Smart TPM

使用手册

Rev. 1001

建議您至技嘉網站下載最新版Smart TPM。
 若系統已安裝Ultra TPM,無需移除即可安裝Smart TPM,且原有設定皆會被保存。

目錄

PM晶片設定與使用流程	TPM晶片設
1. BIOS設定	1.
2. Infineon TPM驅動程式及Smart TPM程式安裝	2.
2.1. 安裝Infineon TPM驅動程式	
2.2. 安裝Smart TPM程式	
3. TPM晶片初始化設定	3.
3.1. 使用Smart TPM初始化TPM晶片	
3.2. Advanced Mode進階設定模式	
4. Smart TPM設定與使用18	4.
4.1. 設定USB隨身金鑰1	
4.2. 設定藍芽行動電話隨身金鑰1	
4.3. 設定藍芽功能2	
4.4. 其他功能2	

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Smart TPM程式安装
- 3. TPM晶片初始化設定
- 4. Smart 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:

開機後進入BIOS設定程式,選擇「Security Chip Configuration」會出現以下畫面,將「Security Chip」設為「Enabled/Activate」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(此選項需於BIOS設定程式的主畫面按<Ctrl>+ <F1>才會出現)。

清除TPM晶片內容後,原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。

CMOS Setup Utility-Copyright (C) 1984-2009 Award Software Security Chip Configuration				
Security Chip	[Enabled/Activate]	Item Help		
Clear Security Chip	[Enter]	Menu Level 🕨		
Security Chip State				
$\uparrow \downarrow \rightarrow \leftarrow$: Move Enter: Select	+/-/PU/PD: Value F10: Save ESC:	Exit F1: General Help		
F5: Previous Values	F6: Fail-Safe Defaults F7: C	Defaults		

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Smart TPM程式安裝

啟動Smart TPM功能前請先安裝Infineon TPM驅動程式及Smart TPM程式。

2.1. 安裝Infineon TPM驅動程式

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」安裝所有勾選的驅動程式,包含Infineon TPM驅動程式。

IGABYT		
	小姐姐 计就回路的一种	
品月組	文物解开推导期任為 連接為你的主應服安裝出下所列之解動現代 博點環 Xoress Install 本自動完造所有的原動展示	
AND ALL TA		
10 M	Xpress Install 軍點安裝	
應用程式		
all when the t	Xpress Install #####	
技術支援		
(112月)		
	Browser Configuration Utility	
PART IN BURN	「 数本:1.1.6.0 開始した 0.001/D	
W 46 28 XING	看其大小 Z Z3MB	
	This doiny optimizes the internet browser search experience based on your country and language.	
*****	✓ INF Update Utility	
	版本:9.1.0.1007	
	檔案大小:6.22MB	
Download	This utility installs INF files that inform the operating system how to properly configure the chipset for specific	
Center	functionality such as PCI-Express or USB interface.	- II.
(h)	Infineon TPM Driver	
ART	版本:2.00.0000	
	檔案大小:189.70MB	
	Infineon Trusted Platform Module Driver	1
	Realtek HD Audio Driver	
	版本:))P=5.10.0.5780-VISTA=6.0.1.5780	
	檔案大小:114.44MB	1
	Realtek High Definition Audio Driver	1 🗐

2.2. 安裝Smart TPM程式

點選左下角的新工具程式標籤,選擇「安裝新工具程式」頁面,在「Smart TPM」按下「安裝」,建進行安裝。

品月組 場動程式 軟體 度用程式	軟體應用程式交裝 認起臺安裝 深軟行所需要給應用程式 受裝該蓋工具程式 安裝施加工具程式 安裝施加工具程式
技術支援 (説明)	Smart 6 家式であります。 GCABYTE Smart 6 Program
A統資訊 Download Center	Opmanic Concry Save 2 \$
	Smart TP丛 Smart TPM 第二次小71.04/8 TPM TPM TPM TPM TPM Cuck installaton version provides a user-friendly interface allowing users to generate TPM keys more quickly and easily.

有些主機板驅動程式光碟片的Smart TPM程式是包含在「Xpress Install」中,按下「Xpress Install完整 整安裝」即可安裝Infineon TPM驅動程式及Smart TPM程式。

3. TPM晶片初始化設定

完成BIOS設定及驅動程式的安裝並重新啟動系統後,在通知區域會出現Infineon Security Platform的圖示圖(此圖示顯示Infineon Security Platform尚未初始化),可雙擊此圖示或在Smart TPM 圖示●按下右鍵選擇「Initialization Wizard」,以啟動Smart TPM。

您可以在Smart TPM進行TPM晶片初始化、密碼設定、Personal Secure Drive (PSD)設定以及製 作隨身金鑰(請參考3.1章節的說明),或是選擇「Advanced mode」(請參考3.2章節的說明)進入 「Infineon Security Platform初始化精靈」,進行Infineon所提供的各項進階設定。

3.1. 使用Smart TPM初始化TPM晶片

Smart TPM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、密碼設定及Personal Secure Drive (PSD)的設定。



- Smart TPM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。
 - Smart TPM僅提供「檔案和資料夾加密 Personal Secure Drive (PSD)」設定,若要執行「安全電子 郵件」或是「檔案和資料夾加密 · 加密檔案系統(EFS)」加密,請點選「Advanced mode」進入 Infineon Security Platform的設定工具。

3.1.1. Smart TPM使用介面介绍

Initialization Wizard	
Smart	ТРМ
This wizard assists you with Security Platform features	th your Security Platform initialization and configuration.
Set Your TPM Password	
Auto Generated Password	bgymmexh Generate
User Defined Password	•••••
Confirm User Password	•••••
The default minim m length of t	he nereword is 5 characters
Z • My PSD will be saved on drive	Personal Secure Drive Storage space of my PSD:
C -	200 🔆 MB
Create Your Smart TPM Key	
Use USB storage	Use Bluetooth Device
Refresh	Refresh
USB Key 0(F:)	BT Key 0(USERS-U952039-N) 🔺
USB Key 1(G:)	BT Key 1(TPE-U944093-NB) BT Key 2(W550i) BT Key 3(TPE-U93C022)
Enable Backup to BIOS	
Ad	Ivanced mode OK Exit

● Set Your TPM Password (設定密碼)

Smart TPM會自動提供一組密碼,或是自行設定。請 務必記住此組密碼,以進行藍芽行動電話/USB隨身金 鑰的製作。

- Set up your Personal Secure Drive(PSD) (設定PSD) 在此設定Personal Secure Drive (PSD),包括此虛擬磁碟 機的代號、名稱、實際儲存的磁碟機以及分配給PSD 的磁碟機空間。
- Create Your Smart TPM Key (製作Smart TPM金鑰) 在此可以製作藍芽行動電話或USB隨身碟的TPM金 鑰,透過藍芽行動電話的連結或USB隨身碟的插拔就 能自動開啟或關閉PSD加密檔案。

3.1.2. Smart TPM初始化使用步骤

步驟一: Set Your TPM Password (設定密碼)

Auto Generated Password	bgymmexh	Generate
User Defined Password	•••••	
Confirm User Password		

1. 自動密碼(Auto Generated Password):

開啟Smart TPM後即立刻產生一組密碼,也可以按下「Generate」重新產生密碼。

2. 自行定義密碼/確認密碼(User Defined Password/Confirm User Password):

在「User Defined Password」輸入自行設定的密碼(密碼長度限制為16個字元),並在「Confirm User Password」再輸入一次以確認密碼。



▲• 建議您在BIOS設定程式設定「User Password」,以避免其他使用者清除TPM晶片的設定。

◆● 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: Set up your Personal Secure Drive(PSD) (設定PSD)

My PSD will be mapped to drive:	Drive label for my PSD:
Ζ -	Personal Secure Drive
My PSD will be saved on drive:	Storage space of my PSD: 200 MR

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「Mv 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。

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 1 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。

步驟三: Create Your Smart TPM Kev (製作Smart TPM金鑰)

Use USB storage	Use Bluetooth Device
Refresh	Refresh
USB Key 0(F:) USB Key 1(G:)	BT Key 0(USERS-U952039-N) BT Key 1(TPE-U944093-NB) BT Key 200550)
	BT Key 3(TPE-U93C022)

1. 製作USB隨身金鑰:

勾選「Use USB storage」後按下「Refresh」搜尋連接的USB隨身碟,選擇欲製作為Smart TPM金鑰的USB隨身碟即可(可同時勾選多個USB隨身碟)。勾選「Enable Backup to BIOS」能 將已加密的密碼儲存至系統BIOS內。



若有兩位以上使用者選擇將已加密的密碼儲存至BIOS時,後者的密碼將取代前一位使用者所儲 ▲ 存的密碼。

2. 製作藍芽行動電話隨身金鑰:



◎ 勾選「Use Bluetooth Device」後按下「Refresh」搜尋已 開啟藍芽功能的行動電話,選擇欲製作為Smart TPM金 鑰的行動電話後會出現如左圖,在「密碼金鑰」輸入 一組用來與行動電話配對用的密碼(密碼長度建議使 用8~16個字元),接著在行動電話上輸入相同的密碼以 進行配對。

要進行藍芽行動電話隨身金鑰製作前,請確認您的主機板已具備藍芽接收器,且行動電話的藍芽及搜尋功能已開啟。

完成上述步驟後,按下「OK」即開始進行TPM晶片的初使化、密碼設定、Personal Secure Drive (PSD)設定及TPM隨身金鑰的製作。

3.2. Advanced Mode進階設定模式

在「Smart TPM」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」後會出現「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)。此設定精靈提供詳畫的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」,以設定擁有者密碼。



密碼設定說明:

- 請在「密碼」欄鍵入自行設定的擁 有者密碼,或按「隨機」自動產生 密碼。
- 在「確認密碼」欄再次輸入密碼以 進行確認(使用隨機密碼則無需進行 此項操作)。
- 使用隨機密碼,請務必取消「隱藏 鍵入」,並列印或儲存隨機密碼。

which a to be a showing		
建立 Security Platform 班月石 提供 Security Platform 所有者密報	5	8- <mark>0-8-8-8-8-</mark> 8-
Security Platform 必須先進行初始化, 將成為此 Security Platform 的所有者。 注:您應點住 Security Platform 所有者。 理 Security Platform 任務。您可以稍能	然後使用者才可使用 Security Platf 。對 Security Platform 所有者功能的 首密碼或保存到檔案。如果忘記此 後變更此密碼。	om 功能。完成此諸靈後,2 存取受所有者容碼保護。 密碼,您將無法執行重要的智
密碼 (2): ●●●●●●●		随機(<u>R</u>)
審認容碼():		随機® 至文件(1)
· · · · · · · · · · · · · · · · · · ·		簡據 (E) 至文件(D) 列印(P)
 密碼②: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●		簡機(R) 至文件(D) 列印(P)
 密碼(2): ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●		路總金) 至文件① 列印①

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」。

👺 Infineon Security Platform 初始化精靈	×
情份 設定自動備份	
自動排程備份將儲存 Security Platform 的認識及設定到「情份檔案」中	1.
(詹份位置(A):	
C.\Users\GIGABYTE\Documents\SecurityPlatform\SPSystemBackup.xml	瀏覽(W)
根據預證,僅份將排程為每天晚上12點自動執行。 按一下「排程」以做視及修改備份排程。	排程(6)
您在完成此糖靈後可立即進行備份。	
<上一步(B) (下一步(N) >) (取消 說明

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。

Infineon Security Platform 初始	化精靈	
緊急復原 設定緊急復原權杖	-	
緊急復原需要復原權杖。此權	支使用専用密碼保護。	
● 建立新復原權杖(C) ○ 使用現有復原權杖(U)		
檔案位置(F):	C:Wsers/GIGABYTE/Documents/Security Ple	㎝ 瀏覽(₩)
建議:在保證安全的で 杖。	可移動媒體上(例如 USB 快閃記憶體磁碟機)保存緊急恢復權
勒 入權杖密碼(6256 字元)	•	
密碼(P):	•••••	
確認密碼(O):	00000	
☑ 臆識違入(H)		
	《上一步图》下一步图》>	V:16 19:88

A-6. 建立一個「密碼重設權仗」,並輸入一組權仗密碼。

蹸 Infineon Security Platform 初始化	請靈	×
密碼重設 設定密碼重設權杖	-	
重設使用者密碼需要密碼重設權	杖。此權杖使用專用密碼保護。	
 ● 建立新權杖(C) ● 使用現有權杖(U) 		
檔案位置(A):	C:Wsers/GIGABYTE/Documents/Security Plat	瀏覽(₩)
 連議:在保證安全的可 杖。 	移動媒體上(例如 USB 快問記憶體磁碟機)	保存密碼重置權
朝八権快省時(0230 子元)。		
密碼(P):	•••••	
確認密碼(O):	•••••]
☑ 聽載違入(H)		
	<上─步(B) 下─步(N) > 取	M NO

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。



A 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」)

🖉 Infineon Security Platform	1初始化精盛
	成功完成精整•
Cinfineon	擒要: 日建立 Security Flatform 殘有者。 Security Flatform 初始伯己元成。 Security Flatform 初始伯己元成。 Wandow House 版上不提供) 的「魚階設置」配置。 一個竹(伝統我必須厚) - 希臘其代。 Security Flatform
TPM	加重要自己用此 Security Flatform 功能 ・ 部可以統動 Security Flatform 使用者初始に描蓋。 I 記動 Security Flatform 使用者初始化結查(C) I 現在目動執行信(G)(R)
	(<上一步(B) 完成 取消 說明

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 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」。

🜉 Infineon Security Platform	使用者初始化精靈	×
	教迎使用 Infineon Security Platform 使用者初始化 積量	
Infineon	計算圖將幫助您為當前使用者進行 Security Flatform 初始任和功能 配置。	
e) Marson TPM	要繼續,諸徐一下「下一步」。	
	<上一步(B) 下一步(N) ▶ 取消 說明	9

B-2. 設定使用者密碼,並按「下一步」。

基本使用者密碼 設定密碼	174 TE 199 200	••••••	
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):			
•••••			
使用不同密碼用於不同目的。 長度:6256 個字元.			
☑ 聽載違入(H)			

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」。

Not the security Platform 使用者初始化精盛	
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	••••••
図 設用在緊急(情況下重設我的基本使用者密碼(E)。 準備將個人秘密導入檔案。 指定路徑和檔案名。	
個人秘密位置(P): C:WsertW3[GABY TEDocuments'Security Platform'SPPwdRes	setSecret.xonl
諸總比屬當儲存在安全位置。如果您必須在 · 您將需要已。	E號急情況下重設基本使用者密碼
《上一步(B) 下一	步(N)

B-4. 按「下一步」以繼續完成初始化作業。



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-5. 選擇所要設定的加密功能,並按「下一步」。

Infineon Security Platform 使用者初始化储量 Security Platform 功能 進择 Security Platform 功能		
請選擇要設定的 Security Platform 功能並按一下「下一步」#	ŝi责 ◆	
有關 Security Platform 功能的詳細資訊,請按一下「說明」。	•	
Security Platform Inf (S):		
		_
功能	狀態	
功能 ▼ (安全電子郵件	狀態 不可檢測	
功能 ダ 安全電子動件 ダ 福奈和資料夾加密 - 加密福奈糸紙 (EPS)	狀態 不可檢測 未設定	
功能 ② 安全電子郵件 ② 檔案印資料及加密 - 加密檔案系統 (EFS) ② 檔案印資料及加密 - Perconal Secure Drive (FSD)	狀態 不可検測 未設定 未設定	
カ焼 愛 (変変量) - 2000 ((1000) ((100)) ((1000) ((100)) ((100)) ((100)) ((100))	狀態 不可検測 未設定 未設定	
功能 図 (安全電子郵件 図 (安全電子郵件 図 編集和資料天加密 - 加密編案条紙 (ERS) 図 編集和資料天加密 - Fenoral Secure Drive (FSD)	狀態 不可検測 未設定 未設定	
功能 ② 医全電子動件 図 振電和算得天加密 - 加密傷案系統 (GES) 図 傷案和資料天加密 - Percoal Secure Drive (FSD)	款器 不可検測 未設定 未設定	
功能 型 (安全電子動件 型 (安全電子動件 型 (電楽和2算相天加密・加密確案系統 (GER)) 型 福楽和2算相天加密・Personal Secure Drive (FSD)	狀態 不可檢測 未設定 未設定	
が施 型 (安主電子朝叶 型 (安主電子朝叶 型 儒素和近葉科夫加密 - Jaca権素糸銃 (BFS) ■ 儒素和近葉科夫加密 - Feronal Secure Drive (FSD)	欺傷 不可権測 未設定 未設定	

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。

檔案和資料夾加密 - 加密檔案系統(EFS)

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。

檔案和資料夾加密 - Personal Secure Drive (PSD)

Personal Secure Drive (PSD)顧示與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. 在此以建立「檔案和資料夾加密 - Personal Secure Drive (PSD)」為例: 此頁提供「加密憑證」的設定,如果沒有任何可用的憑證,則此精靈將建立一個新憑證,然後自 動選擇該憑證。您可以按「下一步」由精靈自動建立或按「變更」手動建立憑證。

🐺 Infineon Security Platf	orm 使用者初始化精盛
Security Platform 功能 加密憑證	• • • • • • • • • • • • • • • • • • •
Infineon Security Platform 料夾加密。	可以透過提供對用於加密和解密資料的金鑰的額外保護,來增強檔案和資
有關 Infineon Security Plat	form 檔案和資料夾加密增強措施的更多資訊,請按一下「說明」。
當前憑證:	沒 有註冊憑證。
新憑證:	積靈將自動建立並註冊。
變更(C) 新憑證的密論長度(K): 1024 位 ▼	手動選擇其他現用憑證,或者創建新憑證供使用。
	<上一步(B)〕(下一步(N)>) 取消 説明

新憑證的密鑰長度: 可在此處選擇新建立的加密憑證的密 鑰長度,選項有1024位元及2048位元。

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」。

	簽發者	到期日	預定目的	Cryptographic Provider
SIGABYTE	GIGABYTE	2019/6/26	加密檔案系統	Infineon TPM Cryptogra
檢視(V)	匯入()	建立	(C) 申請(R)	
私人金鑰				
	rovider :			
- years and a				
金鏑大小:		TPM 産生	E的金鋼;	

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」。

🕎 Infineon Security Platform 使用者初始化精器	×
Security Platform 功能 設定 Personal Secure Drive	
您的 Personal Secure Drive (PSD) 為敏感資料提供保護 磁片,其他使用者看不見。網現有檔案和資料灭移3	性儲存。它看起來像是電腦上的其他 JPSD 以對其進行保護。
在建立此磁碟機之後,您將無法變更 PSD 的儲存空间	₩] +
我的 Personal Secure Drive 的磁碟機代號(D):	
P: ▼ 必須在所有目標平台上可用	
我的 Personal Secure Drive 的磁碟機代號(P):	
Personal Secure Drive	
☑ 登錄時載入我的 Personal Secure Drive(L)	
☑ 建立桌面快捷方式(C)	
<上一步(B) (下一步(N) 》 取消 說明

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」。

說定 Personal Secure Drive 我的 Personal Secure Drive	將具 📶 🗼 儲存	空間 MB(M) *	
選擇應保存 PSD 映射檔案	約磁碟機(P):		
卷	檔案系統	可用空間	最大 PSD 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。 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。

Infineon Security Platfor	m 設定工具
資訊 使用者設定 備低	8 移植 密碼重読
Copyright (c) Infineon Technologies AG	nfineon
教迎使用	Infineon Security Platform 解決方案
Security Platform 解決方案	:
版本:	3.5.1
操作模式:	獨立
Security Platform 狀態:	
晶片:	歐用
摘有者:	已初始化
使用者:	已初始化
Trusted Platform Module :	
供應商:	Infinenn Technologies AG
版本:	1.2
	自測(\$) 更多內容(D)
	RAM RAM

4. Smart TPM設定與使用

技嘉獨特的Smart 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 讓使用者僅需透過藍芽行動電話的連結或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,Smart TPM讓使用者可以輕易地製作多份藍芽行動電 話/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。



4.1. 設定USB隨身金鑰

步驟一:

完成TPM晶片初始化、密碼設定及Personal Secure Drive (PSD)的設定後,再至通知區域內的 Smart TPM圖示圖按下右鍵,即可出現下圖。



步驟二:

點選「Configure Smart TPM Devices」開啟Smart TPM設定程式。若要製作USB隨身金鑰請選擇「Configure USB Storages」,勾選欲製作為隨身金鑰的USB隨身碟(若有未列出的USB隨身碟,請按「Refresh」讓Smart TPM重新掃描)。



勾選「Enable Backup to BIOS」能將已加密的密碼儲存至系統BIOS內。若有雨位以上使用者選擇將 已加密的密碼儲存至BIOS時,後者的密碼將取代前一位使用者所儲存的密碼。 步驟三:

輸入先前設定的使用者密碼,按下「OK」即可完成USB隨身金鑰的製作,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:

若要移除USB隨身金鑰,只需在「Configure USB Storages」取消勾選已是USB隨身金鑰的USB 隨身碟,在確認對話框中按「是」,即可移除此USB隨身金鑰的功能。



4.2. 設定藍芽行動電話隨身金鑰

步驟一:

若要製作藍芽行動電話隨身金鑰,請選擇「Configure BT Devices」再勾選欲製作為隨身金鑰 的藍芽行動電話(若有未列出的藍芽行動電話,請按「Refresh」讓Smart TPM重新掃描)。





要進行藍芽行動電話隨身金鑰製作前,請確認您的主機板已具備藍芽接收器,且行動電話的藍 芽及搜尋功能已開啟。 步驟二:

當「新增Bluetooth裝置精靈」出現時,請輸入一組用來與行動電話配對用的密碼(密碼長度 建議使用8~16個字元)。

新増 Bluetooth 装置構整	×
輸入 Bluetooth 裝置的密碼金論。	*
🖲 W550i	
使用和您在裝置上輸入的相同密碼金鑰。	
密碼金鑰(P): 12345678	
包度以本後期間空活金資金,將非常的後提不全接受損益。 約16個數子具的包碼金換,包括金貨總是和成金。	
<上一步(B) 下一步(N) > 版	Ħ

步驟三:

接著在行動電話上輸入相同的密碼以進行配對,當輸入密碼確認正確再按下「完成」後, 即完成藍芽行動電話隨身金鑰的製作。之後只要啟動或關閉行動電話的藍芽功能,或當藍 芽行動電話靠近/離開電腦時,即可載入/卸載Personal Secure Drive (PSD)。



移除藍芽行動電話隨身金鑰:

若要移除藍芽行動電話隨身金鑰,只需在「Configure BT Devices」取消勾選已是藍芽行動電 話隨身金鑰的行動電話,在確認對話框中按「是」,即可移除此藍芽行動電話隨身金鑰的 功能。

Remove Keys 🛛 🕅
Do you want remove BT Key 3(W550i:Used)
是(Y) 香(L)

在「Other Settings」頁面可以設定藍芽裝置掃描的時間及次數,以確認藍芽行動電話隨身金 鑰是否在電腦的搜尋範圍內。

• Device Scan Time (sec.) :

設定藍芽裝置掃描的時間,時間以每5秒為單位,調整幅度為5秒至30秒。Smart TPM會以 此設定的時間來掃描藍芽行動電話隨身金鑰是否存在。

• Rescan Times :

設定藍芽裝置掃描的次數,調整幅度為1次至10次。當未搜尋到藍芽行動電話隨身金鑰時,Smart TPM會以此設定持續掃描,若到達設定的次數仍未搜尋到藍芽行動電話隨身金 鑰時,Smart TPM將會關閉TPM功能。



4.4. 其他功能

A. 手動登入/登出TPM晶片功能

當隨身金鑰不在時仍可以密碼來啟動TPM晶片功能。在通知區域內的Smart TPM圖示查按下 右鍵會出現下圖,選擇「Manual Login」,輸入使用者密碼即可啟動TPM晶片功能。



要卸載TPM晶片功能時,只需選擇「Manual Logout」即可。



B. 查看密碼


