200805204

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號： 96108099

※ 申請日期： 96-03-09 ※IPC 分類： G07F 7/08 (2006.01)
H04L 9/28 (2006.01)
H04L 9/32 (2006.01)

一、發明名稱：（中文/英文）

安全地處理敏感的資訊之方法與裝置

METHOD AND APPARATUS FOR SAFELY PROCESSING SENSITIVE INFORMATION

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

拜耳創新有限公司

BAYER INNOVATION GMBH

□ 指定　　為應受送達人

代表人：（中文/英文）（簽章）

翁迪特/ WOLLWEBER, DETLET

住居所或營業所地址：（中文/英文）

德國杜塞爾都佛城莫溫格茲街 1 號

MEROWINGERPLATZ 1, D 40225 DUESSELDORF, GERMANY

國　籍：（中文/英文）

德國/ GERMANY

三、發明人：（共 3 人）

姓　名：（中文/英文）

1. 瓦肯尼/VOELKENING, STEPHAN
2. 朱杰曼/JUENGERMANN, HARDY
3. 胡托騰/HUPE, TORSTEN

國　籍：（中文/英文）

1.-3.均為德國/GERMANY

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

德國；西元 2006 年 3 月 11 日；10 2006 011 402.7

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係有關於一種安全地處理資訊(特別是敏感資訊)之系統與方法，具體言之，係有關於根據申請專利範圍第 1、12、13 以及 14 項對應的子句之系統與方法的使用。

【先前技術】

安全地處理資訊(特別是敏感資訊)的系統與方法是眾所皆知的。

例如，大家都知道存取控制裝置(例如自動現金提款機(automatic cash dispenser))僅提供透過認證的存取，例如磁條卡(magnetic strip card)、晶片卡或是智慧卡(smart card)，有時亦會與 PIN 結合。敏感資訊係儲存於卡中，使用卡前需要訊問(interrogation)其他資訊(例如 PIN)以防未授權的使用卡。在適用於電子現金提款機之磁條卡或晶片卡的例子中，係儲存加密資料。在被動式(passive)卡(例如磁條卡)中的資料經過外部加密，也就是分開的讀取機中。在主動式卡中，計算單元(例如晶片)係整合於卡中。如此一來，資訊可於晶片上加密。為了避免誤用晶片卡，故藉由 PIN 或是訊問生物特徵來控制對晶片的存取。

磁卡與晶片卡的缺點在於其容易受到電磁作用而損毀。再者，由於卡的預定尺寸使得磁卡與晶片卡的儲存量非

常的小。相較於磁條卡，晶片卡具有較大的儲存量，且比較沒有被竄改或複製的風險。

基於此理由，現今的一些認證方法仍受到晶片卡的限制。因此，僅有晶片卡才可以在卡上簽名並藉由電子的方式驗證敏感資訊的真實性以及完整性。

然而，製造晶片卡的花費相當昂貴(是製造磁條卡的好幾倍)。

【發明內容】

本發明的目的係為製造一種可安全地傳送敏感資訊的系統及/或方法，其可以廣泛的應用且特別容易為一般大眾操作。

本發明其他目的為製造一種可安全地傳送敏感資訊之可靠系統及/或方法，其可快速可靠且不易受到干擾地傳送大量資料並且可預防未授權的使用。

本發明之目的可藉由包含申請專利範圍第 1 項所述之特徵的系統，以及包含申請專利範圍第 12 及/或 13 項所述之特徵的方法而達成。

本發明包含藉由簽名及/或加密原則之方式可靠地處理資訊的系統，該系統至少包含下列裝置：第一行動裝置(mobile)；被動儲存單元，用於可取回地儲存第一資訊；處理裝置，用來與第一儲存單元互動以處理資訊，包含：具有

解密防護之第二儲存單元，用於可取回地儲存對應於第一資訊之第二資訊；用於處理之電腦單元，較佳為用來密碼地(cryptographically)處理資訊；資訊傳輸單元，用來將第一及/或第二儲存單元之資訊傳送至電腦單元。

在後文中，"處理"通常代表根據 IPO 原則-輸入(input)、處理(processing)、輸出(output)(儲存)來執行處理。一般而言，其亦被稱為處置(handling)資訊。

資訊通常被理解為所有的資訊，特別是免於受到未授權存取之資訊，也就是一般敏感及/或機密資訊，例如：包含診斷病症、治療的私人資料以及金融資料(例如銀行連線資料)等等。

為了藉由第三方及/或檢查資訊的整體性及/或真實性使資訊免於受到未授權的存取，本發明係提供一種適用於處理的簽名及/或加密原則。

處理資訊的系統或裝置包含至少一第一行動裝置儲存單元，用於可取回地儲存之第一資訊。第一儲存單元同樣與物件或人相關並且受到物件或人為管理而儲存於其中。第一儲存單元係適用於行動裝置，使其可隨著物件或人而移動。對應的裝置於必要時可讀取行動性第一儲存單元中所儲存的資料或資訊。該資訊包含例如電子金鑰，例如金鑰對之私密金鑰(private key)及/或簽章或電子簽章(electronic signature)。再者，該資訊可包含避免其他人存取的資料或是難以取得的資料。其可以是銀行帳戶資料、臨床資料、身份

資料等等。此資訊較佳以對應的金鑰來加密及/或簽署。

該系統必須提供處理裝置以於必要時處理此資訊。處理裝置係藉由此方法與第一儲存單元互動，使得機密資訊可藉由處理裝置讀取或是可儲存於第一儲存單元中。

處理裝置包含至少一第二儲存單元。第二儲存單元較佳為可避免解密。其可藉由實體防護而實現，例如封閉外殼(closed housing)，其難以被未授權而存取，及/或其他防護裝置(例如資料防護)。

在第二儲存單元中係儲存第二資訊。第二資訊(特別是第二敏感及/或機密資訊)對應至第一儲存單元中之第一資訊。例如，第二資訊可包含對應於第一儲存單元之金鑰的計數金鑰(counter key)以形成金鑰對。再者，用來驗證對應於第一儲存單元之資料的相關資料可儲存於第二儲存單元中。

為了處理至少部分加密及/或簽署的第一資訊，必須先將其解密及/或確認簽章。基於此理由，處理裝置包含一電腦單元，用來密碼地處理資訊。此電腦單元係處理至少部分的加密及/或簽署的資料，使得交易可被執行，其必須僅藉由第一儲存單元之載體(carrier)來進行。

為了將資訊從第一及/或第二儲存單元傳送至電腦單元，亦提供資訊傳送單元。此亦可用來安全地傳送對應的資訊。

至少一個儲存單元較佳為非電子儲存單元，儲存於其

中的機密資訊(具體而言，該第一資訊)可以非電子的方式儲存及/或取回。非電子儲存單元包含例如磁性或光學儲存單元。

至少一個儲存單元較佳為光學儲存單元，包含作為儲存媒體之光尋址聚合物(photoaddressable polymer)群組及/或來自光儲存單元之機密資訊(具體而言，該第一資訊)可由光學的方式執行儲存及/或取回。

透過一事實可區別出光尋址聚合物所形成的材料，上述事實為該材料可以藉由光將方向性雙折射寫入材料(Polymers as Electrooptical and Photooptical Active Media, V.P. Shibaev (Editor), Springer Verlag, New Yourk, 1995; Natansohn et al., Chem. Mater. 1993, 403-411)。在美國專利第5173381 號中說明這些光尋址聚合物為具有功能化偶氮苯側鍊(azobenzene-functionalized side chain)之聚合物。

藉由光儲存裝置之資訊，此可以是設置為可靠、避免外部影響且在非常小的空間中具有大容量的裝置。光儲存資訊之設置特別可免於受到例如磁場或電子的影響。光儲存可產生容量與儲存尺寸之間的最佳比值。再者，光儲存單元比電子儲存單元(例如晶片)具有更多的優點。基於此理由，光儲存亦可產生容量與成本之間的最佳比值。

至少一儲存單元較佳為從晶片卡(chip card)、儲存卡(storage card)以及智慧卡(smart card)之群組中所挑選出來的卡之型式。設計為卡是為了記憶體之輕易操作以及可攜式結

構。卡較佳為與其他常用的卡具有相同的尺寸，例如信用卡等等。此型式的卡使得行動記憶體較容易保存於例如不需要製造特殊儲存單元的錢包等等。卡較佳為具有 ID-1 格式，又定義於 ISO/IEC 7810 標準中。此格式具有傳統讀取器等並且可較佳的使用。

為了儘可能於卡及/或行動儲存單元中儲存資訊及/或資料，至少一個儲存單元的儲存容量較佳為大於 0.5 百萬位元組(Mbyte)，更佳為大於 1Mbyte，更佳為大於 1.5Mbyte。傳統記憶體例如磁條、晶片等具有較小的記憶體，只能儲存有限的資訊項目。因此，只能儲存少量的項目。使用根據本發明所述之較佳的儲存容量便可儲存大量的資料以及經過加密的資料。

為了確保高儲存容量，用以形成儲存單元的儲存媒體(較佳為第一行動儲存單元)係適於聚合物(特別是作為來自光尋址聚合物群組之聚合物)。

具體而言，資訊可以全像地(holographically)方式儲存於行動記憶體中，較佳為一或多個極化全像(polarization hologram)。全像儲存(holographic storage)資訊提供有效的及改良的資訊防護，使其免於受到未授權人士的操作(例如複製或其他操作)。

全像儲存是一種類比儲存方法，也就是儲存於第一行動記憶體中的資訊為類比型式。

儲存於第一行動記憶體中的敏感資訊在儲存於行動記

憶體前及/或在其從行動記憶體讀出後較佳為數位型式。

在儲存於行動記憶體及/或在從行動記憶體中讀出後，其較佳顯示為加密及/或簽署的型式。

較佳實施例係提供至少一儲存單元，且第二儲存單元較佳為數位儲存單元，資訊可以數位的方式儲存於其中或是可以數位的方式來擷取儲存於其中的資訊。資訊較佳為以數位的方式儲存於對應的儲存單元中(特別是第二儲存單元)，然其並不是為了儲存空間的理由。數位機密資訊較佳為以數位的方式加密及/或簽署。在此例子中的敏感資訊已經過簽署，且該簽章較佳為與敏感資訊一起儲存於儲存單元中。基於此理由，至少一儲存單元(特別是第二儲存單元)較佳為加密儲存單元，較佳第一機密資訊可儲存於其中或是可以擷取儲存於其中的加密資訊。

為了儲存大量的資訊，對應的儲存單元較佳為被動式記憶體。行動儲存單元特別儲存大量的資訊。基於此理由，被動式儲存單元中不具有任何區域可藉由對應演算法主動地執行資訊計算、處理以及加密等。

相比之下，通常比較少資訊會儲存於第二儲存單元，因此用來處理資訊的演算法可儲存於第二儲存單元中。基於此理由，第二儲存單元較佳為主動儲存單元。在此系統中，行動儲存單元係為主動式記憶體(晶片卡)或是具有小且安全的記憶體之行動儲存單元(全像記憶卡)。

將第一行動記憶體製造為被動式且具有高儲存容量的

安全記憶體，而將第二記憶體製造為主動式記憶體或是主動式儲存單元，因而可產生一安全、堅固且具成本效益的系統。因此，第二儲存單元較佳為電子儲存單元，第二資訊可電性儲存於其中或是可電性地擷取儲存於其中的第二資訊。相對於磁性或非電性儲存裝置，敏感資訊以及演算法較佳為可電子地儲存於電子儲存單元，且與電腦單元之間的相關通訊可在不使用類比/數位轉換器的情況下實現。

在本發明較佳實施例中係將第一記憶體製造為光學記憶體(也就是被動式記憶體)，且將第二記憶體製造為電子記憶體。由於第二記憶體係耦接至電腦單元，因此具有對應第二記憶體之卡又叫做主動式儲存卡。

在第一記憶體中的資訊係以光學或是全像的方式儲存。為了藉由資訊傳送單元將傳送資料至第二電子儲存單元，資料必須從類比狀態更改為電子或數位狀態。因此將光源與相機結合來作為資訊傳送單元。接下來光源照射第一儲存單元上的全像。由於光束於全像處產生繞射(diffraction)因而產生儲存資訊之影像。所產生包含敏感資訊的影像係為由相機所挑選所反應的結果。相機接著從光學信號產生對應於第二儲存單元之電子或數位信號。

為了處理敏感資訊，第二記憶體係連接至第一電腦單元。此第一電腦單元單獨存取第二記憶體中的資訊。未授權的人士無法從外部讀取及/或操作第二記憶體中的資訊。只有第一電腦單元可以與第二儲存單元進行通訊並於兩者之間

傳送資料。

第一電腦單元具有密碼功能，藉此可以將資訊加密以及解密或是簽署。該功能又包含建立及/或檢查簽章的可能性。如同第二儲存單元免於受到未授權人士的存取，第一電腦單元亦可免於未授權人士之存取。

電腦單元、第二儲存單元以及資訊傳輸單元較佳為適用於電腦單元與第二記憶體之間在一單元或設備中交換資料。藉由此單元便可於第一與第二記憶體之間交換資訊。

電腦單元較佳為以智慧卡或晶片卡的方式結合於第二儲存單元中。為了避免未授權的操作，電腦單元以及儲存單元較佳為具有憑證，例如根據一般標準達到 EAL+4 或是更高層級，此提供非常高的安全性。

如上所述，介於行動第一記憶體與第二記憶體之間的資訊傳送單元較佳為光學資訊傳送單元，以藉由至少一光束徑(beam path)來傳送資訊。

電腦單元較佳為具有至少一傳輸通道，藉由傳輸通道可以將資訊傳送至其他電腦或是接收來自其他電腦的資訊。

這樣的傳輸通道較佳為防護通道。防護通道可以為加密通道(邏輯防護)，由於該通道設置於受監視的環境，因此這也可以是未授權人士無法從外部入侵或存取(實體防護)的通道。

為了在不同電腦單元之間交換資料，該電腦單元必須

於進行資料交換前彼此互相認證。

資訊傳輸單元較佳為寫入及/或讀取單元。

本發明較佳實施例提供光學傳送單元，用以藉由至少一光束以光學的方式發射包含雷射群組之偏光(polarize light)。

本發明可提供另一電腦單元來增加安全性，另外可提供第三儲存單元來儲存與第一及/或第二資訊相關之第三資訊。另外可藉由虹膜掃描(iris scan)、PIN 輸入以及取得其他生物資料(例如指紋等)來實施進一步的安全性詢問。

為了管理不同使用者的金鑰及/或憑證，該系統較佳為提供金鑰管理單元來管理金鑰及/或簽章。

本發明亦包含教導以密碼的方式安全地處理及/或傳輸資訊之方法，包含下列步驟：讀取及/或儲存第一被動式行動記憶體中的第一加密資訊，讀取及/或儲存與第一資訊相關的第二資訊，在電腦單元中傳送第一加密資訊以及第二加密資訊，藉由電腦單元中的第二資訊以密碼的方式處理第一資訊，其中至少部分讀取及/或儲存第一資訊的步驟及/或傳送第一資訊的步驟是以非電子的方式執行。

根據本發明所述之用來處理機密資訊的方法包含下列步驟。

先前儲存於行動記憶體中的資訊(特別是敏感資訊)係藉由資訊傳輸單元從第一行動記憶體傳送至第一電腦單

元。若資訊為數位加密，則可藉由第一電腦單元以及資訊(例如儲存於第二記憶體中的密碼的金鑰)來解密。若資訊被簽署，則必須檢查簽章。

第一行動記憶體中的資訊係藉由對稱加密系統而加密。基於此理由便可使用 AES 等型式的加密方法。簽章較佳為使用適用於電子加密之標準程序。基於此理由便可使用 RSA 或橢圓曲線數字簽名演算法(Elliptic Curve Digital Signature Algorithm, ECDSA)型式之加密方法。

讀取及/或儲存第一資訊之步驟及/或傳送第一資訊的步驟較佳為以光學的方式執行。在此方法中，傳輸係根據傳輸速度與資料安全性而執行最佳化。

根據本發明實施例所述方法之至少一步驟較佳為以數位的方式實現。數位處理的好處在於不需要 AD 轉換器即可進行處理，使得系統具有叫簡單的配置且具有較簡潔之方法。

為了使資訊只能被授權人士所存取，"讀取及/或儲存"及/或"傳送"之至少一步驟必須以加密的方式實現，以確保具有高階的資料安全性。在光學、數位處理的例子中加密可達到較高階的資料安全，因此極機密資訊亦可藉由此方法來處理。整體來說，藉由此方法可達到較高階的資料安全性。

第一資訊較佳為以光學可傳輸型式存在。再者，"讀取及/或儲存"及/或"傳送第二資訊"之步驟較佳以電性的方式實現。在任何例子中，免於未授權存取之第二資訊通常不會

儲存於行動儲存單元中，因而很容易藉由電腦單元來處理資訊。基於此理由，習知記憶體及/或處理媒體可使用於根據本發明實施例所述之相關應用系統。

本發明之優點在於第二資訊之"讀取及/或儲存"之步驟以及密碼處理可實現於一元件中。在此方法中，必須加密與解密的裝置符合節省空間的元件。

此元件因而可免於外部或第三者之存取。由於這些步驟可實現於一元件中，因此該元件也不需要提供消耗時間的傳輸媒體來傳送資料。由於整合於一元件中，因此僅需要避免對此元件作執行不必要的存取。

為了產生對資訊有效的防護與驗證，因此必須提供簽署及/或加密。基於此理由，若"讀取及/或儲存"步驟中包含"讀取以及或儲存簽署及/或金鑰資料"步驟將會是有助益的，因此簽章及/或金鑰資料可置放於許多儲存單元中(例如行動儲存單元中)。若資料係以全像的方式儲存則可達到高安全標準，因此幾乎無法讀取簽章與金鑰。

特別是當機密資訊被讀取及/或儲存為包含極化全像之全像時，由於第三者無法藉由簡單的方式讀取全像，因此因此係以光學的方式來避免不必要的操作。

再者，儲存為全像亦可有效的防護對資訊操作及/或複製。

為了儘可能管理更多使用者之資訊，較佳為對所有的

資訊提供簽章或是將資訊以對應之個別金鑰加密，且敏感資訊較佳為藉由金鑰管理裝置來管理。金鑰管理裝置為本發明之元件。

在金鑰管理中係藉由此方法來定義、選取及/或取得以及配置金鑰以及憑證至系統的不同元件，以確保安全地處理敏感資訊。再者，透過金鑰管理可確保在不需要完全交換金鑰及/或憑證的情況下將元件從系統中移除及/或將元件整合至系統中。

對於選擇金鑰與配置金鑰而言係將所有的元件群組定義為屬於一系統。這樣的系統具有複數個行動記憶體以及適用於行動記憶體之至少一讀取/寫入裝置。每個讀取/寫入裝置中包含與電腦單元結合之至少一第二記憶體類型之記憶體。

這樣的系統可以是例如一公司發放員工卡給所有的員工來存取控制應用程式。在此例子中，員工卡以及讀取/寫入裝置為屬於系統的元件。

該系統也可以是例如一銀行發放信用卡給其客戶(行動記憶體)。在此例子中，信用卡以及讀取/寫入裝置為屬於系統之元件。

對於具有全球金鑰 K 的系統來說，該金鑰係安全的儲存於第二記憶體中(系統之每個讀取/寫入裝置)。對於屬於該系統之每個行動記憶體(ID_i)係取得獨特的金鑰 $Ki = f(K,ID_i)$，其中 f 為金鑰推衍函數(key derivation function)。

機密資訊係以第一行動記憶體上之金鑰 K_i 來加密。在解密期間，以 K_i 所加密並且儲存於行動記憶體中之資訊係藉由資訊傳輸單元傳送至第一計算單元並且以設置於第二記憶體中的金鑰 K 來執行解密。

該系統亦具有由信託公司(TC)所發行之全球憑證<TC>。全球憑證<TC>包含私鑰(secret key) t。全球憑證亦儲存於系統的每個讀取/寫入裝置之第二記憶體中。每個行動記憶體 ID_i 具有一憑證$<ID_i>_t$。為了證明資訊 m 之可靠度及/或完整性，因此係藉由對應的私鑰 ki 將行動記憶體中的資訊簽署為 $S:=Sig(m,k_i)$。簽章 S 與憑證一起儲存於行動記憶體中。在簽章確認期間，資料 m、簽章 S 以及憑證$<ID_i>_t$係藉由資訊傳輸單元從行動記憶體傳送至第一計算單元。首先係藉由儲存於第二記憶體中的第一計算單元與全球憑證<TC>來驗證憑證$<ID_i>_t$。接下來，藉由憑證$<ID_i>_t$來驗證簽章 S。若所有的驗證皆成功才會接收此簽章。

根據本發明另一實施例，較高階級的單元(TC)係藉由私鑰 t 直接簽署資料 m。生物統計存取控制會對此方法感興趣。首先，較高階級的單元會檢查資訊是否被置放於所屬之行動記憶體中。在生物統計存取控制的例子中，較高階級之組織係確認生物統計資料(資訊 m)是否被置放於所屬卡擁有者之辨識卡(行動記憶體)中以及簽署是否正確。

接下來，上述適用於簽署之系統之資訊 m 係簽署為 S:=Sig(m,t)。簽章 S 與資料 m 係共同儲存於行動記憶體中，

並且可藉由<TC>來執行驗證。

可以先簽署資訊再對資料與簽署執行加密，也可以先對資料加密再簽署加密資料。

如上所述便可理解第一電腦單元係藉由傳輸通道連接至其他電腦單元。特別感興趣的是這些電腦可以結合為敏感資訊之安全傳輸。在此例子中，其他電腦單元係屬於在較高階級中稱為裝置之該系統。

系統中有對應於私鑰 g 之群組憑證<G>。群組憑證<G>係儲存於屬於系統之每個裝置。具有識別號碼 ID_i 之每個裝置皆具有藉由私鑰 g 所簽署之憑證$<ID_i, A_i>_g$，其包含屬性 A_i，可提供關於裝置類型的資訊(例如生物統計取得系統、資料庫等等)。兩個裝置係藉由加密通道互相進行通訊來交換其憑證，並藉由<G>來驗證憑證$<ID_i, A_i>_g$之簽署並且驗證其屬性。當確認簽署無誤後即建立裝置間的安全傳輸通道。

所提供的憑證$<ID_i, A_i>_g$較佳為具有有限的有效性週期(validity period)。可以以智慧卡的型式將憑證引入裝置中，以提供交換的可能性。

當憑證過了有效期限後便會更新金鑰。在以智慧卡型式將憑證引入裝置之例子中，可藉由交換裝置中的智慧卡來更新金鑰。

為了避免裝置之間交換安全性資訊，因此會將其封鎖。每個裝置包含撤銷憑證(revoked certificate)列表。這些

憑證可以為群組憑證或是裝置憑證。在群組憑證的例子中會封鎖整個裝置群組，而在裝置憑證的例子中會封鎖個別裝置。撤銷裝置之封鎖清單必須載入每個裝置中。封鎖清單係以全球憑證來簽署，例如上述之憑證<TC>。接下來會將封鎖清單與簽章 Sig(CRL,t)一起載入裝置中。因此可以將被攻擊者侵佔之裝置封鎖，使得攻擊者無法藉由所侵佔的裝置來存取資訊。

封鎖清單亦可藉由詢問中央伺服器而更新或被詢問。不論目前是否有適用於驗證之項目必須要確認，伺服器皆會執行確認。

使用本發明所述之系統及/或方法較佳為

存取控制系統，

入口(entry)控制系統，

自動現金提款機，

辨識系統，

用來管理醫療資料(例如健保卡)之系統。

【實施方式】

為讓本發明之上述和其他目的、特徵、和優點能更明顯易懂，下文特舉出較佳實施例，並配合所附圖式，作詳細說明如下：

第 1 圖顯示根據本發明實施例所述之用來處理資訊(特別是敏感資訊)之系統 1 的示意圖。系統 1 包含製造為行動儲存單元(特別是行動被動式儲存單元)之儲存單元 2。儲存單元可以為任何型式，而本發明之儲存單元為記憶卡型式(顯示為圖中對應之盒子)。在此實施例中，儲存單元 2 係以光學的方式來儲存資訊或資料。所儲存之資訊特別是包含生物統計資料及/或包含錯誤更正資料之簽章資料的機密或敏感資訊。資料係以全像及/或數位加密的方式儲存於儲存單元 2 中。

除了儲存單元 2 之外，系統 1 亦包含顯示為虛線之處理裝置 3。處理裝置 3 與儲存單元 2 之間的互動為從儲存單元 2 讀取資料或是將資料寫入儲存單元 2 中。從儲存單元 2 至處理裝置 3 之雙向箭頭係分別代表從儲存單元 2 讀取資料或是將資料寫入儲存單元 2 中。

對於從儲存單元 2 所傳送之資訊來說，處理裝置 3 包含一第一資訊傳輸單元 4，其包含一偵測單元(相機)4a 來執行信號處理。該資訊傳輸單元通常包含介於不同單元、元件等之間的所有傳輸裝置。如圖所示對應於第一資訊傳輸單元 4a 之箭頭分別表示用來傳送資訊之第一資訊傳輸單元 4 以及感測單元 4a。

再者，系統 1 包含用來以密碼的方式處理資訊之電腦單元 5。基於此目的，資料或資訊係從感測單元 4a 或是第一資訊傳輸單元 4 傳送至電腦單元 5 或是從電腦單元 5 將資料

或資訊傳送至感測單元 4a 或是第一資訊傳輸單元 4。

第 1 圖亦包含第二儲存單元 6。第二儲存單元 6 係用以防止解密並用於對應至第一資訊之第二資訊之可取回的儲存。具體而言，這些資料是進一步的安全相關資料可與第一資訊結合而提供存取或入口。第二儲存單元包含區域 6a，用來儲存對應之用以解密敏感資訊的金鑰。在此區域中可取得的資料可以為用於解密、簽章以及訊息驗證碼(message authentication code ,MAC)或是另一方面用來加密或驗證的資料。

對應至第一儲存單元 2 所讀入之相關資料係藉由安全的第二資訊傳輸單元 7 從第二儲存單元 6 或 6a 傳送至電腦單元 5。資訊傳輸單元 7 具有有效防護機制來防止攻擊者，使其無法監視交換資訊之通訊及/或操作。

在第 1 圖中所建立的電腦單元 5 係由模組 5a 與 5b 所構成。模組 5a 係處理密碼的計算，而模組 5b 係控制整個序列並且負責與其他連接元件(8,9)之間的通訊。

為了藉由行動儲存單元 2 之預期載體的個人輸入來確保進一步的防護，系統 1 係提供與行動儲存單元 2 之預期載體的外部通訊。基於此理由，系統具有適用於處理裝置之外部通訊之介面 8。

第一介面 8a 係用於輸入以及顯示輸入請求或是詢問何者是用來確認載體。此第一介面 8a 係作為顯示器。顯示器用來顯示例如輸入請求來輸入個人辨識號碼(personal

identification number, PIN)。

第二介面 8b 係藉由處理裝置 3 之使用者來輸入資訊。第二介面 8b 在此應用為藉由游標移動來控制輸入之數字輸入。處理裝置 3 之使用者可藉由此輸入單元輸入控制參數或個別資料，例如 PIN。

第一介面 8a 係單向地連接至電腦單元 5，更精確的來說是藉由安全的第二資料傳輸單元 7 連接至第二模組 5b，方向性為從第二模組 5b 至第一介面 8a。

第二介面 8b 係單向地連接至電腦單元 5，更精確的來說是藉由安全的第二資料傳輸單元 7 連接至第二模組 5b，方向性為從第二介面 8b 至第二模組 5b。

第 1 圖所示之系統 1 除了形成系統核心之行動儲存單元以及處理單元 3 之外包含其他週邊 9 或連接系統，藉由對應的連接可交換資料或資訊。因此，該週邊 9 可具有第一連接系統 9a 來取得生物統計或是用來比對資訊。基於此理由，為了傳送控制信號，第二模組 5b 係雙向地連接至第一連接系統 9a。換句話說，第二模組 5b 係藉由安全的連接而雙向地連接至第一連接系統 9a，以傳送生物統計資料以及送回驗證結果。安全連接係為無法由被攻擊者從外部存取之連接。第一連接系統 9a 可以為虹膜掃瞄裝置或是用來偵測生物統計資料之其他裝置，例如指紋、虹膜樣本以及聲音等等。

再者，週邊 9 可包含第二連接系統 9b。第二連接系統 9b 可以為包含電腦網路或是伺服器之資料庫。資料庫中可儲

存相關的資訊並且透過經過驗證之使用者來存取。第二連接系統 9b 係連接至處理裝置 3，更精確的來說是藉由安全或簡單的連接而連接至第二模組 5，因此可於兩者之間傳輸資料或資訊 M。在交換敏感資訊的例子中的連接係為安全的第二資訊傳輸單元 7。在交換較不重要的資訊之例子中可選擇簡單的第一資訊傳輸單元 4。

再者，週邊 9 可包含第三連接系統 9c。第三連接系統 9c 可以為允許經過驗證或認證之資訊或使用者來存取之入口(例如門鎖)。第三連接系統 9c 係藉由雙向連接而連接至電腦單元 5。為了避免攻擊者從外部傳送信號至作為入口之連接系統 9c 來打開入口，連接系統 9c 較佳為藉由安全的連接 7 而連接至電腦單元 5。

再者，週邊 9 可包含第四連接系統 9d。第四連接系統 9d 可以為允許詢問時間或是限時存取之時間處理裝置。第四連接系統 9d 係藉由安全的連接而雙向地連接至電腦單元 5 以傳送時間資訊。

在交換敏感資訊的例子中，連接可分別作為安全的連接或是第二資訊傳輸單元 7。在交換較不重要的資訊的例子中可選擇簡單的連接或是第一資訊傳輸單元 4。

在每個例子中，週邊 9 僅可包含連接系統 9a 至 9d 之其中一者或是上述之任何組合。

【圖式簡單說明】

第 1 圖顯示根據本發明實施例所述之藉由簽章及/或加密原則來處理資訊之系統。

【主要元件符號說明】

1 系統

2、6 儲存單元

3 處理裝置

4、7 資訊傳輸單元

4a 感測單元

5 電腦單元

5a、5b 模組

6a 區域

8、8a、8b 介面

9 週邊

9a、9b、9c、9d 連接系統

五、中文發明摘要：

本發明之目的係有關於可藉由簽章及/或加密原則以安全地處理資訊(特別是敏感資訊)之系統(1)與方法，該系統至少包含下列裝置：用以可取回地儲存第一資訊之行動被動式第一儲存單元(1)；適用於與第一儲存單元(2)互動以處理資訊之處理裝置(3)，包含：用以儲存與第一資訊相關之第二資訊之操作受到保護之第二儲存單元(6)；用以密碼地(cryptographically)處理資訊之計算單元(5)；用以於第一及/或第二儲存單元(2,6)與計算單元(5)之間傳送資訊之資訊傳輸單元(4)。

六、英文發明摘要：

The subject matter of the invention relates to a system (1) and to a method for securely processing information, particularly sensitive information by means of a signature and/or encryption principle, comprising at least the following: a mobile passive first storage unit (1) for retrievably storing first information, a processing device (3) which is adapted for interacting with the first storage unit (2) in order to process information, comprising: a decryption-protected second storage unit (6) for retrievably storing second information corresponding to the first information, a computer unit (5) for (cryptographically) processing information, an information transmission unit (4), for transmitting the information of the first and/or the second storage unit (2,6) to the computer unit (5).

十、申請專利範圍：

1.一種藉由簽章及/或加密原則以安全地處理資訊之系統(1)，至少包含：

一行動被動式第一儲存單元(2)，用一清楚的識別號碼 IDS_i 以可取回地儲存一第一資訊，其中索引 i 係指出屬於上述系統(1)之上述第一儲存單元(2)的號碼，

一處理裝置(3)，適用於與上述第一儲存單元(2)互動，以處理資訊，包含：

一清楚的識別號碼 IDV_n，其中索引 n 係指出屬於上述系統(1)之上述處理裝置(3)的號碼，

一操作受到保護之第二儲存單元(6)，無法從外部讀取，以安全地儲存對應至上述第一資訊之一第二資訊，

一計算單元(5)，以密碼的方式來處理資訊，

一資訊傳輸單元(4)，用以從上述第一及/或第二儲存單元(2,6)傳送資訊至該計算單元(5)，以及於上述處理裝置(3)與連接的週邊(9)之間傳送資訊；

其中，該資訊為敏感資訊。

2.如申請專利範圍第 1 項所述之系統(1)，其中：

至少一上述儲存單元(2,6)係作為一光學儲存單元，較佳為卡式之全像儲存單元，資訊可以光學地(較佳為全像地)儲存於其中及/或光學地(較佳為全像地)取得其中的資訊，

至少一上述資訊傳輸單元(4)係作為一光學資訊傳送單元，以藉由至少一光束徑來傳送資訊。

3.如申請專利範圍第 1-2 項中任一項所述之系統(1)，其中

上述計算單元(5)係以智慧卡或是晶片卡的方式整合於上述第二儲存單元(6)中。

4.如申請專利範圍第 1-3 項中任一項所述之系統(1)，其中：

一(全球)密碼的金鑰 K 係儲存於無法由外部讀取之上述操作受到保護之第二儲存單元(6)，

資訊 m 係藉由金鑰 K_i 加密儲存於上述第一儲存單元(2)之其中一者，其中上述金鑰可藉由一金鑰推衍函數 $f:K_i=f(K,IDS_i)$從上述第二儲存單元(6)中的金鑰 K 而唯一地取得。

5.如申請專利範圍第 1-3 項中任一項所述之系統(1)，其中：

一私鑰 t 所歸屬之一(全球)憑證<TC>係儲存於無法由外部讀取之上述操作受到保護之第二儲存單元(6)，

在屬於上述系統之至少一第一儲存單元 IDS_i(2)中，從上述全球憑證<TC>所取得之一憑證$<IDS_i>_t$ 係儲存於一私鑰 k_i 所屬之處，

在屬於上述系統之至少一第一儲存單元 IDS_i(2)中，係儲存有藉由上述金鑰 k_i 根據資訊 m 所產生之一簽章 S，$S:=Sig(m,k_i)$。

6.如申請專利範圍第 1-3 項中任一項所述之系統(1)，其中：

一私鑰 t 所歸屬之一(全球)憑證<TC>係儲存於無法由外部讀取之上述操作受到保護之第二儲存單元(6)，

在屬於上述系統之至少一第一儲存單元 $IDS_i(2)$中，係儲存有藉由上述金鑰 k_i 根據資訊 m 所產生之一簽章 S，S:=Sig(m,t)。

7.如申請專利範圍第 4 項所述之系統(1)，其中：

一私鑰 t 所歸屬之一(全球)憑證<TC>係儲存於無法由外部讀取之上述操作受到保護之第二儲存單元(6)，

在屬於上述系統之至少一第一儲存單元 $IDS_i(2)$中，從上述全球憑證<TC>所取得之一憑證$<IDS_i>_t$ 係儲存於一私鑰 k_i 所屬之處，

在屬於上述系統之至少一第一儲存單元 $IDS_i(2)$中，係儲存有藉由上述金鑰 k_i 根據以 K_i 所加密之上述資訊所產生之一簽章 S。

8.如申請專利範圍第 4 項所述之系統(1)，其中：

一私鑰 t 所歸屬之一(全球)憑證<TC>係儲存於無法由外部讀取之上述操作受到保護之第二儲存單元(6)，

在屬於上述系統之至少一第一儲存單元 $IDS_i(2)$中，係儲存有藉由上述金鑰 k_i 根據以 t 所加密之上述資訊所產生之一簽章 S。

9.如申請專利範圍第 1-3 項中任一項所述之系統(1)，其中：

一(全球)密碼的金鑰 K 係儲存於無法由外部讀取之上述操作受到保護之第二儲存單元(6)，

一私鑰 t 所歸屬之一(全球)憑證<TC>係儲存於無法由外部讀取之上述操作受到保護之第二儲存單元(6)，

一私鑰 k_i 所歸屬且從上述全球憑證<TC>所取得之一憑證 $<IDS_i>_t$ 係儲存於屬於上述系統之至少一第一儲存單元 $IDS_i(2)$，

一唯一金鑰 K_i 係藉由上述金鑰推衍函式 f 根據適用於屬於上述系統之至少一上述第一儲存單元 $IDS_i(2)$之上述密碼的金鑰 K 而產生：$K_i=f(K,IDS_i)$，

一簽章 S 係藉由一金鑰 k_i 根據上述資訊 m 而產生 $S:=Sig(m,k_i)$，上述簽章係藉由上述金鑰 K_i 來加密且設置於屬於上述系統之至少一上述第一儲存單元 $IDS_i(2)$中。

10.如申請專利範圍第 1-3 項中任一項所述之系統(1)，其中：

一(全球)密碼的金鑰 K 係儲存於無法由外部讀取之上述操作受到保護之第二儲存單元(6)，

一私鑰 t 所歸屬之一(全球)憑證<TC>係儲存於無法由外部讀取之上述操作受到保護之第二儲存單元(6)，

一唯一金鑰 K_i 係藉由上述金鑰推衍函式 f 根據適用於屬於上述系統之至少一上述第一儲存單元 $IDS_i(2)$之上述密碼的金鑰 K 而產生：$K_i=f(K,IDS_i)$，

一簽章 S 係藉由一金鑰 k_i 根據上述資訊 m 而產生 $S:=Sig(m,t)$，上述簽章係藉由上述金鑰 K_i 來加密且設置於屬於上述系統之至少一上述第一儲存單元 $IDS_i(2)$中。

11.如申請專利範圍第 1-10 項中任一項所述之系統(1)，其中：

具有對應私鑰 g 之一群組憑證<G>係適用於一些(至少兩

個)處理裝置(3)及/或連接的週邊(9)之元件的群組，上述私鑰 g 係儲存於屬於該群組之上述處理裝置/元件，

對於屬於上述群組之上述連接的週邊(9)之每個上述處理裝置(3)及/或元件，皆具有藉由上述私鑰 g 所簽署之一憑證 $<IDV_n,A_n>_g$，上述憑證 $<IDV_n,A_n>_g$ 係儲存於屬於該群組之每個處理裝置及/或元件中，其中 A_n 代表可提供處理裝置及/或元件的特性之資訊的屬性，

在屬於上述群組之上述連接的週邊(9)之每個上述處理裝置(3)及/或元件中，係儲存一撤銷憑證列表，上述列表係藉由憑證<TC>來簽署並且此簽章亦儲存於屬於該群組之每個處理裝置及/或元件中。

12.一種藉由申請專利範圍第 1 至 11 項中任一項所述之系統(1)以用於安全的(密碼的)處理/操作/傳送資訊之方法包含下列步驟：

藉由一資訊傳輸單元(4)將一資訊從一第一行動儲存單元(2)傳送至系統(1)之處理裝置(3)之其中一者，

若所傳送的上述資訊為加密資訊，則藉由儲存於上述操作受保護之第二儲存單元(6)中的金鑰 K 來解密，

若具有憑證 $<IDS_i>_t$，則藉由儲存於上述操作受保護之第二儲存單元(6)中的憑證<TC>來檢查憑證 $<IDS_i>_t$，

若具有簽章 $S:=Sig(m,k_i)$，則藉由上述憑證 $<IDS_i>_t$ 來檢查簽章 $S: =Sig(m,k_i)$，

若具有簽章 $S: =Sig(t,k_i)$，則藉由上述憑證<TC>來檢查簽章 $S: =Sig(t,k_i)$，

藉由一資訊傳輸單元(4)將資訊從上述系統(1)傳送至上述連接的週邊(9)。

13.如申請範圍第 12 項所述之方法，其中：

在交換敏感資訊之前，上述處理裝置(3)以及上述週邊(9)先透過應用程式<G>來交換並驗證其憑證<IDV_n,A_n>$_g$，

在交換敏感資訊之前，上述處理裝置(3)以及上述週邊(9)係藉由該撤銷憑證列表來檢查其他憑證的有效性，

在上述處理裝置(3)與週邊(9)之間的傳送較佳以加密及/或保護的方式進行。

14.如申請專利範圍第 1 至 11 項中任一項所述之系統(1)及/或如申請範圍第 12 項所述之方法，係使用於：

存取控制系統，

入口控制系統，

自動現金提款機系統，

辨識系統，

管理醫療資料的系統。

七、指定代表圖：

(一)本案指定代表圖為：第（1）圖。

(二)本代表圖之元件符號簡單說明:

1 系統

2、6 儲存單元

3 處理裝置

4、7 資訊傳輸單元

4a 感測單元

5 電腦單元

5a、5b 模組

6a 區域

8、8a、8b 介面

9 週邊

9a、9b、9c、9d 連接系統

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無