)。



- 「Easy Mode」簡易設定模式簡化了 Infineon Security Platform 初始化的設定步驟與功能，若要更詳細的設定，請點選「Advanced Mode」進階設定模式。
- 「Easy Mode」簡易設定模式僅提供「Personal Secure Drive (PSD)的檔案和資料夾加密」的設定，若您要執行「加密檔案(EFS)的檔案和資料夾加密」或是「安全電子郵件」的加密，請點選「Advanced Mode」進階設定模式。

步驟一：密碼設定

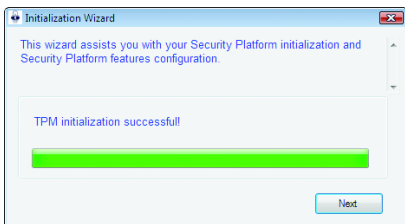
開啟技嘉「Initialization Wizard」後，設定精靈會要求設定一組密碼，鍵入密碼後按「OK」即開始進行 Infineon Security Platform 初始化作業。



此組密碼結合了 Infineon Security Platform 的「擁有者密碼」、「使用者密碼」、「緊急復原權杖密碼」及「密碼重設權杖密碼」，因此請務必記住此組密碼以管理及使用 Security Platform。詳細密碼定義與使用方法請參閱 Infineon Security Platform 相關說明。

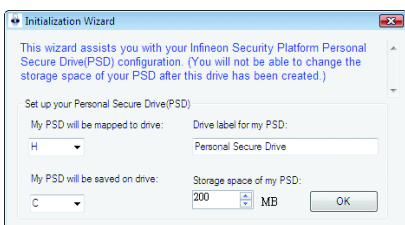
步驟二：Infineon Security Platform 初始化作業

開始 Infineon Security Platform 初始化作業，完成後會顯示「TPM Initialization Successful!」，按「NEXT」繼續設定 Personal Secure Drive (PSD)。



在完成所有設定作業前，請勿關閉電源、進入節能狀態或是拔除電源線。

步驟三：設定 Personal Secure Drive (PSD)



三-1.設定 Personal Secure Drive (PSD)的虛擬磁碟機代號與名稱

要設定 Personal Secure Drive (PSD) 虛擬磁碟機代號，請從「My PSD will be mapped to drive:」下拉清單中選擇一個尚未使用的磁碟機代號。若要設定 PSD 磁碟名稱，直接在「Drive label for my PSD:」文字方塊列中輸入名稱，並注意長度不能超過 32 位元。

三-2.設定 Personal Secure Drive 儲存空間大小與指定儲存 Personal Secure Drive 的實體磁碟機

在「My PSD will be saved on drive:」選擇實際要儲存 PSD 的實體磁碟機代號，並在「Storage space of my PSD:」設定需要分配給 PSD 磁碟的儲存空間大小。



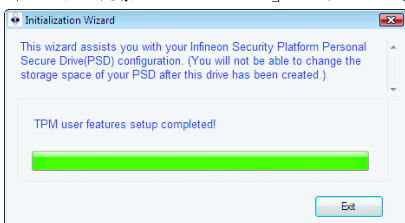
Personal Secure Drive (PSD) 的儲存空間在設定以後不能變更，因此請確保指定的空間可以滿足您的需要。並注意因為檔案系統要分配一定空間，所以您不能使用最大的磁碟機大小。同時也請注意，最大的 PSD 磁碟機大小是有限制的：

FAT16 PSD 磁碟機最大為 2 GB。

FAT32 PSD 磁碟機最大為 4 GB。

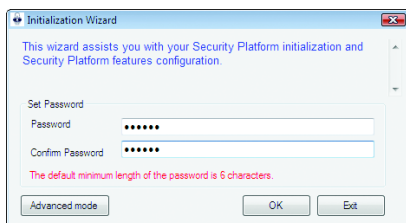
步驟四：設定完成

按「Exit」離開即已完成 TPM 晶片初始化及 Personal Secure Drive (PSD) 的設定，接著即可進入技嘉「Ultra TPM」設定 USB 隨身金鑰。



3.2. Advanced Mode 進階設定模式

雙擊常駐程式列的 Infineon Security Platform 圖示 開啟技嘉「Initialization Wizard」後，若做進一步的設定，直接點選「Advanced Mode」即可進入 Infineon Security Platform 的原始設定程序。



A. Infineon Security Platform 初始化精靈 - 擁有者

點選「Advanced Mode」會出現「Infineon Security Platform 初始化精靈」，依據畫面指示即可初始化 Security Platform 擁有者，並設定 Security Platform 功能(備份包括緊急復原、密碼重設、增強型驗證)。此設定精靈提供詳盡的 Infineon Security Platform 操作設定。

A-1. 進入「Infineon Security Platform 初始化精靈」，如要繼續請按「下一步」。



A-2. 選擇「Security Platform 初始化」後，按「下一步」並建立擁有者密碼。



建立的 Infineon Security Platform 擁有者金鑰，會與 Infineon Security Platform 擁有者秘密資訊一起儲存在 Infineon Trusted Platform Module 之中。在此建立的擁有者密碼主要用以保護金鑰。您必須記住此密碼以管理 Security Platform。

A-3. 設定 Security Platform 功能，此功能包含自動備份與密碼重設，選擇「下一步」。



功能說明：

備份 (包括緊急復原)

選擇此功能可以設定自動 Security Platform 備份。強烈建議設定備份，否則在意外事件下可能會遺失所有的使用者資料。



如果啟動了原則強制設定備份 (包括緊急復原)，您就無法取消選擇此功能。

密碼重設

選擇此功能，以便為所有使用者建立密碼重設權杖。強烈建議設定密碼重設。否則將無法重設基本使用者密碼。



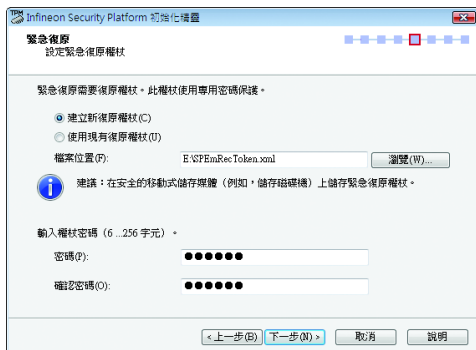
如果啟動了原則強制設定密碼重設，您就無法取消選擇此功能。此功能只能設定一次。

如果已設定了密碼重設，則此選項被停用。

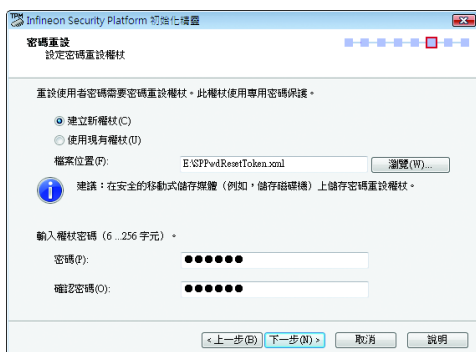
A-4. 此頁面可以設定自動 Security Platform 備份，包含使用者的憑證與設定及 PSD 加密資料等，以避免因硬體或是儲存設備故障後，能還原特定的使用者設定。選擇「下一步」。



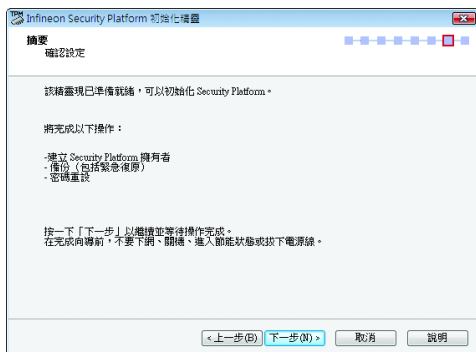
A-5. 選擇「建立新復原權杖」，並鍵入一組新密碼，以執行後續緊急還原作業。



A-6. 建立一個「密碼重設權杖」，並輸入一組權杖密碼。



A-7. 確認所欲執行的功能均已被選取，按「下一步」以繼續完成作業。



在完成所有設定作業前，請勿關閉電源、進入節能狀態或是拔除電源線。

A-8. 按下「完成」即完成 Infineon Security Platform 初始化與功能設定。接著將進入「Infineon Security Platform 使用者初始化」設定程序。(請勾選「啟動 Security Platform 使用者初始化精靈」)



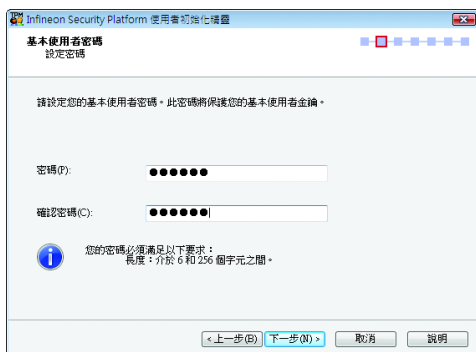
B. Infineon Security Platform 初始化精靈 - 使用者

使用「Infineon Security Platform 使用者初始化精靈」來初始化 Security Platform 使用者，以及設定特定於使用者的功能(安全的電子郵件、帶有 EFS 和 PSD 的檔案和資料夾加密以及增強驗證)。為每一位元電腦使用者啟動此精靈，這樣使用者可以使用個人化的 Infineon Security Platform 功能(意即，將要成為 Infineon Security Platform 使用者的電腦使用者)。

B-1. 進入「Infineon Security Platform 使用者初始化精靈」，如要繼續請按「下一步」。



B-2. 設定使用者密碼，並按「下一步」。



Infineon Security Platform 使用者初始化設置

基本使用者密碼

設定密碼

請設定您的基本使用者密碼。此密碼將保護您的基本使用者金鑰。

密碼(P):

確認密碼(C):

 您的密碼必須滿足以下要求：
長度：介於 6 和 256 個字元之間。

< 上一步(B) 下一步(N) > 取消 說明

B-3. 設定啟用使用者密碼重設功能，選擇欲儲存的位置後按「下一步」。



Infineon Security Platform 使用者初始化設置

基本使用者密碼重設

為我的基本使用者密碼啟用重設功能

☒ 啟用在緊急情況下重設我的基本使用者密碼(P)。

準備將個人秘密寫入檔案。
指定路徑和檔案名。

個人秘密位置(P): 瀏覽(B)...

 請將此檔案儲存在安全位置。如果您必須在緊急情況下重設基本使用者密碼，您將需要它。

< 上一步(B) 下一步(N) > 取消 說明

B-4. 按「下一步」以繼續完成初始化作業。



Infineon Security Platform 使用者初始化設置

密碼和驗證

確認設定

該精靈現已準備就緒，可以初始化目前使用者。

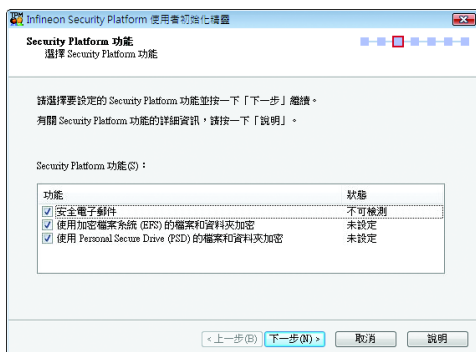
將完成以下操作：

- 產生基本使用者金鑰
- 啟用緊急情況下重設我的基本使用者密碼

按一下「下一步」以繼續並等待操作完成。
在完內再導引，不要下調、開機，進入節能狀態或拔下電源線。

< 上一步(B) 下一步(N) > 取消 說明

B-5. 選擇所要設定的加密功能，並按「下一步」。



功能說明：

安全電子郵件

特定於使用者的電子郵件加密和 / 或簽名以防止未經授權的人讀取或變更您的電子郵件。使用此功能可以確保只有電子郵件的建立者和指定的收件人才可以解密並閱讀郵件，或驗證發件人的身份。

如果選擇設定此功能，可以為安全電子郵件申請證書(如果在原則設定中設定了憑證申請網址)。該精靈將提供如何設定安全電子郵件的資訊。此精靈不提供郵件使用者端的設定，因此，無法在此處顯示狀態。

加密檔案系統(EFS)的檔案和資料夾加密

作業系統可以透過使用 Microsoft 加密檔案系統(EFS)收編在本機電腦上所執行的檔案和資料夾內容，以提供給特定使用者進行加密的功能。只有在這些資料夾中建立檔案的使用者才有權存取檔案的內容，其他使用者必須在顯式管理操作中被授予存取 EFS 資料夾的權力才可以在其中使用檔案。

如果您選擇設定此功能，您可以為 EFS 選擇憑證，也可以申請或建立新的憑證。



Windows Vista Home Basic、Vista Home Premium 及 XP Home Editions 不支援 EFS。

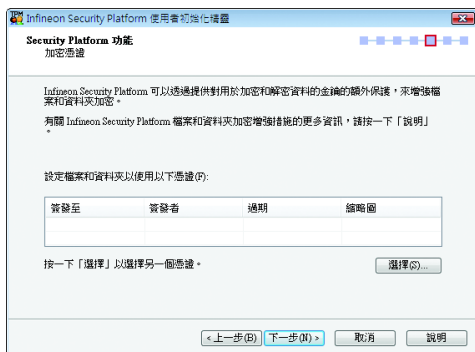
Personal Secure Drive (PSD)的檔案和資料夾加密

Personal Secure Drive (PSD)顯示與 EFS 相似的檔案和資料夾加密。與 EFS 不同的是，Windows Vista Home Basic、Vista Home Premium 及 XP Home Editions 皆支援 PSD。

這是為許可使用者所提供的邏輯磁碟機。此磁碟機可以為其所有內容提供存取許可權的保護和加密，加密將自動執行。PSD 能透過其 UNC 識別字進行存取以獲取可讀數據，且只能安裝在本機電腦上，不能存取網路磁碟。

如果您選擇設定此功能，則您可以設定、修改或刪除 PSD。與 EFS 設定相似，您可以為 PSD 選擇憑證，也可以申請或建立新的憑證。

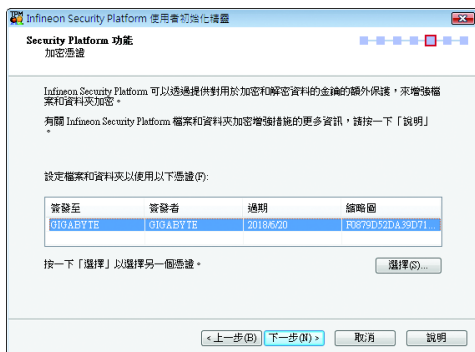
B-5-1. 以建立「Personal Secure Drive (PSD)」的檔案和資料夾加密」為例：
設定「加密憑證」，按「選擇」。



B-5-2. 按「建立」以建立憑證。待憑證出現後，點選憑證再按「選擇」。



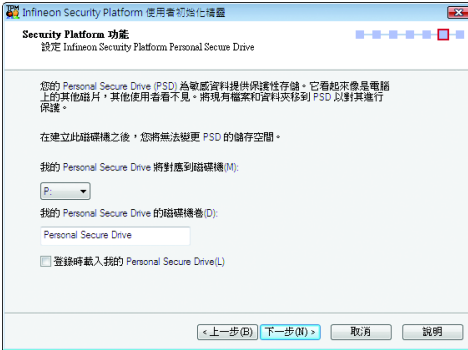
B-5-3. 憑證已選擇，按「下一步」。



B-6. 設定 Personal Secure Drive (PSD)。

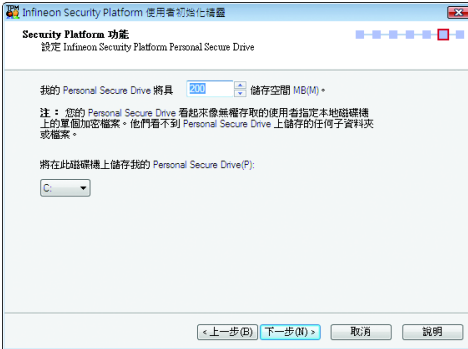
B-6-1. 設定 Personal Secure Drive (PSD)的虛擬磁碟機代號與名稱。

要設定 Personal Secure Drive (PSD) 虛擬磁碟機代號，請從下拉清單中選擇一個尚未使用的磁碟機代號。若要設定磁碟機名稱，直接在文字方塊列中輸入名稱，並注意長度不能超過 32 位元。如果要在登錄時直接載入 Personal Secure Drive (PSD)，請勾選「登錄時載入我的 Personal Secure Drive」。完成後按「下一步」。



B-6-2. 設定 Personal Secure Drive 儲存空間大小與指定儲存 Personal Secure Drive 的實體磁碟機。

完成後按「下一步」。



Personal Secure Drive (PSD) 的儲存空間在設定以後不能變更，因此請確保指定的空間可以滿足您的需要。並注意因為檔案系統要分配一定空間，所以您不能使用最大的磁碟機大小。同時也請注意，最大的 PSD 磁碟機大小是有限制的：

FAT16 PSD 磁碟機最大為 2 GB。

FAT32 PSD 磁碟機最大為 4 GB。

B-7. 按「下一步」以繼續完成作業。



在完成所有設定作業前，請勿關閉電源、進入節能狀態或是拔除電源線。

B-8. 按下「完成」即完成 Infineon Security Platform 使用者初始化與功能設定。



C. Infineon Security Platform 設定工具

日後可以利用「Security Platform 設定工具」查詢 Security Platform 的各項資訊，也可以執行多種管理任務，包含變更使用者密碼、備份、匯入 / 匯出使用者金鑰和憑證…等。



4. 技嘉 Ultra TPM 設定與使用

技嘉獨特的 Ultra TPM 技術，除了支援業界最先進的硬體加密外，更能透過簡單的程式介面讓使用者將金鑰儲存及備份於 USB 隨身碟或 BIOS。經由 Ultra TPM 將金鑰儲存於 USB 隨身碟 / BIOS 後能同時刪除存放於電腦裡的金鑰，即可避免未經授權的使用者竊取資料，且使用者僅需透過 USB 隨身碟的插拔就能自動開啟或關閉 PSD 加密檔案，而無須再執行繁複的設定。另外，Ultra TPM 讓使用者可以輕易地備份 USB 隨身金鑰，以避免使用者因遺失金鑰而造成資料無法開啟。



- 與 TPM 相關的密碼及金鑰設定後，請務必小心存放並備份。如果遺失了金鑰或忘記密碼，原經由 TPM 加密的檔案將無法被破解或讀取。
- TPM 提供最新的資料保全功能，但無法保證資料的完整性及硬體的保護。因此若因硬體的損毀而導致加密檔案遺失，本公司並不承擔此責任。

4.1. Ultra TPM 使用說明

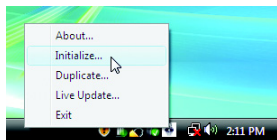
啟動 Ultra TPM 前，請確認已初始化 TPM 晶片，並已設定加密檔案(至少需設定 Personal Secure Drive (PSD)，如何設定請參考「3. TPM 晶片初始化設定」的說明)。

A. Initialize...

步驟一：

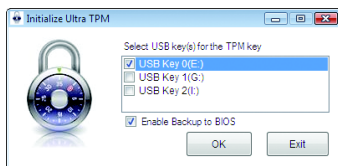
Ultra TPM 程式安裝完成後在常駐程式列會出現 Ultra TPM 的小圖示。

若要製作 USB 隨身金鑰，在此圖示按下右鍵選擇「Initialize...」。



步驟二：

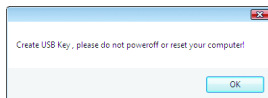
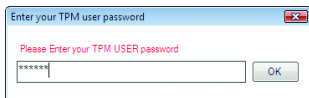
出現「Initialize Ultra TPM」的畫面後，請務必勾選一個 USB 隨身碟及勾選「Enable Backup to BIOS」，或是勾選兩個以上的 USB 隨身碟，按下「OK」。



若有兩位以上使用者選擇將金鑰備份至 BIOS 時，後者備份至 BIOS 的金鑰將會取代前一位使用者所備份的金鑰。

步驟三：

輸入在「Easy Mode」簡易設定模式或「Advanced Mode」進階設定模式所設定的使用者密碼，按下「OK」。



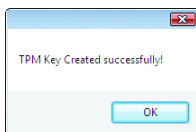
若輸入三次錯誤的密碼，Ultra TPM 將會被鎖住，此時請進入 BIOS 設定程式，選擇「Security Chip Configuration」將「Security Chip」設為「Enabled/Activate」，即可再輸入密碼。



在建立 USB 隨身金鑰時請勿關機或重新啟動電腦。

步驟四：

按下「OK」離開即完成 USB 隨身金鑰的設定，之後僅需經由 USB 隨身碟的插拔即可載入 / 卸載 Personal Secure Drive (PSD)。



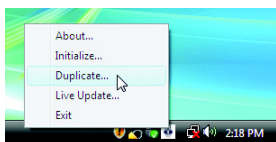
移除 USB 隨身金鑰時，「Infineon Security Platform 設定工具」會出現如下警語，此為正常狀況。

功能需要重新設定。
按一下此處以重新設定 Security Platform 功能。

B. Duplicate...

步驟一：

若要将 USB 隨身金鑰複製至另一 USB 隨身碟，在此圖示按下右鍵選擇「Duplicate...」。



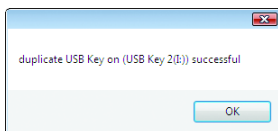
步驟二：

出現「Duplicate USB Key」的畫面後，先勾選原 USB 隨身金鑰的 USB 隨身碟代碼，再勾選欲存入的 USB 隨身碟代碼，按下「OK」。



步驟三：

按下「OK」離開即完成 USB 隨身金鑰的複製。



若要移除 Ultra TPM 程式時，請先將存有金鑰的 USB 隨身碟插入，再進行移除的動作。