拾壹、圖式：

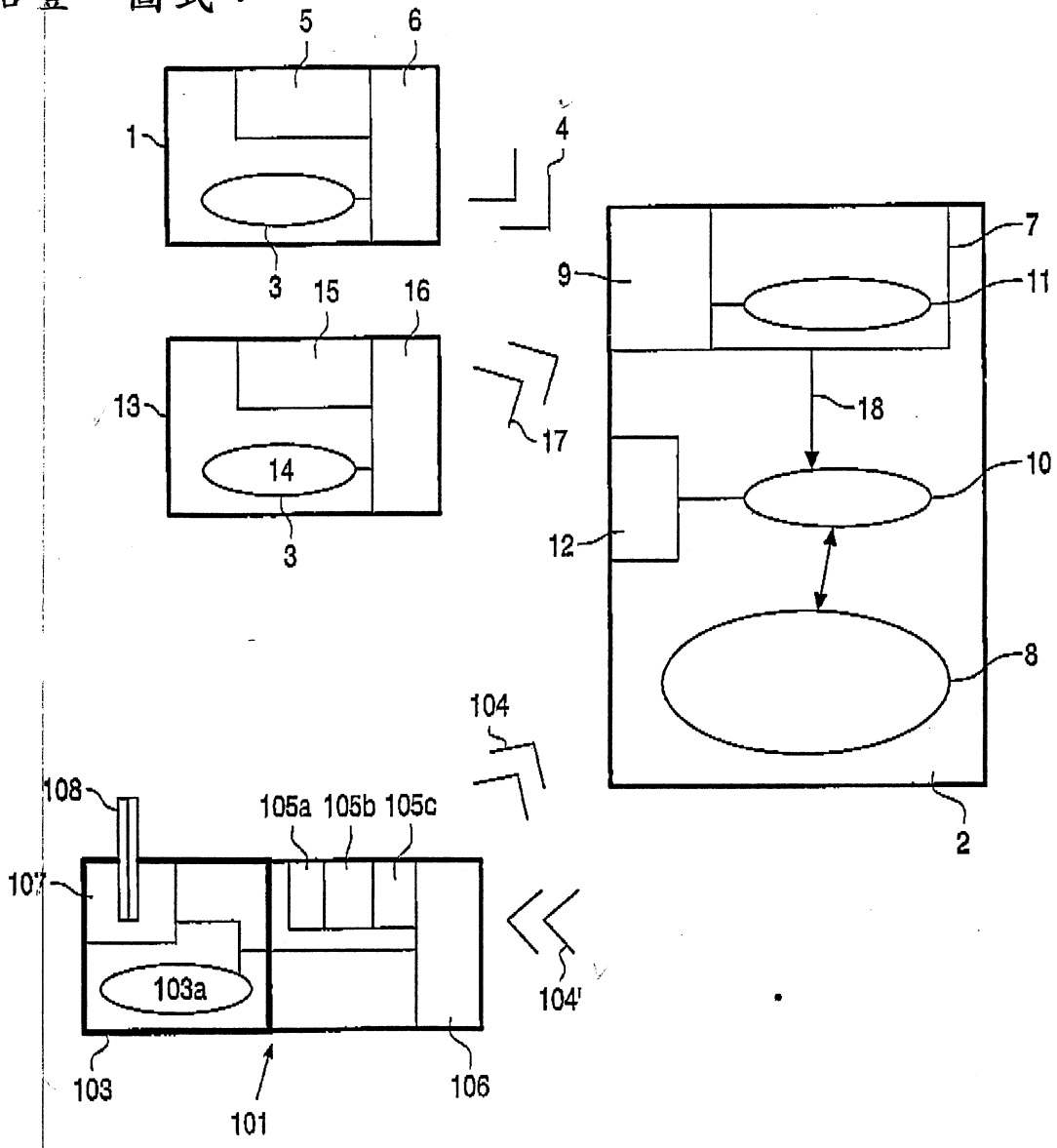
5
6
1
4
3
15
16
13
14
17
7
9
11
18
10
12
8
2
104
108
105a 105b 105c
107
103a
104'
103
101
106

圖　1

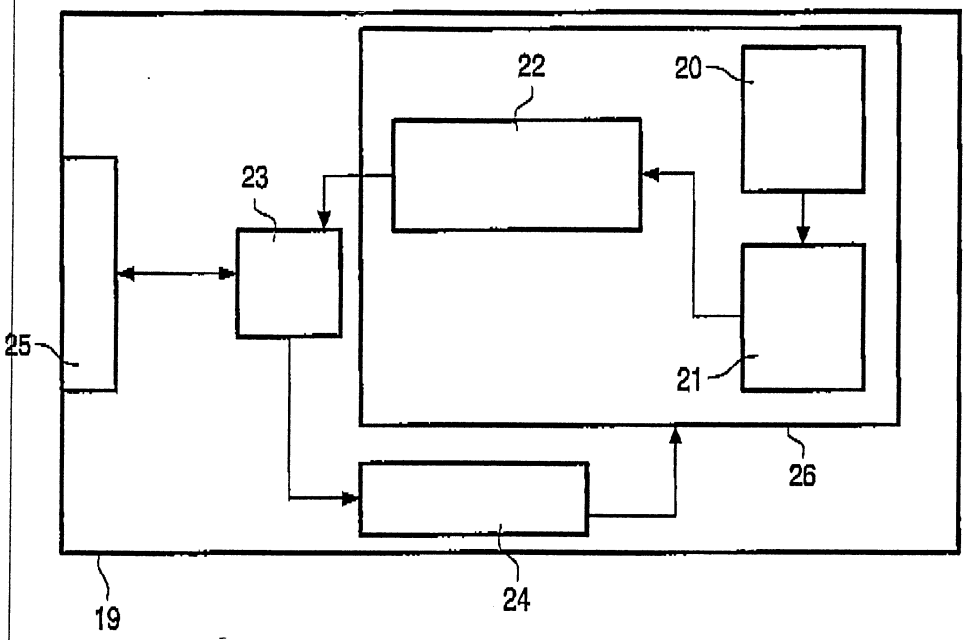
22
20
23
25
21
26
19
24

圖　2

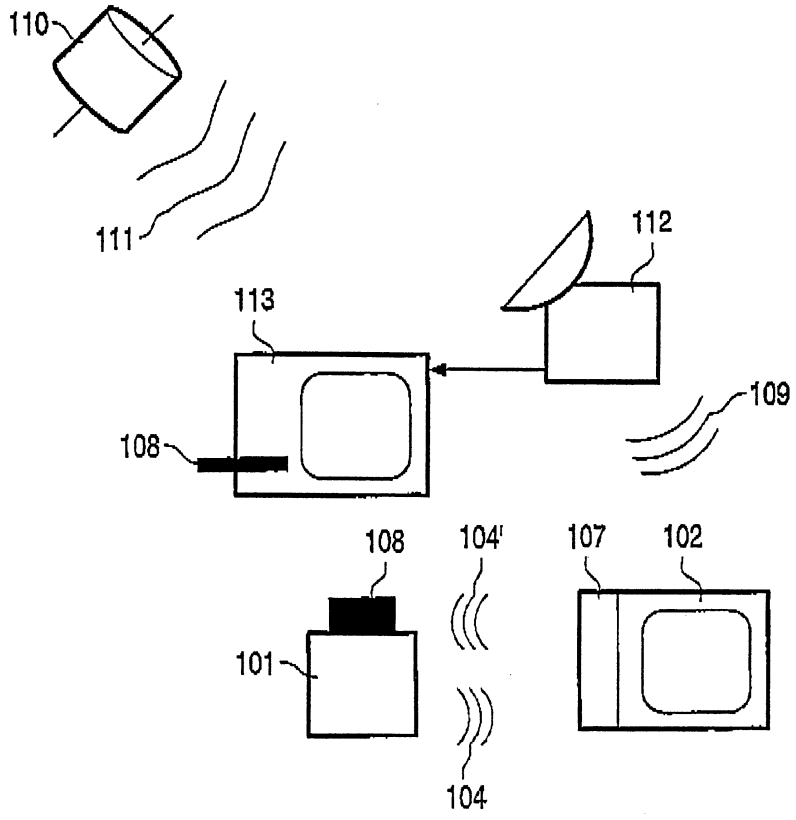
110
111
112
113
109
108
108
104'
107
102
101
104

圖　5

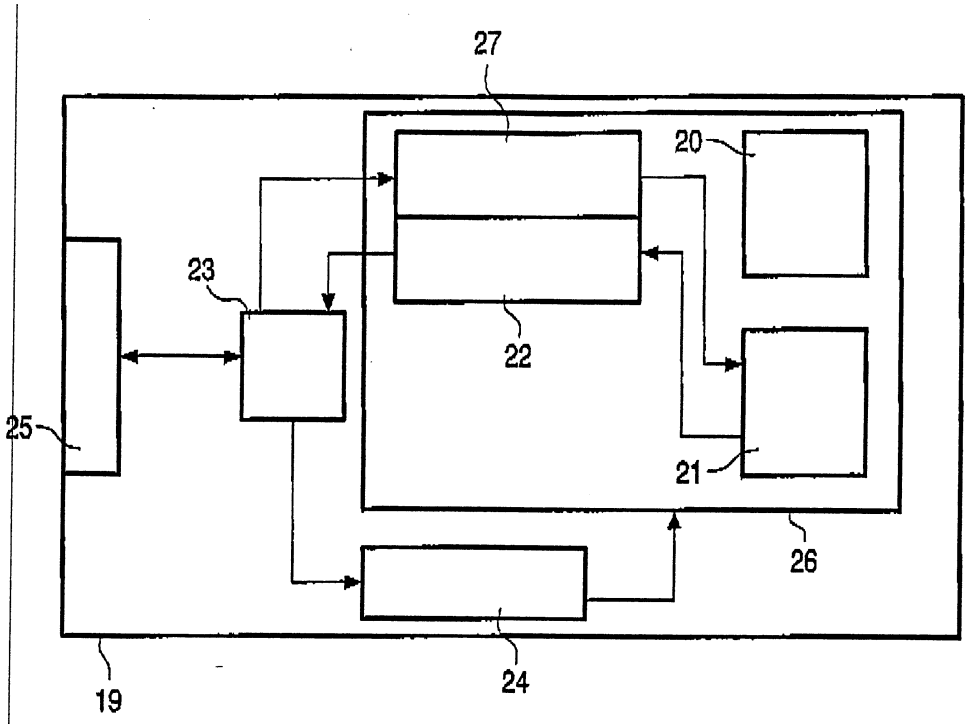

圖 3

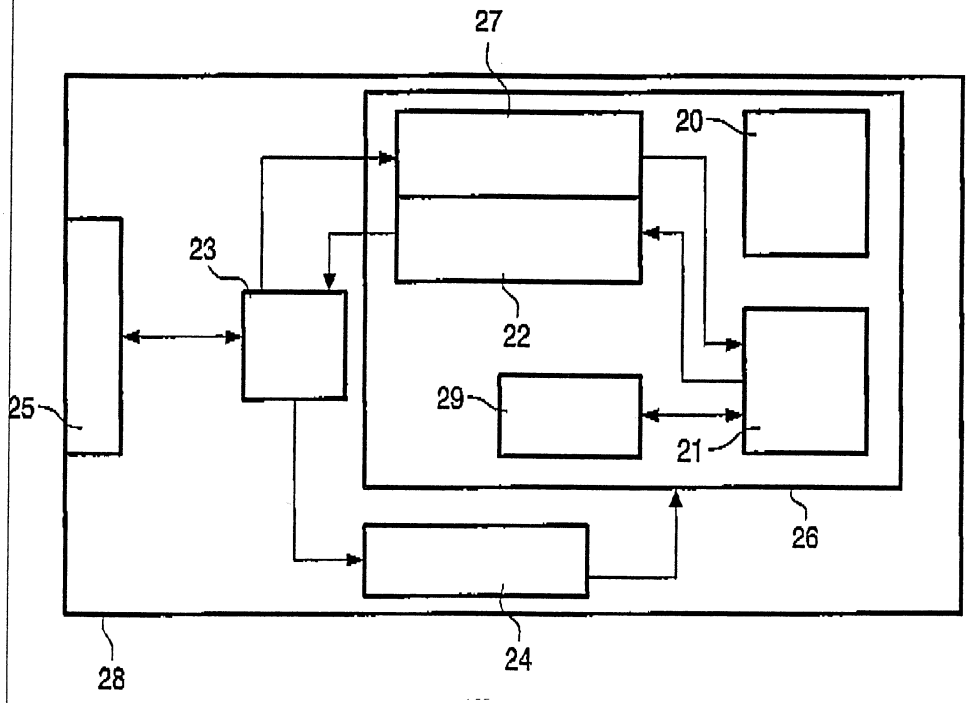

圖 4

公告本

95年10月30日修(更)替換頁

I281809

發明專利說明書

中文說明書替換本(95 年 10 月)

（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：092120404

※ 申請日期：92-7-25　　※IPC 分類：H04L 9/08 (2006.01)

壹、發明名稱：（中文/英文）

供無線網路中裝置用之安全系統

SECURITY SYSTEM FOR APPARATUSES IN A WIRELESS NETWORK

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

荷蘭商皇家飛利浦電子股份有限公司

KONINKLIJKE PHILIPS ELECTRONICS N.V.

代表人：（中文/英文）

J. L. 凡　德　渥

J. L. VAN DER VEER

住居所或營業所地址：（中文/英文）

荷蘭愛因和文市格羅尼渥街1號

GROENEWOUDSEWEG 1 5621 BA EINDHOVEN THE NETHERLANDS

國　籍：（中文/英文）

荷蘭　　THE NETHERLANDS

參、發明人：(共 4 人)

姓　名：(中文/英文)

1. 托比亞斯　黑爾畢格
   TOBIAS HELBIG
2. 沃夫甘　奧圖　布狄
   WOLFGANG OTTO BUDDE
3. 奧利佛　史利爾
   OLIVER SCHREYER
4. 亞曼德　雷肯斯
   ARMAND LELKENS

住居所地址：(中文/英文)

1. 德國艾辰市亞爾特街88號
   ALTSTR. 88. 52066 AACHEN, GERMANY
2. 德國艾辰市森克街6號
   SENKESTR. 6, 52076 AACHEN, GERMANY
3. 德國赫索真萊斯市朵倫路30號
   DOHLENWEG 30, 52134 HERZOGENRATH, GERMANY
4. 荷蘭西爾蘭市卓克史密特街5號
   JOKE SMITSTRAAT 15, 6416 HS HEERLEN, THE NETHERLANDS

國　籍：(中文/英文)

1. 德國　GERMANY
2. 德國　GERMANY
3. 德國　GERMANY
4. 荷蘭　THE NETHERLANDS

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為： 年 月 日。

☐ **本案申請前已向下列國家（地區）申請專利：**

1. 德國；2002年07月29日；10234643.7
2. 德國；2002年11月23日；10254747.5
3.
4.
5.

☐ **主張國際優先權(專利法第二十四條)：**

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1. 德國；2002年07月29日；10234643.7
2. 德國；2002年11月23日；10254747.5
3.
4.
5.

☐ **主張國內優先權(專利法第二十五條之一)：**

【格式請依：申請日；申請案號數 順序註記】

1.
2.

☐ **主張專利法第二十六條微生物：**

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明：

【發明所屬之技術領域】

本發明通常係有關用於網路(特別是無線網路)的安全系統。

【先前技術】

用於支援行動裝置(例如行動電話)或取代在靜止裝置(例如，個人電腦與電話連接)間的有線解決方案之無線通訊已廣泛使用。

對於未來數位家用網路，此表示他們不僅只典型地由複數個有線裝置組成，而且亦由複數個無線裝置組成。當實施數位無線網路時，可使用例如藍芽、DECT與特別是"無線區域網路"的IEEE 802.11標準的家用網路、無線電技術。無線通訊亦經由紅外線(IrDA)連接實施。

同樣地，用於通知或娛樂使用者的網路未來亦特別包含以無線方式而彼此通訊的裝置。特別是提到的所謂特別網路(暫時安裝的網路)通常具有不同擁有者的裝置。此特殊網路範例可在旅館找到：例如，一用戶想要經由旅館房間的立體音響安裝而將在他MP3播放器上的音樂歌曲再生。一進一步範例是使用通訊無線裝置的人彼此符合以交換資料或媒體內容(影像、影片、音樂)的各種類型遭遇。

當使用無線電技術時，例如一MP3儲存裝置與一高傳真安裝的裝置可經由如同資料連接的無線電波而以無線方式彼此通訊。主要是有兩個模式。裝置可隨著不同裝置(如同一對等網路)、或經由當作一分配器台的中央存取點而直接

彼此通訊。

無線電技術在建築物內具有數十公尺的範圍(在IEEE 802.11多達30公尺)，而在空曠區域具有數百公尺範圍(在IEEE 802.11多達300公尺)，此是因標準而定。無線電波亦可貫穿住處或房子的牆壁。在無線電網路的頻率涵蓋中(亦即在它的範圍內)，傳送的資訊主要是經由具有一對應無線電介面的任何接收器而接收。

此使它需要從未經認可或無意間聽到、或偷聽傳送的資訊、以及對網路及其資源未經認可存取來保護無線網路。

傳輸資訊的存取控制與保護的方法在無線電標準方面描述(例如，在 傳送資訊的存取控制與保護的方法是在無線電標準(例如，1999年8月於紐約第8章"IEEE802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Standard, IEEE"中描述。在無線網路與特別是在IEEE 802.11標準中，任何形式的資料安全性最後是根據只有經認可的通訊夥伴知道的秘密加密碼(鑰匙)或密碼。

存取控制表示一區別可在經認可與未經認可的裝置之間達成，亦即一裝置允許存取(例如，獲得通訊請求的一存取點、或一住家裝置或特別網路)是經由一裝置請求存取是否授權的的傳送資訊而決定。在例如容易聽的無線電媒體中，因為一未經認可的裝置可透過監聽此傳輸而獲得存取需要的存取資訊，所以存取碼的簡單傳輸、或識別符的使用(透過裝置允許存取與經認可的裝置的識別符清單的比較)會不適用。

與IEEE 802.11有關使用的MAC位址過濾不能確保在簡單形式的安全保護。在此方法中，存取點可儲存授權存取網路的裝置的MAC(媒體存取控制)位址清單。當一未經認可的裝置嘗試存取網路時，它便會被拒絕，因為存取點不知道MAC位址。除了需要管理家用網路的MAC位址清單之外的無法接受的使用者不友善，此方法的特殊缺點是可能有假的MAC位址。未合法的使用者只需要獲得有關"經認可"MAC位址，當在無線電路由上偷聽時，此"經認可"MAC位址可簡單獲得。存取控制因此耦合到根據秘密或密碼的確認。

IEEE 802.11標準係定義經認可的裝置是透過知道一秘密鑰匙而區別的"共用鑰匙授權"。認證然後依下列執行。若要確定授權，用以確保存取的裝置係傳送一任意值(要求)，而且該用以請求存取的裝置係使用秘密鑰匙來加密，並將它傳回。如此，用以允許存取的裝置可確認鑰匙，因此給予存取授權(此方法通常亦稱為"要求反應方法")。

在加密期間，傳送的資訊是透過傳輸裝置加密，並經由接收裝置解密，所以資料對於未經認可或無心的收聽者是無用的。為了此目的，IEEE 802.11標準使用 Wired Equivalent Privacy (WEP)加密方法。在此方法中，在網路的所有裝置知道但是對於其他裝置是秘密一鑰匙(40個位元或104個位元WEP鑰匙)是在加密演算法中當作參數使用，而且是在用以將傳送的資料加密的IEEE 802.11標準中定義。

在WEP的情況，相同鑰匙亦用於認證。除了"對稱"加密

方法(使用一共用鑰匙)之外，亦使用公眾/私人鑰匙方法，其中每個裝置可提供作為加密的的一般已知鑰匙(公眾鑰匙)，而且具有只有此裝置知道的一相關秘密鑰匙(私人鑰匙)，其可提供將經由公眾鑰匙加密的資訊解密的可能性。

此可在沒有預先知道一秘密共用鑰匙來提供監聽安全性。然而，當使用此方法時，在使用通常已知的鑰匙的情況，對於任意裝置採取與一裝置(例如，允許存取的裝置)通訊是可能的。因此，用於存取控制的認證在此情況亦需要，而且是再次根據通訊夥伴預先知道的一秘密鑰匙。

對於較大的資料安全性而言，網路裝置包含用於暫時鑰匙協議的機構，即是於一段時間用於加密的鑰匙，所以相同的秘密鑰匙不會始終使用。然而，這些暫時鑰匙的交換需要一安全監聽傳輸，其次需要通訊夥伴預先知道的至少一第一秘密鑰匙。對於本發明而言，經由加密的資料安全性亦根據通訊夥伴預先知道的一(第一)秘密鑰匙是必要的。結果，產生所有相關裝置的一秘密鑰匙(用於認證及/或加密)的一建構步驟對於提供有關無線網路的安全系統是必需的。

無線網路的一特殊觀點是此鑰匙不應該將清楚的本文(未加密)經由無線通訊介面傳送，因為未經認可的裝置透過監聽而未經認可存取鑰匙來獲得資訊。例如迪費-赫爾曼(Diffie-Hellman)方法的一編碼方法可在經由一無線電介面的兩個通訊夥伴之間的一秘密共用鑰匙上確保協議竊聽的安全性。然而，若要未經認可的裝置開始與網路的一(存取

允許)裝置的鑰匙協議，此方法必須亦耦合到通訊夥伴的認證，其次需要通訊夥伴預先知道的一(第一)秘密鑰匙。

在根據DECT標準的行動電話，一第一鑰匙已透過在裝置(基地台與收聽者)中的業者儲存。若要識別基地台的新收聽者，儲存在基地台的鑰匙(PIN碼)應該由使用者提供給新的收聽者。既然使用者應該知道此目的的鑰匙，所以鑰匙可在例如基地台的標籤上獲得。

使用專屬基本結構的以IEEE 802.11為主之公司或校園網路通常是透過專家系統管理者建置。他們通常使用具有與每個存取點線路連接的系統管理電腦。經由這些線路連接(因此，類似安全監聽)，秘密鑰匙(例如，WEP鑰匙)便會傳送給存取點。輸入客戶端(例如，無線膝上型電腦)的鑰匙便能手動生效。

假設執行用於安裝一第一秘密鑰匙的結構步驟(與必需的建構步驟是在軟體介面中定義)，但是他們的實施是不固定。為了此目的，IEEE 802.11標準的第8.1.2章包含下列敘述："必需的秘密共用鑰匙是假設經由與IEEE 802.11無關的一安全通道而傳遞給參與的STAs(台)。共用鑰匙是經由MAC管理路徑而包含在唯寫的管理資訊庫(MIB)屬性"。

在網路元件之間的無線通訊中發生的進一步問題是數位資料屬性權限的安全或保護。此一數位資料保護是透過所謂數位權限管理(DRM)而確保。例如"付費電視"或"觀賞付費"的應用是根據典型儲存在晶片卡上的一解碼鑰匙，而且該解碼鑰匙可經由傳統郵局通道而規律(例如，每月)傳送給

使用者。若要讀取晶片卡，一卡片讀取裝置便整合在一解碼器，而且當使用該解碼的鑰匙時，解碼器可透過資訊供應器而將以加密形式傳送的資料解密。因為資料的未經認可使用，所以加密的資料不能以未加密的形式而從解碼器外部傳送，而不管可能的屬性權限。

然而，裝置的消費者與業者亦想要在任何地方使用供資訊再生的無線網路裝置。然而，於此目的所需的無線資訊傳輸可保護資料被監聽與濫用。

【發明內容】

本發明的目的是要在無線網路的裝置中實施一秘密鑰匙的使用者友善安裝。

目的可透過網路的安全系統解決，特別是無線網路，其包含：

- 一(第一)可攜式單元，該(第一)可攜式單元具有一鑰匙單元，用以產生可用的鑰匙記錄，並提供作為鑰匙記錄的短程資訊傳輸；及

- 在網路的至少一無線裝置中的至少一接收單元，該接收單元包含：一接收器，用以接收鑰匙記錄；及該無線裝置的一評估元件，用以儲存、處理及/或傳遞該鑰匙記錄、或一部分鑰匙記錄給第二元件。

網路的每個無線裝置包含：一無線電介面，用以傳送有用的資料；以及一接收單元，用以從第一可攜式單元接收一鑰匙記錄。若要在裝置之間的無線有用資料安全路由，一鑰匙記錄便要不被攔截而供應給每個裝置，其中這些裝

置可獲得具傳送有用資料的秘密共用鑰匙，及/或認證可被加密與解碼。如必要，有用資料的有線交換亦可使用秘密共用鑰匙而確保。此外，此鑰匙可用於保護數位內容的屬性權限，此在於相關的資料可使用一特殊加密而由擁有者傳送給末端裝置。

鑰匙記錄是由可攜式單元的鑰匙單元而產生使用，其中該可攜式單元包含一發射器、或具有一偵測器單元而可供短程傳輸的一發射器。藉使鑰匙記錄可不受攔截供應給網路的每個無線裝置。在單元上的一按鈕可用於一鑰匙記錄傳輸的觸發。此是因短程資訊傳輸的使用方法，一鑰匙記錄的傳輸亦可透過裝裝置放置在接收單元附近、及透過使偵測器單元觸發鑰匙記錄的傳輸而觸發。

鑰匙記錄包含當作一必要(而且可能單一)組成的秘密鑰匙碼("鑰匙")。若要接收鑰匙記錄，網路的每個無線裝置包含一接收單元，該接收單元是由一接收器與一評估元件所組成，在獲得鑰匙記錄之後，擷取鑰匙，並經由一內部介面而將此鑰匙傳遞給第二元件，用以將有用的資料加密及解碼(例如，用於控制無線電介面的驅動程式軟體)。

經由可攜式單元使用的短程資訊傳輸的方法是根據例如紅外線、或可見光、或超音波、或啞聲、或任何其他可控制範圍傳輸技術的磁場、電磁場。鑰匙記錄的傳輸亦能經由發射器表面上可由接收單元讀取的多維圖案實施。對於本發明而言，本質上具有非常短範圍(數公分)或短範圍與一強區域邊界(例如，紅外線)的技術可使用，所以鑰匙記錄能

從非常短的範圍供應，而且沒有穿透房間牆壁的情形。

此解決的特殊優點是未經認可的人不能夠接收鑰匙記錄。鑰匙記錄的傳輸可透過按下在可攜式單元上的按鈕、或例如當使用亦透過在接收單元附近放置可攜式單元的射頻異頻雷達收發機技術(不接觸射頻標籤技術)而觸發器。透過處理具可攜式單元的裝置(或使該單元朝向裝置)與在單元上的可能按鈕啟動，將鑰匙記錄輸入一裝置如此對於使用者是非常簡單，而且不複雜。使用者皆不需要具有關於鑰匙記錄的內容或關於秘密鑰匙的任何知識。用以輸入及管理鑰匙記錄的專家是不必需。使用者友善是此解決的進一步特殊優點。

特別是家用網路的無線網路應該不僅可供家用網路(例如，擁有者)的永久使用者的存取，而且亦提供例如用戶的暫時性使用者的限制存取。

本發明的進一步具體實施例的優點包含如鑰匙產生器表示的一元件，其中該鑰匙單元包含在鑰匙單元，並用於產生額外鑰匙記錄。鑰匙產生器是第一可攜式單元的額外元件、或在第二分開的可攜式單元中實施。

透過鑰匙產生器產生的鑰匙記錄(在此稱為用戶鑰匙記錄)是以它始終可從在單元記憶體中所儲存的一(家用)鑰匙記錄區別(例如，透過在鑰匙記錄中的特殊位元)的方式而建立。當輸入一鑰匙記錄時，它便亦始終可分明它是否為一家用鑰匙記錄輸入、或一用戶鑰匙記錄輸入。為了此目的，具記憶體與鑰匙產生器的可攜式單元具有至少兩個按鈕

(一按鈕是用於觸發來自記憶體的家鑰匙記錄傳輸，而且另一按鈕是用於觸發一用戶鑰匙記錄的傳輸)。當鑰匙產生器是在分開的第二單元中實施時，它便可明確從具家用鑰匙記錄的單元區別(例如，經由它的顏色、描述等)。

一用戶鑰匙記錄是用來允許用戶對網路資源的存取。為了此目的，一用戶鑰匙記錄要輸入家用網路的所有相關裝置(即是，能與用戶裝置使用的裝置)與用戶裝置(不屬於家用網路)。隨著此用戶鑰匙記錄的幫助，用戶裝置(例如，膝上型電腦)能與家用網路的相關裝置通訊。在另一版本，網路知道用戶鑰匙記錄(例如，透過將它輸入屬於網路的該等裝置之一)，而且當需要時，便會在用戶裝置中輸入；網路的所有裝置然後能與用戶裝置使用。在用戶允許存取的可用裝置中的資料控制應可在另一位置實施。

若要允許使用者控制對家用網路允許用戶存取的持續時間，在家用網路裝置中的用戶鑰匙記錄便會於固定時段之後、或經由使用者互作用而自動刪除。用以刪除用戶鑰匙記錄的使用者互作用可以是例如將目前家用鑰匙記錄重新輸入、按下在相關家用網路裝置或該等相關家用網路裝置之一網路裝置上的特殊按鈕、以及透過此裝置的所有其他相關家用網路裝置的隨後自動資訊。

若要避免先前用戶的未經認可使用用戶鑰匙記錄，在用戶鑰匙記錄最後傳輸之後，鑰匙產生器可於一固定時段(例如，60分鐘)之後根據激發反應方法而自動產生一新的用戶鑰匙記錄。如此，一新的用戶鑰匙記錄便會接收不同於先

前用戶鑰匙記錄的用戶鑰匙記錄，所以可確保先前的用戶不能使用可用於非法存取家用網路的新用戶。

特別網路表示許多裝置可暫時用於共用網路通訊的進一步無線網路發展。同樣是用於用戶對家用網路的存取(其中個別用戶裝置是經由一用戶鑰匙記錄而用於家用網路存取)其他使用者的裝置應可在特別網路中與使用者的至少一裝置通訊。為了此目的，使用者可將鑰匙記錄(在此稱為特別鑰匙記錄)輸入特別網路的所有裝置(他本身的裝置與其他使用者的裝置)。特別鑰匙記錄可以是一用戶鑰匙記錄，但是亦可以是如同一特別鑰匙記錄的明確特徵。

鑰匙記錄最好是由位元序列所組成，其中每個位元序列是以一預定格式(例如，1024個位元序列)傳送。整個位元序列、或一部分位元序列是透過接收單元而當作一鑰匙來傳遞。如果位元序列包含除了鑰匙之外的額外位元，它便可正確決定位元序列的那一部分是當作一鑰匙使用(例如，128個較低位元)，而且其中位元序列的位元包含額外資訊。如果複數個鑰匙記錄同時傳送，進一步資訊便可以是有關鑰匙記錄類型(家用、用戶、特別、或解碼鑰匙記錄)的特徵通知、或包含有關鑰匙記錄的長度與數量的細節。如果接收單元用於進一步應用，額外的位元的特徵是亦可將位元序列當作一鑰匙記錄使用。

為了要避免在兩個相鄰家用網路中使用相同(家用)鑰匙，鑰匙記錄對整個網路而言應該是很明確。此可於例如在不同單元業者使用鑰匙記錄的不同範圍值來達成，而且

當目前為止是可能的，不要在一檔案上將在這些範圍內的相同鑰匙記錄儲存在兩個單元。

根據IEEE 802.11標準而操作的網路是無線家用網路的廣泛已知範例。在一IEEE 802.11網路，傳送的鑰匙記錄包含一或多個有線等效隱私(WEP)鑰匙。

(家用)鑰匙記錄的輸入亦會在用於建構網路的步驟中發生，所以鑰匙記錄的輸入/安裝在建構的開始上是需要的。在整個建構處理期間，如此可確保在裝置與存取控制(經認可的具有鑰匙記錄之所有裝置)之間的一不受攔截的相互通訊。當應用自動建構方法(即是在沒有任何使用者互作用)時，此會特別有利的(根據據例如IPv6自動建構與萬用即插即玩(UPnp)方法的機構)。

在較佳具體實施例中，可攜式單元是整合在家用網路裝置的一遠端控制單元。

如前述，鑰匙單元包含用以儲存全球明確鑰匙記錄的一記憶體。當使用用於保護數位資料屬性權限的安全系統時，鑰匙單元包含用以讀取一行動資料記憶體的讀取裝置會是較佳的。行動資料記憶體可以是儲存一解碼鑰匙記錄的一特別晶片卡，而且可由受保護的數位資訊供應者有規則地用於合法的使用者(例如，傳統郵件)。透過使可攜式單元具有一讀卡機，它可在這些裝置本身不必包含一整合讀卡機而產生可用於(無線)網路不同裝置的解碼鑰匙記錄。

根據上述具體實施例的進一步發展，鑰匙單元不僅包含讀取裝置，而且包含資料可寫入行動資料記憶體的一寫入

裝置。此可在有關使用受保護數位資訊範圍的行動資料記憶體中特別能提供存檔資訊的可能性。

此外，可攜式單元與網路裝置能將一確認從裝置傳送給單元，其中該確認是表示是否執行由單元預先傳送給裝置的指令結果(是或否)。例如，確認表示從單元傳送給裝置的一鑰匙記錄是否成功接收及安裝。同樣地，確認表示用以刪除在裝置中安裝一鑰匙記錄的指令是否成功執行。該等確認如此允許可攜式單元來保持追蹤在裝置上傳送鑰匙記錄的安裝與動作。

用以執行一指令的確認最好包含一識別碼，以明確識別用以傳送確認的裝置，如此可支援該可攜式單元的追蹤功能。

根據包含行動資料記憶體的安全系統的進一步具體實施例，該可攜式單元的鑰匙單元適於：

- 將有用的資料儲存在行動資料記憶體，以允許管理從資料記憶體讀取及在裝置上安裝的鑰匙記錄；及

- 在該有用的資料符合一預定的標準時，便停止將一鑰匙記錄從行動資料記憶體傳送給一裝置。

前述安全系統的具體實施例可提供數位資料屬性權限的非常廣泛保護的可能性。在一方面，此可實施，在與行動資料記憶體中儲存的解碼鑰匙記錄使用有關的所有有用的資料是再次儲存在行動資料記憶體。連同行動資料記憶體，如此便始終知道解碼的鑰匙記錄多久安裝在任何裝置或在不同裝置、或者在這些裝置上保持主動。當這些有用

的資料符合一預定標準時，從行動資料記憶體到一裝置的鑰匙記錄的進一步傳輸便會停止。例如，此標準可以是鑰匙記錄不應該安裝在超過N(=1, 2, 3, ...)個不同裝置，而且可以是主動。另一重要觀點是必需的有用資料是儲存在行動資料記憶體本身(而且不是在例如可攜式單元)，所以使用解碼鑰匙記錄的限制不能透過取代另一讀取裝置的行動資料記憶體而避免。

此外，可攜式單元包含一觸發單元，其觸發可使裝置刪除一鑰匙記錄。如此，它便可例如解除安裝先前傳送給裝置的一解碼鑰匙記錄，所以當維持使用限制時，解碼的鑰匙記錄便可在別處重新安裝。

本發明亦與用以在(特別是無線)網路的至少一裝置上安裝一最好是共用鑰匙的一可攜式單元有關，該網路包含一鑰匙單元，用以產生可用的鑰匙記錄，並提供作為該鑰匙記錄的短程資訊傳輸。

單元能以將它使用在前述類型安全系統的方式而進一步發展。

此外，本發明係有關具一接收單元的電裝置，其中該接收單元包含：一接收器，用以接收一鑰匙記錄；及該無線裝置的一評估元件，用以儲存、處理及/或傳遞該鑰匙記錄或一部分鑰匙記錄給一第二元件。

電裝置能以將它使用在前述類型安全系統的方式而特別進一步發展。

【實施方式】

在此由無線與有線裝置(未在圖顯示)組成的家用網路電裝置安裝是參考圖1描述。此圖顯示當作在家用網路中新裝置的一第一可攜式單元1、一用戶單元13、一DRM單元101與一個人電腦(PC)2。在家用網路的所有無線裝置具有經由PC 2範例描述的對應元件8至12。

第一單元1包含：記憶體3形式的一鑰匙單元4，用以儲存一鑰匙記錄；當作一單元的一第一按鈕5，用以觸發一鑰匙傳輸；及當作一無線介面使用的第一發射器6，用以傳送鑰匙4。單元1具有最大約50公分的短程範圍。

用戶單元13包含：一鑰匙單元3及如鑰匙產生器14所示的一元件，用以例如根據激發反應原理而產生鑰匙記錄；一第二按鈕15與第二發射器16。用戶單元13允許用戶使用他們本身的裝置(不屬於家用網路)來限制對家用網路的裝置與應用的存取。因此，透過鑰匙產生器14產生的一鑰匙記錄是以用戶鑰匙記錄17表示。

DRM單元101包含：具一記憶體103a的鑰匙單元103，用以儲存一鑰匙記錄；及一寫入/讀取裝置107，以讀取及寫入一插入的晶片卡108。此外，DRM單元101具有：一第一按鈕105a，以觸發來自記憶體103a的一(家用)鑰匙記錄傳輸；一第二按鈕105b，以由晶片卡108刪除一鑰匙記錄的傳輸；一第三按鈕105c，用於刪除一鑰匙記錄的指令傳送給一裝置；及一傳輸/接收單元106，用以將鑰匙記錄104傳送給一裝置，並從裝置接收回授信號104'。DRM單元101的操作將參考圖5進一步闡述。

PC 2是具根據IEEE 802.11標準而操作的一無線電介面12之裝置。此無線電介面12是透過以驅動程式軟體10所示一元件的控制，並用於傳送有用的資料(音樂、影像、一般資料、以及控制資料)。驅動程式軟體10能經由標準化軟體介面(APIs)而透過其他軟體元件操作。PC 2亦具有一接收單元7。接收單元7包含當作一介面提供的接收器9，用以接收經由發射器6、16或106傳送的鑰匙記錄4、17或104。接收單元7是以當作一評估元件的接收器軟體11而提供，在獲得鑰匙記錄之後，從其擷取一鑰匙(例如，在IEEE 802.11標準中定義的Wired Equivalent Privacy (WEP)鑰匙)，並經由一標準化管理介面(如在IEEE 802.11標準管理資訊庫(MIB)性質)將此鑰匙18傳送給驅動程式軟體10。PC 2具有操作個人電腦所需的應用軟體8。

使用者想要在家用網路安裝PC 2，並將它無線連接到在家用網路的高傳真安裝，為了要使它能在高傳真安裝上使用MP3格式來播放複數個音樂檔案，其中MP3是儲存在PC 2。為了此目的，使用者可使用單元1來處理PC 2，並透過與接收器9有數公分距離的單元1的發射器6並按下在單元1的按鈕5而開始在記憶體3中儲存的鑰匙記錄4傳輸。

當傳送鑰匙記錄4時，紅外線信號便會使用。鑰匙記錄4的格式是1024位元序列，其中接收器軟體11擷取128個較低位元，並將他們當作一(WEP)鑰匙18傳送給驅動程式軟體1。在驅動程式軟體10，此鑰匙18是用於將在PC 2與高傳真安裝、以及使用鑰匙記錄4供應的其他裝置之間的資料路由

加密。此亦與在網路提供的裝置的所需通訊，及隨後個人電腦到家用網路(例如，一IP位址建構)網路連接的自動建構有關。

例如當使用者遺失單元、當一新裝置必須安裝、或當使用者懷疑他的家用網路不再受保護時，不同環境需要新的鑰匙安裝。基本上，具新鑰匙記錄的新單元可覆寫(舊)鑰匙記錄的最近輸入，其中新鑰匙記錄必須然後供應給家用網路的所有裝置。

一新的鑰匙記錄濫用輸入至家用網路係可避免的，此在於家用網路的至少一裝置不能接達任意未經認可的人。在新鑰匙記錄未經認可輸入家用網路的另一裝置之後，此裝置便不再與這些裝置通訊，並觸發例如一對應的警報。

然而，為了要提高家用網路的安全性，在輸入新的鑰匙記錄時，額外提供舊鑰匙記錄4是必要的。為了此目的，使用者可使用舊與新單元來接達家用網路中的PC 2或另一裝置。使用者在舊單元1上按下用以(重新)傳輸舊鑰匙記錄4的按鈕5。在一短暫時間後，使用者便可透過按下位於用以觸發傳輸的新單元上的按鈕而開始新鑰匙記錄的傳送。

PC 2的接收器軟體11可註冊舊鑰匙記錄4的接收，並隨後接收新鑰匙記錄。只有在接收器軟體11先前已註冊舊鑰匙記錄4的接收，接收器軟體便可經由管理介面而在新鑰匙記錄或鑰匙上傳遞給無線電介面12的驅動程式軟體10。如上所述，為了要在新鑰匙的基礎上將資料路由加密，新鑰匙記錄必須供應給家用網路的所有裝置。

當接收器軟體11只接受一新鑰匙記錄的輸入時，增加安全性範圍可在輸入一新的鑰匙記錄時達成，即是當新鑰匙記錄已數次以及在某些時間間隔上供應給裝置時，在此記錄的鑰匙上傳遞，其中使用者知道輸入次數與時間間隔。

家用網路的安全性範圍增加亦可達成，此在於一特定時間(數日/數星期/數月)之後，一鑰匙記錄必須重新有規律供應給家用網路裝置之至少一者。

經由用戶單元13，使用者允許用戶存取PC 2。為了此目的，用戶或使用者可透過按下按鈕15來觸發由鑰匙產生器14所產生的用戶鑰匙記錄17的傳輸而接達PC 2。

用戶鑰匙記錄17是由使用供傳送進一步資訊的額外位元的一位元序列所組成。如果接收單元當作進一步應用的介面使用，額外位元可使當作用戶鑰匙記錄的鑰匙記錄特徵化，並用於從其他資訊區別鑰匙記錄。

接收單元7是接收用戶鑰匙記錄17。接收器軟體11是經由當作用戶鑰匙記錄17的額外位元來識別鑰匙記錄，並經由管理介面而在當作一額外(WEP)鑰匙的擷取鑰匙上傳遞給無線電介面12的驅動程式軟體10。驅動程式軟體10是將鑰匙當作用以將資料路由加密的額外鑰匙使用。

在IEEE 802.11標準中定義的有線設備隱私(WEP)加密，多達四個WEP鑰匙的平行應用可提供。網路的裝置可識別WEP鑰匙是否目前用於加密。

用戶鑰匙記錄17的輸入可重複於家用網路的用戶想要使用的所有裝置、像是他想要用來在家用網路上進行存取，

例如：存取PC 2的MP3檔案，的所有裝置(例如，膝上型電腦)。

為了要允許使用者可控制對家用網路存取的持續時間，在一段固定時間過去(例如，10h)之後，用戶鑰匙記錄17便要在家用網路的裝置中自動、或透過使用者手動(例如，將家用鑰匙記錄4輸入家用網路裝置)刪除。

為了要避免先前用戶未經認可使用一用戶鑰匙記錄，鑰匙產生器要在一固定時段過去之後可根據激勵反應原理而自動產生一新的用戶鑰匙。

圖2是使用射頻異頻雷達收發機技術以傳送傳輸鑰匙記錄4的一可攜式單元19 的方塊圖。可攜式單元19是由一數位部分26所組成，其中該數位部分26包含：一記憶體20(例如，ROM)，用以儲存鑰匙記錄；一程式執行控制單元21與一調變器22，用以將來自程式執行控制單元21的位元流轉換成傳送的射頻信號。此外，單元19包含：一分離器23，用以將從指定為天線25的被動元件接收的電磁能量從傳送的射頻信號分開；具一電壓偵測器的電源供應器單元24，以使用工作電壓來供應數位部分26；及天線25，用以傳送來自分離器23的位元流及接收用於操作所需的能量。

若要傳送鑰匙記錄4，使用者用能使用可攜式單元19來接達接收單元7。天線25可使用電壓偵測器而經由分離器23將來自接收單元7的輸入能量傳遞給電源供應器單元24。當一電壓臨界值在電壓偵測器中超過時，電源供應器單元24便會在單元19中提供一工作電壓。透過工作電壓的刺激，程

式執行控制單元21便會被初始化，並讀取在記憶體20中儲存的鑰匙記錄。鑰匙記錄是透過程式執行控制單元21而以一適當訊息格式嵌入，並傳遞給調變器21，用以轉換成類比射頻信號。射頻信號是經由分離器23而由天線25傳送。

圖3顯示當應用與圖2相同技術時當作一接收與傳輸單元的單元19。在此圖中，相同或對應元件是使用與圖2相同的編號。到目前為止，參考圖2的描述，而且只有不同將稍後說明。

在此具體實施例，單元19包含調變器21、以及一解調變器27。記憶體20能以一可抹除的記憶體實施，例如，EEPROM的電可抹除記憶體。

由於解調變器27，所以單元19可將天線25接收的射頻信號(輸入能量)轉換，並經過分離器23傳遞給位元序列。來自解調變器27的位元序列是由程式執行控制單元21處理。如果程式執行控制單元21決定位元序列包含授權接收單元接收鑰匙記錄的資訊，位元序列的處理會造成程式執行控制單元21存取記憶體20。如果接收單元授權來接收鑰匙記錄，程式執行控制單元21便會讀取鑰匙記錄，並以圖2描述的方式將它傳遞給天線25來傳送。

解調變器27將新鑰匙記錄的可能性進一步提供給單元19。當記憶體20能以一可寫記憶體(例如，EEPROM)實施時，在單元19的鑰匙記錄便能以一新的鑰匙記錄來取代。

圖4顯示當應用與圖2的相同技術時當作一用戶單元28的單元19。在此圖中，相同或對應的元件亦使用與圖3相同的

參考數字。到目前為止，它是參考圖3描述，而且只有不同將稍後說明。

用戶單元28額外包含一鑰匙產生器29，而且該鑰匙產生器29連接到程式執行控制單元21，並用於產生一連串的用戶鑰匙記錄。

使用電源供應器單元24中的電壓偵測器偵測到透過接收單元7附近的天線25所輸入的能量之後，便可透過電源供應器單元24供應工作電壓給數位單元26。程式執行控制單元21可讀取由鑰匙產生器29產生的鑰匙記錄。在程式執行控制單元21接收鑰匙記錄，並以適當訊息格式將它嵌入之後，它便可在此記錄傳遞，以傳送給調變器22，並同時將鑰匙記錄寫入記憶體20，而且記憶體20必須以用於此目的一可寫記憶體(例如，EEPROM)形成。

在第二操作模式，一新鑰匙記錄是以固定間隔時間(例如，數分鐘或數小時)由鑰匙產生器產生，並儲存在可寫記憶體20。進一步程序然後對應圖2與3的描述。

使用如圖4所示鑰匙產生器的單元19具體實施例亦與在圖2顯示的具體實施例(沒有解調變器27)組合。

圖5顯示當使用供保護數位資料屬性權限的安全系統時所使用的元件圖。目前，屬性權限或數位權限管理(DRM)的保護可依下列實施。數位資料的供應器111(例如，付費電視)是例如經由衛星110來傳送這些使用只有他知道的鑰匙加密的資料。加密資料111可透過適當的接收器112接收，並傳遞給例如機上盒的裝置113。為了要可使用加密資料的

內容，裝置113應該知道資料供應器的秘密鑰匙。此鑰匙是經由一晶片卡108而使用，其可透過資料供應器例如每月一次郵寄給經認可與付費的使用者。晶片卡108然後插入連接到裝置113的一讀卡機，因此裝置113可讀取並使用在卡片上儲存的解碼鑰匙記錄。此系統的特徵是傳送的資料絕對不以數位、未加密形式離開裝置113，進而使他們的使用與晶片卡108的擁有耦合，如此便可控制。

然而，在現階段的數位網路，逐漸想要使用在不同裝置的資料，特別是耦合到網路的無線裝置。若要避免在此裝置每一者上的讀卡機的使用，DRM單元101(圖1、圖5)便要使用。如圖1的描述，此單元包含可讀取的一讀卡機107(類似在行動電話的SIM讀卡機)，而且最好是亦可寫入晶片卡108。因此，DRM單元101可特別讀取在在晶片卡108上的存檔的解碼鑰匙記錄，並經由短程傳輸而傳送給一裝置102的對應接收器107。裝置102(當它包含對應的軟體時)然後可經由解碼鑰匙記錄104而將加密的資料109解密，並透過(經由無線連接)上述衛星接收器112傳送。因此，這些資料109的使用在裝置102上是可能的，而且不需要它本身讀卡裝置的裝置。

描述的系統可進一步發展，在於它可避免一解碼鑰匙記錄104的未經認可多重傳送給不同裝置。根據第一具體實施例，此能以在裝置102上的解碼鑰匙記錄104期滿、或在規則成比例的短時間間隔中自動刪除的方式實施，所以它必須由DRM單元101半穩定重新傳送。然後，複數個裝置的同

時使用可實質免除。

在使用裝置的更複雜控制方面，一雙向通訊是在DRM單元101與裝置102之間執行。每當裝置102從DRM單元101接收及成功安裝一鑰匙記錄104時，它便可經由一確認104而回應，此表示鑰匙記錄是否成功傳送，並包含用於裝置102的識別碼ID。此ID然後是由DRM單元101儲存在晶片卡108。當一預定允許數量的裝置到達(此數目可儲存在例如晶片卡)時，DRM單元101便可將此確認，而且在反應方面，不再將任何進一步解碼的鑰匙記錄104傳送給任何其他裝置。

透過DRM單元101將解碼的鑰匙記錄重新傳輸是不可能發生，直到被啟動的鑰匙記錄的裝置數量減少為止。這可以是例如在預定時間間隔終止之後而自動的情況。然而，DRM單元101最好包含一"刪除按鈕"105c(圖1)，以便在按下之後，能與一目標裝置102互動。DRM單元101會先要求裝置102的ID。因此，裝置102傳送能由DRM單元101接收的ID，並使用被啟動的鑰匙記錄而與儲存在裝置的晶片卡108上的IDs相比較。如果ID出現在卡片上，DRM單元便會將一指令傳送給裝置102，以刪除在裝置的解碼鑰匙記錄。透過裝置102傳送的確認可通知DRM單元101是否想要執行刪除。如果鑰匙記錄被成功刪除，裝置102的ID便可從晶片卡108刪除，所以在另一裝置上的解碼鑰匙記錄的隨後使用是可能的。

【圖式簡單說明】

本發明的這些及其他觀點可從下面描述的具體實施例闡述而更顯然：

圖1顯示三個單元與一裝置圖；

圖2是當使用射頻異頻雷達收發機技術時當作一傳輸單元的單元方塊圖；

圖3是當使用射頻異頻雷達收發機技術時當作一接收與傳輸單元的單元方塊圖。

圖4是當使用射頻異頻雷達收發機技術時當作一用戶單元的單元方塊圖；及

圖5顯示數位權限管理(DRM)的安全系統使用。

【圖式代表符號說明】

1, 13, 19, 101	可攜式單元
2, 102	無線裝置
3, 103	鑰匙單元
4, 17, 104	鑰匙記錄
5, 15, 105a, 105b, 105c	觸發單元(按鈕)
6	第一發射器
7	接收單元
8	元件
9	接收器
10	驅動程式軟體
11	評估元件
12	無線電介面
14	鑰匙產生器

16	第二發射器
18	鑰匙
20	記憶體
21	程式執行控制單元
22	調變器
23	分離器
24	電源供應器單元
25	天線
26	數位部分
27	解調變器
28	用戶單元
29	鑰匙產生器
101	數位權限管理單元
104'	回授信號
106	傳輸/接收單元
107	讀取裝置
108	晶片卡
109	資料
110	衛星
111	加密資料
112	衛星接收器
113	機上盒的裝置

伍、中文發明摘要：

本發明係揭示關於無線網路之安全系統，該安全系統包含一可攜式單元(1)與一與鑰匙單元(3)，以產生可用的一鑰匙記錄(4、17、104)，並提供作為鑰匙記錄(4、17、104)的短程資訊傳輸。該網路的至少一無線裝置(2)具有一接收單元(7)，其中該接收單元(7)包含一接收器(9)，用以接收鑰匙記錄(4、17、104)；及該無線裝置的一評估元件(11)，用以儲存、處理及/或傳遞該鑰匙記錄(4、17、104)、或一部分鑰匙記錄給一第二元件。由於該鑰匙記錄，所以該無線網路的裝置可獲得一秘密共用鑰匙，以供用於執行傳送的有用資料及/或認證的加密及解密。該單元(101)進一步包含用於一晶片卡(108)的讀取裝置(107)，其中該晶片卡(108)最好包含複製保護數位資料的解碼鑰匙記錄(104)。

陸、英文發明摘要：

The invention relates to a security system for wireless networks, comprising a portable unit (1) with a key unit (3) for making a key record (4, 17, 104) available and being provided for short-range information transmission of the key record (4, 17, 104). At least one wireless apparatus (2) of the network is provided with a receiving unit (7) comprising a receiver (9) for receiving the key record (4, 17, 104) and an evaluation component (11) of the apparatus for storing, processing and/or passing on the key record (4, 17, 104) or a part of the key record to a second component. Due to the key record, the apparatuses of the wireless network acquire a secret shared key with which the encryption and decryption of the transmitted useful data and/or the authentication is performed. The unit (101) may further comprise a reading device (107) for a chip card (108), which chip card (108) preferably comprises the decoding key record (104) of copy-protected digital data.

拾、申請專利範圍：

1. 一種用於特別是無線網路之網路安全系統，其包含：

- 一可攜式單元(1、13、101)，其具有一鑰匙單元(3、103)，用以產生一可用的鑰匙記錄(4、17、104)，並提供作為鑰匙記錄(4、17、104)的短程資訊傳輸；及

- 在網路的至少一裝置(2、102)中的至少一接收單元(7、107)，該接收單元包含一接收器(9)，以接收鑰匙記錄(4、17、104)與裝置的一評估元件(11)，以儲存、處理及/或傳遞該鑰匙記錄(4、17、104)或一部分鑰匙記錄給一第二元件。

2. 如申請專利範圍第1項之安全系統，其特徵為該可攜式單元(1、13、101)包含至少一觸發單元(5、15、105a、105b、105c)，用以觸發資訊的短程傳輸，特別是鑰匙記錄(4、17、104)的短程資訊傳輸。

3. 如申請專利範圍第1或2項之安全系統，其特徵為只要使用者接近該接收單元(7、107)，該可攜式單元(1、13、101)的一偵測器便會觸發該鑰匙記錄(4、17、104)的短程資訊傳輸。

4. 如申請專利範圍第1或2項之安全系統，其特徵該鑰匙單元(3)包含鑰匙產生器(14)，用以產生一連串用戶鑰匙記錄(17)。

5. 如申請專利範圍第1或2項之安全系統，其特徵為該無線裝置(2、102)係被提供以刪除該鑰匙記錄(17、104)。

6. 如申請專利範圍第1或2項之安全系統，其特徵為該鑰匙記

錄(4、17、104)是由一位元序列所組成。

7. 如申請專利範圍第6項之安全系統，其特徵為該位元序列包含用於區別的特徵位元及特徵鑰匙記錄(4、17、104)。

8. 如申請專利範圍第1或2項之安全系統，其特徵為該可攜式單元(1、13、101)是該無線裝置的一部分，特別是一遠端控制單元。

9. 如申請專利範圍第1或2項之安全系統，其特徵為該鑰匙記錄(4、17、104)是在網路建構期間或在網路建構之前供應，特別是一裝置(2、102)的自動網路建構。

10. 如申請專利範圍第1或2項之安全系統，其特徵為該無線裝置(2、102)係經由網路裝置間傳送有用資料(109)的鑰匙記錄(4、17、104)中的一鑰匙而提供作為認證、加密及/或解密。

11. 如申請專利範圍第1或2項之安全系統，其特徵為該鑰匙單元包含一記憶體(3、103a)，用以儲存全球明確的鑰匙記錄(4、104)。

12. 如申請專利範圍第1或2項之安全系統，其特徵為該鑰匙單元(103)包含一讀取裝置(107)，用以讀取一行動資料記憶體，特別是具有在該行動資料記憶體上儲存一解碼鑰匙記錄(104)的晶片卡(108)。

13. 如申請專利範圍第12項之安全系統，其特徵為該鑰匙單元(3)包含一寫入裝置(107)，用以將資料寫入該行動資料記憶體(108)。

14. 如申請專利範圍第1或2項之安全系統，其特徵為該單元

(101)與該無線裝置(2、102)適於由該無線裝置(2、102)將一確證(104')傳送給該單元(101)，以表示執行將一指令從單元(101)傳送給裝置(2、102)的結果。

15. 如申請專利範圍第14項之安全系統，其特徵為該確認(104')包含該無線裝置(2、102)的一識別碼。

16. 如申請專利範圍第13項之安全系統，其特徵為該鑰匙單元(3)適用於：

- 將有用的資料儲存在該行動資料記憶體(108)，以允許管理鑰匙記錄(104)，該鑰匙記錄(104)係從該資料記憶體(108)所讀取，且安裝在裝置(2、102)中；及

- 在該有用的資料符合一預定標準的情況，便阻止從該行動資料記憶體(108)到一裝置(2、102)的鑰匙記錄(104)傳輸。

17. 如申請專利範圍第5項之安全系統，其特徵為該單元(101)包含一觸發單元(105c)，其觸發可使該無線裝置(2、102)刪除一鑰匙記錄(104)。

18. 一種用以在無線網路的至少一裝置(2、102)中安裝一鑰匙之可攜式單元(1、13、101)，其中該可攜式單元包含用以提供一鑰匙記錄(4、17、104)的鑰匙單元(3、103)，以用於鑰匙記錄的短程資訊傳輸。

19. 一種具接收單元(7、107)之電裝置(2、102)，該接收單元(7、107)包含：一接收器(9)，用以接收一鑰匙記錄(4、17、104)；及該無線裝置(2、102)的一評估元件(11)，用以儲存、處理及/或傳該遞鑰匙記錄或一部分鑰匙記錄給一第

二元件(10)。

柒、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件代表符號簡單說明：

1, 13, 101	可攜式單元
2	無線裝置
3, 103	鑰匙單元
4, 17, 104	鑰匙記錄
5, 15, 105a, 105b, 105c	觸發單元(按鈕)
6	第一發射器
7	接收單元
8	元件
9	接收器
10	驅動程式軟體
11	評估元件
12	無線電介面
14	鑰匙產生器
16	第二發射器
18	鑰匙
101	數位權限管理單元
104'	回授信號
106	傳輸/接收單元
107	讀取裝置
108	晶片卡

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：