發明專利說明書 200306746

（填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫）

※ 申請案號：P21086 ※IPC分類：H04N 7/16

※ 申請日期：P2.4.15

壹、發明名稱

（中文）藉控制字元所編碼之事件的儲存方法

（英文）MANAGEMENT METHOD OF RIGHTS OF A CONTENT ENCRYPTED AND STORED IN A PERSONAL DIGITAL RECORDER

貳、發明人（共 1 人）

發明人 1 （如發明人超過一人，請填說明書發明人續頁）

姓名：（中文）馬可薩塞利

（英文）SASSELLI Marco

住居所地址：（中文）瑞士夏當 1803 羅契斯路 20 號

（英文）Ch. des Roches 20, 1803 Chardonne, Switzerland

國籍：（中文）瑞士 （英文）Switzerland

參、申請人（共 1 人）

申請人 1 （如申請人超過一人，請填說明書申請人續頁）

姓名或名稱：（中文）納格拉威遜股份有限公司

（英文）Nagravision S.A.

住居所或營業所地址：（中文）瑞士赤夕奧斯蘇洛桑 1033 日內瓦路 22 號

（英文）22, route de Genève, 1033 Cheseaux-sur-Lausanne, Switzerland

國籍：（中文）瑞士 （英文）Switzerland

代表人：（中文）尼可拉斯哥史曼 及 珍傑克斯杜渥遜

（英文）Nicolas Goetschmann & Jean-Jacques Duvoision

☐ 續發明人或申請人續頁 （發明人或申請人欄位不敷使用時，請註記並使用續頁）

捌、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，其日期爲：＿＿＿＿＿＿＿＿＿＿

☑ 本案已向下列國家（地區）申請專利，申請日期及案號資料如下：

【格式請依：申請國家（地區）；申請日期；申請案號　順序註記】

1. 瑞士　2002.04.19　2002 0664/02
2.
3.

☑ 主張專利法第二十四條第一項優先權：

【格式請依：受理國家（地區）；日期；案號　順序註記】

1. 瑞士　2002.04.19　2002 0664/02
2.
3.
4.
5.
6.
7.
8.
9.
10.

☐ 主張專利法第二十五條之一第一項優先權：

【格式請依：申請日；申請案號　順序註記】

1.
2.
3.

☐ 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】

1.
2.
3.

☐國外微生物　【格式請依：寄存國名；機構；日期；號碼　順序註記】

1.
2.
3.

☐熟習該項技術者易於獲得，不須寄存。

玖、發明說明

（發明說明應敘明：發明所屬之技術領域、先前技術、內容、實施方式及圖式簡單說明）

1.發明所屬之技術領域

本發明揭示一種條件接達服務之接收器／解碼器的欄位，尤其具有儲存單元諸如硬碟機之接收器的欄位。

2.先前技術

磁碟機(硬碟)之儲存容量及速度之領域的技術進步，使得其可儲存所傳送影像信號之內容，而使得可離線(offline)來接達使用者。

此種錄影器眾所週告之品牌名稱 ReplayTV ®或 Tivo，提供數位傳輸之數千小時的儲存容量。然而，這些錄影器沒有直接地整合在條件接達服務之接收器／解碼器中；尤其，儲存之內容在碟片上沒有特別的保護，使得以商業分銷目的來複數碟片之情形中，不可能收取有關於複製內容之作者版權費。

反之，在數位付費電視系統中，所傳送到這些接收機之數位流加密，以便能控制使用及定義此一用途之條件。本加密是以規則時隔(通常在5及30秒之間)改變控制字元來實施，使得阻止嘗試恢復此控制字元之侵入。

根據特定實施例，控制字元以更長時隔改變，其意即用於已知事件以一個單一控制字元來加密。

對於可使得以這些控制字元所加密之數位流來解密的接收機，數位流傳送到接收機，無關於使用者單元之作業系統(CAS)及安全模組兩者間傳輸系統之特定鍵所加密控制訊

息(ECM)流。事實上，在安全單元(SC)所實施安全作業，通常是智慧形式，所謂不可違反。本單元可具有可分離型式或可直接整合在接收機。

在控制訊息(ECM)之解密期間，以安全單元(SC)來證實接達所考慮數位流之權利存在。本權利可以控制在安全單元(SC)內之此一權利的授權訊息(EMM)來管理。其他可能性同樣地可能，如解密鍵之傳送。

在本說明書中，將使用"事件"用於根據習知控制字元方法來加密之影像、語音(例如 MP3)或資料的內容名稱，各事件可以各具有預定有效性期間之一個或數個控制字元來加密。

今天，此事件使用之記帳是根據事件之預購、購買或以每時間單位收費的原則。

預購允許來定義相關於這些事件之一個或數個傳輸頻道的權利，而且如果該權利存在安全單元，則允許使用者獲得在加密形式之這些事件。

同時，可定義特定於事件之權利，諸如電影或足球比賽。使用者可獲得本權利(例如購買)，而且本事件特定地以本權利來管理。本方法稱爲按收視付費(PPV)。

至於每時間單位收費，安全單元包含視使用者實際消費來扣款之信用額度(credit)。如此，例如，單元之信用額度將根據所選擇頻道或事件而以每分鐘來扣款。其可根據技術應用以期間或所指定時間之價值來變動記帳單元，甚至組合這兩種參數而調用(adapt)所傳送事件型式之帳單。

控制訊息(ECM)包含不僅控制字元，也包含本控制字元存在接收機／解碼機之條件。在本控制字元之解密期間，將驗證關連於所發表訊息之接達條件在安全單元內具有權利或所有權的存在。

控制字元僅當比較爲正時才回轉到使用者單元。控制字元包含在以傳輸鍵 TK 所加密之控制訊息 ECM 內。

對於安全單元內存在之權利，在本單元內通常以權利管理訊息(EMM)來收費，由於安全理由，其通常以稱爲權利鍵(RK)之不同鍵來加密。

根據習知付費電視系統形式，在已知時間使得事件加密必需有下述三個元素：

- 以一個或數個控制字元(CW)來使得事件加密；
- 控制訊息或訊息等(ECM)包含控制字元(CW)及接達條件(AC)；
- 安全單元內所儲存之對應的權利允許來驗證該接達條件。

根據已知設計，儲存單元諸如硬碟機內所儲存之加密事件，至少伴隨一個或數個控制訊息 ECM。

由於加密之事實，ECM 訊息之後段(posteriori)可能是問題，尤其因爲傳輸鍵之改變，所以在歐洲專利文獻第 EP 0 912 052 號中建議第一種解決方案，該方案意指安全單元內之這些訊息在儲存到硬碟機上之前先解密及重新加密。

本解決方案解決傳輸鍵之工作壽命的問題，但是在錄影時使得安全單元上放置大量處理負擔，而且不知道錄影內容是否將在那一天使用。更進一步，安全系統之其中之一

基本規則，僅在權利存在時才使得控制字元回轉到使用者單元。在本情形中，如果考慮按收視付費，則很可能這些權利不存在。當使用者決定收視本事件時，權利將可在很久以後進行之購買期間來獲得。

本文獻 EP 0 912 052 號沒有解決權利接達之問題，因爲在購買時，權利訊息 EMM 總是必需傳送使得在安全單元內來收費。

如此，在本文件所述解決方案僅可適用於所傳輸事件，其中權利已出現在安全單元內，使得授權 ECM 之解密及重新加密。

另一方面在持有者之權利保有。例如，當持有者 A 具有頻道 M, N, P 之接收權利時，則他／她具有權利來收視這些頻道，如此來任意地錄影及收視在他的／她的儲存單元內之事件。隨著此一事件之各自使用，安全單元需要使得訊息 ECM 解密，而且歸還控制字元。然後，重要在關連本事件之權利出現在安全單元內。

在以預購來獲得事件之情形中，本事件之識別關連到預購頻道，例如 M。如此，授權帶有識別證 M 之全部事件，而且控制字元歸還到解碼器。

然後，這些權利關連到識別證諸如 M 所定義之特別頻道。當預購者取消他的／她的預購、或將其修改用於其他頻道時，結果儲存單元內所錄影之事件將不能接達，因爲安全單元將拒絕重新傳送控制字元，所對應之權利不再出現。

如果新識別證歸屬通道 M，則本情形也會發生。如此，

可使得頻道重新組織使得識別證 J4 替代 M 來歸屬本頻道。因傳輸權利之觀點，安全單元及時地通知改變，而且使用者記錄沒有解約(disagreement)。

所記錄事件之結果更加戲劇性。本重新指定(re-assignment)導致所錄影事件不能接達，因爲在安全單元內不再出現所對應之權利。

3.發明內容

本發明之目的在於提出一種以控制字元(CW)來加密事件之儲存方法，其即使在儲存時間及收視時間之中發生某些修改，也保證在任何所期望之時間來接達本事件。

本目的是以事件之儲存方法來達成，其以連接到安全單元(SC)之接收及解密單元(即，設定盒(Set Top Box)或 STB)內的一個或數個控制字元(CW)來加密，這些控制字元(CW)及必要之權利包含在控制訊息(ECM)內；特徵在其包含下列步驟：

- 在儲存單元內儲存加密事件及控制訊息(ECM)；
- 傳送控制訊息(ECM)到安全單元(SC)；
- 證實本事件之接達權利是否包含在安全單元(SC)內；
- 判定收執(receipt)具有(Q)使用安全單元(SC)內所包含及特定於各安全單元(SC)之祕密鍵(K)全部或部分控制訊息(ECM)；
- 使得本收執(Q)儲存在儲存單元內。

根據本發明之第一實施例，本收執是根據全部或部分控制訊息之簽名來構成，而且立隨後地允許事件之後續使用

的超級權利，在驗證安全單元之一般權利之前，優先地驗證本收執。本收執出現一旦由已知控制訊息所承認，則導致一般接達條件被忽視。

根據本發明之第二實施例，在收執產生期間，除了簽名之外，也增添說明當本控制訊息出現在安全單元時其將如何處理的新部分。本條件將可忽視本訊息內所發表之條件(其使得回到前一解決方案)，或發表其他條件諸如來處置重新製造之權利、或定義時間視窗來授權此一重新製造。

爲判定簽名，較佳地採取在整個事件不會改變之部分。事實上，訊息 ECM 大致上包含兩部分：

a.用於解密之控制字元(或偶數及奇數字元)

b.歸還控制字元所需要之權利

本收執允許控制訊息之標示及其他資訊增添目的在重新製造模態之處理。然後，本目的在識別非模棱兩可形式之控制訊息。實際上，可見部分 b，即必要之權利，比較控制字元更不常改變。這是爲什麼較佳地選擇這部分來計算簽名。儘管如此，其沒有排除判定關於控制字元或兩部分群組之簽名。

爲本簽名之計算，決定一種以單向函數所考慮而沒有和這些資料碰撞之部分的唯一影像。其承認沒有和本函數產生相同結果之不同資訊群組存在。本影像 H 以散列型式(Hash type)函數來產生。所使用演算法可以具有 SHA-1 或 MD5 型式，而且本影像以唯一方法來顯示資料群組。

由於加密鍵 K，下述運算在於使得這些資料加密。

在加密運算之前，可以鍵 K 來添加說明新接達條件之資料欄 CD。然後，建立收執的這些資料群組(H 及 CD)以簽名鍵 K 來加密。

在本發明之精神中，用語"收執"意指其以代表接達條件(例如在在最簡單情形中)之資料群組及因爲加密鍵 K 所關係一個安全單元之唯一性來決定。根據其一實施例，可直接地以本鍵使得控制訊息之接達條件來加密，而不用通過散列運算。

根據另一實施例，可判定關於接達條件之唯一影像(散列型式)，然後以第一鍵 K1 來使得本影像加密，以相同鍵 K1 或以第二鍵 K2 來添加新接達條件 CD 及使得其全部加密。

4.實施方式

第 1 圖所示解碼器 STB 接收加密形式之輸入資料。這些資料儲存在儲存單元 HD 內，而且顯然地包含所考慮事件 EV 及控制訊息 ECM。

如此，根據本發明，這兩個資料群組附帶著在附第 2 圖中以收執 Q 方塊來圖示說明之新群組。

在本文中以不同方塊大小做爲實例。因而，可考慮事件 EV 佔用最大部分、控制訊息 ECM 一小部分，而且根據實施例，一個單一收執足夠用於這些資料群組。

事實上，如果在控制訊息之接達條件部分上來實施簽名，則其用於全部所考慮事件將不變動。

在第 3 圖上表示控制訊息 ECM 之結構。本訊息如上所述也包含控制字元 CW 及接達條件。

這些條件畫分成兩部分，其一部分特定用於傳輸條件ACB，及另一部分特定用於重新製造條件 ACR。本訊息也包含時間標示 TP。

在這些條件中，可發現：

- 頻道(或服務)之數量，尤其可使用於預購；
- 事件之主題(例如，運動、新聞、成人)；
- 分級(level)(主要時間、午間、重新傳輸)
- 刺激購買之數目

條件之複製(duplication)開啓在重新製造期間對事件管理之可能性。收執 Q 可意指必要僅符合重新製造之條件，或相反地，其可意指來忽視這些條件。

例如，地理區域斷電功能(blackout function)之實例。例如本功能允許在包圍運動場 30 km 內之運動事件接收的斷電。雖然在事件時候斷電具有意義，但是在數天之後此斷電沒有理由。

傳輸條件 ACB 可包括安全單元號碼區段或郵遞區碼之斷電條件。重新製造 ACR 之條件可包括自某一日期起全部之簡單授權(祇要其他條件諸如預購履行)。

在重新製造期間；先接達收執 Q 而且以祕密鍵 K 來解密而獲得簽名 SGN 及新接達條件 CD。

然後，簽名 SGN 及新 CD 條件保留在安全單元之記憶體內。當控制訊息提供到安全單元時，以散列函數來判定包含權利 AC 之 ECM 部分上的唯一影像 H'，而且根據本實例來比較影像 H'值及簽名 SGN。

如果兩個值完全相同，安全單元應用在收執之CD條件部分所定義的條件。如果本CD條件是"免費接達"，這消除驗證在控制訊息ECM中所包含之條件的需要，而且如此，消除傳輸頻道之結構改變所造成的問題。

根據另一實施例，新條件CD重新傳送重新製造條件ACR。在這些條件中，沒有根據可隨時間變動(結構條件)之頻道或其他元件，而是在允許本接達期間或允許接達許多次之時間的條件。當然，在本情形中，所連結預購或其他之接達條件已在收執形成期間驗證。

本接收可進化。在某些情形，儲存新收執可見有意義比較舊收執更佳。這明顯地是衝動購買之情形。在本情形中，沒有使用者購買本事件，而在儲存期間產生第一收執。

在本收執所包含之條件將重新傳送控制訊息ECM所包含的條件。

當使用者決定購買本事件的時候，如果條件如此地定義，則產生新收執其開啓使用之途徑而沒有保留本事件。然後，本收執傳送到儲存單元來替代舊收執。

5.圖式簡單說明

本發明以下文詳細說明之輔助及參考非限定實例所附之附圖，將更好理解，其中：

第1圖說明根據本發明其一實施例之具有儲存單元的使用者單元STB圖示；

第2圖表示附第1圖之儲存單元內所儲存資料群組的圖示；及

第 3 圖表示根據本發明其一實施例之控制訊息 ECM 結構。

主要部分之代表符號說明

CW	控制字元
STB	接收及解密單元
SC	安全單元
ECM	控制訊息
Q	收執
K	保密鍵
CD	條件部分
SGN	簽名
HD	儲存單元

肆、中文發明摘要

本發明之目的在於提供一種以控制字元(CW)來加密事件之儲存方法，其在所期望時隨時地，甚至如果在儲存時候及收視時候兩者間發生這些事件識別者之指定的一些修改時，也保證接達到該事件。

本目的以安全單元(SC)所連接接收及解密單元(STB)內此一事件之儲存方法來獲得，該控制字元(CW)及必要之權利包含在控制訊息(ECM)內，本方法之特徵包含下列步驟：

- 在安全單元(SC)內儲存加密事件以及控制訊息(ECM)；
- 傳送控制訊息到安全單元(SC)；
- 驗證本事件之接達權利是否包含在安全單元(SC)內；
- 如果這是本情形，則根據安全單元(SC)所包含及特定於各安全單元之保密鍵，來判定控制訊息(ECM)之全部或部分的收執(Q)；及
- 儲存本收執(Q)在安全單元內。

伍、英文發明摘要

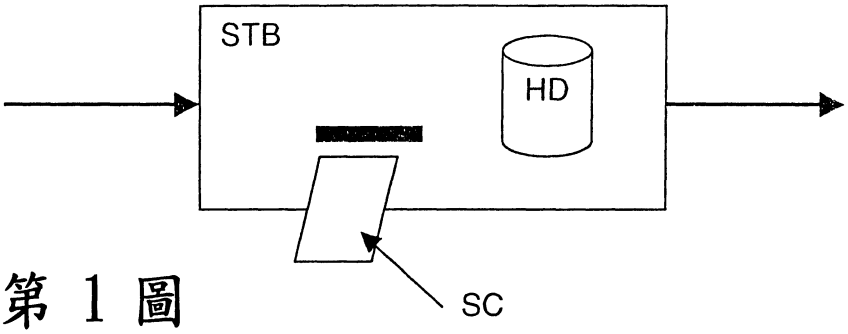
The aim of the present invention is to propose a storage method of an event encrypted by control words (CW) that guarantees the access to this event whichever the moment is desired, even if certain modifications in the designation of the identifiers of these events occur between the moment of storage and the moment of viewing.

This aim is achieved by a storage method of such an event in the reception and decryption unit (STB) connected to a security unit (SC), said control words (CW) and the necessary rights being contained in control messages (ECM), characterized in that it comprises the following stages:

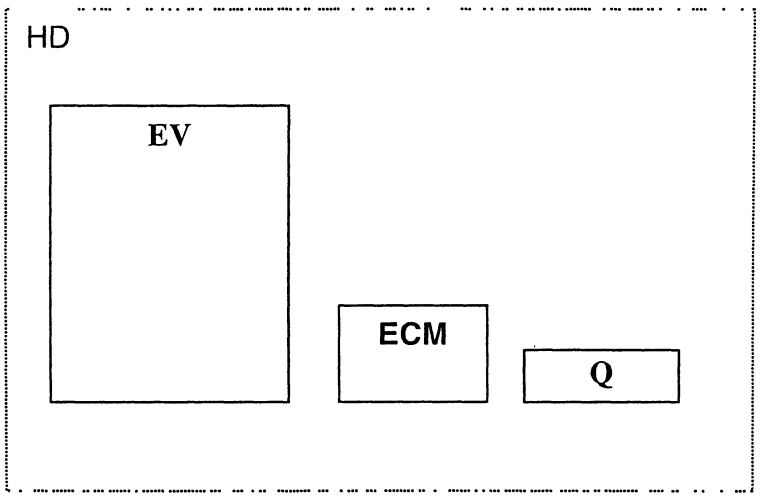
- storing the encrypted event as well as the control messages (ECM) in the storage unit,
- transmitting the control messages (ECM) to the security unit (SC),
- verifying if the access rights to this event are contained in the security unit (SC),
- if this is the case, determining a receipt (Q) of all or part of the control message (ECM) thanks to a secret key (K) contained in the security unit (SC) and specific to each security unit,
- storing this receipt (Q) in the storage unit.

拾、申請專利範圍

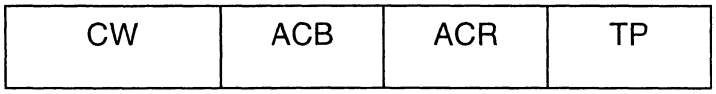
1. 一種在安全單元(SC)所連接接收及解密單元(STB)中以一種或數種控制字元(CW)來加密事件之儲存方法，用於接達本事件之該控制字元(CW)及必要之權利包含在控制訊息(ECM)內，本方法之特徵包含下列步驟：
   - 在儲存單元中儲存加密事件以及控制訊息或訊息(ECM)；
   - 傳送該控制訊息(ECM)到該安全單元(SC)；
   - 驗證該事件之接達權利是否包含在該安全單元(SC)內；
   - 根據該安全單元(SC)內所包含及特定於各安全單元之保密鍵(K)，來判定收執(Q)包含該控制訊息(ECM)之全部或部分的簽名(SGN)；及
   - 儲存本收執(Q)在該儲存單元內。
2. 如申請專利範圍第 1 項之方法，其中該收執(Q)僅在該接達權利出現在該安全單元才計算。
3. 如申請專利範圍第 1 項之方法，其中該收執(Q)也包含條件部分(CD)，說明和事件傳輸之結構架構無關的新條件。



第 1 圖



第 2 圖



第 3 圖

陸、(一)、本案指定代表圖爲：第__1__圖

(二)、本代表圖之元件代表符號簡單說明：

SC	安全單元
HD	儲存單元
STB	接收及解密單元

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：