公告本

406233

申請日期	87、4、28
案號	87106407
類別	G06F 17/60

（以上各欄由本局填註）

A4
C4

406233

發明 新型 專利說明書

一、發明 新型 名稱	中文	用於密碼匙保密處理之方法及設備
	英文	METHOD AND APPARATUS FOR SECURE PROCESSING OF CRYPTOGRAPHIC KEYS
二、發明 創作 人	姓名	1.吳松叢 2.方 寬
	國籍	美 國
	住、居所	1.美國,加州 92649,杭丁頓海灘,麥克法登大道 5171 號 2.美國,加州 92782,它斯丁,薩拉托加路 13281 號
三、申請人	姓名（名稱）	菲尼克斯科技公司
	國籍	美 國
	住、居所（事務所）	美國,加州 95134,聖荷西,東普魯梅瑞爾 411 號
	代表人姓名	史托特 J.尼可拉斯

裝 訂 線

406233

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

美　國（地區）　申請專利，申請日期：1997.05.02　案號：08/848,963　☑有　☐無主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（1）

發明背景

發明領域

本發明一般而言，係有關於電腦保密之領域，更特別的是，係有關一種用於密碼匙保密處理之方法及設備。

相關發明之描述

電腦保密關心到的是能讓使用者採取特別的方法以保護保密的資訊。電腦系統應用各種不同存取資訊的限制以確保僅有經過驗證之使用者可以取得存取系統資源之資格。利用複雜的電腦加密與解密之演算法以避免當保密資訊於公眾網路上傳送時被截取與解碼。此外，新的技術，例如，數位式簽證、數位式加封、驗證、認證與非拋棄等技術已經應用於驗證使用者，允許特許的資料存取，以及促進保密之線上電子商業行爲。所有這些技術需要某些“保密”形式之資訊，稱爲“鑰匙”，以確保這些資訊之保密性。用於保護資訊、允許資訊存取、以及驗證使用者等的鑰匙統稱爲“密碼匙”。這些密碼匙，爲了要達到最佳之效率，必須於一個保密的環境下處理，如此，侵犯保密處理程式便無法發現這些“保密”資訊。密碼學技術於 Bruce Schneier 所著，John Wiley 與 Sons，Inc.於 1996 年所出版的應用密碼學第二版中有通盤的討論，此書亦提供本發明專利申請之參考。

舉例說明，一種遠端使用者存取資訊的方法包含一個儲存於一個電腦代符之保密匙的應用，便是已知的盤問/回應鑑定程序。此電腦代符可以由任何形式之可移除儲存設備，例如一個軟式磁碟機、Fortezza 卡、PCMCIA 卡、智慧

五、發明說明（ 2 ）

卡，或甚至是一個僅存在於軟體的 “虛擬”智慧卡所組成。使用者實際地擁有電腦代符便可以存取遠端伺服器之資訊。於此機制中，主機送出一個隨機的號碼給使用者當作一個*盤問*。使用者根據對此*盤問*信號之數學運算結果傳回一個*回應*，且兩方皆獲知一個保密匙。藉由兩端獨立地執行相同的數學運算，最後可以確立使用者之識別資料。此保密匙本身從未被傳送，因此消除其於公眾網路上被竊取的可能性。

但是，於使用者的電腦上處理*盤問*信號與保密匙會產生保密性的問題。使用者可以觀察到保密匙以及確認程式並拷貝此保密匙及/或確認程式。其他於電腦上執行的程式亦可以觀察到並拷貝此保密資訊。因此，保密匙與確認程式必須於一個不會被使用者或其他電腦處理程式干擾或觀測到的保密環境下處理。

爲了要保護保密匙與確認程式不受到干擾，已經被利用之較受歡迎的方法是使用智慧卡。每張智慧卡是與信用卡一般大小的塑膠卡片，其具有特殊型態之嵌入式積體電路。此積體電路儲存電子形式之資訊並於卡片的範圍內處理這些資訊。因爲保密匙與任何必要之加密/解密演算法或確認程式皆於此智慧卡內處理，所以外部的處理程式便無法觀測到保密資訊。智慧卡之內部處理甚至無法被使用者所看見。智慧卡通常包含以下的組成元件：

※ 一顆微處理器（通常爲 8 位元）

※ EEPROM（通常爲 8 至 32 千位元）

五、發明說明（３）

※ 一個晶片上作業系統

※ 嵌入式密碼軟體（執行 DES、零-知識，或 RSA 演算法）

※ 一個以預先寫入 EEPROM 之永久 PIN 碼加密的保密匙

此智慧卡提供一個保密的環境以儲存與處理保密匙，這是因爲所有依據保密匙所執行的操作程序皆於此卡的範圍內執行。此保密匙或加密演算法因此絕對不會暴露於外部的環境中，也因此不會被未經許可之使用者所觀測到。智慧卡不僅已經使用於實施密碼確認的機制中，亦已應用於加密/解密演算法、使用者驗證以及非拋棄之方法上。任何需要某些保密資訊以處理資料的應用，都可以利用使用智慧卡之保密處理環境所帶來的好處及優點。但是，實體智慧卡之機制卻是非常昂貴與難以處理的，因爲每個使用者必須擁有一張實際的智慧卡以及智慧卡讀卡機之配合以獲得系統的資訊存取權。智慧卡讀卡機於少量購買時，目前的價格約爲每個 100 美金，而智慧卡本身的價格約爲每張 6 至 8 美元。於每台電腦上安裝實體智慧卡讀卡機，即使是一個小型的應用仍可能會是一筆可觀的花費。

了解到應用實體智慧卡驗證系統所需的費用之後，一些公司已提出應用 "虛擬智慧卡"的對策以因應費用實體智慧卡驗證系統昂貴的現象。如目前已實施的範例而言，一個虛擬智慧卡是存在於電腦軟體中，並如同應用程式一般地於電腦上執行。保密匙通常儲存於一個硬式磁碟機或是一個軟式磁碟機上，並且由一個個人識別碼（Personal

五、發明說明（ 4 ）

Identification Number，PIN）所保護著。因此，任何具有虛擬智慧卡電腦軟體和與其結合的 PIN 之機器，便可以進接遠端系統。但是，此種方式的問題是，保密匙的處理程序是在 “公開”的場合下進行的-意即，保密匙先被讀取並存入系統的記憶體，且於 “公開”模式下並未上鎖。此舉會造成保密匙與其處理程序容易被其他於同一系統上執行的處理程序所侵擾。

因此，需要有一個電腦保密系統，於其中密碼匙、演算法與相關程式於一個保密的處理環境下儲存並處理，此環境無法被其他系統處理程式進接或被使用者所觀測到。對保密系統而言，利用既有的硬體，而不須任何額外的周邊設備也是必需的。

發明概要

本發明爲一種應用一種保密處理器模式及相關的一個保密記憶體，而使用於保密儲存與處理密碼匙之方法與設備。一個處理器起始成爲一種保密處理模式，該模式無法被其他中斷程式所中斷。相關的保密記憶體，當處理器未處於保密處理模式下時，則無法被其他處理程序存取。於執行時期，當處理器進入保密處理模式時，則作業系統會暫停作業。

一個以加密的形式儲存之密碼匙，儲存於一個可移除的儲存設備中，例如一個軟式磁碟機、CD-ROM、dongle 等。系統會僅於系統已進入保密處理器模式時，由可移除的儲存設備中讀取此密碼匙並將其載入保密記憶體中。任

五、發明說明（5）

何必須之密碼程式，其可能儲存於系統之基本輸入輸出系統（Basic Input Output System，BIOS）中，當處理器處於保密模式時，亦會載入保密記憶體中。若有所需要，此保密記憶體會鎖上，以避免其他處理程序存取這些儲存的資料。一旦密碼匙與程式被載入保密記憶體後，使用者會被提示以移去可移除之儲存設備，且處理器會離開保密模式。因此，密碼匙與程式載入保密記憶體的情形對作業系統與其他處理程式而言是無形的。

使用者可能需要鍵入一個 PIN 碼來開啓儲存於保密記憶體內之密碼匙。藉由將密碼匙載入保密記憶體，並以 PIN 碼開啓此密碼匙，系統便具有與一個實體智慧卡所相同的功能。應用程式可以請求加密的服務，就如同一個實體的智慧卡加裝於系統一樣。每次於一個應用程式請求一個加密服務時，處理器便會進入保密處理器模式以執行被要求的操作。因此，密碼匙之儲存與處理程序對作業系統與其他處理程式是透明的。爲了清除密碼匙，使用者可以請求系統清除保密記憶體內之資訊。

如同在此所要討論的，系統會進入保密處理器模式，以便將保密匙與必需的加密程式載入保密記憶體。系統可能會進入保密模式，以便於執行時間內的任何時間，或於開機期間，將保密匙與必需的加密程式載入與處理。但是，處理器並不需要爲了載入或處理保密匙而於開機時間時處於保密模式，因爲此時並沒有其他的處理程式正在執行中。因此在不需要附加任何額外的硬體之情況下，便可獲

五、發明說明（ 6 ）

得密碼匙的保密處理模式。

圖式簡單說明

本發明確實的特性，連同其目的與優點，將會藉由以下圖式所描述的說明敘述，變得顯而易見，於圖式中：

圖一爲顯示應用本發明的一個電力啓動序列之流程圖；

圖二爲一個描述本發明執行時間處理程序的流程圖；

圖三爲一個描述確認使用者之個人識別碼（PIN）較佳方法的流程圖；

圖四爲一個描述執行時間載入保密匙的流程圖；以及

圖五爲一個描述本發明的方塊圖。

較佳實施例之詳細說明

以下的描述是爲了提供讓任何專精於此領域者能夠製造與利用本發明，並且由發明者提出經深思熟慮後最佳的模式以實現本發明。不同的修改，無論如何，對那些專精於此研究領域者仍會非常的明顯，因爲已經於此特別地定義本發明基本之原理精神，以提供一種用於密碼匙保密處理的方法與設備。

本發明使用一種特別的保密處理模式來處理一個於電腦代符上提供的密碼匙，與一個相配合之特殊保密記憶體區域其對於作業系統而言是透明的。保密模式的一個範例爲英代爾 X86（Intel x86，80386 或後來的處理器）之系統管理模式（System Management Mode，SMM）處理器架構，與相容的處理器。配合的記憶體則是眾所周知之系統管理

五、發明說明（ 7 ）

隨機存取記憶體（System Management RAM，SMRAM）。處理器的系統管理模式（SMM）與系統管理隨機存取記憶體（SMRAM）兩者對作業系統與其應用程式皆爲透明的（無形的）。密碼匙與演算法，一旦儲存於 SMRAM 中，便可使用於 SMM 期間，因此密碼匙與其處理程序兩者絕對不會暴露於外。此方法與設備因此提供了保密的密碼匙處理程序，而不需要昂貴的智慧卡硬體，且較虛擬智慧卡之處理更具保密性。

本發明的一個較佳實施例將參考圖 1 加以討論。以下對較佳實施例之敘述應用於一種電腦系統之電力供應序列上。既然於電力供應序列期間並不會載入任何作業系統，則可以不需要任何其他處理程式觀測其內容而載入密碼匙與程式，因此並不嚴格要求要進入 SMM。本發明可以藉由採用 SMM 而不脫離本發明之範圍內，使用於其他系統操作的階段中。

於步驟一，一個電腦系統開啓電源，且於步驟二啓動一顆 Intel x86（80386 或以後的版本）之系統管理模式（SMM）。於步驟三，會判斷 I電腦代符I是否已連接上電腦系統了。此I電腦代符I可以包括任何形式之可移除實體儲存設備，例如磁帶機、PCMCIA 卡、軟式磁碟機、CD-ROM 或任何其他類似之可移除儲存設備。此電腦代符包含了加密程式所需的密碼匙與其他相關資訊。雖然不像一個實體的智慧卡一般，但此電腦代符並不需要包含本身自有的處理器與相關的硬體，因爲處理程序會於保密模式下之

五、發明說明（ 8 ）

主要系統處理器進行。因此，這些可移除儲存設備便較實體的智慧卡便宜許多。

若電腦代符並未出現於系統中時，一個標準系統開機程序會於步驟 10 繼續進行，且此時系統不會具有任何智慧卡的功能。否則，一個使用者之個人識別碼（PIN）會於步驟 4 加以驗證。藉由除了電腦代符外要求一個 PIN，本發明因此執行了「兩個鑑定因子」之處理程序，其較單一密碼機制提供更多的保密性。本方法所使用的這兩個「因子」便是使用者之 PIN 與保密密碼匙。藉由要求這兩個因子，保密被侵害的風險性便大大地降低了。本發明亦可以不需要要求一個 PIN 來執行，但是保密的好處將會因此而減少。若於步驟 5，使用者之 PIN 不正確，則標準系統開機程序會於步驟 10 繼續進行，且此時系統不會具有任何智慧卡的功能。

一旦使用者之 PIN 經確認後，儲存於電腦代符之密碼匙便會載入系管理隨機存取記憶體（SMRAM）中。加密處理程序中可能需要的一個加密程式以及其他資料或是資訊也會於步驟 6 載入 SMRAM 中。加密程式與相關的演算法一開始儲存於何處並不是關鍵所在，假設其仍未被警示。這些演算法一開始可以儲存於基本輸入輸出系統快閃唯讀記憶體（BIOS Fresh ROM）中，或甚至是一個軟式磁碟機。於較佳的實施例中，這些加密程式與演算法是載入系統之基本輸入輸出系統（BIOS）中。

隨後 SMRAM 於步驟 7 時上鎖，此舉是爲了防止其他

五、發明說明（9）

任何的處理程式存取儲存於 SMRAM 中之資料。若所設計之記憶體能夠僅於保密處理器模式時允許資料被存取時，則其他的架構或是硬體之解決方案可能不需要額外的上鎖步驟。既然移除密碼匙與相關的演算法是於開機時間完成的，則加密處理程序便可以免於被其他的處理程式所侵擾（無任何其他的處理程式於此時執行）。此外，因 SMRAM 藉由晶片組於作業系統載入前上鎖並隱藏，此舉使得 SMRAM 的內容是不會被作業系統所干擾的。因此系統管理模式提供了一個保密的處理環境，類似於一個實體智慧卡所提供的環境一樣，但並不需要任何額外的硬體，也不需要與安裝一個實體智慧卡一樣地昂貴。

使用者於步驟 8 時被要求移除質體的電腦代符，以維持系統的完整性。一旦電腦代符已經被移除後（步驟 9），正常的系統開機程序於步驟 10 繼續進行。密碼匙從不會被使用者觀測到，亦不會被任何於電腦系統上執行的保密侵擾程序所看到。因此，本發明提供了與實體智慧卡相符的保密特性。密碼匙的處理程序，若需要時，可於電力啓動序列期間完成。無論如何，於較佳的實施例中，處理程序會於一個應用程式請求保密服務時才會開始執行，以模擬一張智慧卡的功能。

本發明一個較佳實施例的執行時期處理程序描述於圖二中。於步驟 20 中，需要進接保密電腦系統或網路，例如遠端伺服器的一個應用程式，會利用本發明的保密服務標準程式。此保密服務標準程式會於步驟 21 依序地執行一個

五、發明說明（10）

軟體系統管理中斷程式（System Management Interrupt，SMI）。此 SMI 是 Intel x86 架構最高階的中斷模式，且不會被被其他中斷程式所中斷。SMI 會啓動系統處理器進入 SMM 模式。一旦系統處理器處於 SMM 模式時，一個軟體 SMI 處程式會於步驟 22 執行保密功能。此保密功能會於步驟 23 存取儲存於 SMRAM 中之密碼匙與程式。處理器於 SMM 中執行請求的保密處理程序。此處理程序可能包含文件之加密/解密、密碼確認之保密匙處理程序、使用者驗證等。一旦處理程序完成後，處理器會於步驟 24 離開 SMM 模式，同時正常之系統操作程序於步驟 25 繼續進行。於步驟 25，適當的密碼資訊會提供給應用程式。整個處理程序會於無法被先前處理器上執行的應用程式看到的一個保密模式與一塊保密記憶體區域中進行。同時，應用程式不受缺少一張實際智慧卡所影響。

更進一步地描述本發明，考慮一個已經採用本發明而做修正之典型虛擬智慧卡應用。一個使用者可以利用一個軟體應用程式登錄遠端伺服器。此遠端伺服器可能發出一個*盤問*，並於允許使用者進接之前等待一個合適的*回應*。於接收來自於遠端伺服器的*盤問*之後，使用者會執行一個回應計算機程式，以計算出一個*回應*傳回給遠端伺服器。此回應計算機程式經一個軟體 SMI 程序（步驟 20、21）將盤問列傳送給主要系統處理器。於此處，SMM 接管程序，且整個作業系統與其應用程式會置於一個 “睡眠模式”。計算*回應*的操作程序是根據密碼匙的資訊，隨後便執行*盤問*

五、發明說明（ 11 ）

信號（步驟 22、23）。*回應*信號傳遞至回應計算機程式，此時作業系統恢復執行（步驟 25）。此回應計算機程式傳送*回應*信號給遠端伺服器以完成整個驗證程序。作業系統完全未察覺到回應計算處理程序，也因此無法干擾到回應計算處理程序的執行。

上述圖一與圖二的描述是假設密碼匙與程式於開機期間被載入保密記憶體。且只要是載入的動作是於保密模式，意即 SMM 中完成的，則密碼匙與程式亦可於系統已經開機後再載入記憶體。同時，密碼匙與程式可於不同的時間載入。密碼程式可於開機期間載入，而密碼匙可於稍後的時間載入。這樣的實施方法對擁有多個使用者，因此需要多個密碼匙的電腦系統，是有所幫助的。於這樣的電腦系統中，所有的密碼匙皆依賴同一個處理演算法。當每個使用者分別要求保密服務時，此演算法可於開機期間載入，而密碼匙於稍後的時間載入。專精於此領域者將可了解到，只要載入與處理程序是於利用保密記憶體的保密處理器模式下執行，於本發明的範疇中，會許多可能的載入與處理密碼匙及程式的方法。

於圖一中，使用者於電力啓動序列時鍵入一個 PIN 碼，以開啓保密密碼匙。藉由於作業系統已經載入之前要求鍵入 PIN 碼，其他程式便無法侵擾此 PIN 碼。同樣地，本發明可以不要求 PIN 碼而加以實現，雖然保密性的好處會減少一些。同時，若需要的話，即使是在作業系統已經載入之後，可於處理程序的不同階段要求一個 PIN 碼。舉例

五、發明說明（12）

說明，於某些特定的應用中，可於以載入系統之後使用一個電腦代符。於此例中，鍵入 PIN 碼，連同密碼資訊與程式經由一個軟體 SMI 傳送給 SMM 處理程序。當處理密碼匙時，作業系統處於一個 “睡眠模式”。

一個於電力啓動序列期間使用的 PIN 驗證方法（步驟 4）較佳的實施例描述於圖三中。於步驟 30 開始 PIN 驗證處理程序，並讀取一個儲存於電腦代符中之加密過的密碼匙。使用者會於步驟 32 被提示鍵入一個 PIN 碼。隨後於步驟 33 利用此 PIN 碼解密密碼匙。利用一個 HASH 函式以於步驟 34 產生此密碼匙的摘要資訊。一個 HASH 函式爲一個無需輸入參數的數學函式，其製造一個固定長度之密碼匙代號當作是輸出。HASH 函式的範例包括 MD5、SHA、與 RIPEMD-160 等。由 HASH 函式於步驟 34 產生的摘要與儲存於系統 BIOS 之摘要複製作比較。比較的結果於步驟 36 傳回。若摘要相符，則 PIN 驗證於圖一的步驟 5。一旦 PIN 被驗證過了，電腦代符的內容資訊便可以載入 SMRAM 中。因此，PIN 驗證步驟附加上其他層次的系統保密以避免非授權的資訊存取，即使是有人已經竊取電腦代符了。

圖四描述本發明的一個實例，於其中是於系統已經開機的狀態下才載入保密匙。其假設於開機序列時，必要的密碼程式已經事先載入 SMRAM 中了。如以上所描述的，在同一個密碼演算法同時被具有不同的保密匙之不同使用者使用的情況下，此實施例是很有效的。一個使用者應用程式於步驟 41 要求使用者鍵入一個 PIN 碼，並執行一個

五、發明說明（13）

SMI 程序。處理器進入 SMM 模式並於步驟 42 要求使用者插入電腦代符（可移除之儲存設備）。於步驟 43，一個儲存於電腦代符的加密匙載入於 SMRAM 中，且此保密匙於步驟 44 時利用 PIN 碼解密。此匙於步驟 45 使用一個 HASH 函式產生一個摘要加以處理。於步驟 46 時，此 HASH 函式之摘要與儲存於 BIOS 之摘要互相比較。若摘要相符，則 PIN 碼於步驟 47 確認過了，且於步驟 48 將此匙載入 SMRAM 中。使用者於步驟 49 被提示移除電腦代符，以確保系統之保密，隨後處理器於步驟 50 離開 SMM 模式。本發明此時正準備處理眼前的使用者應用程式可能需要的任何保密服務請求。同樣地，若需要，加密處理程序可以於步驟 48 與步驟 49 之間，立刻執行。

圖五爲本發明一個設備之功能方塊圖。一個電腦系統 60 包含了一個中央處理單元（Central Processing Unit，CPU）64 其具有一個不會被其他中斷程式所中斷的保密處理模式。CPU 64 有一個中斷行 641，於此一個保密模式中斷會啓動 CPU 64 進入保密模式。一個保密記憶體 66 連接至 CPU 64，且僅能於 CPU 64 處於保密處理模式時，由 CPU 64 存取。一個主要系統記憶體 68 亦連接於 CPU 64，且由作業系統與應用程式所使用。一個系統 BIOS 62 儲存一個 PIN 碼之 HASH 函式摘要 621，其與一個使用者藉由鍵盤 70 鍵入之 PIN 碼所計算出的摘要做比較。一個電腦代符讀取器 72 讀取儲存於電腦代符 74 中之密碼匙、資訊與程式。此電腦代符讀取器 72 可以包含一個感應器以偵測電

五、發明說明（14）

腦代符 74 之存在與否。本發明設備之操作連同本發明之方法與相關的流程圖，便如同以上所描述的一般。

必須注意的是本發明能夠應用於任何形式之密碼匙的儲存與處理。密碼匙可以是一個對稱密碼匙系統中的密碼匙，或是一個使用於公眾匙密碼系統（Public Key Cryptography System）中的私有匙。經由本發明，在不需要實際應用實體智慧卡的花費下，便能達到智慧卡之保密處理能力。可以利用本發明於改進虛擬智慧卡的保密性，與任何其他僅使用軟體來處理與儲存密碼匙的應用程式。

雖然較佳的實施例已經於此以 Intel x86 相容的架構（80386 或稍後的版本）來描述，但本發明可以應用於任何具有不會被其他中斷程式所中斷的保密處理模式，與一個僅當處理器處於保密處理模式時才能被存取的保密記憶體區域的處理器架構。大部分已知的處理器皆具有一個可以滿足第一個需求之最高階中斷階層，而記憶體需求可以藉由適當的晶片組設計或由處理器外接邏輯電路來達成。

專精於此領域者將會了解到，在不脫離本發明的範疇與精神下，可以對上述較佳實施例做各種不同的改變與修正。因此，可以了解到，於附錄之申請專利範圍內，本發明可以不同於上述之方法施行。

四、中文發明摘要（發明之名稱：　　）

用於密碼匙保密處理之方法及設備

一種用於密碼匙保密處理之方法及設備，於其中，儲存於一個電腦代符中的密碼匙於保密處理器模式期間，利用一個保密記憶體加以處理。一種主要系統處理器起始化於一個保密處理模式，其於電力啓動序列期間不會被其他中斷程式所中斷。一個使用者鍵入一個個人識別碼（Personal Identification Number，PIN）以開啓儲存於一個電腦代符中的密碼匙。密碼匙與相關的密碼程式隨後載入保密記憶體。保密記憶體會上鎖以避免其他處理程式存取儲存的資訊。使用者隨後會被提示移除電腦代符，處理器會

英文發明摘要（發明之名稱：METHOD AND APPARATUS FOR SECURE PROCESSING OF CRYPTOGRAPHIC KEYS　　）

A method and apparatus for secure processing of cryptographic keys, wherein a cryptographic key stored on a token is processed in a secure processor mode using a secure memory. A main system processor is initialized into a secure processing mode, which cannot be interrupted by other interrupts, during a power-on sequence. A user enters a Personal Identification Number (PIN) to unlock the cryptographic key stored on the token. The cryptographic key and associated cryptographic program are then loaded into the secure memory. The secure memory is locked to prevent access to the stored data from any other processes. The user is then prompted to remove the token and the processor exits the secure mode and the system continues normal boot-up operations. When an application requests security processing, the cryptographic program is executed by the processor in the secure mode such that no other programs or processes can observe the execution of the program. Two-factor authentication is thus obtained without the need for any additional hardware.

A5
B5

四、中文發明摘要（發明之名稱：　　）

離開保密模式且系統繼續進行正常開機操作程序。當一個應用程式請求保密處理程序時，密碼程式會於保密模式期間由處理器執行，因此其他程式或處理程式皆無法觀測到程式之執行。兩個因子驗證程序便可以在不需要任何額外的硬體情況下達到。

英文發明摘要（發明之名稱：　　）

A8
B8
C8
D8

六、申請專利範圍

1.一種方法，其用於密碼匙之保密處理，其使用一個具有一個保密處理器模式之主要系統處理器，包含步驟如下：

於一個保密處理器模式期間或於一個電力啓動起始序列期間，載入一個密碼匙、加密程式與任何其他必需的密碼資訊於一個保密記憶體中；及

於保密處理器模式或於電力啓動起始序列期間，利用儲存於保密記憶體中之密碼匙執行密碼程式。

2.如申請專利範圍第１項之方法，於其中，保密記憶體僅能由當處於保密處理器模式時之處理器存取。

3.如申請專利範圍第２項之方法，於其中，保密處理器模式爲一個不會被其他處理器中斷程式所中斷之最高階中斷處理模式。

4.如申請專利範圍第１項之方法，於其中，載入之步驟是於一個電力啓動起始序列期間展開的，且執行的步驟則於作業系統已經載入後開始進行。

5.如申請專利範圍第４項之方法，於其中，密碼程式與資訊於一個電力啓動起始序列期間載入，且密碼匙於一個於作業系統已經載入後啓動之保密處理器模式期間載入。

6.如申請專利範圍第３項之方法，更包含以下之步驟：

於將密碼匙載入保密記憶體之前，確認一個個人識別碼（Personal Identification Number，PIN）。

六、申請專利範圍

7.如申請專利範圍第5項之方法，更包含以下之步驟：

若系統架構需要用來避免其他處理程式存取保密記憶體，可在電力啓動起始期間執行的密碼程式載入步驟之後，鎖住保密記憶體。

8.如申請專利範圍第3項之方法，於其中，處理器爲一個與 Intel 386 家族相容之處理器，或更後面的 x86 模式處理器，且保密處理器模式是一個系統管理模式（System Management Mode，SMM）。

9.如申請專利範圍第8項之方法，於其中，保密記憶體爲一個系統管理隨機存取記憶體（System Management Random Access Memory，SMRAM），且處理器之初始化包含執行一個系統管理中斷程式（System Management Interrupt，SMI）的步驟。

10.如申請專利範圍第6項之方法，於其中，確認一個 PIN 碼的步驟包含以下的步驟：

由電腦代符讀取一個加密匙；

要求使用者鍵入一個 PIN 碼；

使用 PIN 碼解密密碼匙；

於解密過的密碼匙執行一個 HASH 函式以產生一個摘要；及

將產生的摘要與儲存於系統 BIOS 之摘要比較。

11.一種使用一個主要系統處理器之密碼匙保密處理的方法，包含以下的步驟：

六、申請專利範圍

確認一個使用者識別碼（PIN）；

若使用者之 PIN 碼已經確認，則將儲存於一個電腦代符中的一個密碼程式與其他必需的密碼資訊載入保密記憶體；

若系統架構需要用來避免其他處理程式存取保密記憶體，可於載入密碼程式與其他資訊之後，鎖住保密記憶體；

離開保密處理器模式，並繼續進行正常的開機程序。

12.如申請專利範圍第１１項之方法，於其中，密碼匙於一個於作業系統已經載入後啓動之保密處理器模式期間載入保密記憶體。

13.如申請專利範圍第１１項之方法，於其中，密碼匙於作業系統載入之前，連同密碼程式與其他資訊一起載入保密記憶體。

14.如申請專利範圍第１１項之方法，更包含以下的步驟：

於確認使用者之 PIN 碼之前判斷是否有電腦代符可以利用。

15.如申請專利範圍第１４項之方法，於其中，確認 PIN 碼的程序包含以下的步驟：

由電腦代符中讀取一個加密匙；

要求使用者鍵入一個 PIN 碼；

利用此 PIN 碼解密加密匙；

於解密過的密碼匙執行一個 HASH 函式以產生一個摘

六、申請專利範圍

要；及

將產生的摘要與儲存於系統 BIOS 之摘要比較。

16.如申請專利範圍第１１項之方法，於其中，保密記憶體僅能由當處於保密處理器模式時之處理器存取。

17.如申請專利範圍第１６項之方法，於其中保密處理器模式爲最高階之中斷處理模式，其不會被其他處理器中斷程式所中斷。

18.如申請專利範圍第１１項之方法，於其中，處理器爲一個與 Intel 386 家族相容之處理器，或更後面的 x86 模式處理器，且保密處理器模式是一個系統管理模式（System Management Mode，SMM）。

19.如申請專利範圍第１８項之方法，於其中，保密記憶體爲一個系統管理隨機存取記憶體（System Management Random Access Memory，SMRAM），且處理器之初始化步驟包含執行一個系統管理中斷程式（System Management Interrupt，SMI）的步驟。

20.如申請專利範圍第１２項之方法，於其中，當應用程式請求保密服務時，處理器會起始進入保密模式，作業系統會處於睡眠模式，且會執行密碼程式。

21.一種用於密碼匙保密處理程式之保密處理設備，該設備包含：

一個具有保密處理器模式之主要系統處理器；

一個保密記憶體，其僅能由當處於保密處理器模式時之處理器所存取；

六、申請專利範圍

儲存於一個電腦代符之一個密碼匙、程式與相關資訊，於其中，密碼匙、程式與相關資訊於電力啓動初始期間或於保密處理器模式期間儲存於保密記憶體，且於其中，密碼匙、程式與相關資訊於電力啓動初始期間或於保密處理器模式期間由處理器加以處理。

22.如申請專利範圍第２１項之保密處理設備，於其中，保密處理器模式爲最高階之中斷處理模式，其不會被其他處理器中斷程式所中斷。

23.如申請專利範圍第２２項之保密處理設備，更包含：

電腦代符判斷裝置，其用來判斷於密碼匙與程式載入保密記憶體之前是否有電腦代符可以利用。

24.如申請專利範圍第２３項之保密處理設備，更包含：

個人識別碼（Personal Identification Number，PIN）確認裝置，其用來於判定有電腦代符可以使用之後以及於載入密碼匙與程式之前確認使用者之 PIN 碼。

25.如申請專利範圍第２４項之保密處理設備，於其中處理器爲一個與 Intel 386 家族相容之處理器，或更後面的 x86 模式處理器，且保密處理器模式是一個系統管理模式（System Management Mode，SMM）。

26.如申請專利範圍第２５項之保密處理設備，於其中保密記憶體爲一個系統管理隨機存取記憶體（System Management Random Access Memory，SMRAM），且藉由執

六、申請專利範圍

行一個系統管理中斷（System Management Interrupt，SMI），將處理器初始化。

27.如申請專利範圍第２４項之保密處理設備，於其中，PIN 確認裝置包含：

讀取儲存於電腦代符中之加密匙之讀取裝置；

要求使用者鍵入 PIN 碼之 PIN 要求裝置；

利用此 PIN 碼解密加密匙之解密裝置；

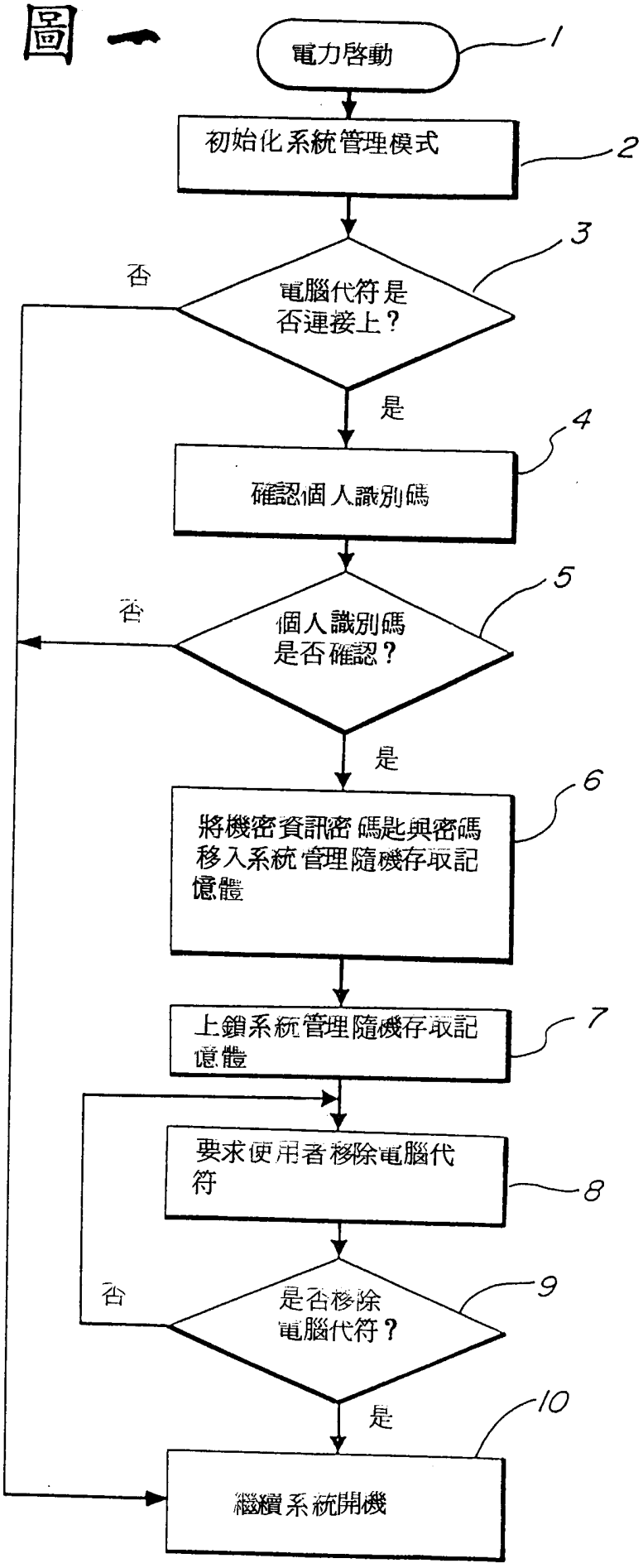
於解密過的密碼匙計算一個 HASH 函式以產生一個摘要之一個 HASH 函式計算裝置；及

將產生的摘要與儲存於系統 BIOS 之摘要比較之比較裝置。

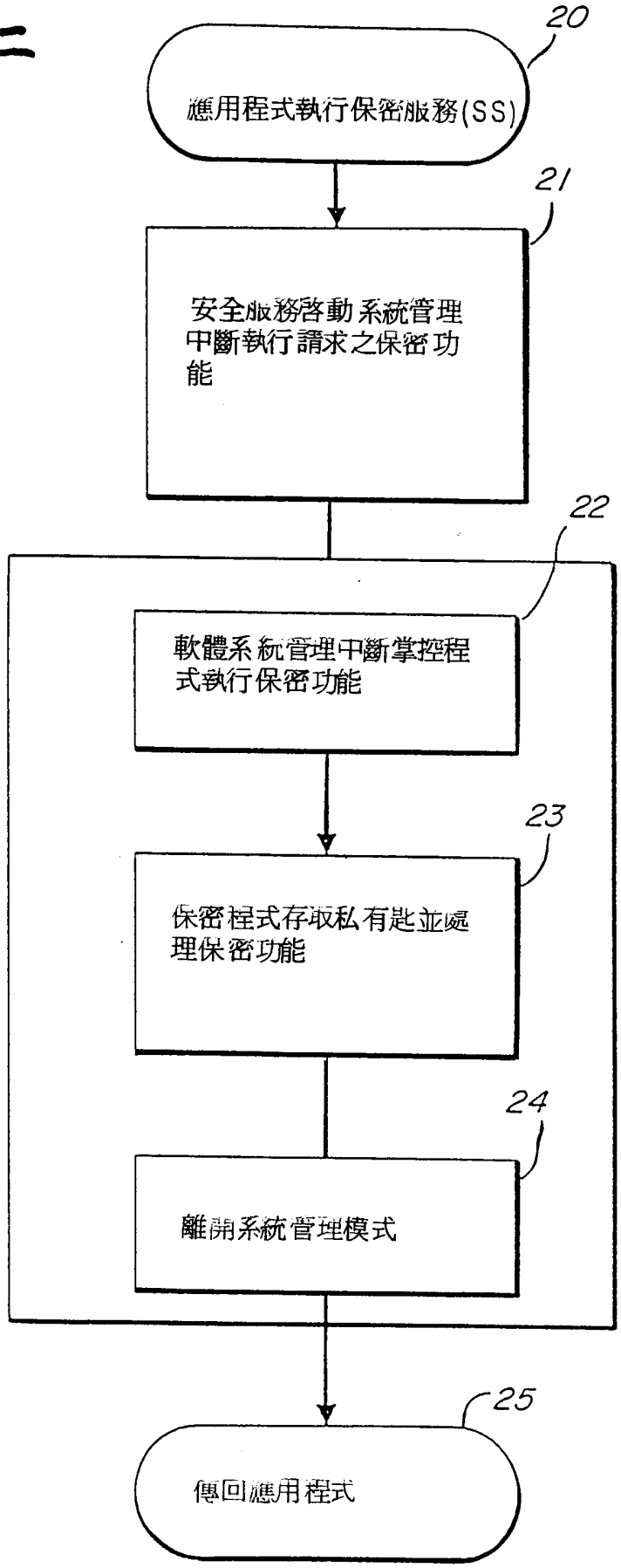
28.如申請專利範圍第２３項之保密處理設備，更包含：若系統架構需要鎖上記憶體以避免其他處理程式存取保密記憶體之上鎖裝置。

406233

圖一

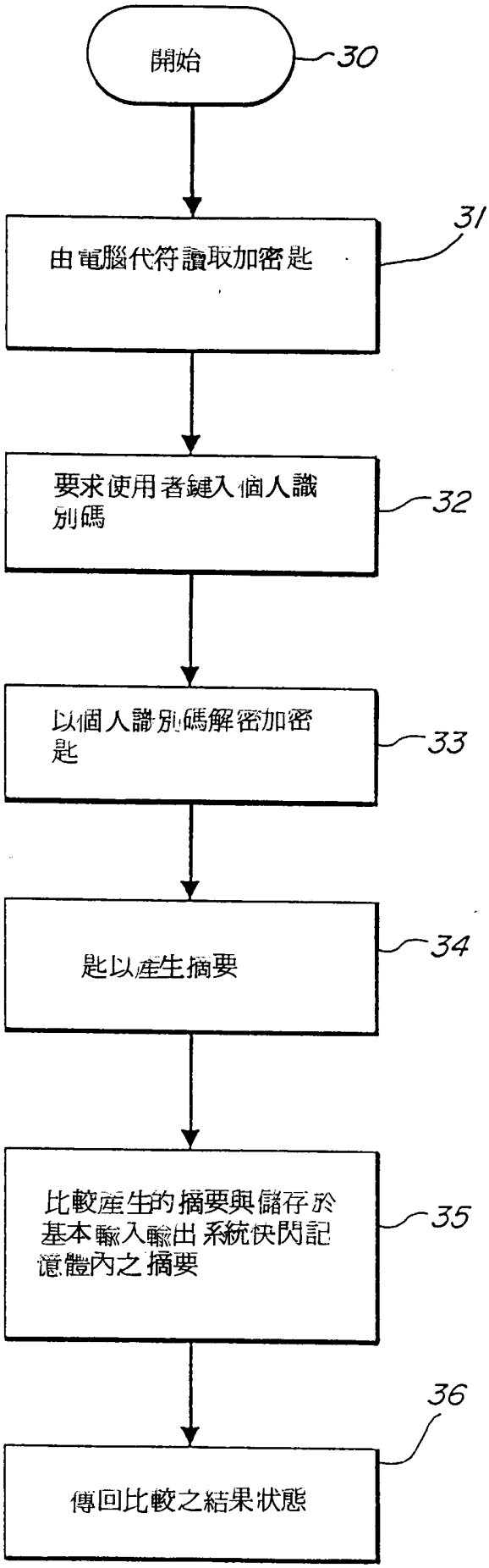

電力啓動
1
初始化系統管理模式
2
電腦代符是否連接上？
3
否
是
確認個人識別碼
4
個人識別碼是否確認？
5
否
是
將機密資訊密碼匙與密碼移入系統管理隨機存取記憶體
6
上鎖系統管理隨機存取記憶體
7
要求使用者移除電腦代符
8
是否移除電腦代符？
9
否
是
繼續系統開機
10

圖二

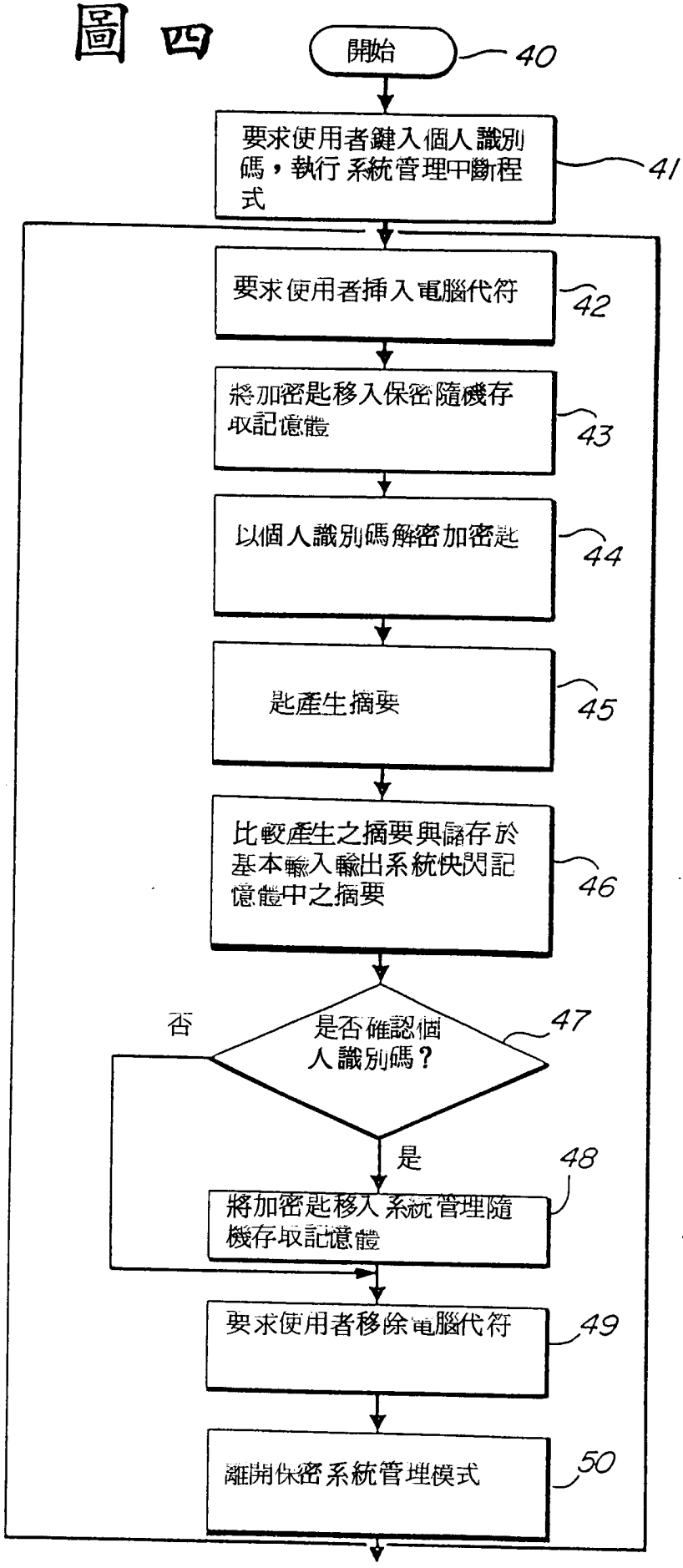

20
應用程式執行保密服務(SS)
21
安全服務啓動系統管理中斷執行請求之保密功能
22
軟體系統管理中斷掌控程式執行保密功能
23
保密程式存取私有匙並處理保密功能
24
離開系統管理模式
25
傳回應用程式

406233

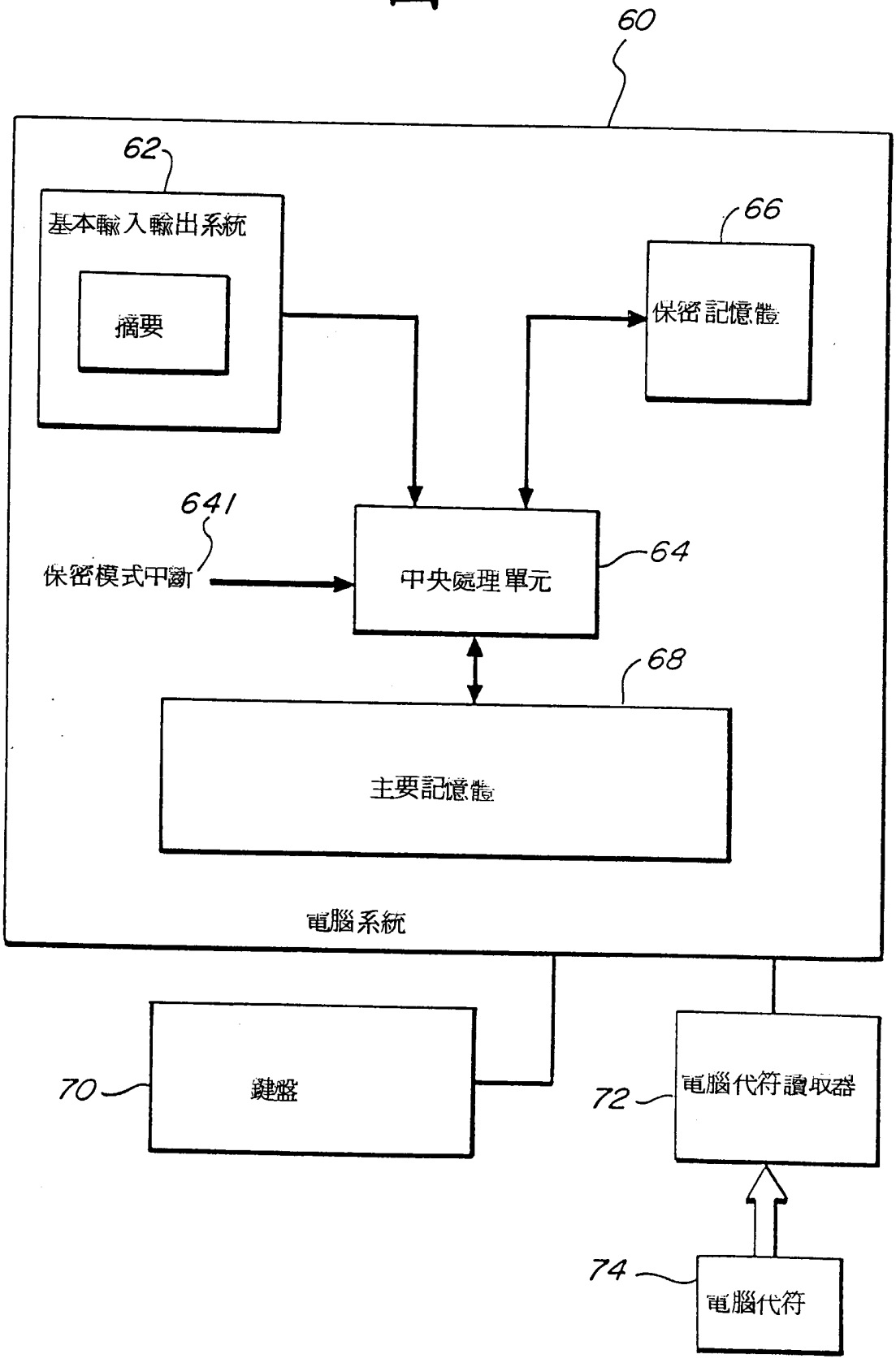
圖三


開始
30
由電腦代符讀取加密匙
31
要求使用者鍵入個人識別碼
32
以個人識別碼解密加密匙
33
匙以產生摘要
34
比較產生的摘要與儲存於基本輸入輸出系統快閃記憶體內之摘要
35
傳回比較之結果狀態
36

圖四


開始
40
要求使用者鍵入個人識別碼，執行系統管理中斷程式
41
要求使用者插入電腦代符
42
將加密匙移入保密隨機存取記憶體
43
以個人識別碼解密加密匙
44
匙產生摘要
45
比較產生之摘要與儲存於基本輸入輸出系統快閃記憶體中之摘要
46
是否確認個人識別碼？
47
否
是
將加密匙移入系統管理隨機存取記憶體
48
要求使用者移除電腦代符
49
離開保密系統管理模式
50

圖五


60
62
基本輸入輸出系統
摘要
66
保密記憶體
641
保密模式中斷
中央處理單元
64
68
主要記憶體
電腦系統
70
鍵盤
72
電腦代符讀取器
74
電腦代符

A8
B8
C8
D8

六、申請專利範圍

1.一種方法，其用於密碼匙之保密處理，其使用一個具有一個保密處理器模式之主要系統處理器，包含步驟如下：

於一個保密處理器模式期間或於一個電力啓動起始序列期間，載入一個密碼匙、加密程式與任何其他必需的密碼資訊於一個保密記憶體中；及

於保密處理器模式或於電力啓動起始序列期間，利用儲存於保密記憶體中之密碼匙執行密碼程式。

2.如申請專利範圍第１項之方法，於其中，保密記憶體僅能由當處於保密處理器模式時之處理器存取。

3.如申請專利範圍第２項之方法，於其中，保密處理器模式爲一個不會被其他處理器中斷程式所中斷之最高階中斷處理模式。

4.如申請專利範圍第１項之方法，於其中，載入之步驟是於一個電力啓動起始序列期間展開的，且執行的步驟則於作業系統已經載入後開始進行。

5.如申請專利範圍第４項之方法，於其中，密碼程式與資訊於一個電力啓動起始序列期間載入，且密碼匙於一個於作業系統已經載入後啓動之保密處理器模式期間載入。

6.如申請專利範圍第３項之方法，更包含以下之步驟：

於將密碼匙載入保密記憶體之前，確認一個個人識別碼（Personal Identification Number，PIN）。