

國籍：(中文/英文) 1-2 韓國/KR

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：

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。

國籍：(中文/英文) 1-2 韓國/KR

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：

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】

本發明是關於一種具有標籤讀取功能的行動通訊終端和提供真實產品鑑定服務的方法，且特別是有關於能透過讀取和顯示附加在不同品牌產品上的標籤資訊而確定產品的真偽並提供關於產品的資訊的行動通訊終端，以及一種提供真實產品鑑定服務的方法，其中關於產品真偽的資訊由用戶透過解密儲存在標籤裡的資訊並輸出解密過的資訊而得到。

【先前技術】

日本專利申請案早期公開第 Hei 14-215749 號和第 Hei 14-209692 號公開技術，利用電子記錄在標籤上的產品資訊來識別產品資訊和實現採買、貨品的管理，以非接觸的模式進行通訊，便攜式標籤讀取器讀出記錄在標籤裡的資訊。但是，由於這些技術不涉及產品真偽的確定，資訊的記錄或讀出非常薄弱，有可能有偽造資訊或假造資訊的記錄。

如另一個習知的途徑，韓國專利第 2002-85144 號和日本專利申請案早期公開第 Hei 13-354310 號和第 Hei 13-341810 號公開的網路類型的真偽確定系統，讀出電子記錄在非接觸通訊標籤上的產品資訊，透過如網際網路的通訊網路，參照產品管理數據庫，確定相應產品的真偽。但是，為了使用網路類型的系統，在透過有線通訊網與產品管理數據庫交換數據的情況下，標籤讀取器必須製造成

桌上型電腦(desktop)的形式。結果是，為了確定產品的真偽，必須訪問指定的地點。還有，在透過無線通訊網與產品管理數據庫交換數據的情況下，隨著標籤讀取器大小的增加，標籤讀取器變得不方便攜帶，標籤讀取器的成本價增加，每次用標籤讀取器時，用無線通訊網路都要收費。此外，標籤讀取器生產成桌上型電腦的形式，由於產品的真偽只能在指定的地點確定，所以產品的真偽不能在購買前確定。

如另一個習知的途徑，日本專利申請案早期公開第 Hei 12-348148 號和第 Hei 12-148950 號公開的技術，其中標籤讀取器透過讀出電子記錄在非接觸通訊標籤上的產品資訊，並將讀出的資訊與以前儲存在其中的參考數據（產品號、生產日期、產品生產品牌名、管理歷史資訊、產品描述）進行比較，來確定產品的真偽。但是，這種離線類型的鑑定設備解決了網路類型系統的問題，卻由於標籤讀取器事先必須儲存每樣產品的所有產品資訊，記憶體容量增加了。另外，由於標籤讀取器自己確定產品的真偽，只提供自己確定的結果，用戶不能直接檢查鑑定過程的資訊，鑑定過程的可靠性就低了。換句話說，這個習知的標籤讀取器只考慮到產品批發商的角度，沒有滿足產品購買者的需求。另外，這個習知的標籤讀取器的問題是：在購買標籤讀取器後發行的新產品和新加入公司的產品不能確定出真偽，或者必須更新已經發行的標籤讀取器的產品資訊。再有，上述習知的途徑沒有考慮到標籤被從產品上揭

下來貼到偽造的產品上的情形。

為了解決這些問題，韓國專利第 2001-89216 號，韓國實用新型註冊號 252202，和日本專利申請案早期公開第 Hei 12-251164 號公開的真偽確定設備，包括非接觸通訊標籤和標籤讀取器，附在產品上的產品資訊儲存在標籤中。此真偽確定設備可以防止標籤的再使用，辦法是，如果標籤被揭離原產品，其天線就被損壞。但是，這些習知真偽確定設備的應用僅侷限於特殊的產品，諸如瓶裝產品，並且為了防止標籤的毀壞，可能需要進行事先測量。另外，由於標籤本身被毀壞，即使是生產者也不能讀出標籤的讀取歷史資訊，不能把標籤的讀取歷史資訊用於消費者傾向的銷售。

【發明內容】

本發明提供了一種能確定產品真偽的行動通訊終端，它把從非接觸通訊標籤收到的資訊解密，並輸出解密過的資訊。

本發明也提供了一種產品真實鑑定服務的方法，其中關於產品真偽的資訊由用戶透過對儲存在標籤裡的資訊解密並輸出解密的資訊而得到。

在本發明的一方面，提供了一種行動通訊終端，其接收來自非接觸通訊標籤的資訊。行動通訊終端包括第一通訊單元，與非接觸通訊標籤無線地交換數據，並無線地發送非接觸通訊標籤需要的電能；第二通訊單元，透過無線通訊網向服務管理伺服器發送和接收數據；儲存單元，儲

存至少一個密鑰相關資訊；解密單元，基於密鑰相關資訊，把從非接觸通訊標籤收到的數據解密，該密鑰相關資訊是透過接收自非接觸通訊標籤的密鑰說明資訊而從密鑰相關資訊中選出的；資訊讀取設備，向附在產品上的非接觸通訊標籤要求產品資訊，並讀出來自非接觸通訊標籤的產品資訊；輸出單元，輸出讀出的產品資訊。

在本發明的另一個方面，提供了管理產品鑑定服務的方法，適用在產品鑑定服務管理伺服器裡。該產品鑑定服務管理伺服器透過網路與行動通訊公司的用戶伺服器通訊，並可透過行動通訊網與行動通訊終端通訊。該方法包括：接收讀取細節資訊，包括分發給每個標籤可被讀取的產品的產品識別號，和從行動通訊終端分發給行動通訊終端的讀取器識別號；詢問用戶伺服器查詢含在讀取細節資訊裡基於行動通訊終端的識別號的用戶資訊，並接收來自用戶伺服器的用戶資訊；創建與儲存客戶管理資訊，包括基於讀取細節資訊與用戶資訊的用戶分類資訊與產品資訊讀取細節；回應從外部設備輸入的資訊輸出請求而讀出並輸出客戶管理資訊。

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

【實施方式】

圖 1 是根據本發明解釋其工作的概觀。

參照圖 1，根據本發明，具有標籤讀取功能的行動通

訊終端 20-1 和 20-2，讀出非接觸通訊標籤 10-1、10-2 和 10-3 的資訊，顯示讀出的資訊。非接觸通訊標籤 10-1、10-2 和 10-3 附在諸如服裝、鞋類、皮革製品、飲料、農產品 & 家畜物品、毒品 & 藥品、電子產品、機械產品、首飾、工藝品、估價報告書、入場券、證書、用於設備、錢、銷售的有價証券、重要文件的票據等的各種產品上。

非接觸通訊標籤 10-1、10-2 和 10-3 是正方形、薄膜類型的被動標籤，每個寬度和長度是 10~18 毫米。

標籤讀取器安裝在行動通訊終端 20-1 和 20-2 裡。帶有行動通訊終端 20-1 和 20-2 的人可以基於行動通訊終端 20-1 和 20-2 顯示單元裡顯示的產品資訊、透過將他們的行動通訊終端 20-1 和 20-2 靠近產品來確定商標的真偽。換句話說，當個人把他的行動通訊終端靠近一個陌生的飲料標籤，如果這個陌生的飲料是真實的，真實產品代碼 '7' 會顯示在行動通訊終端的顯示單元上；當個人把他的行動通訊終端靠近一個皮革錢包，如果這個皮革錢包是偽造品，就輸出一個偽造品警告消息（如“錯誤”或預定的某種聲音）而不是真實產品代碼 '9'。另一方面，根據讀取結果可輸出信號聲或語音消息。例如，如果檢測到一個非法標籤，行動通訊終端重複地多次輸出短脈波音調。如果成功地讀出產品代碼，行動通訊終端發出短的讀取聲音，同時顯示輸出單元裡讀出的產品代碼。還有，行動通訊終端可混合輸出讀出的產品代碼和語音。如果產品代碼限於一個數字的話，語音數據量不大，可儲存在低容量的

記憶體裡。進而，還可以用一種顏色來代表產品代碼。這種情況下，只要在真實產品上標記顏色碼，打印在貼有標籤的產品上。標籤讀取器從標籤上讀出顏色碼，透過多個發光二極體（LED）的開／關組合顯示讀出的結果，例如，根據讀出的顏色碼，有紅、綠、黃、藍色。當檢測到有非法標籤時，行動通訊終端可透過用預定的顏色模式輸出錯誤消息來表示偽造標籤或壞標籤。

另外，行動通訊終端讀取一次，在行動通訊終端的顯示單元上會多次連續地顯示產品代碼。在行動通訊終端的顯示單元上連續地顯示的產品代碼對應於產品資訊，包括生產商、產業類型、品牌與產品名裡的至少一項。貼有標籤的產品都有表格，寫有對應於產品標籤每項的產品資訊。如果標籤讀取器靠近一個標籤，多個產品代碼按表格的順序連續顯示。例如，根據本發明，具有標籤讀取功能的行動通訊終端靠近一個貼有標籤的陌生的飲料，首先顯示的是產品代碼‘7501’，基於第一個表—產品類型表的項目，可識別出這是一種飲料類產品。其次，按預定的時間間隔顯示數據‘0014’，基於列印在產品上的另一個表—商標表的項目，識別出此產品的商標是‘Valentine’。然後，按預定的時間間隔顯示數據‘0017’，基於列印在產品上的又一個表—老化年齡表的項目，可識別出此產品的新舊是‘17年’。

根據本發明的行動通訊終端 20-1 和 20-2 可把從標籤讀出的資訊讀取細節透過行動通訊網，發送到真實產品鑑

定服務管理伺服器 40（以下，稱作服務管理伺服器 40）。資訊讀取細節包括：分發給每個標籤可讀取的產品的產品識別號，和分發給每個行動通訊終端 20-1 和 20-2 的讀取器識別號。資訊讀取細節也包括真實產品詳細鑑定資訊，如產業類型、生產商、品牌、等級、式樣名、生產中心、生產日期、序列號、價格與鑑定日期。資訊讀取細節還可包括已鑑定真偽的產品中已售出產品的有關購買資訊。購買資訊除了真實產品詳細鑑定資訊之外，可包括購買價格、購買日期與時間。

在收到來自行動通訊終端 20-1 和 20-2 的讀取細節資訊（步驟①和②）後，服務管理伺服器 40 可把含在接收到的讀取細節資訊裡的行動通訊終端 20-1 和 20-2 的識別資訊提交給行動通訊公司的用戶伺服器 30（步驟③），而得到相應用戶的個人資訊。透過利用服務管理伺服器 40 的這種功能，批發商可進行更精確的客戶管理。換句話說，諸如用戶的性別、年紀、位址、學術成就、工作與愛好等的詳細個人資訊由行動通訊公司儲存在用戶伺服器 30 裡。服務管理伺服器 40 可透過收集接收的讀取細節資訊和這些用戶資訊，分析指定年齡人群的購買傾向，有指定工作的人群的購買傾向或產品偏好。這些資訊可提供給其產品被鑑定為真實的生產商，作為市場資訊。服務管理伺服器 40 把收集的資訊儲存為客戶管理資訊，生成報告，根據產品被鑑定為真實的生產商或鑑定服務管理公司的請求，輸出此報告。另外，服務管理伺服器 40 有時也生成此報告，並

把它發送給品牌擁有人伺服器 50，透過網路與之通訊（步驟④）。這種生成市場報告的技術在此領域眾所周知，就不再詳述。

這種資訊的收集可在採買完成後或真實產品鑑定後，有規律或無規律地由用戶操作手動進行。透過在行動通訊終端裡安裝指定的應用程式，這種上傳過程可在用戶沒注意到它時進行。指定的應用程式監控累積資訊的總量和通訊狀態，在語音通訊或數據通訊期間，把指定的數據通道分發給指定的應用程式，指定的應用程式發送累積的讀取細節資訊。還有，指定的應用程式監控累積資訊的總量，如果累積資訊的總量達到預定量，指定的應用程式把累積的資訊以純文字形式發給服務伺服器。

服務管理伺服器 40 可進一步包括‘積分點’資訊作為用戶管理資訊。換句話說，服務管理公司儲存積分點作為給用戶幫助收集採買資訊的獎勵。由於積分點是累積的，服務管理公司提供產品給用戶，或透過把積分點轉換成電子貨幣而允許用戶使用儲存的積分點來採買產品，或附屬公司裡的目錄。這種積分點的儲存是透過根據由服務管理伺服器 40 接收的讀取細節資訊的種類和內容來處理相應用戶的儲蓄實現的。例如，根據已購買的產品價格或根據生產商或產品名累積的積分點可能不同。

另外，服務管理伺服器 40 能透過檢測含在讀取細節資訊裡的產品資訊識別號和讀取器識別號是否與先前收到的產品讀取細節資訊一致，來附加檢測收到的產品讀取細節

資訊是否是重發的細節資訊。換句話說，為了防止客戶透過重複發送採買細節資訊來試圖累積積分點，服務管理伺服器 40 鑑定以完全文字形式發送的採買細節資訊。行動通訊終端 20-1 和 20-2 在發送採買細節資訊時，發送標籤讀取器的識別號和讀取標籤的識別號。服務管理伺服器 40 透過忽略標籤讀取器識別號與標籤識別號相同的採買細節資訊，來防止同一個採買細節資訊的重複及積分點的累積。

圖 2 表明根據本發明的非接觸通訊標籤的架構。在下面的描述裡，標籤讀取器的概念包括具有標籤讀取功能的行動通訊終端。

參照圖 2，根據本發明的較佳實施例的非接觸通訊標籤 10 包括非接觸通訊裝置 100、控制單元 200、儲存單元 300。

非接觸通訊裝置 100 以無線模式與標籤讀取器 20 交換數據，從接收的無線信號裡提取能量成分，把提取出的能量提供給整個系統作為其能源。控制單元 200 把儲存在儲存單元 300 裡的產品資訊加密成密鑰，把密鑰透過非接觸通訊裝置 100 輸出到外部設備。產品資訊和密鑰儲存在儲存單元 300 裡。

非接觸通訊裝置 100 包括天線 110、能量供給單元 131、解調單元 133 與調變單元 135。天線 110 以無線模式把資訊發送給標籤讀取器 20 且從它接收資訊。能量供給單元 131 透過處理從天線 110 接收的信號中的能量電波信號，給非接觸通訊標籤 10 提供能源。解調單元 133 解調從

標籤讀取器 20 收到的信號。調變單元 135 把要發送到標籤讀取器 20 的信號進行調變。天線 110 是印刷圖案或線圈沿著標籤周遭形成的。由於調變單元 135 和解調單元 133 對於那些很熟悉此技藝者是眾所周知的，就不詳述。由於根據本發明的非接觸通訊標籤 10 必須生產的很小很薄，希望把非接觸通訊標籤 10 生產成被動形式。因此，能量供給單元 131 從標籤讀取器 20 接收的無線信號提取能量成分，把提取的能量成分提供給整個系統作為其能源。能量供給單元 131 的工作和架構是眾所周知的，就不詳述。

儲存單元 300 包括非易失性(nonvolatile)半導體記憶體，像電子可抹除可編程唯讀記憶體 (Electrical Erasable Programmable Read-Only Memory, EEPROM) 或快閃唯讀記憶體(flash ROM)，在沒有能源時，也可保存數據。儲存單元 300 實際上可包括兩個記憶體，如唯讀記憶體和讀／寫記憶體。但是，在本發明的較佳實施例裡，儲存單元 300 包括單個可讀／可寫非易失性記憶體。關於貼標籤的產品的產品資訊 370，如產業類型、生產商、品牌、產品名、等級、式樣名、生產中心、生產日期、交貨日期與序列號，以數據儲存在儲存單元 300 裡。儲存單元 300 也儲存非接觸通訊標籤 10 和標籤讀取器 20 之間通訊加密所需要的密鑰 330。儲存單元 300 還儲存密鑰說明資訊 310，該資訊是在標籤讀取器端詳細說明密鑰 330 所需要的。儲存單元 300 更包括計數區，儲存非接觸通訊標籤 10 的產品資訊被標籤讀取器 20 讀取的次數。儲存單元 300 可儲存與執行讀操作

的標籤讀取器 20 有關的資訊和讀取細節資訊，如讀取日期和時間。

儲存在儲存單元 300 裡的產品資訊 370 可以以產品代碼的形式出現，該產品代碼由數字的組合、顏色的組合或字母的組合而組成。由數字的組合而組成的產品代碼輸出到標籤讀取器 20 的顯示單元。產品代碼還可以由按順序排列的二進制碼和／或顏色碼組成。可以只有單個產品代碼儲存在儲存單元 300 裡，但多個產品碼也可以儲存在儲存單元 300 裡並連續地被讀出、顯示。這時，產品代碼可事先根據生產商、品牌、產業類型、產品名確定。因此，擁有代碼表的用戶可以透過連續顯示的產品碼得到產品資訊，如生產商、品牌、產業類型、產品名。

根據本發明，控制單元 200 控制非接觸通訊標籤 10 的整個系統，它僅由硬體實現，主要是狀態機等數位邏輯電路，如基於正反器(flip-flop)和閘極(gate)設計的特定用途積體電路 (Application Specific Integrated Circuit, ASIC)。這種電路可由那些很熟悉此技藝者，在通用各種計算機輔助設計 (Computer Aided Design, CAD) 工具的支持下很容易地實現，此處不再詳述。由於未使用附加的儲存主程式，可避免包括非易失性記憶體保存期限的問題。有時在這種情況下，那些可能因標籤而變化的產品資訊或密鑰相關資訊也可以作為數據儲存在非易失性記憶體裡。關於保存期限限制的對策在後面描述。當然，本發明不侷限於僅適於數位邏輯的硬體，控制單元 200 還可用微處理器實現。本

發明特有的功能也可透過軟體控制來實現。這時候，主程式額外地儲存在儲存單元 300 裡。在本發明的另一個實施例裡，儲存單元 300 實際上包括兩個記憶體，包含主程式的部分可儲存在單獨的記憶體裡。

控制單元 200 包括加密／解密單元 210、資訊提供單元 250、重送(replay)攻擊防止單元 230 與後管理(post management)處理單元 270。這些部件的每一個均可獨立於控制單元 200，重送攻擊防止單元 230 和後管理處理單元 270 可選擇放在控制單元 200 裡。加密／解密單元 210 把從非接觸通訊裝置 100 裡收到的信號進行解密，或給要發送的信號加密，把加密過的信號輸出到非接觸通訊裝置 100。

資訊提供單元 250 讀出儲存在儲存單元 300 裡的產品資訊 370，把讀出的產品資訊 370 提供給加密／解密單元 210。資訊提供單元 250 還讀出儲存在儲存單元 300 裡的產品資訊 370，回應來自標籤讀取器 20 的讀取命令，透過非接觸通訊裝置 100 輸出讀出的產品資訊 370。每次讀出產品資訊 370 時，資訊提供單元 250 把儲存單元 300 的計數值增加 1，並在讀出產品資訊 370 前，檢測儲存單元 300 的計數值。如果計數值多於預定值，資訊提供單元 250 不回應來自標籤讀取器 20 的讀取命令，或輸出表明標籤被不適當地多次讀取的消息，而不輸出產品資訊 370。但是，在此情況下，計數值在內部被連續地增加並記錄。計數值可由管理員攜帶的特殊讀取器檢測。

透過這種對標籤被讀取次數的管理，可以有效地防止標籤被重複使用，例如從真實產品上揭下來貼到偽造產品上，或從用過的真實產品分離出廢棄的標籤貼到偽造產品上。另外，透過把計數值儲存在外部無法訪問的區域、檢測儲存的計數值，可有效地防止標籤被重複使用，與物理的方法相比沒有額外的費用。如果把標籤用很牢的粘合劑附在產品上，當標籤被從產品上揭下來時，可採用物理阻止方法，如毀壞印刷圖案的天線。但是，這種方法就不可能進行標籤資訊的後管理或為了使用標籤而訪問標籤。這種方法開始還不能防止試圖仔細地把標籤從產品上揭下來。另外，在大規模生產時也有困難。

由於放在顯示台上的產品被標籤讀取器讀取很多次，當真正需要確定產品真偽時，可能無法讀出附在產品上的標籤。為了解決這個問題，最好在標籤暴露的表面放一個覆蓋膜，防止在交貨時讀取標籤。保護膜可以是鋁薄膜之類的，透過蓋在標籤暴露的表面而阻止無線通訊。當需要確定真偽時，從標籤上揭去覆蓋膜。

計數器的讀取次數限制的參考值可以根據不同產品設置成不同值。例如，在諸如陌生的飲料、農產品&家畜產品此類的食品裡，考慮到標籤可能在交貨時讀一次，在使用時讀2~4次，希望計數器的讀取次數限制參考值限在3~5次。對於服裝類，由於真實產品的鑑定在銷售時和採買後可能進行多次，希望計數器的讀取次數限制參考值限在幾十次。用這種方法，讀取次數限制參考值可大致根據

產品特徵或發行管道的步驟數設置。但是，本發明不侷限於檢測計數器的計數值去限制讀取的實施例，例如，至於把標籤附在著名的畫、古董或文件上時，讀取次數可不受限制。在這種情況下，資訊提供單元 250 讀出儲存在儲存單元 300 裡的產品資訊 370，透過非接觸通訊裝置 100、回應來自標籤讀取器 20 的讀取命令輸出讀出的產品資訊 370，每次讀產品資訊 370 時，儲存單元 300 的計數值增加。在這種情況下，資訊提供單元 250 不限制基於計數值的資訊提供。

在用產品碼連續顯示產品資訊 370 的實施例裡，資訊提供單元 250 可根據來自標籤讀取器 20 的請求，或者一次給標籤讀取器 20 提供多個產品碼，或者連續多次提供多個產品碼的一個。當資訊提供單元 250 多次連續提供產品碼時，每個數據都要使用加密／解密方法和重送攻擊阻止。

加密／解密單元 210 把要發送的資訊透過非接觸通訊裝置 100 加密，把從非接觸通訊裝置 100 接收的資訊解密。使用三數據加密標準（3-Data Encryption Standard, 3-DES）算法作為加密算法，但是加密算法不侷限於三數據加密標準算法。三數據加密標準算法三重地應用數據加密標準，採用各種形式。在本實施例裡，採用層疊三數據加密標準，連續地用三個密鑰。由於這些算法都是對稱的密鑰算法，相同的密鑰用於加密和解密。

根據習知的真偽產品鑑定方法，真偽產品鑑定包括：把內在的鑑定碼儲存在標籤裡，透過從讀取器讀出內在的

鑑定碼，確定內在的鑑定碼是否是對應於真實產品的代碼。而根據本發明，真實產品鑑定依靠人工，根據在讀取器的顯示單元上顯示的資訊來判斷，必須經歷加密／解密過程才能正確顯示產品資訊。

在根據本發明的非接觸通訊標籤 10 的第一實施例裡，產品資訊由唯一的萬能鑰匙(master key)加密和解密。這種情況下，萬能鑰匙 330 作為各種產品的公共唯一密鑰，儲存在非接觸通訊標籤 10 的儲存單元 300 裡。標籤讀取器也有單個唯一的密鑰，但可以讀取各種產品的產品資訊。加密／解密單元 210 由資訊提供單元 250 利用萬能鑰匙 330 作為加密密鑰，把發送到外部設備的資訊加密，解釋從外部設備接收的加密過的消息，把解釋過的消息提供給資訊提供單元 250。由於產品可被顯示在標籤讀取器 20 上的產品資訊透過加密／解密單元 210 的操作而識別，所以可提供許多產品的真偽資訊。此外，如果用在新產品的標籤是新製的，則不需升級已存在的標籤讀取器就可讀出標籤資訊。

在根據本發明的非接觸通訊標籤 10 的第二實施例裡，作為單個密鑰的萬能鑰匙 330 和適合於萬能鑰匙 330 的密鑰說明資訊 310 都儲存在非接觸通訊標籤 10 的儲存單元 300 裡。使用非接觸通訊標籤 10 的公司準備多個密鑰，根據產業類型、生產商、品牌及產品類型進行不同分發。例如，在主要為商標的情況下，可根據同一品牌的產品類型決定使用不同的密鑰。在生產少量產品的公司裡，可給

公司指定單個的密鑰。讀取相應產品標籤所需的全部密鑰含在標籤讀取器 20 裡。

當收到來自標籤讀取器 20 的產品資訊請求，加密／解密單元 210 把密鑰說明資訊 310 發送到標籤讀取器 20，使標籤讀取器 20 選擇同樣的密鑰作為密鑰 330 儲存在標籤讀取器 20 裡。例如，密鑰說明資訊 310 可以是分發給多個密鑰的索引。其後，加密／解密單元 210 把要發送到外部設備的資訊由資訊提供單元 250 利用這個密鑰進行加密，解釋從外部設備接收的加密過的消息，把解釋過的消息提供給資訊提供單元 250。

同樣的，透過利用密鑰說明資訊 310，儘管一些密鑰被洩漏，損失只限於相應的產業類型、生產商、品牌或相應的產品。還有，與使用唯一的萬能鑰匙的實施例一樣，包括同樣的密鑰，而不需把已有的標籤讀取器升級。當然，也有可能又需要組合新標籤並儲存新的產品資訊。還有，如果足夠量的密鑰被保護在標籤讀取器裡，可以透過分發多餘的密鑰，給新產品設置更高級的安全性。換句話說，當生產新標籤時，透過儲存一個被作為多餘密鑰而保護的密鑰，和對應此密鑰的索引，標籤讀取器接收索引，可指定一個密鑰，把它作為多餘密鑰、作為新標籤的密鑰而被保護。

在根據本發明的非接觸通訊標籤 10 的第三實施例裡，基於產業類型、生產商、品牌、商標各要素之中至少兩個要素，兩個或更多密鑰 330 被分隔分發，和對應於密

鑰 330 的密鑰說明資訊 310 都儲存在非接觸通訊標籤 10 的儲存單元 300 裡。

圖 4A 根據本發明的非接觸通訊標籤 10 的第三實施例，表明示範密鑰 410 和示範密鑰說明資訊 420。參照圖 4A，儲存在非接觸通訊標籤 10 裡的密鑰 410 包括三個密鑰 411、413 與 415，每個是根據產業類型、生產商與品牌而確定。全部的密鑰 433、453 與 473 及其對應的密鑰說明資訊索引 431、451 與 471 都儲存在標籤讀取器 20 裡。標籤讀取器 20 的密鑰分成三組，每組是一個密鑰分發表，用於一個產業類型、生產商與品牌。例如，多個密鑰 411、413 與 415 可以是用在三數據加密標準算法每一步的三個密鑰。

當收到來自標籤讀取器 20 的產品資訊請求，非接觸通訊標籤 10 的加密／解密單元 210 把密鑰說明資訊 310 的索引，如 02、01 和 04 發送到標籤讀取器 20。標籤讀取器 20 從索引裡查閱相應的密鑰表，選擇與儲存在非接觸通訊標籤 10 裡的密鑰 410 一樣的密鑰組，如 1324、abcd 和 2345，作為密鑰用來讀取當前的非接觸通訊標籤 10。隨後，非接觸通訊標籤 10 的加密／解密單元 210 透過連續地使用多個密鑰把要發送到和接收自標籤讀取器的資訊加密、解密。

一旦指定密鑰，標籤讀取器 20 可識別出密鑰所屬的產業類型、生產商、品牌或產品名。就是說，在圖 4A 裡，標籤讀取器 20 能從收到的密鑰索引 421、423 與 425 裡識別出貼有標籤 10 的產品是包括在：附件類型、生產商是

‘Sam—Ah 產業’、商標是 ‘CAPACCI’ 的產品類型裡。因此，儲存在儲存單元 300 裡的產品資訊 370 和密鑰說明資訊 310 在實用中可部分互相重疊。換句話說，索引 421、423 與 425 本身可以是產品資訊的一部分。第三實施例具有第一實施例和第二實施例兩者的優點，可透過連續地使用多個密鑰而加強安全級別，充分保護引進新產品的利潤。

在根據本發明的非接觸通訊標籤 10 的第四實施例裡，多個密鑰 330 和密鑰說明資訊 310 儲存在非接觸通訊標籤 10 裡，標籤讀取器 20 包括讀取全部相應產品的產品資訊所需的密鑰。在此實施例裡，當收到來自標籤讀取器 20 的讀取請求，非接觸通訊標籤 10 選擇多個密鑰 330 中的一個，把對應於選出的密鑰的密鑰說明資訊發送到標籤讀取器 20，使得共有的密鑰互相一致。非接觸通訊標籤 10 的密鑰的選擇是利用輪換或隨機方案進行。隨後，非接觸通訊標籤 10 利用選出的密鑰，把與標籤讀取器 20 交換的資訊進行加密和解密。根據本發明的非接觸通訊標籤 10 的第四實施例具有第一實施例的兩個優點。由於非接觸通訊標籤 10 在每次讀操作時，透過改變其密鑰作出回應，第二實施例可以提升處理偽造讀取器的能力。

在根據本發明的非接觸通訊標籤 10 的第五實施例裡，多個密鑰 330 和密鑰說明資訊 310 儲存在非接觸通訊標籤 10 裡，標籤讀取器 20 包括讀取全部相應產品的產品資訊所需的密鑰。非接觸通訊標籤 10 的每個密鑰組包括至少兩個密鑰，根據在產業類型、生產商、品牌與產品名諸

要素中至少兩個要素，被分類與分發。例如，多個密鑰可以是用在三數據加密標準算法每一步的三個密鑰。換句話說，本發明的第五實施例裡，非接觸通訊標籤 10 包括圖 4A 所示的多個密鑰組 411、413 與 415 和多個密鑰說明資訊組 421、423 與 425。加密／解密單元 210 連續地使用多個密鑰，並處理加密與解密。標籤的密鑰的選擇是利用輪換或隨機方案進行的。其後，標籤利用選出的密鑰組連續地把與標籤讀取器交換的資訊進行加密和解密。與非接觸通訊標籤 10 的第三實施例相似的情形，在第五實施例裡，一旦指定密鑰，標籤讀取器 20 可以識別出產業類型、生產商、品牌與產品名。因此，在第五實施例的各種形式裡，儲存單元 300 的產品資訊 370 和密鑰說明資訊 310 可能互相部分地重疊。根據本發明的非接觸通訊標籤 10 的第五實施例具有第一實施例到第四實施例的優點。

在根據本發明的非接觸通訊標籤 10 的第六實施例裡，非接觸通訊標籤 10 包括一個密鑰和密鑰創建資訊，它們是給讀取器用來創建與非接觸通訊標籤 10 的密鑰一樣的密鑰。使用非接觸通訊標籤 10 的公司準備多個密鑰，根據諸如產業類型、生產商、品牌及產品類型等，分發不同的密鑰。標籤讀取器 20 包括密鑰創建模組，可創建全部讀取相應產品的標籤所需的密鑰。密鑰創建模組利用一個種子值或多個種子值，和接收自標籤的密鑰創建資訊來創建密鑰。由標籤讀取器 20 利用一個種子值創建的密鑰數目，可根據函數參數值而變。儘管儲存在標籤讀取器 20 裡的種

子值數目有限，但仍然可以把不同的密鑰指派給許多品牌，而不需要升級標籤讀取器 20。因此，根據本發明的真實產品鑑定系統可合併許多新要素，即產業類型、生產商、品牌或產品類型，即使在標籤讀取器 20 被分發使用後，也不需要升級標籤讀取器 20。透過分發新的密鑰給相應產品，給相應產品貼上儲存有創建該新密鑰的創建資訊的標籤，而使這種引進成為可能。還有，根據本發明的真實產品鑑定系統，產品資訊是以句子顯示在顯示單元上，可以用同樣的密鑰進行多種產品的真產品鑑定。

例如，密鑰創建模組可由一個整數作為收到的密鑰創建資訊，創建含種子值的結果。本發明不侷限於這個密鑰創建資訊，但是要理解，密鑰創建資訊包括指定和創建標籤讀取器 20 裡的密鑰的資訊。例如，密鑰創建資訊可以是連續碼序列，包括生產商碼、品牌碼、產品碼或含有包括生產商名、品牌名與產品名的文字資訊。還有，密鑰創建算法包括許多函數和操作，可以用一個種子值、至少一個參數來創建密鑰。因而，透過適當地選擇密鑰創建模組的創建算法，即使當一個種子值儲存在標籤讀取器 20 裡，也有可能實際保護許多密鑰。

還有，在根據本發明的非接觸通訊標籤 10 的第六實施例裡，當收到來自標籤讀取器 20 的產品資訊請求時，非接觸通訊標籤 10 的加密／解密單元 210 把密鑰創建資訊作為密鑰說明資訊 310，發送到標籤讀取器 20，導致標籤讀取器 20 創建與儲存在標籤讀取器 20 裡的密鑰 330 一樣的密

鑰。其後，加密／解密單元 210 透過資訊提供單元 250，利用這個密鑰，把要發送到外部設備的資訊加密，或解釋從外部設備接收的加密過的消息，然後把解釋過的消息輸出到資訊提供單元 250。在非接觸通訊標籤 10 的第六實施例裡，透過更充分地保護密鑰，許多密鑰被充分地分發給產業類型、生產商、品牌或產品。因此，即使當密鑰部分地洩漏，損失也可降到最小。另外，類似於第一實施例，可以又組成具有同樣密鑰卻儲存新產品資訊的新標籤，而不需升級已存在的已分發的標籤讀取器。還有，在此實施例裡，當期望引進新產品時，如果標籤儲存有用於創建密鑰的新密鑰和密鑰創建資訊，標籤讀取器能利用從標籤接收的已儲存的種子值和密鑰說明資訊，創建與相應標籤的密鑰一樣的密鑰。因此，在真實產品鑑定並維持更高的安全等級的方面，使引進更多新產品成為可能。

在根據本發明的非接觸通訊標籤 10 的第七實施例裡，非接觸通訊標籤 10 的儲存單元 300 儲存至少兩個密鑰 330，根據在產業類型、生產商、品牌與產品名諸要素中至少兩個要素，被分類與分發。作為密鑰說明資訊 310 的密鑰創建資訊對應於至少兩個密鑰 330。在此實施例裡，加密／解密單元 210 透過連續地利用已儲存的密鑰給消息加密。標籤讀取器 20 從非接觸通訊標籤 10 接收密鑰創建資訊，透過特定函數、或基於接收到的密鑰創建資訊的操作、或內部種子值，創建與已儲存在非接觸通訊標籤 10 裡的密鑰組一樣的密鑰組。與第六實施例相比，第七實施例的優

點：透過利用多個密鑰的多重加密，提升安全性。

在非接觸通訊標籤 10 的第八實施例裡，非接觸通訊標籤 10 的儲存單元 300 儲存：至少兩個密鑰 330，根據在產業類型、生產商、品牌與產品名諸要素中至少兩個要素，被分類、分發；對應於這兩個密鑰 330 的密鑰創建資訊；用於指定密鑰創建資訊的識別資訊的索引。在此實施例裡，加密／解密單元 210 透過連續地利用已儲存的密鑰給消息進行多重加密。標籤讀取器 20 從非接觸通訊標籤 10 接收關於密鑰創建資訊的索引，透過特定函數、基於接收到的索引的操作和內部種子值，創建與儲存在非接觸通訊標籤 10 裡的密鑰組同樣的密鑰組。

圖 4B 根據非接觸通訊標籤 10 的第八實施例闡明密鑰 410、密鑰創建資訊 420 與對應於密鑰創建資訊 420 的索引。在圖 4B 裡，對應於圖 4A、或與圖 4A 一樣的架構引用同樣的參考數字。參照圖 4B，儲存在非接觸通訊標籤 10 裡的密鑰 410 包括三個密鑰 411、413 與 415，每個都根據產業類型、生產商與商標決定。例如，這多個密鑰 411、413 與 415 可以用在三數據加密標準算法每一步的三個密鑰。密鑰創建資訊 490 能創建這些密鑰 411、413 與 415，作為密鑰創建資訊 490 的參數 491、493 與 495 可儲存在儲存單元 300 裡，但是不是必須的。用於指定密鑰創建資訊 490 的索引 420 儲存在非接觸通訊標籤 10 的儲存單元 300 裡，如果標籤讀取器 20 請求密鑰的詳細說明，就把它們發送到標籤讀取器 20。創建密鑰 '1324' 411 的密鑰創建資

訊是‘133’ 491，用於指定這個密鑰創建資訊的索引是‘02’ 421。同樣的，密鑰‘abcd’ 413，密鑰創建資訊‘256’ 493 和索引‘01’ 423 互相對應；密鑰‘2345’ 415，密鑰創建資訊‘267’ 495 和索引‘04’ 425 互相對應。標籤讀取器 20 的密鑰分成三組，每組是一個密鑰分發表，用於產業類型、生產商及品牌。

當收到來自標籤讀取器 20 的產品資訊，非接觸通訊標籤 10 的加密／解密單元 210 發送索引作為密鑰說明資訊 310，此處即是‘02’、‘01’與‘04’。標籤讀取器 20 從這些索引裡查閱相應的密鑰表，從密鑰分發表的每個密鑰創建資訊域 433、453 與 473 提取出密鑰創建資訊用於創建同樣的密鑰組，此處即是‘1324’、‘abcd’與‘2345’，作為密鑰 410 儲存在非接觸通訊標籤 10 裡，此處即是‘133’、‘256’與‘267’。標籤讀取器 20 透過執行預定的基於密鑰創建資訊的密鑰創建算法，而創建相應的密鑰和種子值，選擇創建的密鑰作為密鑰用來讀取非接觸通訊標籤 10。其後，非接觸通訊標籤 10 的加密／解密單元 210 透過連續地利用這多個密鑰，對發送到和接收自標籤讀取器 20 的資訊進行加密與解密。

根據非接觸通訊標籤 10 的第八實施例，一旦指定密鑰，標籤讀取器 20 可識別出密鑰的產業類型、生產商、品牌或商標。換句話說，參照圖 4B，基於密鑰 410、密鑰創建資訊 420 和索引，標籤讀取器 20 可從收到的密鑰索引 421、423 與 425 識別出貼有非接觸通訊標籤 10 的產品是

否為包含在：附件類型、生產商是‘Samah 產業’、商標是‘CAPACCI’的產品類型裡。因此，在第八實施例的各種形式裡，儲存單元 300 裡的產品資訊 370 和密鑰說明資訊 310 在實用中可部分互相重疊。換句話說，索引 421、423 與 425 可以是產品資訊 370 的一部分。根據本發明的非接觸通訊標籤 10 的第八實施例，具有第六和第七實施例兩者的優點。另外，在第八實施例裡，由於發送與接收的是索引，可增強安全級別，並幫助標籤讀取器 20 的升級。此內容將在後面描述。

透過這個過程，標籤讀取器 20 指定相應的密鑰，請求儲存在非接觸通訊標籤 10 裡的產品資訊，接收對請求的回應，在顯示單元上顯示收到的回應。如果附在產品上的非接觸通訊標籤 10 是正確的，標籤讀取器 20 和非接觸通訊標籤 10 之間會成功地進行加密／解密，相應的產品資訊會成功地顯示在顯示單元上。如果是偽造產品或假產品，加密／解密過程就會失敗，從而不可讀的、無意義的資訊就顯示在顯示單元，或顯示偽造產品警告消息。因此，客戶可以檢查產品的真偽。

根據本發明，標籤讀取器 20 的資訊讀取單元 750 從非接觸通訊標籤 10 接收關於不同產品資訊的多個產品碼，連續地向顯示單元輸出產品碼。換句話說，關於一個產品，有多個產品碼儲存在非接觸通訊標籤 10 的儲存單元 300 裡，標籤讀取器 20 連續地讀出並顯示儲存的產品碼。例如，多個產品碼中，第一個顯示的產品碼是生產商，第二

個顯示的產品碼是品牌，下一個顯示的產品碼是每個產品唯一的產品號。因此，擁有碼表的用戶可從顯示的碼序列裡識別出產品資訊。在顯示單元有多個彩色 LED 的實施例裡，碼序列可以是二進制序列，表明彩色 LED 的開或關。

非接觸通訊標籤 10 或非接觸通訊標籤 10 的控制單元 200 可以包含洩漏密鑰升級單元 220。洩漏密鑰升級單元 220 是裝在非接觸通訊標籤 10 裡的模組，如果協議好的密鑰中至少一個洩漏出去，它就使偽造商標無效。在揭露出密鑰的洩漏後，把此模組裝在新生產的標籤裡。在標籤讀取器 20 試圖讀取非接觸通訊標籤 10 時，洩漏密鑰升級單元 220 放棄已有的關於此標籤讀取器的密鑰，引導標籤讀取器 20 使用由洩漏密鑰升級單元 220 指定的新密鑰。

洩漏密鑰升級單元 220 應用於根據本發明的非接觸通訊標籤 10 的第一實施例，給標籤讀取器 20 發送一個新使用的唯一的萬能鑰匙。標籤讀取器 20 刪除它自己的萬能鑰匙，把收到的萬能鑰匙記錄為新的密鑰。這時，透過適當地定義非接觸通訊標籤 10 和標籤讀取器 20 之間的鑰匙升級協議，可以減少萬能鑰匙被盜用造成的危險。

洩漏密鑰升級單元 220 應用於根據本發明的非接觸通訊標籤 10 的第二實施例，它裝在產業類型、生產商、品牌或產品的標籤裡，與洩漏的密鑰一樣，它把相應的新使用的密鑰發送到標籤讀取器 20。標籤讀取器 20 放棄已有的分發過的密鑰，在對應於非接觸通訊標籤 10 的索引裡儲存一個新接收的密鑰，作為相應產業類型、相應生產商、相

應品牌或相應產品的密鑰。

洩漏密鑰升級單元 220 應用於根據本發明的非接觸通訊標籤 10 的第三實施例，它裝在包含在諸如產業類型、生產商、品牌或產品的種類的非接觸通訊標籤 10 裡，這些種類與洩漏的密鑰的一樣，它把相應的新使用的密鑰發送給標籤讀取器 20。標籤讀取器 20 更新對應於索引的密鑰，這些索引是利用新收到的每個種類的表裡的密鑰，分發給非接觸通訊標籤 10。例如，在圖 4A 所示的非接觸通訊標籤 10 的情況裡，品牌索引指定為 '04'。'2345' 被分發為對應於品牌索引 '04' 的密鑰。但是，洩漏密鑰升級單元 220 可以引導標籤讀取器 20 把密鑰 '2345' 改為 '5678'。為了此目的，洩漏密鑰升級單元 220 可以直接把新密鑰發送到標籤讀取器 20，如果保護有充分數量未分發的多餘密鑰，也可以透過選擇一個多餘密鑰的索引設置新密鑰。例如，如果對應於 '5678' 已有的索引是 '15'，洩漏密鑰升級單元 220 發送 '15' 而不是 '5678'，標籤讀取器 20 從它自己的表裡提取出對應於 '15' 的密鑰 '5678'，把 '5678' 分發為對應於索引 '04' 的密鑰。結果是，在標籤讀取器 20 裡，對應於索引 '04' 和 '15' 的密鑰是一樣的。

洩漏密鑰升級單元 220 應用於根據本發明的非接觸通訊標籤 10 的第四實施例，它從非接觸通訊標籤 10 裡儲存的多個密鑰中，升級洩漏密鑰。標籤讀取器 20 用收到的新密鑰，把儲存在索引裡、對應於密鑰表裡的洩漏密鑰的密

鑰升級。

洩漏密鑰升級單元 220 應用於根據本發明的非接觸通訊標籤 10 的第五實施例，它把非接觸通訊標籤 10 裡儲存的全部多個密鑰組升級。因此，非接觸通訊標籤 10 的洩漏密鑰升級單元 220 把必需的新的多個密鑰組發送到標籤讀取器 20，請求標籤讀取器 20 把對應於標籤讀取器 20 的密鑰組升級。標籤讀取器 20 首先在儲存的密鑰表裡指定分發給非接觸通訊標籤 10 的密鑰組，然後用收到的密鑰按收到的順序連續地升級全部密鑰組。

洩漏密鑰升級單元 220 應用於根據本發明的非接觸通訊標籤 10 的第六實施例，它把應該新使用的密鑰創建資訊發送到標籤讀取器 20。這時，對應於新密鑰創建資訊的密鑰儲存在非接觸通訊標籤 10 裡。標籤讀取器 20 可以把已有的通用的密鑰創建資訊註冊為壞標籤放在黑名單裡。這種情況下，如果特定的標籤請求真偽鑑定，標籤讀取器 20 可以參照黑名單和生產日期，更精確地確定標籤是否是偽造標籤。因此，有可能確定在指定生產日期前生產的標籤是真的，在指定生產日期後生產的標籤是偽造的。

洩漏密鑰升級單元 220 應用於根據本發明的非接觸通訊標籤 10 的第七實施例，它把應該新使用的密鑰創建資訊發送到標籤讀取器 20。例如，假設在圖 4B 的密鑰中，密鑰 '1324' 411 被洩漏出去。這時，新密鑰 '1567' 儲存在新發放的標籤裡，而不是密鑰 '1324'，對應於這個新密鑰 '1567' 的密鑰創建資訊是 '138'。這種情況下，洩

漏密鑰升級單元 220 把對應於索引 '02' 的密鑰創建資訊 '133' 刪除 (其中索引 '02' 分發給標籤的密鑰表 430 裡的標籤), 請求記錄新的密鑰創建資訊是 '138'。從而, 標籤讀取器 20 從密鑰表 430 裡提取出 '138' 作為對應於索引 '02' 的密鑰創建資訊, 創建密鑰 '1567'。結果是, 對於具有密鑰 '1324' 的偽造鑰匙或現有已被分發的標籤, 不能讀出其產品資訊, 從而確定這個偽造的或現有已被分發的標籤是偽造的。

還有, 根據本發明的非接觸通訊標籤 10 或非接觸通訊標籤 10 的控制單元 200, 可包括重送攻擊阻止單元 230。在加密技術裡, 重送攻擊意味著透過盜用一個在已加密的鑑定過程裡被用戶發送的註冊消息, 來試圖訪問伺服器並重發非法消息給伺服器。為了對付這種攻擊, 伺服器發送註冊請求消息給客戶, 在註冊請求消息後面包括一個隨機數字, 給註冊請求消息加密, 客戶在回應註冊消息裡包括同樣的隨機數字。當鑑定收到的註冊消息時, 伺服器檢查隨機數字, 只有當隨機數字和伺服器發出的是一樣的時候才允許註冊。由於隨機數字每次是變化的, 在這個重送阻止技術的幫助下, 有可能防止重複使用同樣的註冊消息的可能性。

本發明在真實產品鑑定時引進了這個重送阻止技術。這個引進可有效地防止標籤讀取器 20 的讀取請求消息或非接觸通訊標籤 10 的回應消息被盜用、複製和使用。因此, 本發明的系統不可能被重送攻擊, 其真偽鑑定可以有

更高的可靠性。

根據本發明的非接觸通訊標籤 10 或其控制單元 200 可包括後管理處理單元 270。讀取細節資訊是儲存在非接觸通訊標籤 10 的儲存單元 300 裡。每次讀取，資訊提供單元 250 把讀取細節資訊，如序列號、標籤讀取器 20 的讀取日期，儲存在儲存單元 300 的指定區域。當儲存在計數區的、管理讀取次數的值比預定的值高時，資訊提供單元 250 不提供產品資訊。設計後管理處理單元 270 不僅用來提供產品資訊，而且提供關於用特定密鑰註冊的特定終端的讀取詳細資訊，如：讀取器的管理，讀取次數的放棄。讀取器硬體配置類似於通用讀取器。它可以透過讀取被用戶放棄的標籤資訊或附在返回產品上的標籤資訊，而識別出銷售日期，進行真偽鑑定的用戶，真偽鑑定的日期。所以，讀取器可以有效地把資訊用作消費者傾向的銷售的後客戶管理資訊。

根據本發明的非接觸通訊標籤 10 或其控制單元 200，還可包括刷新(refresh)處理單元 290。通常，在非易失性記憶體裡，在記錄以後，可用的讀取次數或可用的讀取週期是有限的，大家知道，數據只能保存約 10 年。但是，10 年對於擁有很長時間週期的產品來說是太短了，如調查報告、古董與雕刻。如果在應用時，非接觸通訊標籤 10 裡包括刷新處理單元 290，每次讀取時數據就會被重記錄在儲存單元 300 裡，刷新處理該數據。這種刷新處理必須包含儲存單元 300 裡的全部數據，包括密鑰、產品資訊與計數

值。在這種情況下，非接觸通訊標籤 10 包括一個刷新緩沖器，刷新處理單元 290 透過在大小相當於刷新緩沖器容量的區塊單元裡進行重複讀／寫操作，而進行刷新處理。在刷新處理的產品裡，最好把可用的讀取次數設置成很大或不限制可用的讀取次數。

下文，將闡述標籤讀取器 20 的較佳實施例。

圖 3 是根據本發明的標籤讀取器 20 的架構示意方塊圖。

參照圖 3，根據本發明，具有標籤讀取功能的標籤讀取器 20-1 和 20-2 包括操縱單元 930、顯示單元 950、聲音輸出單元 960、電池（未畫）、標籤通訊單元 500、儲存單元 910、資訊讀取單元 750 與控制單元 700。

操縱單元 930 除了普通行動通訊終端的按鍵外，還包括一或兩個按鈕，如讀取啟動按鈕和資訊發送按鈕。或者，當具有讀取功能的行動通訊終端 20-1 和 20-2 受控進行讀取操作時，行動通訊終端的按鍵中的特定按鈕當作與讀取功能相關的按鍵功能，如讀取啟動按鈕和資訊發送按鈕。顯示單元 950 使用行動通訊終端 20-1 和 20-2 的 LCD。聲音輸出單元 960 使用行動通訊終端 20-1 和 20-2 的喇叭。無線通訊單元 970 提供行動通訊功能的電路，是 Qualcomm 公司的 MSM 組晶片，有關的射頻（RF）電路支持碼分多址（Code Divesion Multiple Access, CDMA）通訊。

標籤通訊單元 500 以無線模式與非接觸通訊標籤 10 交換數據，無線地發送必需的能量。標籤通訊單元 500 包

括天線 510、能量發送單元 531、解調單元 533 與調變單元 535。天線 510 以無線模式對非接觸通訊標籤 10 發送和接收數據。天線 510 可以沿著具有讀取功能的行動通訊終端 20-1 和 20-2 周遭以印刷圖案形成。功率發送單元 531 透過天線 510 無線地給非接觸通訊標籤 10 發送必需的能量。解調單元 533 把透過天線 510、接收自非接觸通訊標籤 10 的信號解調。調變單元 535 把要發送到非接觸通訊標籤 10 的信號進行調變。組成標籤通訊單元 500 的每個組件對應於非接觸通訊標籤 10 的非接觸通訊裝置 100 所包括的天線 110、能量供給單元 131、解調單元 133 與調變單元 135，此處不再詳述。

主程式用於控制整個系統和用於創建資訊交換所需的密鑰的種子值，它儲存在儲存單元 910 裡。另一方面，主程式和資訊交換所需的多個密鑰可儲存在儲存單元 910 裡。儲存單元 910 包括：非易失性記憶體如 ROM、臨時存儲空間 RAM 或單個快閃記憶體。被具有讀取功能的行動通訊終端 20-1 和 20-2 讀取的標籤的有關讀取詳細資訊，也儲存在儲存單元 910 裡。市場人員可以透過讀取來自行動通訊終端 20-1 和 20-2 的、連在他們的計算機上的讀取詳細資訊，而識別出客戶的愛好。

控制單元 700 可與商用微處理器一樣實現。資訊讀取單元 750 和加密／解密單元 710 可以用控制單元 700 裡的軟體實現，或者作為獨立於控制單元 700 的一個部件生產。資訊讀取單元 750 回應來自操縱單元 930 的命令，請

求來自非接觸通訊標籤 10 的產品資訊，在顯示單元 950 上顯示從非接觸通訊標籤 10 收到的產品資訊。加密／解密單元 710 透過標籤通訊單元 500 把發送到或接收自非接觸通訊標籤 10 的資訊加密和解密。

資訊讀取單元 750 和非接觸通訊標籤 10 的資訊提供單元 250 互相作用，加密／解密單元 710 和非接觸通訊標籤 10 的加密／解密單元 210 互相作用。資訊讀取單元 750 在顯示單元 950 上以文字或圖形模式顯示從非接觸通訊標籤 10 收到的產品資訊。當顯示單元 950 包括七段(7-segment)或彩色 LED 時，資訊提供單元 250 在顯示單元 950 上顯示產品碼，即從非接觸通訊標籤 10 收到的產品資訊。在這種情況下，資訊讀取單元 750 從非接觸通訊標籤 10 的資訊提供單元 250 接收多個產品碼並連續地把收到的產品碼輸出到顯示單元 950。多個產品碼被組合成一個消息，從非接觸通訊標籤 10 的資訊提供單元 250 發送，或回應來自行動通訊終端 20-1 和 20-2 的資訊讀取單元 750 的請求，把多個產品碼從資訊提供單元 250 發送到具有讀取功能的行動通訊終端 20-1 和 20-2。資訊讀取單元 750 從收到的消息提取出多個產品碼，按預定的時間間隔把提取出的產品碼連續地顯示在顯示單元 950 上。資訊讀取單元 750 連續地在顯示單元上輸出收到的產品碼。根據資訊讀取單元 750 的讀取結果，聲音輸出單元 960 可以輸出信號聲。資訊讀取單元 750 也包括一個實時時鐘電路，計算當前時間。每次讀取時，資訊讀取單元 750 把讀取時間和讀取器的序列號

發送給標籤，使時間和序列號作為讀取詳細資訊的一部分儲存起來。

加密／解密單元 710 透過標籤通訊單元 500 從非接觸通訊標籤 10 接收密鑰創建資訊，利用收到的密鑰創建資訊和儲存在儲存單元 910 裡的種子值創建一個密鑰，並用創建的密鑰來處理加密／解密。還有，加密／解密單元 710 透過與非接觸通訊標籤 10 的加密／解密單元 210 的通訊來接收密鑰說明資訊，從儲存在儲存單元 910 裡的用於多個產業類型、品牌、產品的密鑰中，選擇與當前讀取的標籤有關的密鑰，用選擇的密鑰處理非接觸通訊標籤 10 和行動通訊終端 20-1 和 20-2 之間的通訊。這種通訊過程在後面描述。行動通訊終端 20-1 和 20-2 的加密／解密單元 710 對應於非接觸通訊標籤 10 的加密／解密單元 210，可以配置成對應於上面描述的非接觸通訊標籤 10 的實施例。加密／解密過程由行動通訊終端 20-1 和 20-2 的實施例的加密／解密單元 710 執行，由於此過程本質上與非接觸通訊標籤 10 的實施例的加密／解密單元 210 執行的過程一樣，這裡不再詳述。

在根據本發明的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的第一實施例裡，加密／解密單元 710 對應於非接觸通訊標籤 10 的第一實施例的加密／解密單元 210。在此實施例裡，儲存單元 910 只儲存萬能鑰匙這單個密鑰。加密／解密單元 710 用萬能鑰匙把發送到和接收自非接觸通訊標籤 10 的資訊加密、解密。

在根據本發明的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的第二實施例裡，加密／解密單元 710 對應於非接觸通訊標籤 10 的第二實施例的加密／解密單元 210。在此實施例裡，儲存單元 910 儲存對應於索引的多個密鑰。加密／解密單元 710 從標籤接收密鑰說明資訊，如索引，指定一個密鑰，用指定的密鑰把發送到和接收自標籤的資訊加密、解密。

在根據本發明的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的第三實施例裡，加密／解密單元 710 對應於非接觸通訊標籤 10 的第三實施例的加密／解密單元 210。在此實施例裡，正如圖 4A 裡下半部分所示的概念，密鑰表是基於每個種類，如產業類型、生產商、品牌和產品名而儲存在儲存單元 910 裡。加密／解密單元 710 從非接觸通訊標籤 10 接收索引當作多個密鑰說明資訊，從每個對應的表裡給非接觸通訊標籤 10 指定一個密鑰組。加密／解密單元 710 用密鑰連續地對發送到和接收自非接觸通訊標籤 10 的資訊進行多重加密、解密。

在根據本發明的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的第四實施例裡，加密／解密單元 710 對應於非接觸通訊標籤 10 的第四實施例的加密／解密單元 210。在此實施例裡，多個密鑰以表的形式儲存在儲存單元 910 裡。加密／解密單元 710 接收索引作為密鑰說明資訊，查閱密鑰表給非接觸通訊標籤 10 指定密鑰。加密／解密單元 710 用指定的密鑰對發送到和接收自非接觸通訊標籤 10 的

資訊進行加密與解密。

在根據本發明的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的第五實施例裡，加密／解密單元 710 對應於非接觸通訊標籤 10 的第五實施例的加密／解密單元 210。在此實施例裡，類似與第三實施例，多個密鑰以表的形式儲存在儲存單元 910 裡。加密／解密單元 710 從非接觸通訊標籤 10 接收索引作為密鑰說明資訊，查閱密鑰表給非接觸通訊標籤 10 指定密鑰。加密／解密單元 710 連續地用密鑰對發送到和接收自非接觸通訊標籤 10 的資訊進行多重加密與解密。

在根據本發明的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的第六實施例裡，加密／解密單元 710 對應於非接觸通訊標籤 10 的第六實施例的加密／解密單元 210。在此實施例裡，加密／解密單元 710 包括密鑰創建模組，密鑰創建模組必需的種子值可儲存在儲存單元 910 的數據區，或引進、儲存為密鑰創建模組的程式碼。加密／解密單元 710 利用從非接觸通訊標籤 10 收到的密鑰創建資訊，再執行密鑰創建模組的程式而創建密鑰，它用密鑰對發送到和接收自非接觸通訊標籤 10 的資訊進行加密與解密。

在根據本發明的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的第七實施例裡，加密／解密單元 710 對應於非接觸通訊標籤 10 的第七實施例的加密／解密單元 210。在此實施例裡，加密／解密單元 710 包括密鑰創建模組。密鑰創建模組必需的種子值可儲存在儲存單元 910 的數據

區，或引進、儲存為密鑰創建模組的程式碼。加密／解密單元 710 利用收到的密鑰創建資訊，連續地執行密鑰創建模組的程式而創建一序列密鑰，再用密鑰連續地對發送到和接收自非接觸通訊標籤 10 的資訊進行多重加密與解密。

在根據本發明的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的第八實施例裡，加密／解密單元 710 對應於非接觸通訊標籤 10 的第八實施例的加密／解密單元 210。正如圖 4B 裡下半部分所示的概念，表格是儲存在儲存單元 910 裡。加密／解密單元 710 從接收自非接觸通訊標籤 10 的索引裡提取出關於密鑰表的密鑰創建資訊。加密／解密單元 710 利用提取出的密鑰創建資訊，連續地執行密鑰創建模組的程式而創建一序列密鑰，再用密鑰連續地對發送到和接收自非接觸通訊標籤 10 的資訊進行多重加密、解密。

如上所示，根據本發明的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 可以從產業類型、生產商、品牌與產品名中指定至少兩個產品資訊，並在顯示單元 950 上顯示指定的產品資訊，產業類型、生產商、品牌與產品是接收自關於密鑰創建資訊的密鑰說明資訊、密鑰創建資訊或索引的。這種指定和顯示至少可以用於第三實施例、第五實施例、第七實施例和第八實施例。如圖 4A 和圖 4B 所示，產品資訊對應於給每個種類的索引，該種類包括相應的密鑰，並把產品資訊儲存在行動通訊終端 20-1 和 20-2 的儲存單元 910 裡。因此，有可能基於接收自非接觸通訊標籤

10 的索引，指定至少一部分產品資訊。

根據本發明，行動通訊終端 20-1 和 20-2 有選擇地包括資訊提供單元 760、洩漏密鑰升級單元 790、重送攻擊阻止單元 730、讀取器鑑定單元 770 與刷新處理單元 720 中的至少一個。這些組件可被引進控制單元 700 裡。

資訊提供單元 760 把資訊讀取單元 750 讀出的資訊讀取細節透過無線通訊單元 970，發送到服務管理伺服器 40。資訊提供單元 760 發送資訊讀取單元 750 讀出的資訊，如產品相關資訊，包括產業類型、生產商、品牌、產品名、等級、樣式名、生產中心、生產日期、序列號和諸如價格、鑑定時間等的讀取細節資訊中的至少一項，透過無線通訊單元 970，發送到服務管理伺服器。至於真偽鑑定後採買的產品，採買資訊可包括在從資訊提供單元 760 發送到服務管理伺服器 40 的資訊裡。行動通訊終端 20-1 和 20-2 的擁有者透過按一個“真實產品鑑定” 按鈕來檢測顯示單元 950 上的產品資訊，再購買產品。如果完成採買後按下操縱單元 930 的“採買完成” 鍵，可以從儲存單元 910 裡儲存的讀取細節中，讀出真偽最近被鑑定過的產品清單，顯示在顯示單元 950 上。一旦用戶從清單中選擇資訊，按一個“確認” 鍵，相應產品就作為採買來處理。採買資訊收集在儲存單元 910 裡，然後在按下操縱單元 930 的“發送” 鍵後一起發送出去。資訊發送透過無線通訊單元 970 或無線網際網路進行，或者資訊可以以簡單短消息的形式發送。另一方面，每次用戶按下“採買完成” 鍵，

按下此鍵時的採買資訊被以短消息的形式發送到服務管理伺服器 40。

當從非接觸通訊標籤 10 收到關於洩漏密鑰的密鑰升級請求資訊時，密鑰升級單元 790 放棄儲存在儲存單元 910 裡的相應密鑰，透過在儲存單元 910 裡儲存一個新分發的密鑰來升級密鑰。詳細的實施例及其操作已經在非接觸通訊標籤 10 的洩漏密鑰升級單元 220 裡描述過，不再描述。

重送攻擊阻止單元 730 產生一次性的用戶隨機數字，把此隨機數字加到要發送的資訊上，給加密／解密單元 710 提供資訊，從作為資訊回應收到的資訊裡提取出隨機數字，檢測提取出的隨機數字是否與原來加到發送資訊上的隨機數字一樣，從而阻止重送攻擊。重送攻擊阻止單元 730 對應於非接觸通訊標籤 10 的重送攻擊阻止單元 230，不再細述。

讀取器鑑定單元 770 與外部便攜式讀取器進行通訊，互相鑑定，在顯示單元 950 上顯示鑑定結果資訊。這種鑑定功能允許標籤讀取器 20 和外部便攜式讀取器互相檢測其可靠性。兩個標籤讀取器之間的鑑定也在標籤通訊單元 500 間進行。為了鑑定，要預定一個特定的密鑰。同樣的，加密／解密單元 710 進行標籤讀取器之間的鑑定。更好的是重送攻擊阻止單元 730 介入鑑定去阻止利用標籤讀取器之間的通訊進行盜用。這種重送攻擊阻止單元 730 的工作原理在後面細述。

刷新處理單元 720 讀出儲存在儲存單元 910 裡的相關

資訊的密鑰,儲存單元 910 是非易失性記憶體,重新記錄讀出的資訊。控制具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的控制單元 700 的主程式,是諸如電子可抹除可編程唯讀記憶體 (EEPROM) 的存儲設備,數據永久地儲存在裡面。另外,如同密鑰相關資訊,資訊必須根據具有標籤讀取功能的行動通訊終端 20-1 和 20-2 不同地儲存,儲存在閃存裡。在閃存的情況下,記錄可讀取數據的期間限制在 10 年。結果是,當閃存使用較長時間,有可能丟失密鑰。因此,當每次讀取密鑰相關資訊時,包括刷新處理單元 720 的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 把讀取數據重新記錄在同樣的位址,從而解決這個問題。

在本發明裡,標籤讀取器在行動通訊終端 20-1 和 20-2 裡實現。這時,操縱單元 930 能從行動通訊終端 20-1 和 20-2 的鍵盤裡使用一個或多個鍵,並使用行動通訊終端 20-1 和 20-2 的 LCD 作為顯示單元 950。儲存單元 910 和控制單元 700 基本上安裝在行動通訊終端 20-1 和 20-2 裡,但是,在這種情況下,關於讀操作的資訊可能被洩漏。因此,具有標籤讀取功能的行動通訊終端 20-1 和 20-2 包括個別設計的 ASIC。ASIC 包括類比無線電路和標籤通訊單元 500 的調變/解調電路,作為儲存單元 910 的非易失性記憶體,作為控制單元 700 的微處理器。ASIC 和用於控制行動通訊終端 20-1 和 20-2 系統的微處理器透過它們各自的主機界面通訊。由於這種通訊只允許有限數目的命令,有可能嚴格地保持安全。因此,根據本發明的具有標籤讀

取功能的行動通訊終端 20-1 和 20-2 可透過給習知的手機增加獨自設計的 ASIC 和天線圖案來完成。這時，用於 ASIC 和用戶界面之間通訊的獨自的軟體模組必須另外地安裝在行動通訊終端 20-1 和 20-2 裡。

圖 5 表明根據本發明的行動通訊終端 20-1 和 20-2 的產品資訊讀出過程的流程圖。

參照圖 5，在第一步 S500 裡，對應於一個密鑰的密鑰相關資訊是基於在產業類型、生產商、品牌與產品名諸要素中至少一個要素被設置的，此密鑰儲存在具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的儲存單元 910 裡。在步驟 S510 裡，行動通訊終端 20-1 和 20-2 基於接收檢測到的非接觸通訊標籤 10 的密鑰說明資訊，從儲存在儲存單元 910 裡的密鑰相關資訊裡指定一個密鑰，選擇指定的密鑰作為密鑰用於當前的通訊。這時，具有標籤讀取功能的行動通訊終端 20-1 和 20-2 透過利用接收來自標籤 10 的密鑰創建資訊和儲存在儲存單元 910 裡的密鑰種子資訊而創建密鑰，指定它為密鑰。在步驟 S520 裡，具有標籤讀取功能的行動通訊終端 20-1 和 20-2 給請求產品資訊的請求消息加密並發送到標籤 10。在步驟 S530 裡，具有標籤讀取功能的行動通訊終端 20-1 和 20-2 把接收自標籤的產品資訊消息如商標、產品名與等級解密，把產品資訊消息顯示為可視資訊。具有標籤讀取功能的行動通訊終端 20-1 和 20-2 透過給資訊請求消息增加一個隨機數而給資訊請求消息加密，把接收自非接觸通訊標籤 10 的產品資訊消息解

密，檢測解密過的產品資訊消息的隨機數是否與原來加到資訊請求消息上的隨機數一樣，從而另外地應付重送攻擊。還有，在步驟 S540 裡，一旦具有標籤讀取功能的行動通訊終端 20-1 和 20-2 接收密鑰升級請求資訊，請求放棄掉洩漏的密鑰，用新密鑰升級，具有標籤讀取功能的行動通訊終端 20-1 和 20-2 在步驟 S550 裡取代密鑰，用新密鑰分發給相應的產品，選擇新密鑰作為密鑰用於當前的通訊。

圖 6 表明標籤 10 和具有讀取功能的行動通訊終端 20-1 和 20-2 之間通訊過程的流程圖。

參照圖 6，在步驟 S600 裡，用戶透過按一個具有讀取功能的行動通訊終端 20-1 和 20-2 的特定按鍵請求產品資訊的檢測。因此，在步驟 S605 裡，具有讀取功能的行動通訊終端 20-1 和 20-2 檢測標籤 10 的存在。這種檢測可以是遵守 ISO14443 標準的檢測方法，但不侷限於此。具有讀取功能的行動通訊終端 20-1 和 20-2 執行一個協議，有選擇地指定密鑰。標籤 10 裡可儲存一個或多個密鑰用於與具有讀取功能的行動通訊終端 20-1 和 20-2 之間的通訊，如果是多個密鑰的情況，在被其後的協議指定後使用其中一個密鑰。為了指定密鑰，在步驟 S610 裡，具有讀取功能的行動通訊終端 20-1 和 20-2 把請求密鑰詳細說明的密鑰詳細說明請求消息發送到標籤 10。這時，具有讀取功能的行動通訊終端 20-1 和 20-2 給密鑰詳細說明請求消息加一個隨機數，發送此密鑰詳細說明請求消息。在步驟 S615

裡，標籤 10 把密鑰的詳細說明必須的密鑰說明資訊，作為對密鑰詳細說明請求消息的回應，如密鑰的索引發送出去。這時，標籤 10 給密鑰詳細說明消息加一個接收自具有讀取功能的行動通訊終端 20-1 和 20-2 的隨機數和在標籤 10 裡產生的隨機數，然後發送密鑰詳細說明消息。因此，不僅可以保護發送消息，而且還能保護從重送攻擊收到的消息。其中用的加密方法是三數據加密標準方法，由於它是對稱密鑰算法，加密密鑰和解密密鑰是一樣的。

標籤 10 可以提供密鑰創建資訊用於創建一個密鑰作為給具有讀取功能的行動通訊終端 20-1 和 20-2 的密鑰說明資訊。密鑰創建資訊是用於密鑰創建函數的一個參數。這裡，密鑰創建函數是以標籤讀取器 20 裡的程式實現的。在步驟 S620 裡，具有讀取功能的行動通訊終端 20-1 和 20-2 使用基於種子值的密鑰創建函數創建一個密鑰，該種子值儲存在儲存單元 910 裡，密鑰創建資訊接收自標籤 10。例如，當種子值是 123456，參數可以用來從種子值的排列與組合而創建的幾個密鑰裡選擇一個的索引。另一方面，參數可以用來從許多密鑰裡選擇一個的索引，這些密鑰是透過加密一個表明區塊單元裡種子值的數據字而抽取出來的。參數還可以是關於算法裡區塊劃分的參數，此算法是用於加密一個表明區塊單元裡種子值的數據字的。關於密鑰的創建，有許多算法都很出名，這裡就忽略其描述。如果多個種子值儲存在標籤讀取器 20 裡，儲存在標籤 10 裡的密鑰創建資訊包括用於指定種子值的索引。這裡，其

它的組件與具有單個種子值的實施例是一樣的，此處省略其描述。透過使用上述的密鑰創建函數，有可能增加具有不同密鑰的、真偽鑑定目標產品，其數目和能創建的密鑰數一樣多，而不需要在用戶購買具有讀取功能的行動通訊終端 20-1 和 20-2 之後，把它升級。

密鑰說明資訊可以是指定多個密鑰的一個的索引。這裡，多個密鑰（如：幾百個密鑰）對應於全部標籤的密鑰，都儲存在具有標籤讀取功能的行動通訊終端 20-1 和 20-2 裡。用於指定標籤 10 的密鑰的索引和多個密鑰的一個，都是儲存在標籤 10 裡。具有讀取功能的行動通訊終端 20-1 和 20-2 接收這些索引，可以從多個密鑰中指定一個密鑰，用於當前的標籤。這樣，透過使用多個密鑰，有可能增加真偽鑑定目標產品，其數目和密鑰數一樣多，而不需要用戶給具有讀取功能的行動通訊終端 20-1 和 20-2 升級。

如果多個密鑰也儲存在標籤 10 裡，密鑰說明資訊可以是儲存在標籤 10 裡指定多個密鑰的多個索引。具有標籤讀取功能的行動通訊終端 20-1 和 20-2 透過隨機選擇多個接收自標籤 10 的索引的一個作出回應。因此在標籤 10 裡，密鑰是指定的。這種情況下，具有標籤讀取功能的行動通訊終端 20-1 和 20-2 指定一個密鑰對應於接收自標籤 10 的多個索引中的一個索引，此密鑰是從儲存的許多個密鑰裡選出的，把它用作標籤 10 的萬能鑰匙。因此，根據本發明，包括標籤 10 和具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的真偽產品鑑定系統可以提供更增強的安全性。

在上述的三個實施例裡，密鑰的選擇可用於產業類型／生產商／品牌／產品而進行。因此，同一個密鑰可用於同一產業類型的產品，或由同一生產商生產的同一產業類型的產品。所以，如果同一產業類型的生產商或同一產業類型的同一生產商生產新產品，該新產品由根據本發明的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 讀取，可以讀出產品資訊，而不需要升級具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的密鑰資訊。還有，當密鑰一般地用於同類產品時，在新產品發布後，更多的新產品可被加到具有標籤讀取功能的行動通訊終端 20-1 和 20-2 裡。

其次，在步驟 S625 裡，具有標籤讀取功能的行動通訊終端 20-1 和 20-2 把請求產品資訊的產品資訊請求消息發送到標籤 10。這時，具有標籤讀取功能的行動通訊終端 20-1 和 20-2 給產品資訊請求消息加一個接收自標籤 10 的隨機數，和一個具有標籤讀取功能的行動通訊終端 20-1 和 20-2 新創建的隨機數，然後用指定的萬能鑰匙給產品資訊請求消息加密。標籤 10 從具有標籤讀取功能的行動通訊終端 20-1 和 20-2 接收產品資訊請求消息，從中提取出收到的產品資訊請求消息所包含的、先前由標籤 10 發送出去的隨機數，並檢測提取出的隨機數是否與先前發送的隨機數一致，從而檢測收到的信號是否為重送攻擊。這時，標籤 10 可進一步執行具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的選擇性的鑑定處理。由標籤 10 執行的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的鑑定，可以透過

接收一個回應消息而進行，該回應消息回應發送到具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的絕對加密消息。如上面提到的，部分產品資訊可以先前從密鑰索引或密鑰創建資訊索引保護。

在步驟 S635 裡，標籤 10 提取儲存單元 300 裡的計數值，檢測提取出的計數值。如果確定已完成的讀取次數超過允許的次數，標籤 10 阻止進一步讀取。另一方面，在步驟 S640 裡，如果提取出的計數值小於允許的次數，標籤 10 從儲存單元 300 裡提取產品資訊，創建產品資訊消息，這是回應消息。這時，給產品資訊加一個接收自具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的隨機數之後，標籤 10 用萬能鑰匙給產品資訊加密，從而創建產品資訊消息。在步驟 S645 裡，標籤 10 把創建的產品資訊消息發送到具有標籤讀取功能的行動通訊終端 20-1 和 20-2。產品資訊發送後，在步驟 S650 裡標籤 10 增加儲存單元 300 的計數值，在步驟 S655 裡儲存讀取歷史資訊，包括讀取日期、時間，請求讀取的具有標籤讀取功能的行動通訊終端 20-1 和 20-2 的序列號。在步驟 S660 裡，具有標籤讀取功能的行動通訊終端 20-1 和 20-2 從標籤 10 接收產品資訊消息，把收到的產品資訊消息解密，透過檢測包含在解密過的消息裡的隨機數是否與以前發送的隨機數一樣，而檢測收到的信號是否是重送攻擊。如果確定收到的信號不是來自重送攻擊的虛假回應，具有標籤讀取功能的行動通訊終端 20-1 和 20-2 在步驟 S665 裡顯示產品資訊。

升級處理過程可以在標籤 10 和具有標籤讀取功能的行動通訊終端 20-1 和 20-2 之間的洩漏密鑰上進行。這種情況下，如圖 4 所示，如果具有標籤讀取功能的行動通訊終端 20-1 和 20-2 給標籤 10 發送密鑰詳細說明請求消息，標籤 10 給具有標籤讀取功能的行動通訊終端 20-1 和 20-2 發送密鑰升級請求消息，而不是密鑰詳細說明消息。一旦具有標籤讀取功能的行動通訊終端 20-1 和 20-2 接收密鑰升級請求消息，內部分發給相應標籤的已有的密鑰被放棄，由新密鑰代替。具有標籤讀取功能的行動通訊終端 20-1 和 20-2 還指定新升級的密鑰作為與標籤 10 通訊的密鑰。透過這些過程，一旦新密鑰被指定為通訊的密鑰，標籤 10 和具有標籤讀取功能的行動通訊終端 20-1 和 20-2 從 S620 執行到 S665。

圖 7 表明根據本發明的實施例在行動通訊終端#1 和行動通訊終端#2 之間執行的鑑定過程的流程圖。

參照圖 7，在鑑定過程中，兩個標籤讀取器中的一個被指定為主讀取器。在步驟 S700 裡，這種指定可允許用戶把第一次按“鑑定請求”鍵的標籤讀取器作為主標籤讀取器。在步驟 S705 裡，主標籤讀取器調查相鄰的副標籤讀取器的存在。主標籤讀取器和副標籤讀取器確定後，在步驟 S710 裡進行一個程式，用於打開兩個終端之間的通訊交談。主標籤讀取器創建一個交談標識符，把交談標識符發送給副標籤讀取器，兩個標籤讀取器之間的通訊包括同樣的交談標識符，從而維持兩個標籤讀取器之間的通訊。

交談。因此，即使在共享同樣的無線電頻率的环境裡，可以維持或管理特定的連接狀態。其後，在步驟 S715 到 S730 裡，透過交換兩個標籤讀取器之間的密鑰詳細說明請求消息、密鑰詳細說明消息，而執行分發通訊所必須的密鑰的程式。這個程式類似於在標籤和標籤讀取器之間指定萬能鑰匙的程式，不再詳述。

標籤讀取器之間的鑑定程式完全倚賴於加密。換句話說，假設在正確的標籤讀取器裡，有正確的密鑰。因此，一旦主標籤讀取器在步驟 S735 裡用它自己的密鑰給檢測消息加密，把加密過的檢測消息發送到副標籤讀取器，則副標籤讀取器在步驟 S745 裡把收到的檢測消息解密，給解密過的檢測消息加密，然後發送加密過的檢測消息。這時，在步驟 S740 裡副標籤讀取器可以在顯示單元上顯示出收到檢測消息。其後，主標籤讀取器把收到的消息解密，透過檢測收到的消息的隨機數而檢測收到的消息是否是重送攻擊。如果提取出的消息與原來發送的消息一樣，主標籤讀取器就確定副標籤讀取器是具有正確密鑰的標籤讀取器。另一方面，如果提取出的消息與原來發送的消息不一樣，主標籤讀取器就確定副標籤讀取器是虛假的標籤讀取器。在步驟 S750 裡，主標籤讀取器顯示出關於副標籤讀取器的確定結果。但是，本發明不侷限於這些實施例，副標籤讀取器可以透過消息處理而進行回應，例如在解密收到的消息後，根據先前約定的規則，用位元組或字單元對收到的消息進行映射(mapping)。

圖 8 表明根據本發明推薦的實施例提供真實產品鑑定服務的方法的流程圖。

參照圖 8，在步驟 S800 裡，服務管理伺服器 40 透過無線通訊網路接收讀取細節資訊，包括分發給每個要從行動通訊終端 20-1 和 20-2 讀取的產品的產品識別號，及分發給每個行動通訊終端 20-1 和 20-2 的讀取器識別號。在步驟 S810 裡，服務管理伺服器 40 檢測包含在選擇讀取的讀取細節資訊裡的產品識別號和讀取器識別號，判斷它們是否與包含在先前從行動通訊終端 20-1 和 20-2 讀取的讀取細節資訊裡的內容一致，從而檢測資訊是否為重複發送。在步驟 S820 裡，服務管理伺服器 40 基於含在行動通訊終端 20-1 和 20-2 裡的、含在收到的讀取細節資訊裡的識別號，向用戶伺服器 30 請求用戶資訊的查詢，從用戶伺服器 30 接收用戶資訊。其次，在步驟 S830 裡，服務管理伺服器 40 創建並儲存客戶管理資訊，包括用戶分類資訊、基於讀取細節資訊的產品資訊讀取細節與用戶資訊。用戶分類資訊包括用戶的年紀、地區、性別與工作中的至少一項；讀取細節資訊包括產業類型、生產商、品牌、等級、式樣名、生產中心、生產日期時間、產品序列號、產品價格與鑑定日期中的至少一項。讀取細節資訊還可進一步包括採買資訊，包括關於已採買產品的購買價格、購買日期時間。其次，在步驟 S840 裡，服務管理伺服器 40 根據讀取細節資訊增加用戶的“積分點”。在步驟 S850 裡，服務管理伺服器 40 回應從外部設備輸入的資訊輸出請求而

讀出並輸出客戶管理資訊。

本發明可以以計算機可讀碼形式在計算機可讀記錄媒體裡實現。計算機可讀記錄媒體包括各種記錄設備，其中儲存可被計算機系統讀取的數據。這種計算機可讀記錄媒體是 ROM、RAM、CD-ROM、磁帶、磁片、光學資料儲存體、載波（如透過網際網路的傳輸）。計算機可讀記錄媒體可以是分佈在連到網路的計算機系統裡，可以以計算機可讀碼的形式儲存和操作。

本發明使用是薄而小的行動通訊終端，也可以把它用於更廣範圍產品的真實產品鑑定，不僅包括在購買時需要進行真實產品鑑定的產品，如衣服、鞋類、皮革製品、飲料、農產品&家畜物品、毒品&藥品、電子產品、機械產品，而且包括需要連續、長期進行真實產品鑑定的產品，如首飾、工藝品、估價報告書、入場券、證書、用於設備、錢、銷售的有價証券、重要文件的票據等。

另外，透過使用根據本發明的具有標籤讀取功能的行動通訊終端，購買者可以隨時隨地很容易很方便地檢測產品的真偽，批發商無法試圖欺騙購買者而賣一個偽造產品，因為批發商不知道購買者何時進行真實產品鑑定。還有，如果行動通訊終端分發給大量的消費者，消費者或批發商的批發和採買傾向可大大降低。由於行動通訊終端以純文字顯示產品資訊，購買者還可直接、容易地檢測真實產品鑑定的結果，從而具有更高可靠性。

還有，根據依照本發明的行動通訊終端，由於真實產

品鑑定倚賴密鑰的有效性，顯示在便攜式終端上的內容倚賴肉眼的確定，就不需要額外地訪問網路或事先評估並儲存大量數據。另外，即使同樣密鑰的情況下，產品可以由顯示的內容而區別。因此，如果同樣的密鑰應用到已分發的新產品或其它種類產品上，也可進行產品的真偽鑑定而不需要升級標籤讀取器。還有，根據依照本發明的標籤和行動通訊終端，透過包含可創建許多密鑰的密鑰創建模組或儲存多個密鑰，可以利用有限的記憶體保護許多密鑰。即使在已經得到行動通訊終端後，有可能透過給引進的產品分發新密鑰，組合更多的產業類型、品牌或產品在真實產品鑑定的項目裡。還有，即使當一個產業類型、品牌或產品的密鑰洩漏出去，其它產業類型、品牌或產品的密鑰是不一樣的，從而維持安全性。如果一個密鑰洩漏出去，透過給額外已發布的產品分發新密鑰，有可能更有效地防止關於額外已發布的產品的偽造讀取器的使用。因此，本發明具有超過以前技術的優點：透過升級已發布的許多標籤讀取器，可以把一個讀取器用於新產品。

另外，根據本發明，透過限制讀取次數，可以防止標籤的重複使用而不毀壞標籤。還可防止不應該被重複使用的標籤被偽造產品重複使用，與物理方法相比具有更高可靠性。還有，透過每次讀取時執行記憶體刷新程式，可以克服電子記憶體裡數據保存期限的限制，用於需要長期擁有的產品，如古董或工藝品，擴展可實用產品的範圍。另外，根據本發明，可以阻止真實產品鑑定消息被盜用、或

透過重送攻擊而試圖複製一個鑑定系統，增強真產品鑑定的可靠性。另外，根據本發明，如果密鑰被洩漏，可以透過一個新分發的標籤而離線地升級行動通訊終端。因此，從用戶的角度，可以升級讀取器而不需要任何操作，可以減少出現偽造產品造成的損壞。另外，根據本發明，由於可以進行行動通訊終端之間的互相鑑定，可防止利用偽造的便攜式標籤讀取器工作於偽造的非接觸通訊標籤。

雖然本發明已以較佳實施例揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

圖 1 是根據本發明解釋真實產品鑑定系統的概觀。

圖 2 表明根據本發明的非接觸通訊標籤的架構。

圖 3 是根據本發明的行動通訊終端架構的示意方塊圖。

圖 4A 是根據加密／解密單元 210 第三實施例解釋示範的密鑰。

圖 4B 是根據加密／解密單元 210 第八實施例解釋示範的密鑰。

圖 5 表明根據本發明的行動通訊終端的產品資訊讀取過程的流程圖。

圖 6 表明標籤和行動通訊終端之間通訊過程的流程圖。

圖 7 表明根據本發明的實施例在行動通訊終端#1 和行動通訊終端#2 之間執行的鑑定過程的流程圖。

圖 8 表明根據本發明的較佳實施例提供真實產品鑑定服務的方法的流程圖。

【主要元件符號說明】

10、10-1、10-2、10-3：非接觸通訊標籤

20：標籤讀取器

20-1、20-2：行動通訊終端

30：用戶伺服器

40：服務管理伺服器

50：品牌擁有者伺服器

①~④：步驟

100：非接觸通訊裝置

110、510：天線

131、531：能量供給單元

133、533：解調單元

135、535：調變單元

200、700：控制單元

210、710：加密／解密單元

220、790：洩漏密鑰升級單元

230、730：重送攻擊防止單元

250、760：資訊提供單元

270：後管理處理單元

290、720：刷新處理單元

- 300、910：儲存單元
- 310：密鑰說明資訊
- 330：密鑰
- 350：計數器
- 370：產品資訊
- 390：讀取細節資訊
- 500：標籤通訊單元
- 711：鑰匙創建單元
- 750：資訊讀取單元
- 770：讀取器鑑定單元
- 930：操縱單元
- 950：顯示單元
- 960：聲音輸出單元
- 970：無線通訊單元
- 410、411、413、415：密鑰
- 420、490：密鑰創建資訊
- 421、423、425：索引
- 430、450、470：密鑰表
- 431、451、471：密鑰說明資訊索引
- 433、453、473：密鑰
- 435、455、475：產業類型
- 491、493、495：參數
- S500～S550、S600～S665、S700～S750、S800～
S850：步驟

五、中文發明摘要：

一種具有標籤讀取功能的行動通訊終端和提供真產品鑑定服務的方法。具有標籤讀取功能的行動通訊終端基於接收自標籤的信號而從自身的多個密鑰裡指定一個密鑰，其對應於儲存在標籤裡的一個密鑰。行動通訊終端從標籤裡接收加密的產品碼或產品資訊，並把收到的產品碼或產品資訊用一個密鑰解密。另外，行動通訊終端在液晶顯示器（LCD）窗口上顯示解密結果，或發出信號聲或語音。

六、英文發明摘要：

Provided are a mobile communication terminal having a tag read function and a method of providing genuine product authentication service. The mobile communication terminal having the tag read function specifies an encryption key corresponding to an encryption key stored in the tag from its own plurality of encryption keys based on a signal received from the tag. The mobile communication terminal receives an encrypted product code or product information from the tag and decrypts the received product code or product code using an encryption key. Also, the mobile communication terminal outputs a result of decryption on a liquid crystal display (LCD) window or as beep sounds or voices.

十、申請專利範圍：

1. 一種行動通訊終端，從一非接觸通訊標籤接收資訊，該行動通訊終端包括：

一第一通訊單元，與該非接觸通訊標籤無線地交換數據，並無線地發送該非接觸通訊標籤需要的電能；

一第二通訊單元，透過一無線通訊網向一服務管理伺服器發送和接收數據；

一儲存單元，儲存有至少一個密鑰相關資訊；

一解密單元，基於密鑰相關資訊對於從該非接觸通訊標籤收到的數據進行解密，前述密鑰相關資訊是透過接收自該非接觸通訊標籤的密鑰說明資訊而從密鑰相關資訊中選出的；

一資訊讀取設備，向附在產品上的該非接觸通訊標籤要求產品資訊，並讀出來自該非接觸通訊標籤的產品資訊；以及

一輸出單元，輸出讀出的產品資訊。

2. 如申請專利範圍第 1 項所述之行動通訊終端，其中密鑰相關資訊包括至少一個密鑰，該解密單元透過選擇出的密鑰把接收自該非接觸通訊標籤的產品資訊解密，這個選擇出的密鑰是基於接收自該非接觸通訊標籤的密鑰說明資訊所選擇。

3. 如申請專利範圍第 2 項所述之行動通訊終端，進一步包括一洩漏密鑰升級單元，當從該非接觸通訊標籤收到關於一洩漏密鑰的密鑰升級請求資訊時，從該儲存單元裡

放棄由密鑰升級請求資訊指定的密鑰，並升級為新分發的密鑰。

4.如申請專利範圍第 1 項所述之行動通訊終端，其中密鑰相關資訊包括多個密鑰，根據分類參考被分類與分發，分類參考包括產業類型、生產商、品牌與產品名至少其中一個；以及

該解密單元利用密鑰把從該非接觸通訊標籤收到的產品資訊解密，這個密鑰是基於接收自該非接觸通訊標籤的密鑰說明資訊而從多個密鑰中選出的。

5.如申請專利範圍第 1 項所述之行動通訊終端，其中密鑰相關資訊包括至少一個種子值，用於不同密鑰的創建；以及

該解密單元利用使用一種子值的密鑰把從該非接觸通訊標籤收到的產品資訊解密，這個種子值是基於接收自該非接觸通訊標籤的密鑰說明資訊選出的。

6.如申請專利範圍第 5 項所述之行動通訊終端，進一步包括一洩漏種子值升級單元，當從該非接觸通訊標籤收到關於一洩漏種子值的種子值升級請求資訊時，從該儲存單元裡刪除由種子值升級請求資訊指定的種子值，並升級為新分發的種子值。

7.如申請專利範圍第 1 項所述之行動通訊終端，其中密鑰相關資訊包括多個種子值，根據分類參考被分類與分發，分類參考包括產業類型、生產商、品牌與產品名至少其中一個；以及

該解密單元利用密鑰把從該非接觸通訊標籤收到的產品資訊解密，這個密鑰是基於從多個種子值裡選出的種子值創建的，多個種子值是基於接收自該非接觸通訊標籤的密鑰說明資訊。

8.如申請專利範圍第 1 項所述之行動通訊終端，進一步包括一洩漏密鑰升級單元，當從該非接觸通訊標籤收到關於洩漏密鑰相關資訊的升級請求資訊時，從該儲存單元裡刪除由升級請求資訊指定的密鑰相關資訊，並升級為新分發的密鑰相關資訊。

9.如申請專利範圍第 1 項所述之行動通訊終端，進一步包括一重送攻擊阻止單元，它產生一一次性使用隨機數字，並把該一次性使用隨機數字加到要發送到標籤讀取器的資訊上，且提供此資訊給該解密單元，並檢測從接收自標籤讀取器的資訊裡提取出的隨機數字是否與該一次性使用隨機數字一樣，從而阻止重送攻擊。

10.如申請專利範圍第 1 項所述之行動通訊終端，其中該儲存單元包括非易失性記憶體，且進一步包括一刷新處理單元，其從該儲存單元裡讀出產品資訊，並把讀出的產品資訊重記錄在該儲存單元裡。

11.如申請專利範圍第 1 項所述之行動通訊終端，其中無線通訊單元的射頻 (RF) 電路、資訊讀取單元、解密單元與儲存單元是由特定用途積體電路 (ASIC) 實現的。

12.如申請專利範圍第 1 項所述之行動通訊終端，其中該資訊讀取單元從基於接收自該非接觸通訊標籤的密鑰說

明資訊的產業類型、生產商、品牌與產品名中指定多個產品資訊，並把指定的多個產品資訊提供給該輸出單元，而該輸出單元輸出指定的多個產品資訊。

13.如申請專利範圍第1項所述之行動通訊終端，進一步包括一讀取器鑑定單元，其透過與具有標籤讀取功能的一外部行動通訊終端的通訊，來鑑定具有標籤讀取功能的該外部行動通訊終端，並把關於具有標籤讀取功能的該外部行動通訊終端的鑑定結果輸出到該輸出單元。

14.如申請專利範圍第1項所述之行動通訊終端，進一步包括一加密單元，基於從密鑰相關資訊中選出的密鑰相關資訊，透過接收自該非接觸通訊標籤的密鑰說明資訊，把要發送到該非接觸通訊標籤的數據加密。

15.如申請專利範圍第1項所述之行動通訊終端，如果透過含在該行動通訊終端裡的一資訊輸入裝置輸入一採買確認命令，其中的資訊發送單元把產品的採買資訊加到確定結果中，並把確定結果發送到該服務管理伺服器。

16.如申請專利範圍第1項所述之行動通訊終端，其中一確定結果在每次讀取產品資訊時都儲存在該儲存單元；以及

如果透過含在行動通訊裝置裡的一資訊輸入裝置輸入一資訊發送命令，資訊發送單元把儲存在該儲存單元的該確定結果發送到該服務管理伺服器。

17.一種管理產品鑑定服務的方法，適用在一產品鑑定服務管理伺服器裡，該產品鑑定服務管理伺服器透過一網

路與一行動通訊公司的一用戶伺服器通訊，並可透過一行動通訊網與行動通訊終端通訊，該管理產品鑑定服務的方法包括：

接收讀取細節資訊，包括分發給每個標籤可讀取的產品的產品識別號，和從行動通訊終端分發給行動通訊終端的讀取器識別號；

詢問該用戶伺服器查詢含在讀取細節資訊裡基於行動通訊終端的識別號的用戶資訊，並接收來自該用戶伺服器的用戶資訊；

創建與儲存客戶管理資訊，包含基於讀取細節資訊與用戶資訊的用戶分類資訊與產品資訊讀取細節；以及

回應從一外部設備輸入的資訊輸出請求而讀出並輸出客戶管理資訊。

18.如申請專利範圍第 17 項所述之管理產品鑑定服務的方法，其中的用戶分類資訊包括用戶的年齡、地區、性別與工作至少其中一項；以及

讀取細節資訊包括產業類型、生產商、品牌、等級、式樣名、生產中心、生產日期時間、產品序列號、產品價格與鑑定日期至少其中一項。

19.如申請專利範圍第 18 項所述之管理產品鑑定服務的方法，其中的讀取細節資訊進一步包括關於已採買的產品的採買資訊，其包括採買價格和採買日期與時間。

20.如申請專利範圍第 17 項所述之管理產品鑑定服務的方法，進一步包括根據讀取細節資訊增加用戶的積分點。

21.如申請專利範圍第 17 項所述之管理產品鑑定服務的方法，進一步包括透過檢測包含在讀取細節資訊裡的產品識別號和讀取器識別號是否與包含在先前從行動通訊終端收到的讀取細節資訊裡的一樣，從而檢測資訊的重複發送。

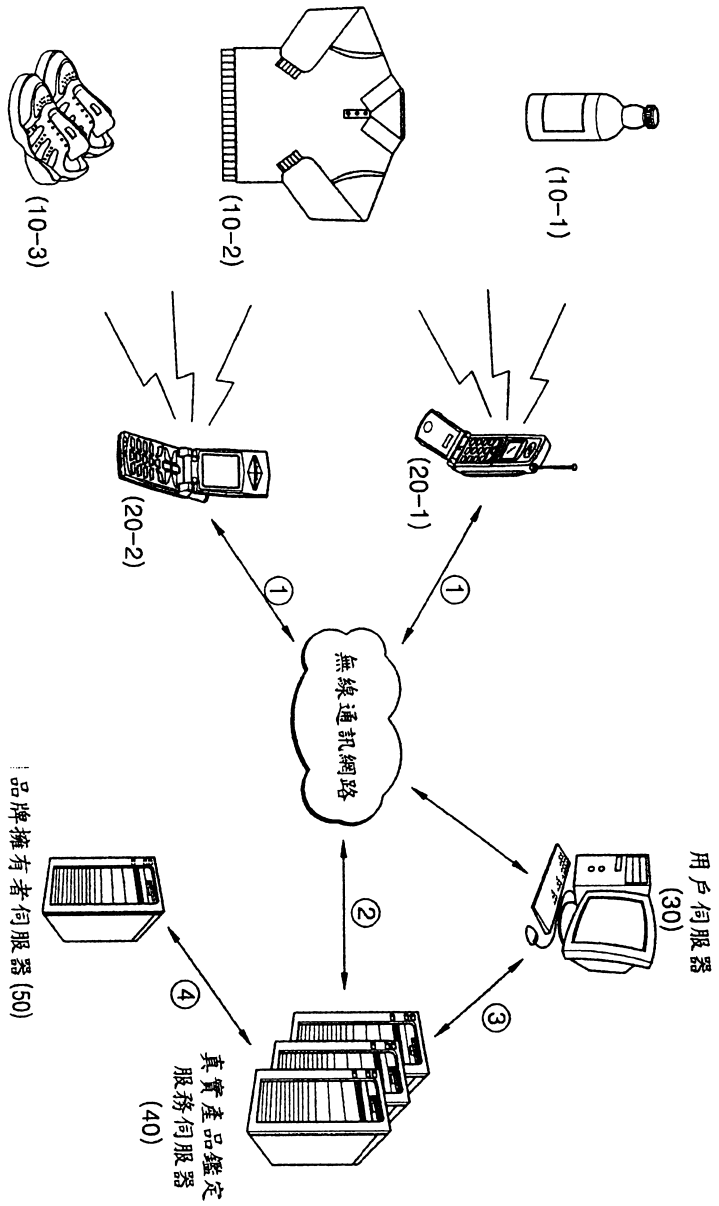


圖 1

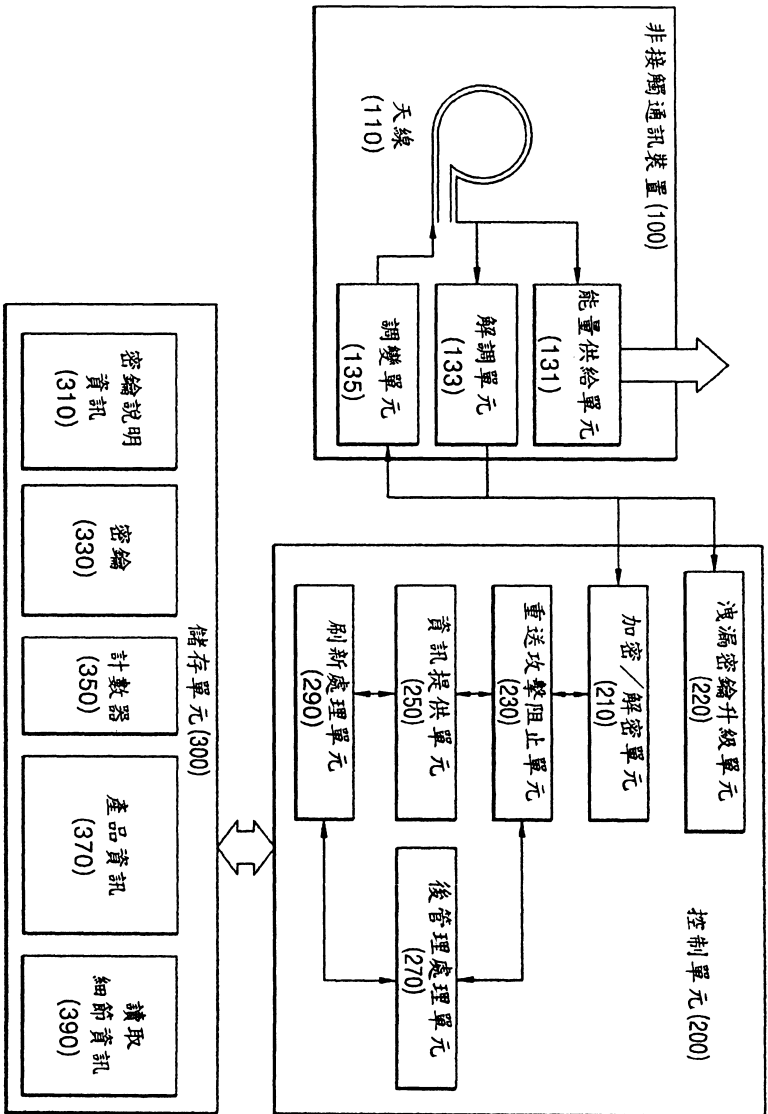


圖 2

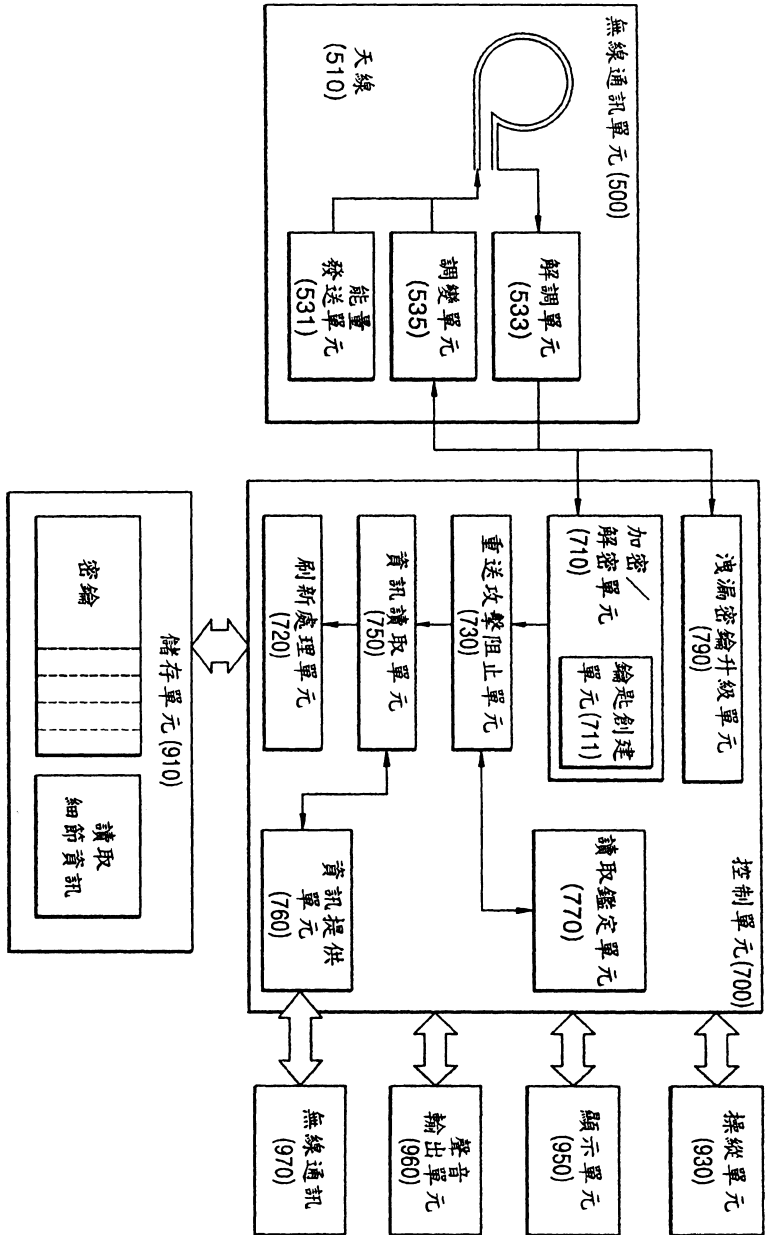


圖 3

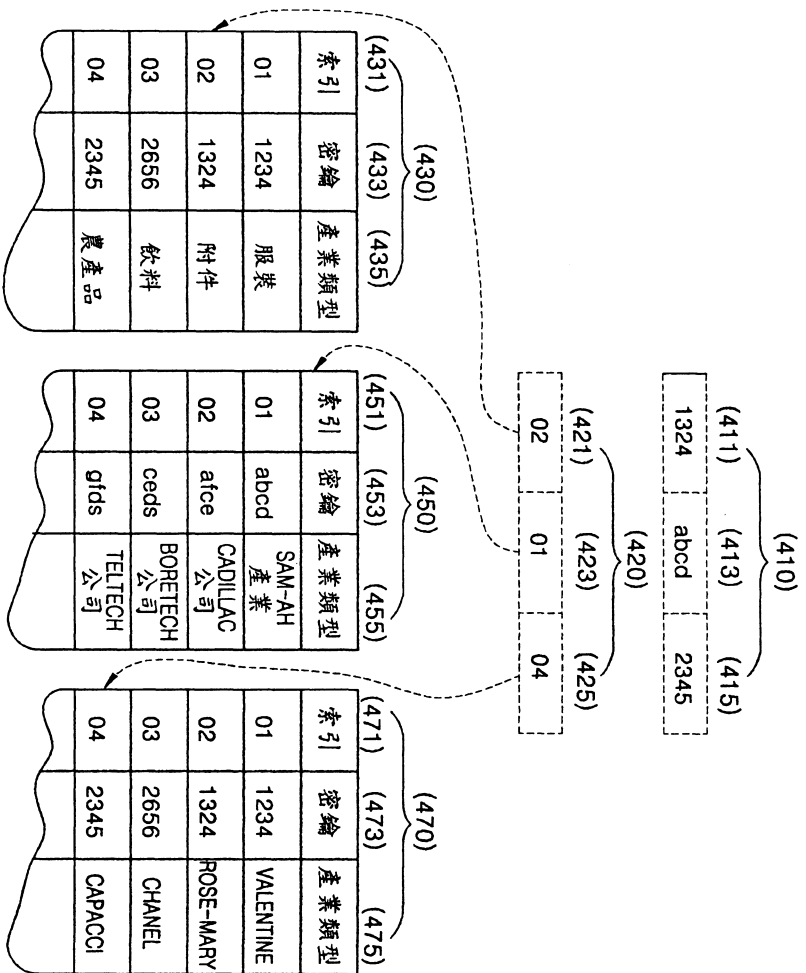


圖 4A

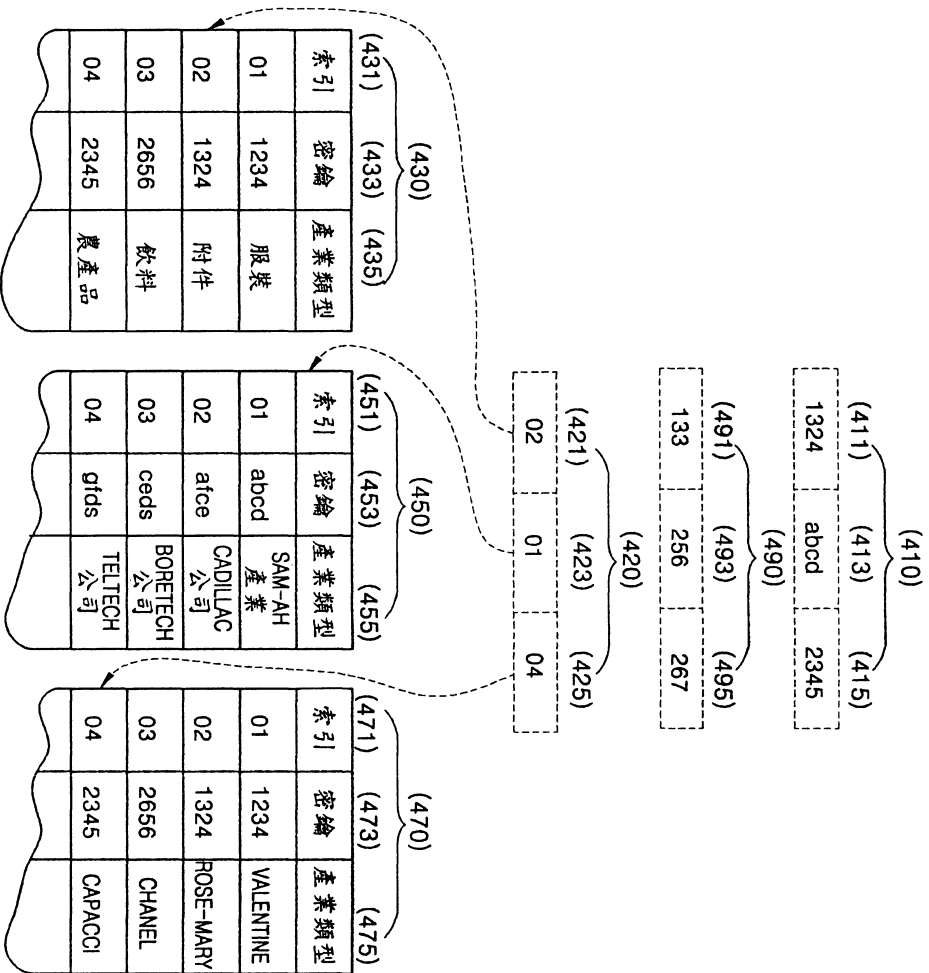


圖 4B

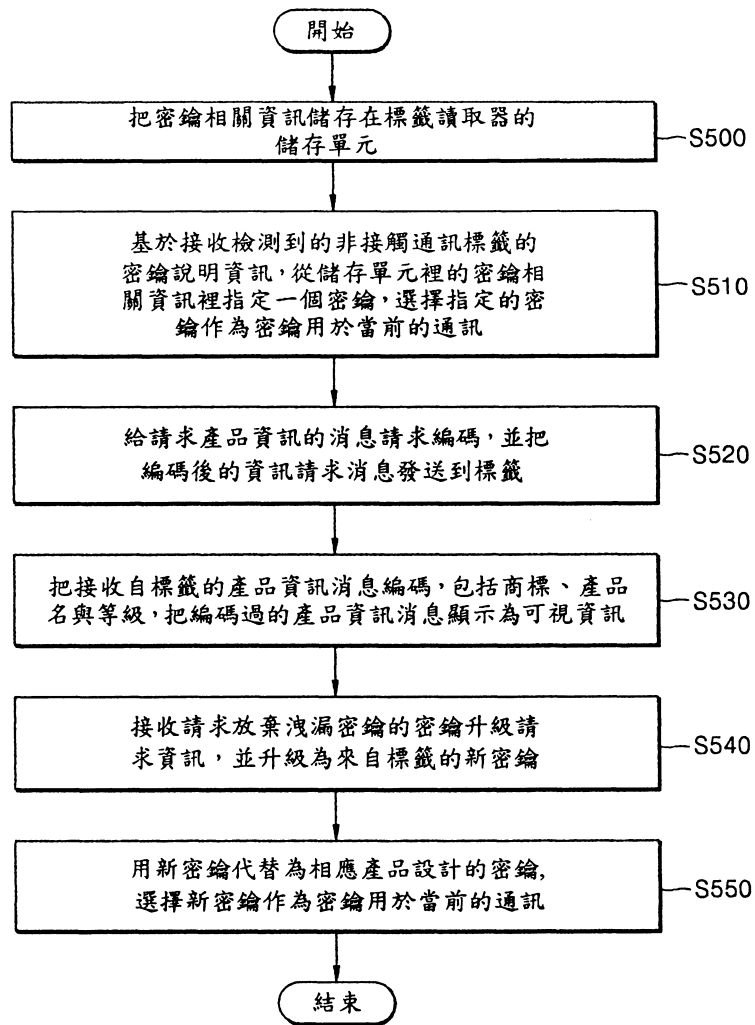


圖 5

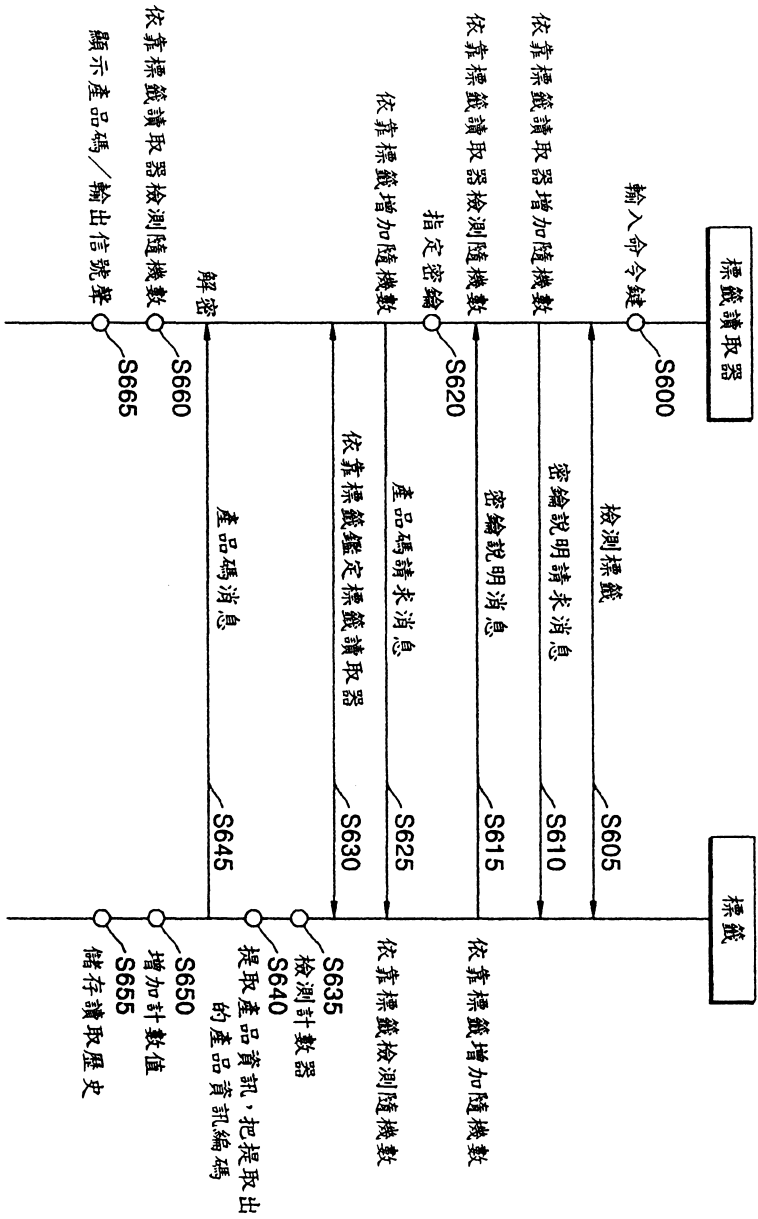


圖 6

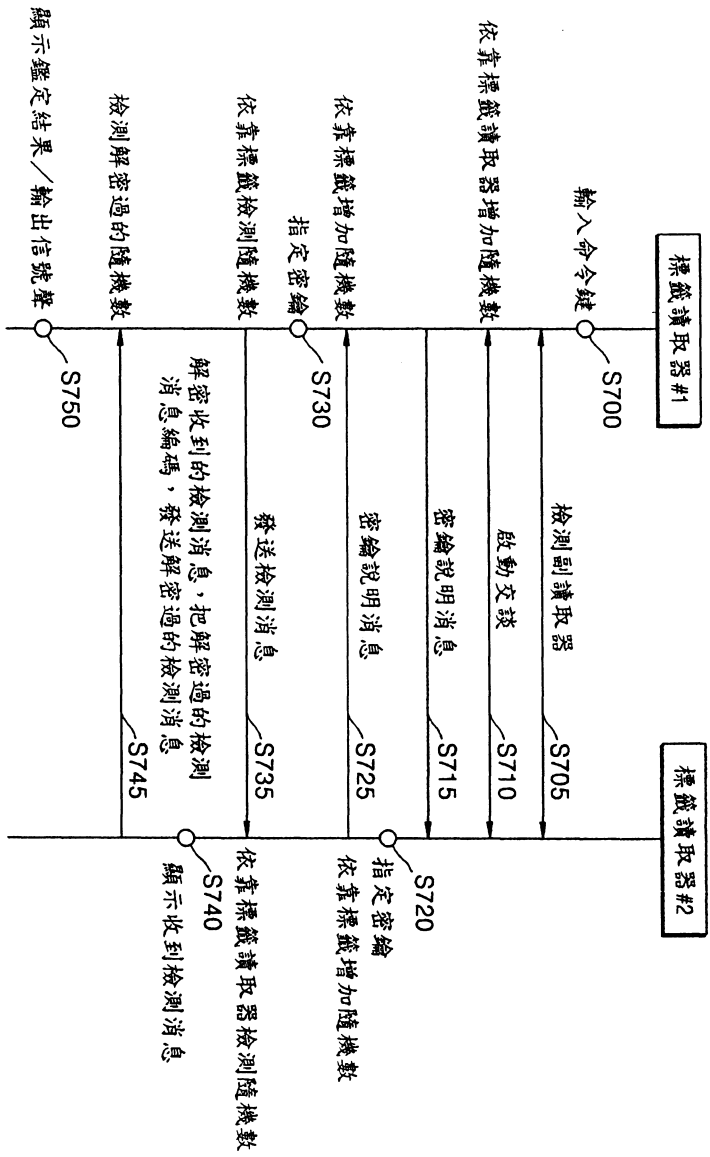


圖 7

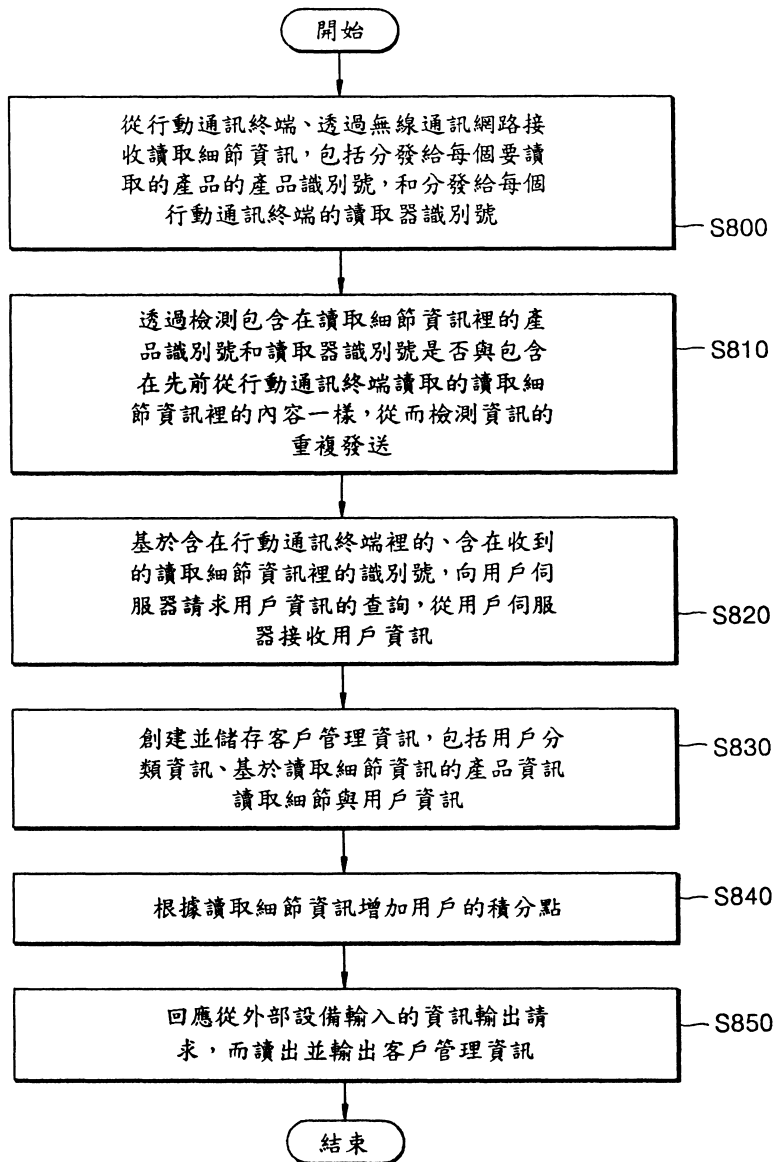


圖 8

七、指定代表圖：

(一)本案指定代表圖為：圖(8)。

(二)本代表圖之元件符號簡單說明：

S800~S850：步驟

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

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：93130200

※ 申請日期：93.10.6

※IPC 分類：G06K 7/00
H04L 9/14

一、發明名稱：(中文/英文)

(2006.01)

具有從非接觸式通訊標籤讀取資訊之功能的行動通訊終端以及管理產品鑑定服務的方法

MOBILE COMMUNICATION TERMINAL HAVING A FUNCTION OF READING OUT INFORMATION FROM CONTACTLESS TYPE COMMUNICATION TAG AND METHOD FOR MANAGING PRODUCT AUTHENTICATION SERVICE

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

朴美卿/PARK, MI KYOUNG

指定 為應受送達人

代表人：(中文/英文)

住居所或營業所地址：(中文/英文)

大韓民國漢城市瑞草區瑞草洞 1608-2 番地西建亞特米納 303 號
RM. 303, SEOGEON ART VILLA, 1608-2, SEOCHO-DONG
SEOCHO-GU, SEOUL, REPUBLIC OF KOREA

國 籍：(中文/英文) 韓國/KR

三、發明人：(共 2 人)

姓 名：(中文/英文) ID :

1. 朴美卿/PARK, MI KYOUNG
2. 玄光哲/HYUN, KWANG CHUL