

型式：MED-IDE-64-CX

# 管理式加密裝置 使用手冊

11/2007 3.01 版

# HTDLINK

Technology Co., Ltd.

Website : <http://www.htdlink.com>

Tel : +886-3-499-4533

## 目 錄

頁次

1.	概 述 .....	1
1.1	簡介 .....	1-2
1.2	特色及規格 .....	2-3
1.3	系統需求 .....	3
1.4	包裝清單 .....	3
2.	MED 組合及安裝 .....	4
2.1	組合 .....	4
2.2	安裝 .....	4-6
3.	加密作業程序 .....	7
3.1	作業系統硬碟加密 .....	7-9
3.2	資料硬碟加密 .....	10-12
4.	選單項目功能說明 .....	13
4.1	Master & Supervisor 密鑰功能 .....	13-15
4.2	User 密鑰功能 .....	15
5.	故障排除要訣 .....	16
6.	其 他 .....	17
6.1	RS-232 傳輸設定 .....	17
6.2	產品保固期 .....	18
7.	附 錄 .....	
A	快速安裝 .....	A-1-A-2
B	問答集 Q&A .....	B-1-B-3

型式：MED- IDE -64-CX

管理式加密裝置

## 使用手冊

### 1. 概述

#### 1.1 簡介

保護硬碟資料內容不被竊取之加密及管理的裝置。工程設計成具有強大的「硬碟加密」能力以及人性化操作界面的「階層式管理」能力。是一種先進的加密技術科技產品，符合美國 Data Encryption Standard (DES)及Advanced Encryption Standard (AES)標準。可以製作成經過加密的作業系統(OS disk)或者是經過加密的資料儲存硬碟(Data disk)。100%適合各作業系統含有IDE介面之電腦。安裝容易，操作簡便，不需要其他額外的軟體支援，非常適合大型企業、政府機關團體、研發、金融機構、軍事單位等等重視「資訊安全保密及管理」單位使用。

#### 1.2 特色及規格

##### 1.2.1 特色

- ◆ 符合美國國家標準與技術局(NIST)及計算機科學工程協會(CSE)認定的硬體 DES/TDES 加密工程，執行效能提升，遠超乎傳統的軟體加密工程。
- ◆ 提供完整、健全的硬體保全架構，實際保護您的“資料安全”。
- ◆ 完全的獨立系統平台作業，不需依賴任何的軟體支援。

#### 1.2 特色及規格

##### 1.2.1 特色(續)

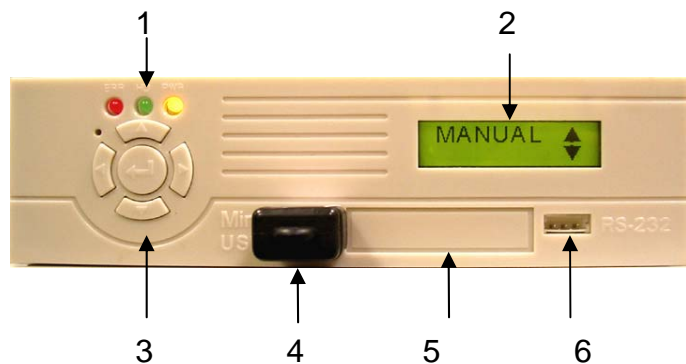
- ◆ 進行即時資料加解密傳輸處理工作，1.1Gbit/sec 的加密傳輸速度符合Ultra ATA mode 6 (133MB/sec) 介面模式。
- ◆ 適用所有的作業系統，主機板有標準PCI南橋晶片的IDE介面。
- ◆ 硬體即時加密速度快，獨立晶片運算不會降低CPU與系統本身效能。
- ◆ 完全可以逕行製作使用者密鑰 (USER E-KEY)，不需透過原廠或者代理商，節省時間及成本，資料可以有更進一步的安全保障，避免資料遺失的風險。
- ◆ 所有登入使用者身份資料將被記錄在加密裝置中，可以藉由RS-232 導線連接，列印及製檔管理。

##### 1.2.2 規格

- (1) 尺寸：L 14.8 x H 4.2 x D 2 0 cm.
- (2) 淨重：280 克
- (3) 電源：
  - 操作電壓：+5v，+12v 來自 PC 電源.
  - 電力消耗：0.80 W, 160 mA. (Max.)
- (4) 通過 CE & FCC 認證標準。

## 1.2 特色及規格(續)

### 1.2.3 位置說明



- |            |              |
|------------|--------------|
| 1. LED 指示燈 | 4. 電子密鑰      |
| 2. LCD 顯示幕 | 5. 商標標示牌     |
| 3. 按鍵操作開關  | 6. RS-232 出口 |

### 1.3 系統需求

1. 所有的作業系統 (OS)。
2. 適用的 ATA-6 介面。
3. 主機板有標準PCI南橋晶片的IDE介面。

### 1.4 包裝清單

購買管理式加密裝置(MED)時應包含下列基本配備：

- |                                |    |
|--------------------------------|----|
| 1. 加密主機盒 (encryption main box) | 1組 |
| 2. 電子密鑰 (Master E-Key)         | 1支 |
| 3. 電子密鑰 (User E-Key)           | 1支 |
| 4. 使用手冊 (User Manual)          | 1本 |
| 5. 電子密鑰(Supervisor E-Key)      | 選購 |
| 6. RS-232導線                    | 選購 |

## 2. MED 組裝及安裝

### 2.1 組裝

#### 注意

確認所需加密的硬碟 (Slave/Master) 及加密主機盒跨接器 (jumper) 已配合完成正確的設定。

依照下列作業程序進行組裝

1. 取得一個容量不拘具有 IDE 介面的硬碟，完成基本設定。
2. 連接主機盒內 IDE 短的排線至硬碟上。
3. 連接主機盒內電源插頭至硬碟上。
4. 將硬碟平放置入主機盒固定座上，以附屬四顆螺絲將硬碟固定。
5. 確認所有的連接線沒有鬆脫的現象並且在正確的位置上。

### 2.2 安裝

#### 警告

**※※ 請先備份好您硬碟中已有存在的資料 ※※**

假在您安裝本管理式加密裝置之前，如在執行硬碟加密作業程序時，您沒有做好備份動作，因此導致資料遺失，本公司將不會有任何的責任為您做任何資料的恢復。

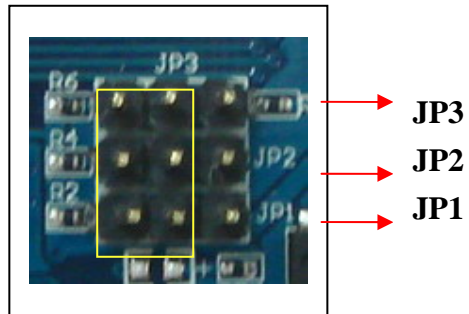
#### 附註

本加密裝置在出廠前均設定為資料硬碟之加密模式，若您需要變更為作業系統硬碟加密模式時，請參照下列模式設定。

## 2.2 安裝(續)

基本加密模式(data disk )型態 jumper 之設定。

JP1: 加密 / 未加密。 JP2: Slave / Master。 JP3: 133 / 100 MHz。



### 注意

因基於設計工程需要，連接電源的插座已經改變方向。在管理式加密裝置中將電源連接插座旋轉 180 度。雖然有防呆裝置，但使用時仍請要特別格外謹慎、小心。

依照下列作業程序進行安裝

1. 將加密主機盒 (encryption main box) 直接推入到桌上型電腦機架 (frame) 內，以四顆螺絲將其鎖定在機架上。
2. 連接電腦內 IDE 排線至主機盒背板之 IDE 連接頭上，確認 IDE 排線已正確插入到位置上。
3. 連接電腦內電源供應器連接頭 (5V, 12V) 至主機盒背板之電源連接頭上，確認電源線插頭已正確連接到位置上。

## 2.2 組裝(續)

4. 詳細快速的安裝作業程序可以參考本手冊—附錄 A 管理式加密硬碟之安裝。

### 3. 加密作業程序

#### 3.1 作業系統硬碟加密

##### 警告

**※※ 請先備份好您硬碟中已有存在的資料 ※※**

假在您安裝本管理式加密裝置之前，如在執行硬碟加密作業程序時，您沒有做好備份動作，因此導致資料遺失，本公司將不會有任何的責任為您做任何資料的恢復。

##### 注意

#### 1. 密碼變更

您在作業格式化 (Format) 硬碟之前一定要做到。這樣您的電腦資料將會受到更完整的保護。因為管理式加密硬碟裝置在出廠前僅設定為基本內建值。

#### 2. 熟記您的密碼

未來售後服務時之用。若你有需要售後服務時，若您忘記密碼，我們亦無法為您實施解密進入電腦系統運作，您的資料可能會因硬碟重新製作而導致資料遺失。

#### 3. 不要隨意變更密碼

每經一次密碼變更就必須重新對硬碟做格式化，以確保資料的安全性。經常變更密碼可能造成您資料的遺失，我們不建議您這麼做。

#### 3.1 作業系統硬碟加密(續)

##### 附記

在您安裝本裝置之前，請在重新檢查您的基本設定。MED 與 HDD 必須與您的需求相同，加密的作業系統 (OS) 必須設定在「MASTER」的位置。

依照下列作業程序進行作業系統硬碟加密

1. 將電子密鑰 (Master E-Key) 插入至主機盒 mini USB 插座內。
2. 開啟電腦電源，忽略電腦螢幕所產生之訊息。
3. 在主機盒之 LCD 上會出現自動辨認電子密鑰” MASTER OK” 字樣後自動返回” MENU ” 選單。
4. 選擇「CHANGE PASSWORD」項目，進行【名稱&密碼設定】；並請務必牢記您的密碼。
  - (1) 在主機盒面板上之選擇控制鍵，按上(▲)或下鍵(▼)選取選單，直到 LCD 上顯示出” CHANGE PASSWORD” 字樣出現，數字為 1~9，字元為 A~Z，特殊符號” 空白及下標橫線”。內建值(default) 為 NAME：00000000，PASSWORD：00000000。
  - (2) NAME 設定：按右鍵→選取，左鍵←刪除，完成設定後按中間 Enter 鍵(●)後自動跳至 PASSWORD。
  - (3) PASSWORD 設定：按右鍵→選取，左鍵←刪除，完成設定後按中間 Enter 鍵(●)自動跳至自動返回至” MENU” 選單。

### 3.1 作業系統硬碟加密(續)

5. 關閉電腦電源 (shutdown power)，非由Ctrl-Alt-Del 熱鍵控制。
6. 重新開啟電源，確認電子密鑰 (Master E-Key) 仍保留在主機盒 mini USB 插座內，否則將電腦將無法搜尋到作業系統的加密硬碟。
7. 依照電腦作業指示，正常格式化、分割以及完成作業系統之安裝。
8. 重新開啟動電源，您的作業系統即成為有經過加密的作業系統。

### 3.2 資料硬碟加密

#### 警告

**※ 請先備份好您硬碟中已有存在的資料 ※**

假在您安裝本管理式加密裝置之前，如在執行硬碟加密作業程序時，您沒有做好備份動作，因此導致資料遺失，本公司將不會有任何的責任為您做任何資料的恢復。

#### 注意

##### 1. 密碼變更

您在作業格式化 (Format) 硬碟之前一定要做到。這樣您的電腦資料將會受到更完整的保護。因為管理式加密硬碟裝置在出廠前僅設定為基本內建值。

##### 2. 熟記您的密碼

未來售後服務時之用。若你需要售後服務時，若您忘記密碼，我們亦無法為您實施解密進入電腦系統運作，您的資料可能會因硬碟重新製作而導致資料遺失。

##### 3. 不要隨意變更密碼

每經一次密碼變更就必須重新對硬碟做格式化，以確保資料的安全性。經常變更密碼可能造成您資料的遺失，我們不建議您這麼做。

依照下列作業程序進行作業系統硬碟加密

1. 將電子密鑰 (Master E-Key) 插入至主機盒 mini USB 插座內。
2. 開啟電腦電源，忽略電腦螢幕所產生之訊息。

### 3.2 資料硬碟加密(續)

3. 在主機盒之 LCD 上會出現自動辨認電子密鑰” MASTER OK” 字樣後自動返回” MENU ” 選單。
4. 選擇「CHANGE PASSWORD」項目，進行【名稱&密碼設定】；並請務必牢記您的密碼。
  - (1) 在主機盒面板上之選擇控制鍵，按上(▲)或下鍵(▼)選取選單，直到 LCD 上顯示出” CHANGE PASSWORD” 字樣出現，數字為 1~9，字元為 A~Z，特殊符號” 空白及下標橫線”。內建值 (default) 為 NAME：00000000，PASSWORD：00000000。
  - (2) NAME 設定：按右鍵→選取，左鍵←刪除，完成設定後按中間 Enter 鍵(●)後自動跳至 PASSWORD。
  - (3) PASSWORD 設定：按右鍵→選取，左鍵←刪除，完成設定後按中間 Enter 鍵(●)自動跳至自動返回至” MENU” 選單。
5. 關閉電腦電源，非由 Ctrl-Alt-Del 鍵控制。
6. 開啟電腦作業系統 (以 Windows xp 為例)
  - (1) 開啟控制台
  - (2) 系統管理工具
  - (3) 電腦管理
  - (4) 磁碟管理
  - (5) 發現一個位配置硬碟 unallocated disk
  - (6) 點選按右鍵後，利用作業系統將資料硬碟格式化 (format) 即可。
7. 關閉電腦電源，非由 Ctrl-Alt-Del 鍵控制。

### 3.2 資料硬碟加密(續)

8. 重新開啟電源，插入電子密鑰 (Master E-Key) 至主機盒 mini USB 插座內，否則將電腦將無法搜尋到資料硬碟。
9. 作業系統重新啟動後亦即自動完成資料硬碟之加密。

## 4. 選單項目功能說明

### 4.1 Master & Supervisor 電子密鑰選單功能

管理者(Master & Supervisor)電子密鑰選單功能說明如下

#### 1. READ LOG (讀取登錄使用資料)

在 LCD 上會逐一顯示使用者登錄之身份及時間。

#### 2. PRINT LOG (列印登錄使用資料)

藉由 RS-232 連線 (選購) 列印出使用者登錄之身份及時間，製成報表，方便管理。

#### 3. CLEAR LOG (清除登錄使用資料)

僅提供給予電子密鑰 Supervisor E-Key 功能 (選購)。

#### 4. USER KEY MAKER (USER KEY 製作)

基本配製作 10 支，餘可選購。

#### 5. E-DISK\_ID CHANGE (加密碟名稱變更)

可隨時變更您喜歡的加密硬碟身份識別名稱，內建值為 EDISK001。

#### 6. E-DISK LOCK (加密硬碟使用者封鎖)

可選擇封鎖個別使用者 (USER) 或所有使用者 (ALL USER)。

#### 7. CHANGE PASSWORD (密碼變更)

提供初次密碼設定，作為辨識認證重要參數；不建議經常變更密碼，否則每次變更密碼後，系統或資料硬碟將必須重新實施格式化 (format)，我們並不建議您經常變更，基本上它是非常安全的。

### 4.1 Master & Supervisor 電子密鑰選單功能(續)

#### 8. TIME SETTING (時間設定)

提供年/月/日/星期/時/分/秒之基本時間設定。

#### 9. SUPERKEY MAKER (超級密鑰製作)

可管理 11 ~ 445 部電腦；由每部電腦主機 Master key 功能提供製作而成。(選購)

#### 10. SUPER\_KEY DELETE.

刪除本機內 SUPER\_KEY 之功能。

#### 11. E-DISK UNLOCK (加密碟使用者解鎖)

可選擇恢復個別使用者 (USER) 或所有使用者 (ALL USER) 使用本基之功能。

#### 12. MASTE KEY REBUILD (MASTE KEY 密鑰重建)

獲得新管理者密鑰 (MASTER KEY)，輸入原設定之名稱及密碼，依照 LCD 顯示操作，選擇本項功能，直到出現 "PLUG NEW KEY"，按下中間鍵，管理者密鑰即可重建，原先舊有之 MASTER KEY 將自動失效作廢。

#### 13. SUPER\_KEY REBUILD. (SUPER\_KEY 密鑰重建)

獲得新管理者超級密鑰 (SUPER\_KEY KEY) 時，經由各主機操作，恢復 SUPER\_KEY 功能。原先舊有之 SUPER\_KEY 將自動失效作廢。

#### 14. DISPLAY ID\_NUM (加密主機序號顯示)

當 MASTER KEY 不存在，輸入原設定之 NAME&PASSWORD，可讀出本機序號，作為後續服務使用。

#### 4.1 **Master & Supervisor 電子密鑰選單功能**(續)

##### **15. AUTO PROTECT (自動保護)**

加密硬碟自動保護裝置；當您臨時短暫離開電腦時，此功能可協助您做好資料保全，若有人侵入操作使用，則作業系統將造成當機現象，內建值為OFF。

#### 4.2 **User 電子密鑰選單功能**

並沒有提供任何功能選單給使用者(USER)，僅允許一般使用者登入及啟動電腦進行作業。

#### 5. 故障排除與要訣

請參考以下說明協助您對於管理式加密裝置(MED)基本問題的排解。若以下說明仍無法為您解決問題，請洽購買的店家或經銷商來協助，或至本公司網站上的服務專區填寫您的問題，我們將盡快為您回覆。

- 檢查硬碟與 MED 的跨接器(jumper)設定是否與您的作業系統需求相同。
- 確定所有的 IDE 匯流排線均正確、固定在位置上。
- 確定所有的電源均正確、固定在位置上。
- 確定您所使用的是正確的電子密鑰並且良好的插入 mini-usb 插孔中。
- 重新開啟電源。

相關更進一步的協助，請參考本公司的網站 website:  
<http://www.htdlink.com>

## 6. 其他

### 6.1 RS-232 傳輸設定

1. 使用電腦所提供的超級終端機 (HyperTerminal)，選擇設定通訊埠。



2. 連接 RS-232 傳輸線。
3. 從電腦硬體裝置中，確認 COM port 編號。
4. 使用電腦中之超級終端機進行設定參數。
5. 每秒傳輸位元：9600 b/s。
6. 資料位元：8 bits。
7. 同位檢查：無。
8. 停止位元：1 bit。
9. 流量控制：無。

## 6. 其他(續)

### 6.2 產品保固期

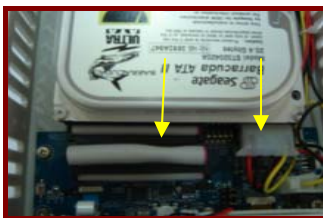
本產品在保固期內正常使用而非人為因素造成損壞者，保固期為二年。

## 附錄 A 快速安裝

有關 MED 的硬體安裝，您可以參考以下的步驟實施或從本公司網站下載安裝之作業流程進行安裝。

### 步驟1

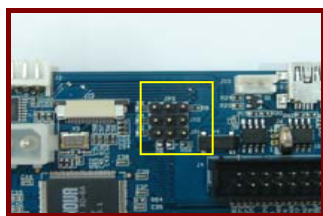
取得一個 IDE 的硬碟，設定 MASTER/SLAVE，連接主機盒內之短排線及電源線到硬碟上。如圖一。



圖一 連接 MED IDE&POWER

### 步驟2

設定加密主機板內之跨接器(jumper) MASTER 或 SLAVE 配合硬碟電腦作業需求設定。如圖二。

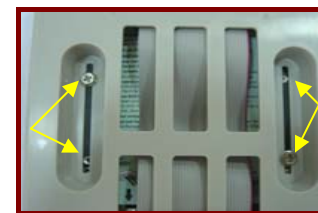


圖二 跨接器(jumper)設定位置

### 步驟 3

以附屬四顆螺絲將硬碟固定在主機盒上。如圖三。

## 附錄 A 快速安裝 (續)



圖三 固定作業硬碟

### 步驟 4

直接將加密主機盒嵌入至 PC 位置上，以所附的螺絲固定。如圖四。



圖四 推入電腦機架中，以螺絲固定

### 步驟5

連接 PC desktop 內 IDE 排線及電源線至加密主機盒上。

### 步驟6

重新檢查及確認安裝是否正常。加密作業程序請參考本手冊中 3.1 或 3.2 節。

## 附錄 B 問答集 Q & A

### Q1: 什麼是管理式加密裝置 (MED) ?

A1: 保護硬碟資料內容不被竊取之加密及管理的裝置。工程設計成具有強大的「硬碟加密」能力以及人性化操作介面的「階層式管理」能力。是一種先進的加密技術科技產品，符合美國Data Encryption Standard (DES)及Advanced Encryption Standard (AES)標準。適合大型企業、政府機關團體、金融機構、軍事單位等需要重視「資訊安全保密」及「資訊管理」之單位使用。參考網站：  
<http://www.htdlink.com> 可以獲得更多的訊息。

### Q2: 管理式加密裝置適合哪些作業系統？

A2: 本產品可適用於不同的作業系統，安裝容易，操作簡便。只要電腦中有 IDE 介面之作業系統均可適用。如 WINDOWS 98/XP/NT/VISTA、LINUX、MAC。

### Q3: 在我的硬碟內儲存有資料時，如何做加密處理？

A3: 當您想要在舊有的硬碟上做加密處理時，您必須先將資料做備份，否則加密過程中，將會因硬碟格式化而導致資料遺失，必須等到舊有的硬碟完成加密程序後，再將備份的資料拷貝到經加密的硬碟內即可，您的資料亦即受到加密硬碟的保護。

### Q4: 當E-KEY遺失時如何處理？

A4: 基本上 E-KEY 分為三種型式：

1. 當 USER KEY 不慎遺失時，可以利用 MASTER KEY 提供之功能，先將遺失 E-KEY 之 USER 編號鎖住，避免外在人為因素之進入。可經由代理商處購得一支或多支 USER E-KEY，重新進行編號即可，原來遺失之 USER E-KEY 將因系統鎖住而無法使用，直到您同意恢復它的功能為止。
2. 當 MASTER KEY 不慎遺失時，您不用擔心，只要您將 MED 上

## 附錄 B 問答集 Q & A(續)

的名稱及密碼，利用 E-Mail 寄回本公司技術支援處，你將重新獲得一支新的、功能相同的 MASTER KEY (但必須另外付費)，按照說明書上重建功能 (MASTER KEY REBUILD function) 之指示，在您的加密裝置上進行重建即可。原來舊有的 MASTER KEY 將自動作廢。

3. 當 SUPER KEY 不慎遺失時，您不用擔心，只要您將 MED 上的名稱及密碼，利用 E-Mail 寄回本公司技術支援處，你將重新獲得一支新的、功能相同的 SUPER KEY (但必須另外付費)，按照說明書上重建功能 (SUPER KEY REBUILD function) 之指示，在您的加密裝置上進行重建即可。原來舊有的 SUPER KEY 將自動作廢。

### Q5: 密碼忘記了，該怎麼處理？

A5: 本產品是非常一種先進的加密技術科技產品，首次安裝必須設定並且牢記，以便於後續的服務；若您真的忘記密碼，基於先進的加密技術保全，本公司亦無任何一種方法為您實施解密，您的加密硬碟可能必須重新格式化而造成資料的流失。

### Q6: 當MED 完全損壞無法使用時，我該怎麼處理？

A6: 經過技術鑑定確認後，在保固期內正常使用而非人為因素造成損壞者，本公司將有責任提供符合您所需要正常功能的 MED，您所使用經加密後的硬碟依然能夠正常的運作。

### Q7: MED產品的保固期為何？

A7: 本產品在保固期內正常使用而非人為因素造成損壞者，保固期為二年。

