公告本

申請日期	90. 11. 7
案　　號	90127665
類　　別	H04L 9/00

A4
C4

（以上各欄由本局填註）

發明 ~~新型~~ 專利說明書

一、發明 ~~新型~~ 名稱	中　文	使用者資料之超分送防護
	英　文	SECURE SUPER DISTRIBUTION OF USER DATA
二、發明 ~~創作~~ 人	姓　名	1. 安東尼歐 亞卓安 瑪瑞亞 史達林 ANTONIUS ADRIAAN MARIA STARING 2. 法蘭西斯科 路卡斯 安東尼歐 強尼斯 崁伯曼 FRANCISCUS LUCAS ANTONIUS JOHANNES KAMPERMAN
	國　籍	均荷蘭
	住、居所	均荷蘭愛因和文市普羅何斯蘭路6號
三、申請人	姓　名 （名　稱）	荷蘭商皇家飛利浦電子股份有限公司 KONINKLIJKE PHILIPS ELECTRONICS N.V.
	國　籍	荷蘭
	住、居所 （事務所）	荷蘭愛因和文市格羅尼渥街1號
	代表人 姓　名	J.L. 凡 德 渥 J.L. VAN DER VEER

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有　□無主張優先權
歐洲專利機構	2000年12月18日	00204637.3	□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　　）

本發明係關於一種將儲存在第一資料載體上的使用者資料做超分送防護的方法。本發明也關於一種將使用者資料做超分送防護的系統、一種再生及/或記錄使用者資料的裝置、及儲存使用者資料的資料載體。

超分送是一種分送軟體的方法，其中軟體是可自由使用且無限制的，但是軟體受到保護使免於被修改及其未經供應者授權的使用模式。譬如從1990年7月之Transaction Of The IEICE，第E73卷第7號第1133-1146頁由R. Mori與M. Kawahara所著"Super distribution - The Concept and the Architecture"(從http://www.virtualschool.edu/mon/electronicproperty/morisuperdist.html網頁中可找到)中所知的超分送架構提供三個原理功能：收集軟體使用與軟體使用費用之帳戶資訊的管理機制；記錄並累計使用收費、付款及不同軟體供應商之間使用收費分配的帳戶處理機制；及利用數位保護模組保護該系統免受干擾而能適當運作的防禦機制。

超分送軟體在公眾管道上以加密形式分送。其有下列甚佳特點的組合：

- 軟體產品被自由分送而無限制。軟體產品的使用者為了使用該產品-而不為了擁有該產品-而付費。
- 軟體產品之供應者可在使用費用表-如果有的話-內設定使用其軟體產品之價格與條款。
- 只要使用者遵守供應者所設定的使用條款並支付供應者所收取的費用，軟體產品可由具有適當設備的任何使用

五、發明說明（2　　）

者執行。

- 超分送系統的適當運作-包括由供應者所設定條款的執行-由譬如智慧卡等防竄改電子裝置確保。

超分送不但能使用於分送軟體而且一般也能使用於分送像是音訊或視訊資料等的使用者資料。音訊與視訊內容的超分送對唱片與電影公司而言是一種有吸引力的商業模式。其原因是在此種模式下，消費者藉著複製譬如他們最愛的唱片集等資料給朋友而扮演一部份配銷商的角色。所以-且譬如隨著唱片集的成功程度而定-可大幅降低製造與分送實體媒體的成本。很清楚的是，依賴超分送技術的商業模式僅在副本的使用有適當付費的條件下可行，而這需要由一種可靠的內容保護系統來執行。此類系統將植基於一種採用加密-最可能是水印技術-的播放控制機制。

本發明的一個目的是提供使用者資料超分送的方法，該方法也讓不同商業模式得以實現。

此目的是藉根據申請專利範圍第1項之方法達成，該方法包括下列步驟：

a)將該使用者資料從該第一資料載體複製到第二資料載體；

b)在該第二資料載體上儲存由服務中心要求有關授予該使用者資料之該副本的存取權的資訊；及

c)藉著傳送至少該儲存資訊到該服務中心以獲得該使用者資料之該副本的存取權，完成交易，並接收額外的存取資訊，其中該服務中心使用該儲存資訊以授予對該第二

五、發明說明（3　　）

資料載體之該使用者資料的該副本之存取權。

本發明係植基於下列觀念：

a)複製控制：複製超分送內容到第二資料載體以外的另一個位置無效，因為服務中心不授權該另一個位置存取-尚不能存取，因為與服務中心之交易尚未完成；及

b)存取控制：在完成與服務中心之交易之後，第二資料載體上的超分送副本僅能在一數位權限管理(Digital Rights Management DRM)系統的支配下存取。

引進像是所謂單一傳播(unicast)超分送概念的另一個基本理由是其提供一種機制以較副本更吸引人的原版交付給使用者—即使二者之間並無明顯差異，並藉此支持零售市場。譬如說，在單一傳播超分送的情況下，原始資料載體擁有者與超分送副本傳遞對象之第二資料載體擁有者之間有直接連結。所以，單一傳播超分送直接(間接)利用現存的人際社會關係，且甚至能藉著鼓勵建立社群來強化這種關係。此外，單一傳播超分送可提供額外的保障，因為在網際網路上公開發行(加密的)使用者資料供一般下載不是非常有用，因為服務中心不會對經由該方式獲得的使用者資料之副本授權存取。

是否授權或拒絕對此一副本存取的判斷完全取決於服務中心，技術上來說服務中心沒有理由譬如因為沒有足夠的訊息而不能授予存取權。最後，藉著僅對原版做合法的超分送-這是譬如因為有一種伴隨超分送之譬如經由贏取相當多〝里程數〞之獎酬系統而比超分送副本更吸引人的

五、發明說明（4　　）

原版交付方法-超分送副本數目的成長率應該會約略等於銷售原版數目的成長率（假設每一銷售的原版約會有對應的一個超分送副本交易）。同樣地這也是支持零售市場的特點。

服務中心授予對使用者資料副本存取權所需的資訊可為服務中心辨識使用者資料所用的任何資訊。譬如該資訊可由下列任何資訊或其組合構成：

- 使用者資料的獨特辨識符號，譬如音樂軌道的ISRC號碼；
- 使用者資料集合的獨特辨識符號，譬如唱片集標題；
- 在服務中心公開金鑰中加密的使用者資料的解密金鑰；
- 原始資料載體的獨特辨識符號；
- 目的資料載體的獨特辨識符號；
- 使用者資料原始擁有者的辨識符號；
- 從上列諸辨識符號中任一個推導出來的代碼值。

為了支持實現植基於防護超分送之商業模式，本發明的一種較佳具體實例植基於採用在第一資料載體上的獨特載體辨識符號-亦即在預先錄製（唯讀記憶體ROM）碟片上的獨特碟片辨識符號-之想法。從此獨特載體辨識符號可較佳地由第一資料載體之播放器決定一代碼值，該代碼值被記錄器連同第一資料載體之獨特載體辨識符號儲存在第二資料載體上。為了致能第二資料載體，亦即第一資料載體之副本，該代碼值與獨特載體辨識符號須傳送到服務中心-譬如第一資料載體上儲存之使用者資料的內容擁有者，這些資

五、發明說明（5　　）

料在服務中心內解碼並/或驗證且當結果為肯定時，所需權利與資訊被傳送回到第二資料載體之記錄器或播放器以致能該第二資料載體。

在本發明的較佳具體實例中還使用其他的辨識符號來增加所提超分送方法的功能性，譬如副本是從誰複製給誰。明確地說，可使用儲存在第一資料載體上並被使用以決定代碼值且在服務中心處驗證該代碼值的超分送辨識符號。

在本發明的另一種具體實例中，可為金鑰階層架構中一部份的一個或更多個金鑰被使用來加密以加密形式儲存在第一資料載體上的使用者資料。這些金鑰須從服務中心提供以致能第二資料載體。此類金鑰譬如可從諸如光學記錄載體上的擺動等實體碟片標記推導出。

在本發明之另一種相態中，超分送播放器金鑰與超分送記錄器金鑰被用來在將代碼值儲存在第二資料載體上之前加密代碼值。然後由服務中心在被加密之代碼值已被傳送到服務中心之後做解密以致能第二資料載體。

此外，在本發明的還有另一種相態中，使用播放器辨識符號與記錄器辨識符號，該等符號也儲存在第二資料載體上並傳送到服務中心以解密超分送播放器金鑰與記錄器金鑰以致能第二資料載體。

或者，兩次加密之代碼值的解密工作也可由播放器及/或記錄器製造商使用播放器及/或記錄器辨識符號執行。所以裝置製造商也涉入致能第二資料載體的處理程序，且可

五、發明說明（6　　）

確定只有符合規定的裝置才可使用，這也提高本發明所提超分送方法的安全度。

在本發明的較佳具體實例中建議因應於儲存在第一資料載體上的使用者資料之防護超分送而將來自服務中心的利益返還給第一資料載體的擁有者。此利益之返還是商業模式的一部份，其中使用者資料之複製與防護分送應予激勵。若超分送內容之存取是由某人購買，則該利益可為具有〝音樂里程〞的此超分送內容之原始來源的獎酬。其他的範例有自由存取〝個人存取碼〞，如歐洲專利申請案00 201 663.2中所述解鎖原始資料載體上的紅利軌跡或對未來購買之回扣的紅利點數。也可能控制以使此利益僅在原始資料載體已經做直接複製時返還。此機制確保購買原始資料載體維持有吸引力，這提供一個對受存取控制的內容做複製保護的機制。

在本發明的還有另一較佳具體實例中，從至少第一資料載體之獨特載體辨識符號產生之獎酬代碼值被傳送到服務中心以便收集被獎酬的利益。服務中心則可決定是否有以及有多少利益應該獎酬給第一資料載體的擁有者。

根據本發明較佳的資料載體宜為光學記錄載體-尤其是可記錄及/或可再寫入光碟或數位視訊光碟。但是根據本發明也可能使用所有其他種類的儲存媒體當作資料載體。根據本發明之方法宜使用做儲存於此類資料載體上之軟體、視訊及/或音訊資料的超分送。

在本發明的一種具體實例中，第二資料載體確實也包括

五、發明說明(7　　)

獨特的載體辨識符號，該載體辨識符號被用以決定代碼值且也被傳送到服務中心以致能第二資料載體。若被使用的資料之目的地很重要，則宜使用第二資料載體的此獨特載體辨識符號。

本發明還關於一種如申請專利範圍第14項之用以對使用者資料做防護超分送的包括播放器與記錄器、傳送裝置與服務中心之系統。此外，本發明係關於一種在此種系統內使用來再生及/或記錄使用者資料的裝置且關於一種用來儲存要使用於根據本發明之防護超分送方法內之使用者資料與超分送資料的資料載體。請注意根據本發明之此類系統、裝置與資料載體可進一步發展且會有其他與上述具體實例及申請專利範圍第1項之附屬項中所陳述者相同或類似的具體實例。

從高階觀點來看，根據本發明之方法與系統以下列方式操作。一預先錄製的碟片包含以資產金鑰加密之內容，該資產金鑰可儲存在諸如歐洲專利申請案00 202 888.4中所描述之金鑰鎖櫃內。而且也使用一譬如光學記錄載體之擺動等由第一實體碟片標記推導出的金鑰。此金鑰可為一金鑰階層架構的一部份，且從而其本身不被使用來直接對內容加密，而是由一組中間金鑰來加密。為了使該方法與系統適當操作，此碟片標記之酬載內容宜被要求為機密-亦即其僅能由符合規定的播放器存取。每個碟片標題有其獨特的酬載內容，但不一定是每個碟片的酬載內容為獨特，亦即所有預先錄製的碟片上之金鑰與加密的內容均完全一樣

五、發明說明（8　　）

。這對內容擁有者而言應該不是問題，因為預先錄製的碟片全部均為已知製造商的原版。

除了第一實體碟片標記之外，有第二-宜為機密的-碟片標記在預先錄製的(ROM)碟片上，每個碟片的該標記為獨特者。此第二標記的酬載內容可在超分送程序的所有階段使用以防止未受控制的超分送。播放的金鑰-亦即資產金鑰-將由服務中心(經防護的)遞送。在副本上採取預防措施以確保該內容只能在該特定碟片上播放，以便防止經由網際網路的未受控制分送。為此目的，可記錄或可再寫入碟片包括獨特的碟片標記，該碟片標記被用以推導內容加密所需的金鑰。對可記錄或可再寫入碟片而言，此獨特碟片標記可預先凸雕在碟片上或由記錄器寫入。

確保只可能複製來源到一個收點是本發明的一個相態。從一個來源複製到多重收點-亦即在網際網路上分送-也可被容許。收點不使用獨特的碟片辨識符號讓這個機能成為可能。但是紅利系統在此情況下可能以不公平的方式操作。若某人安排開立一個大眾化的網站讓每個人從該網站複製檔案，則他會收集到所有的紅利獎酬。反之若經常需要複製原版碟片，則僅有原版碟片的購買者會受到獎酬。

在完成交易之後，內容擁有者-亦即服務中心-提供金鑰，該金鑰被記錄器使用以交付可播放的副本(且僅有該特定副本)。在交易內的某個點上，內容擁有者已經能夠決定原版碟片的獨特載體辨識符號。為了鼓勵消費者製作超分送副本給朋友，內容擁有者可決定提供某種利益給原版碟片

五、發明說明(9　　)

的擁有者。譬如，可給予一〝個人存取碼〞的自由存取權，讓該個人可使用以解鎖原始碟片上的紅利軌跡；所有的紅利點數可累計做日後購買時的回扣。若內容擁有者希望如此，則超分送副本本身可被用以製作另一個超分送副本-或則沒有限制或則只能複製到一預定的限度。在該情況下，內容擁有者可決定返還與超分送內容相關之利益給從原版碟片開始的鏈(像是金字塔系統)內的任何參與者。很明顯的是，內容之防護超分送致能一大量行銷模式，該模式可以每張唱片集為基礎做選擇，且可提供豐富的行銷資訊來源。

現在將參考下列圖式更詳細地說明本發明，諸圖式中

圖1顯示根據本發明之超分送系統的方塊圖，

圖2顯示本發明的一種具體實例中使用的金鑰階層架構之方塊圖，

圖3A、3B顯示原版與副本的碟片配置，

圖4顯示根據本發明之第一種具體實例做複製的步驟，

圖5顯示根據第一種具體實例的致能步驟，

圖6顯示根據第一種具體實例做利益收集的步驟，

圖7顯示根據本發明之第二種具體實例做複製的步驟，

圖8A、8B顯示根據第二種具體實例的致能步驟，且

圖9A、9B顯示根據第二種具體實例做利益收集的步驟。

在顯示根據本發明之超分送系統的一種具體實例的圖1方塊圖中顯示用以再生預先錄製的資料載體-譬如包含譬如軟體、視訊或音訊資料等使用者資料之預先錄製(唯讀記

五、發明說明(10)

憶體ROM)碟片-的播放器1。記錄器2被用以記錄儲存在第一資料載體上可由播放器1再生的資料到譬如可再寫入或可記錄碟片之第二資料載體上。當使用者資料與所有必要的超分送資料已經從播放器1傳送到記錄器2而這些資料已儲存於第二資料載體上之後，此第二資料載體被致能-亦即其具備打算使用第二資料載體所有必要的權限和資訊，致能的方式是藉傳送所需超分送資料到服務中心3，這些資料在服務中心做驗證且若驗證成功則致能資料被返還給記錄器2。為了驗證從記錄器2提供之超分送資料，服務中心3可傳送超分送資料的一部份到播放器製造商4及/或記錄器製造商5做解密及/或驗證。播放器與服務中心之間及服務中心與播放器/記錄器製造商之間的連結不是關鍵而是可選擇的項目。播放器與服務中心之間的連結是為了可能的利益收集用。其他的連結是被用來若需要的話讓製造商〝納入環路中〞。下文將更詳細地說明超分送之系統與方法。

顯示本發明之較佳具體實例中使用的金鑰階層架構之方塊圖顯示於圖2中。首先使用一碟片標記讀取器6讀取提供在碟片上的實體碟片標記以獲得第一組金鑰。從這些金鑰在方塊7內產生所謂金鑰鎖櫃金鑰(key locker key KL_Key)。在此同時，使用一金鑰鎖櫃讀取器8取得資產金鑰的加密版本，其中該資產金鑰係被用來加密使用者資料。金鑰鎖櫃讀取器8的功能是將金鑰鎖櫃的內容從碟片讀出。金鑰鎖櫃本身是碟片上一儲存內容解密金鑰(資產金鑰)與使用權利的特別區域。金鑰鎖櫃之內容被利用金鑰鎖櫃

五、發明說明(11　　)

金鑰加密，金鑰鎖櫃金鑰係根據圖中所示金鑰階層架構推導出。

資產金鑰在方塊9中藉著使用金鑰鎖櫃金鑰解密，接著在方塊10內使用資產金鑰解密被加密的內容-亦即儲存在碟片上的使用者資料。請注意圖2中所示金鑰階層架構僅是可能構成本發明之系統基礎的一種可能的系統。可能有其他可能的設計同樣地可順利運作。

原版與副本資料載體-亦即儲存在二者均為光碟之原版與副本資料載體上的超分送資料-的佈局顯示於圖3A與3B中。圖3A中所示原版碟片包含下列超分送資料：

- 標題辨識符號(title-ID)：資料辨識符號，可為某個數字以辨識內容標題，這不是機密；
- UDI-RO:獨特載體(碟片)辨識符號-特別是唯讀記憶體光碟的辨識符號，這不是機密；UDI-RO儲存在原版(唯讀)碟片上一實體碟片標記內，並辨識一特定碟片(亦即其當作一種序號)。這不是要被複製的。在副本上，UDI-RO的相等物是UDI-R，UDI-R或則(譬如由製造商)預先寫入副本上或則由記錄器以數個強韌性與隨意性規則為條件寫入。請注意UDI-R可位在金鑰鎖櫃的內部。
- EKB：致能金鑰區段(不是機密)，是包含被各種播放器金鑰加密之金鑰的資料區段；
- PDM：實體碟片標記。此實體碟片標記僅能由符合規定的裝置讀取且其宜為機密。若使用致能金鑰區段，則實體碟片標記也可不是機密；

五、發明說明（12　　）

- SD-ID：超分送辨識符號，該辨識符號可為被用以支持超分送功能的某個數字，其為機密且可位於金鑰鎖櫃內；
- AK：資產金鑰，該金鑰被用以加密內容或使用者資料（資產）的某作品。

顯示於圖3B中的副本碟片不包含載體辨識符號UDI-RO而是包含載體辨識符號UDI-R，該符號是可記錄或可再寫入碟片的非機密獨特碟片辨識符號。此外還有資產金鑰AK在當初未儲存在副本碟片上。但是若資產/軌道由服務中心致能，則金鑰AK將被儲存在碟片上。另外還有不同的超分送辨識符號SD-ID'儲存在副本碟片上。SD-ID'可由記錄器產生或者也可藉由某種與服務中心的通信而獲得。在前者情況下，該符號須經由防護鑑別通道(Secure Authenticated Channel SAC)傳送到服務中心。

圖4顯示將儲存在第一資料載體上由播放器再生之使用者資料複製到第二資料載體以在記錄器內進行紀錄的步驟。在第一步驟中，第一資料載體的內容以加密版本傳送到記錄器且記錄在第二資料載體上。在第二步驟中，記錄器返還第二資料載體（目的地碟片）之獨特載體辨識符號UDI-R以使超分送副本僅能在該碟片上致能。在第三步驟中，播放器返還致能超分送副本所需的資訊。此資訊包含譬如為一雜湊函數或一函數F的代碼值，此代碼值包括第一資料載體的辨識此特定原版碟片之獨特載體辨識符號UDI-RO、第二資料載體的辨識此特定目的地碟片之獨特載體辨識符號UDI-R、及確保僅有符合規定的播放器可計算該代碼值

五、發明說明(13　　)

或雜湊函數結果的超分送辨識符號SD-ID。只有符合規定的播放器可計算該代碼，因為只有符合規定的播放器可提取SD-ID。此外，在後續程序中被服務中心要求以驗證代碼值(雜湊函數結果)的獨特載體辨識符號與被服務中心要求以決定超分送辨識符號SD-ID的資料辨識符號title-ID被傳送到記錄器並儲存在第二資料載體上。也可選擇性地單獨提供UDI-R於從播放器到記錄器之第二通信中。

致能第二資料載體的步驟顯示於圖5中。記錄器首先發送致能副本所需的資訊到服務中心，該資訊包含代碼值F、原版的載體辨識符號UDI-RO與資料辨識符號title-ID。副本之載體辨識符號UDI-R被加到此資訊以使服務中心能驗證代碼值(雜湊函數結果)。為了傳送資料，建立了一防護鑑別通道(SAC)以辨識發源的記錄器並作為後續程序使用。此種防護鑑別通道(SAC)是可被使用做資料安全傳輸的介面。

在次一步驟中，服務中心—較佳地使用一資料庫—從資料辨識符號title-ID決定超分送辨識符號SD-ID與資產金鑰AK，並驗證代碼值(雜湊函數結果)。原版的載體辨識符號UDI-RO也在本步驟中連同獎酬利益—如果有的話—儲存在服務中心內。

最終，服務中心在最後步驟中返還資產金鑰AK、由記錄器購買的權利和另一個超分送辨識符號SD-ID'。此外，某種金錢移轉也可包含在該交易中。防護鑑別通道SAC藉此保證僅有符合規定的記錄器可接收此資訊。

五、發明說明（14　　）

下文將參考圖6進一步解釋在第一種具體實例中收集利益的步驟。在第一步驟中，再生原版的播放器發送收集利益所需的資訊到服務中心。此資訊包含異於圖4與5中所示代碼值的另一代碼值或雜湊函數。利益收集所用的雜湊函數包含用以辨識收集利益所屬的碟片之原版的載體辨識符號UDI-RO與確保只有符合規定之播放器可計算雜湊函數結果之原版的超分送辨識符號SD-ID。而且，傳送到服務中心的此資訊包含UDI-RO與資料辨識符號title-ID，UDI-RO在後續程序中被服務中心要求以驗證雜湊函數結果，title-ID被服務中心要求以決定超分送辨識符號SD-ID。再次，一防護鑑別通道SAC被建立以辨識發源播放器並在後續步驟3中使用。

在第二步驟中，服務中心-較佳地藉使用一資料庫-從資料辨識符號title-ID決定超分送辨識符號SD-ID並驗證雜湊函數結果。接著從載體辨識符號UDI-RO-再次較佳地藉使用一資料庫-決定利益。在第三步驟中，利益或利益狀態概要藉著使用確保正確的符合規定之播放器接收此資訊的防護鑑別通道SAC返還給播放器。利益可根據商業需要與來源碟片或播放器結合，而非僅與碟片結合。

圖4到6中所顯示及上文所述的具體實例使用非對稱金鑰密碼技術以建立防護鑑別通道(SAC)並只容許從一原始碟片做複製。此外，裝置製造商不在交易環路中。但是本發明不侷限於具有這些特性的系統與方法。本發明也可只採用對稱金鑰密碼技術而被使用且也容許從已經被複製的

五、發明說明(15　　)

碟片進行複製。此外，裝置製造商可涉入交易環路中，這將顯示在圖7到9中且在下文中的具體實例中描述。

圖7顯示根據本發明第二種具體實例的複製程序之步驟。在步驟1中，第一資料載體的內容以加密形式轉移給記錄器。在步驟2中，記錄器再次返還目的地碟片之載體辨識符號UDI-R以使超分送副本僅能在該碟片上被致能。在步驟3中，播放器返還致能超分送副本所需的資訊，該資訊包含辨識該特定來源碟片之載體辨識符號UDI-RO、辨識該特定目的地碟片之載體辨識符號UDI-R、與確保只有符合規定的播放器可以計算該雜湊函數結果且只有權利保有者可反轉一雜湊函數(較佳地使用一資料庫)的超分送辨識符號SD-ID之雜湊函數(函數F)。在該資訊傳送給記錄器之前，可選擇性地使用一對每個播放器為獨特的超分送播放器金鑰SDPK對雜湊函數結果加密以確保播放器與記錄器製造商在程序的致能階段有對稱角色。此外，在後續程序中被服務中心要求以驗證雜湊函數結果的載體辨識符號UDI-RO與被服務中心要求以決定超分送辨識符號SD-ID的資料辨識符號title-ID，以及辨識發源播放器之播放器辨識符號player-ID被傳送到記錄器。可選擇性地，UDI-R也可在從播放器到記錄器的第二通信中單獨提供。

此具體實例中的致能步驟顯示於圖8A中。在第一步驟中，記錄器發送致能副本所需的資訊。載體辨識符號UDI-R被加至此資訊以使服務中心能驗證雜湊函數結果。在傳送雜湊函數結果之前使用超分送記錄器金鑰SDRK將之加密以

五、發明說明（16　）

保證一特定記錄器已發送該資訊。此外，記錄器辨識符號recorder-ID被加上以辨識發源記錄器。在第二步驟中，服務中心接觸播放器與記錄器製造商以求解密雜湊函數結果，並接著從資料辨識符號title-ID-較佳地使用一資料庫-決定超分送辨識符號SD-ID與資產金鑰AK，並驗證雜湊函數結果。從記錄器提供之載體辨識符號UDI-RO連同獎酬利益儲存在服務中心內。

在第三步驟中，服務中心返還資產金鑰AK與由記錄器購買的權利。此資訊首先藉著使用一從載體辨識符號UDI-R推導出的金鑰做加密以確保記錄器製造商無法濫用此資訊。經加密的資訊接著由記錄器製造商進一步加密以確保只有適當的記錄器可接收該資訊。加密工作確保由服務中心返還的資訊只能被使用以致能一特定副本-亦即由UDI-R辨識的副本。

服務中心與記錄器製造商或播放器製造商之間為了加密而進行的通信顯示於圖8B中。

第二種具體實例中的利益收集步驟顯示於圖9A中。其中播放器在步驟1中發送收集利益所需的資訊到服務中心。此資訊包含雜湊函數，該雜湊函數包含載體辨識符號UDI-RO與超分送辨識符號SD-ID，UDI-RO用來辨識收集利益所屬的碟片，SD-ID用來確保只有符合規定的播放器可計算該雜湊函數結果且只有權利保有者可反轉該雜湊函數。而且，傳送到服務中心的資訊包含載體辨識符號UDI-RO與資料辨識符號title-ID，UDI-RO在後續程序中被服務中心要求以驗

五、發明說明（17　　）

證雜湊函數結果，title-ID被服務中心要求以決定超分送辨識符號SD-ID。雜湊函數結果在被傳送之前以一超分送播放器金鑰加密以保證此資訊係由符合規定的播放器發送出。

在第二步驟中，服務中心接觸播放器製造商以求解密雜湊函數結果，並接著從資料辨識符號title-ID-較佳地使用一資料庫-決定超分送辨識符號SD-ID，並驗證雜湊函數結果。此外，從載體辨識符號UDI-RO-較佳地使用一資料庫-決定利益。

在第三步驟中，利益或利益狀態概要返還給播放器。該資訊在傳送之前首先使用從載體辨識符號UDI-RO推導出的金鑰加密以確保播放器製造商無法濫用此資訊。此資訊的第二加密由記錄器製造商執行以保證只有適當的播放器可接收該資訊。

E{SDRK}與E{SDPK}表明為對稱加密。當然也可能使用非對稱加密或已經存在的防護鑑別通道SAC。因為資產金鑰AK應為機密，所以可在與記錄器製造商的通信中藉由以UDI-R(O)加密的方式加以保護。碟片上的UDI不一定要為機密。但是用UDI-R(O)加密的確賦予較高的機密等級，因為記錄器製造商在超分送期間不知道所用的UDI。

服務中心與記錄器製造商或播放器製造商之間為了加密而進行的通信顯示於圖9B中。

根據本發明建議了一種使用者資料之防護超分送的方法與系統。各種讓內容可藉著受控制的方式在家庭中做複

五、發明說明（18　）

製而分送的商業模式可在本發明之方法與系統中實現。副本以無法播放的形式交付，直到完成一適當交易後才可播放。此外本發明也因為內容擁有者與消費者之間的直接接觸而提供新的行銷機會。本發明可激勵消費者複製使用者資料。譬如，副本可比原版便宜且利益可提供給原版的擁有者—像是自由存取紅利軌道的存取代碼或未來購買時的回扣（〝累積里程〞）。此外，這種超分送方法比從網際網路下載整個唱片集來得方便。

可採取措施讓原版有吸引力，譬如只容許原版做合法的超分送以防止超分送〝工廠〞。

根據本發明之方法與系統可用來收集行銷資訊—譬如藉著使用音樂〝里程〞。交易所用裝置可維持匿名或不匿名。此外也可決定超分送的複製是否只能連線作業或者也容許離線作業。總之，本發明容許對存取受控制的內容執行複製控制。

A5
B5

四、中文發明摘要（發明之名稱：使用者資料之超分送防護）

本發明論及一種將儲存在第一資料載體上的使用者資料做超分送防護的方法，該方法包括下列步驟：

a）將該使用者資料從該第一資料載體複製到第二資料載體；

b）在該第二資料載體上儲存由服務中心要求有關授予該使用者資料之該副本的存取權的資訊；及

c）藉著傳送至少該儲存資訊到該服務中心以獲得該使用者資料之該副本的存取權，完成交易，並接收額外的存取資訊；

該方法的特點在於該服務中心使用該儲存資訊以授予對

英文發明摘要（發明之名稱：SECURE SUPER DISTRIBUTION OF USER DATA）

The invention refers to a method for secure super distribution of user data stored on a first data carrier comprising the steps of

a) copying said user data from said first data carrier to a second data carrier;

b) storing on said second data carrier information that is required by a service center for granting access rights to said copy of said user data; and

c) obtaining access rights to said copy of said user data by transmitting at least said stored information to said service center, completing a transaction, and receiving additional access information;

characterized in that said service center uses said stored information to grant access rights to said copy of said user data for said second data carrier.

Thus copy control is performed over access-controlled content. Additionally, benefits can be given to the owner of original data carriers. The invention also refers to a system for secure super distribution, an apparatus for reproduction and/or recording of user data and to a data carrier.

A5
B5

四、中文發明摘要（發明之名稱：　　）

該第二資料載體之該使用者資料的該副本的存取權。

所以可對存取受控制的內容執行複製控制。此外，原始資料載體的擁有者也可獲益。本發明也論及一種將使用者資料做超分送防護的系統、一種再生及/或記錄使用者資料的裝置、及儲存使用者資料的資料載體。

英文發明摘要（發明之名稱：　　）

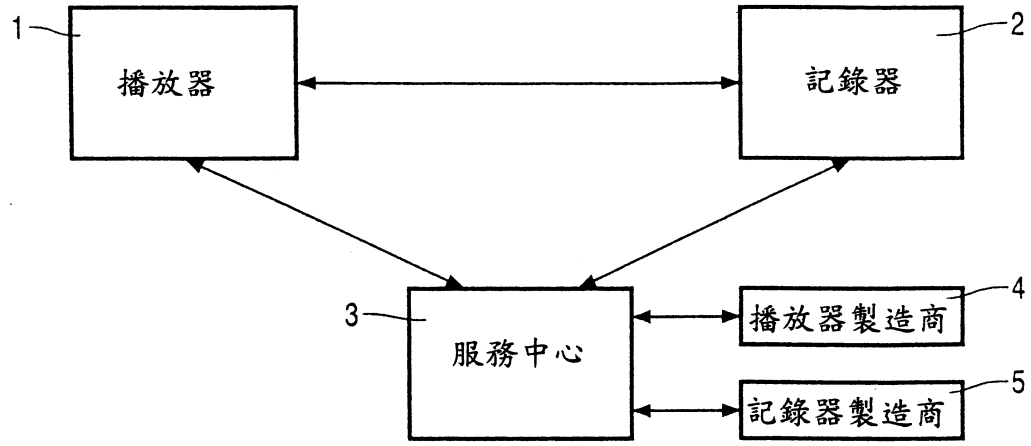
1
播放器
2
記錄器
3
服務中心
播放器製造商
4
記錄器製造商
5

圖 1

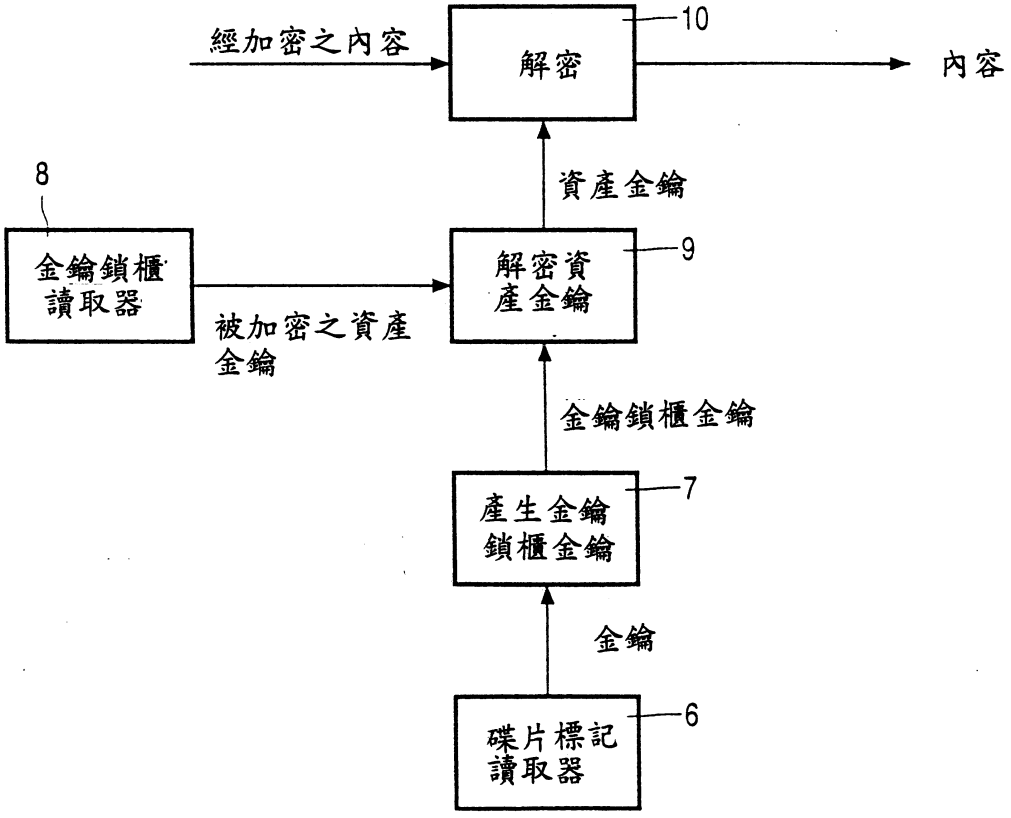
經加密之內容
解密
10
內容
資產金鑰
8
金鑰鎖櫃
讀取器
解密資
產金鑰
9
被加密之資產
金鑰
金鑰鎖櫃金鑰
產生金鑰
鎖櫃金鑰
7
金鑰
碟片標記
讀取器
6

圖 2

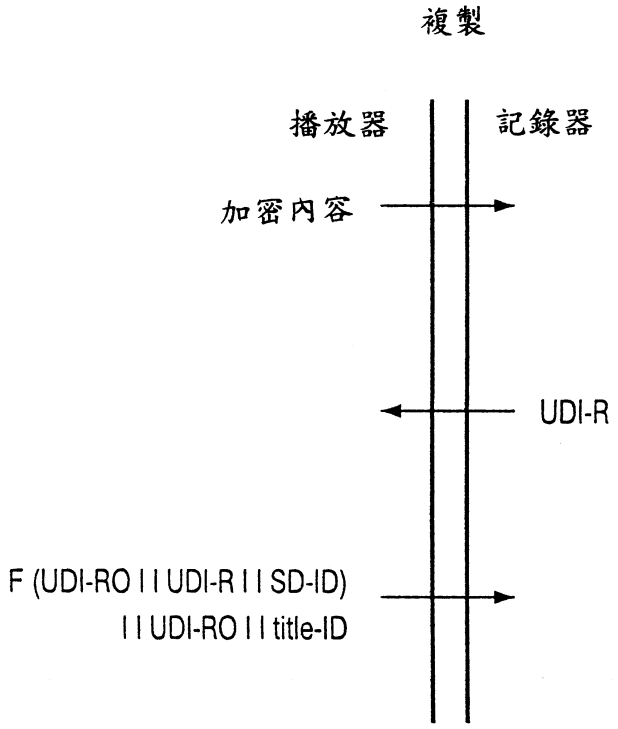
複製
播放器
記錄器
加密內容
UDI-R
F (UDI-RO I I UDI-R I I SD-ID)
I I UDI-RO I I title-ID

圖 4

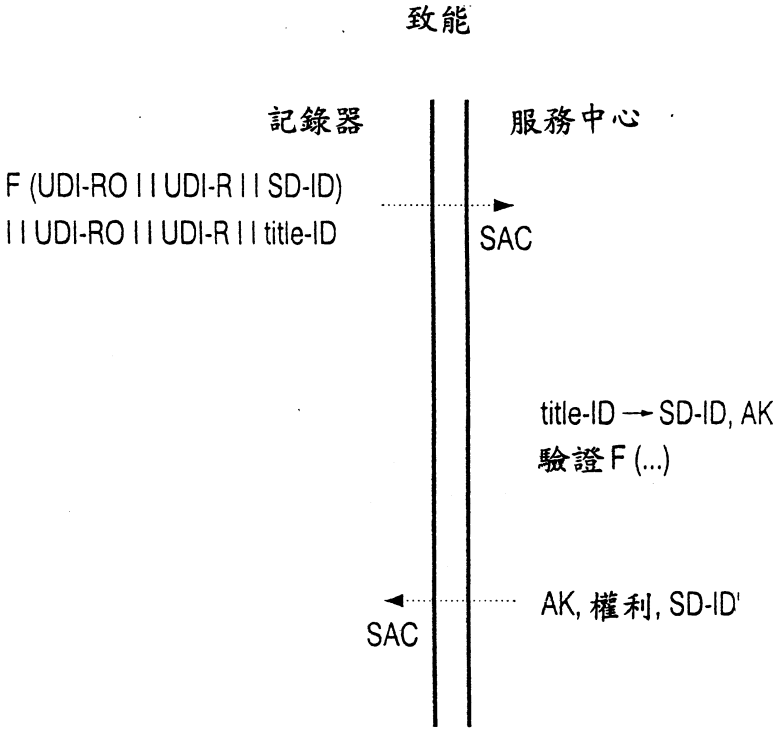
致能
記錄器
服務中心
F (UDI-RO I I UDI-R I I SD-ID)
I I UDI-RO I I UDI-R I I title-ID
SAC
title-ID → SD-ID, AK
驗證 F (...)
AK, 權利, SD-ID'
SAC

圖 5

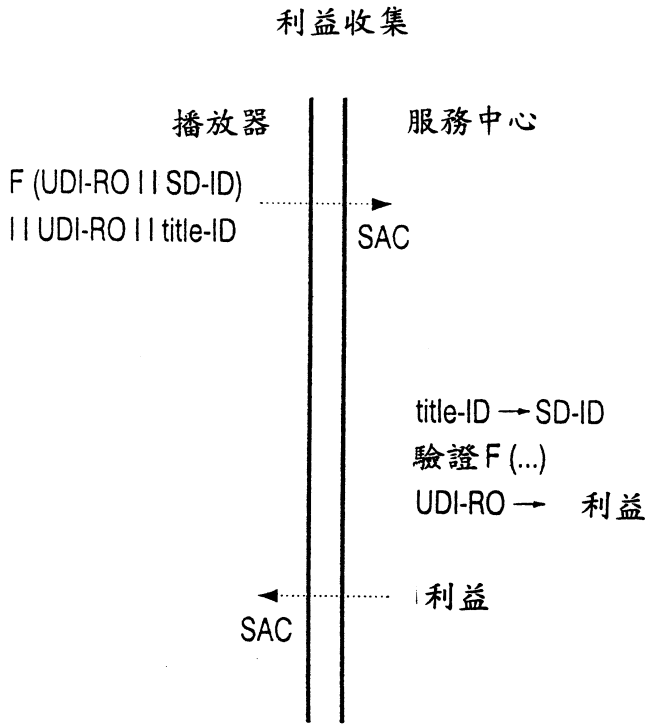
利益收集
播放器
服務中心
F (UDI-RO I I SD-ID)
I I UDI-RO I I title-ID
SAC
title-ID → SD-ID
驗證 F (...)
UDI-RO → 利益
利益
SAC

圖 6

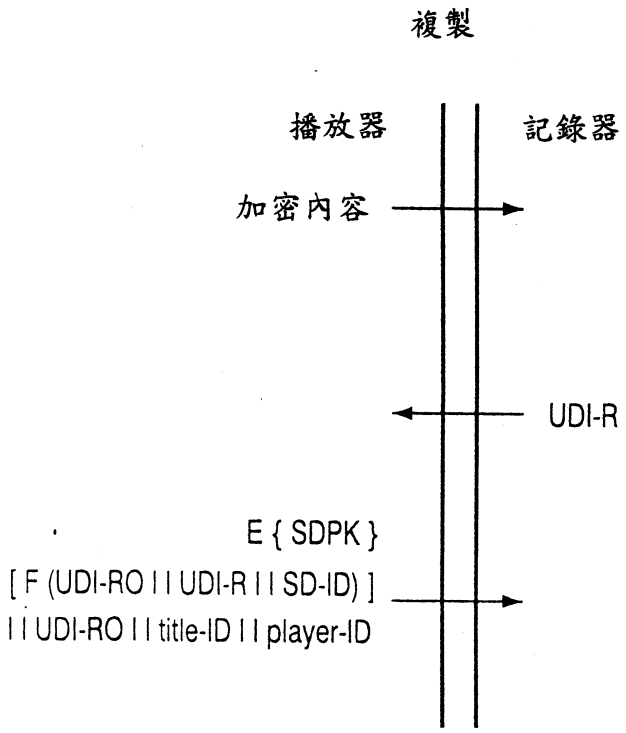
複製
播放器
記錄器
加密內容
UDI-R
E { SDPK }
[F (UDI-RO I I UDI-R I I SD-ID)]
I I UDI-RO I I title-ID I I player-ID

圖 7

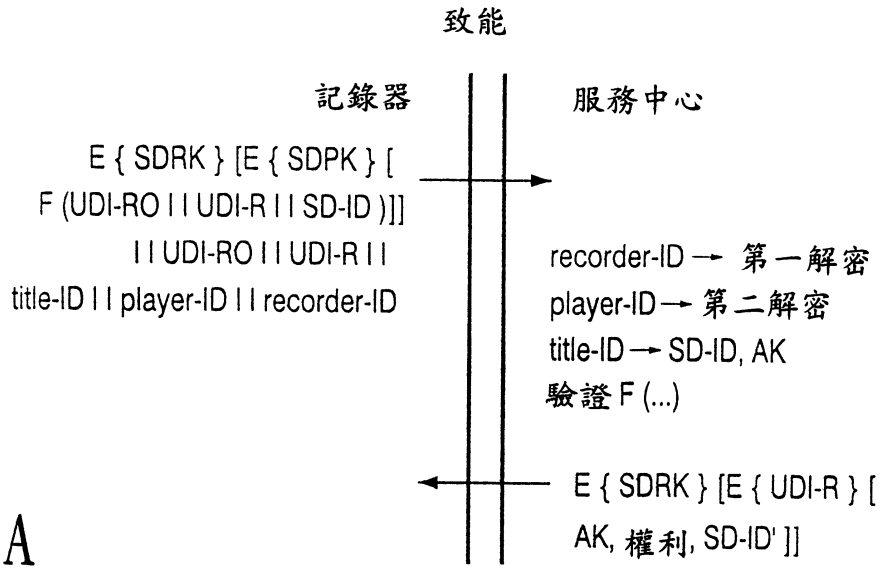
致能
記錄器
服務中心
E { SDRK } [E { SDPK } [
F (UDI-RO I I UDI-R I I SD-ID)]]
I I UDI-RO I I UDI-R I I
title-ID I I player-ID I I recorder-ID
recorder-ID → 第一解密
player-ID → 第二解密
title-ID → SD-ID, AK
驗證 F (...)
E { SDRK } [E { UDI-R } [
AK, 權利, SD-ID']]

圖 8A

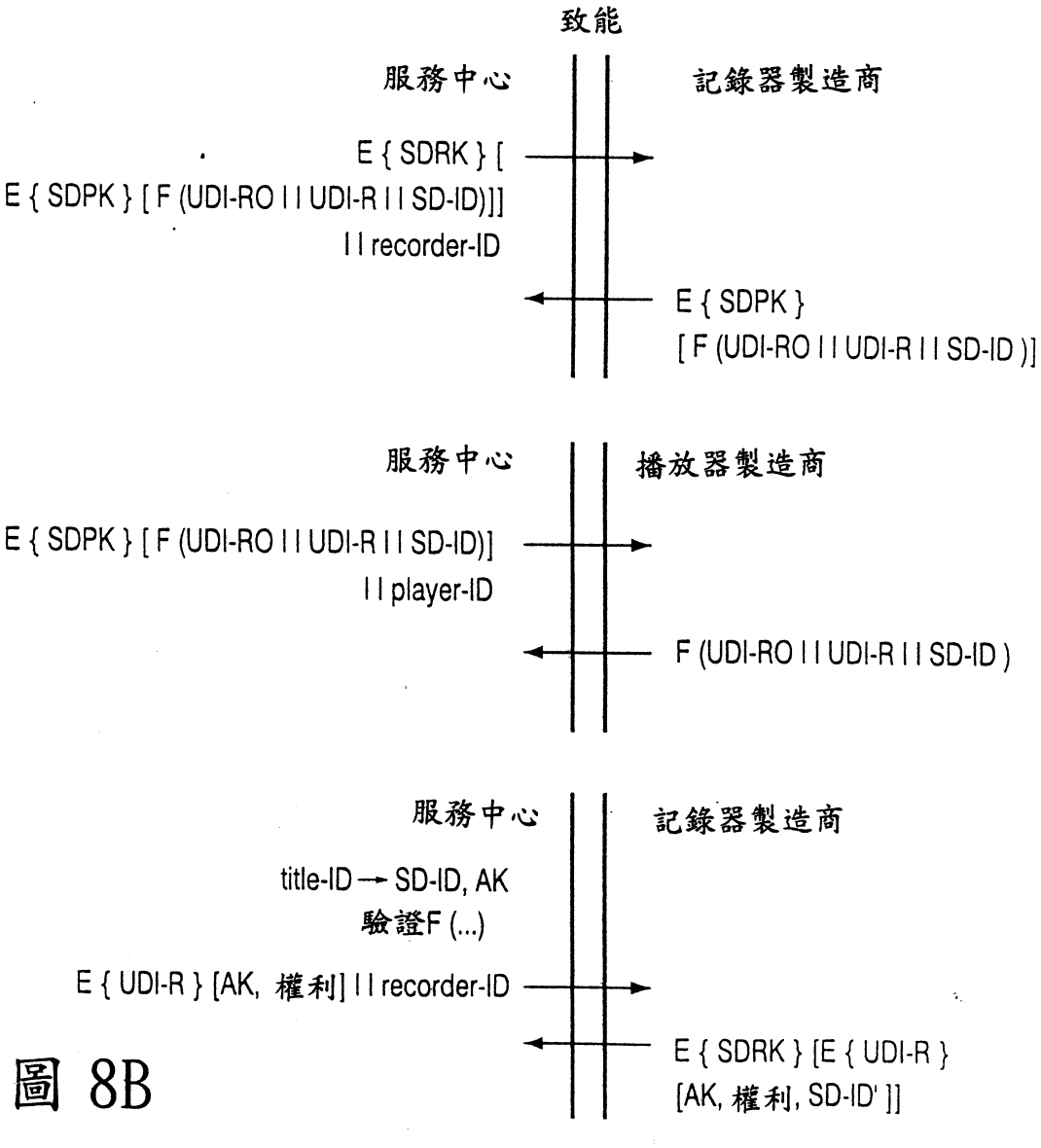
致能
服務中心
記錄器製造商
E { SDRK } [
E { SDPK } [F (UDI-RO I I UDI-R I I SD-ID)]]
I I recorder-ID
E { SDPK }
[F (UDI-RO I I UDI-R I I SD-ID)]
服務中心
播放器製造商
E { SDPK } [F (UDI-RO I I UDI-R I I SD-ID)]
I I player-ID
F (UDI-RO I I UDI-R I I SD-ID)
服務中心
記錄器製造商
title-ID → SD-ID, AK
驗證F (...)
E { UDI-R } [AK, 權利] I I recorder-ID
E { SDRK } [E { UDI-R }
[AK, 權利, SD-ID']]

圖 8B

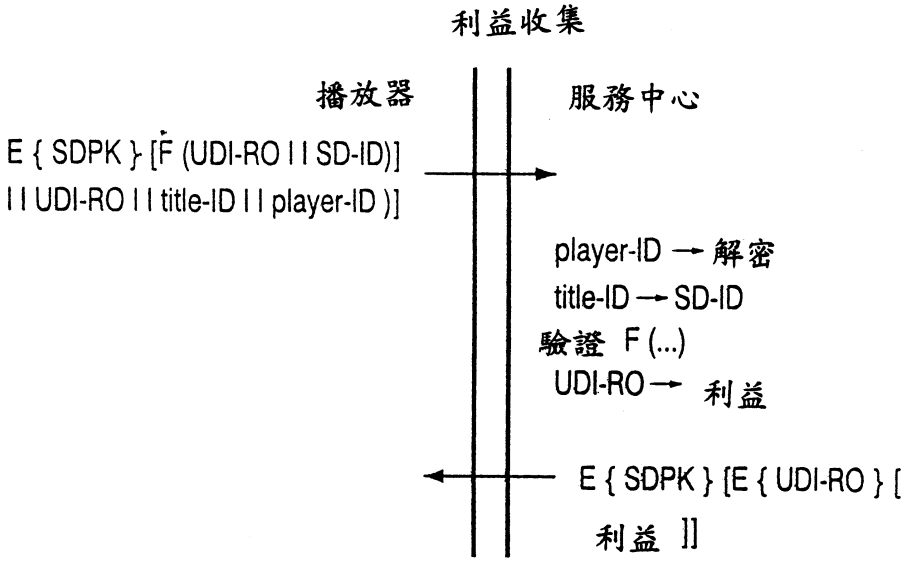
利益收集
播放器
服務中心
E { SDPK } [F (UDI-RO I I SD-ID)]
I I UDI-RO I I title-ID I I player-ID)]
player-ID → 解密
title-ID → SD-ID
驗證 F (...)
UDI-RO → 利益
E { SDPK } [E { UDI-RO } [
利益]]

圖 9A

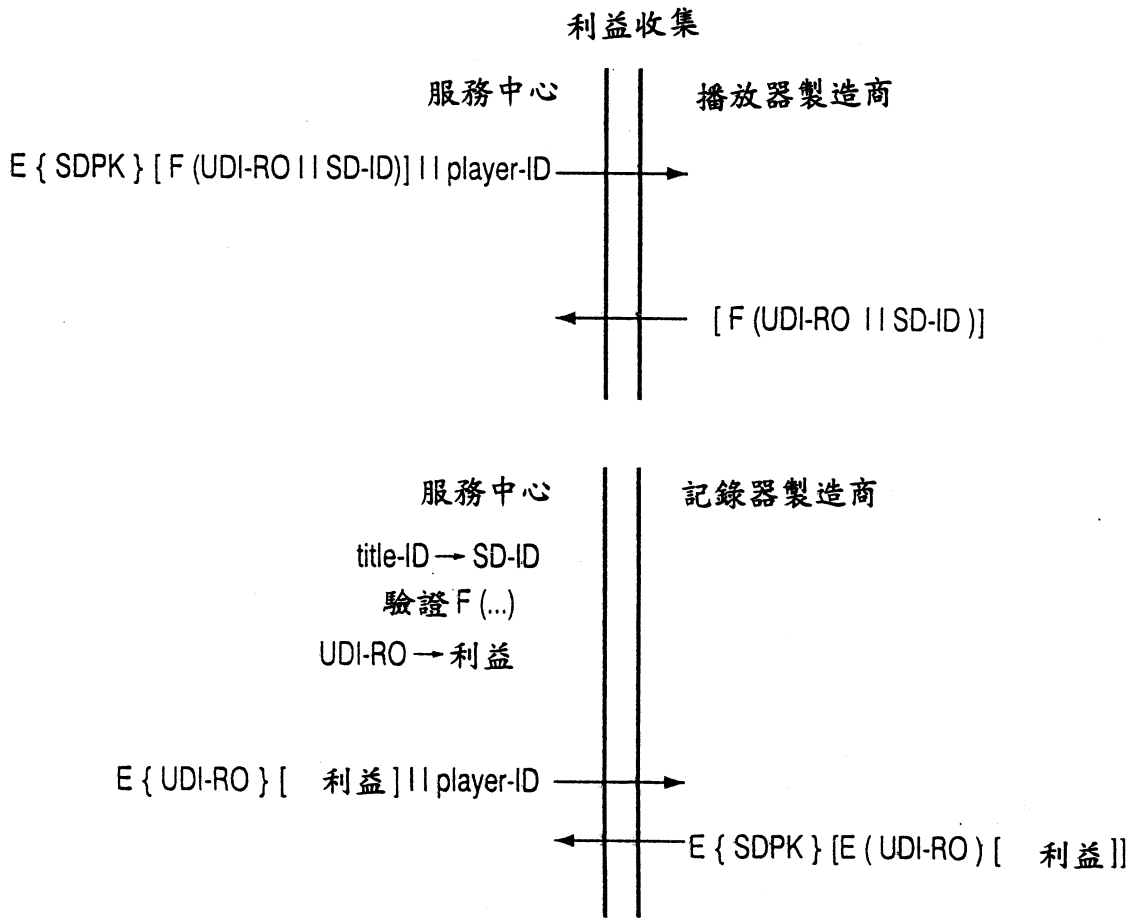
利益收集
服務中心
播放器製造商
E { SDPK } [F (UDI-RO I I SD-ID)] I I player-ID
[F (UDI-RO I I SD-ID)]
服務中心
記錄器製造商
title-ID → SD-ID
驗證 F (...)
UDI-RO → 利益
E { UDI-RO } [利益] I I player-ID
E { SDPK } [E (UDI-RO) [利益]]

圖 9B

五、發明說明（ 19 ）

圖式元件符號說明

1	播放器
2	記錄器
3	服務中心
4	播放器製造商
5	記錄器製造商
6	碟片標記讀取器
7	金鑰鎖櫃金鑰(KL-Key)產生器
8	金鑰鎖櫃讀取器
9	資產金鑰解密器
10	解密器

六、申請專利範圍

1. 一種對儲存在第一資料載體上之使用者資料做超分送防護之方法，該方法包括下列步驟：

   a)將該使用者資料從該第一資料載體複製到第二資料載體；

   b)在該第二資料載體上儲存由服務中心要求有關授予該使用者資料之該副本的存取權的資訊；及

   c)藉著傳送至少該儲存資訊到該服務中心以獲得該使用者資料之該副本的存取權，完成交易，並接收額外的存取資訊；

   該方法的特徵是該服務中心使用該儲存資訊以授予對該第二資料載體之該使用者資料的該副本的存取權。

2. 如申請專利範圍第1項之方法，其特徵是對儲存在該第一資料載體上之該使用者資料的存取由數位權限管理或條件式存取系統控制。

3. 如申請專利範圍第1或2項之方法，其特徵是該第一與第二資料載體各包括獨特的載體辨識符號，且該被儲存的資訊由該第一與第二資料載體的至少該等獨特載體辨識符號決定之至少一代碼值組成。

4. 如申請專利範圍第3項之方法，其特徵是該等獨特載體辨識符號也被傳送到該服務中心。

5. 如申請專利範圍第3項之方法，其特徵是該第一資料載體包括被用以決定該代碼值的超分送辨識符號。

6. 如申請專利範圍第3項之方法，其特徵是該代碼值在被儲存到該第二資料載體之前由一超分送播放器金鑰加

六、申請專利範圍

密，且該經加密之代碼值在被傳送到該服務中心之前還由一超分送記錄器金鑰進一步加密。

7. 如申請專利範圍第6項之方法，其特徵是對應於該超分送播放器金鑰之該播放器辨識符號儲存在該第二資料載體上，且該播放器辨識符號與對應於該超分送記錄器金鑰之記錄器辨識符號傳送到該服務中心。

8. 如申請專利範圍第7項之方法，其特徵是該經加密之代碼值的解密工作是由各自的播放器及/或記錄器製造商執行。

9. 如申請專利範圍第1或2項之方法，其特徵是該服務中心因應於儲存在該第一資料載體上之該使用者資料的超分送程序之完成而獎酬該第一資料載體的擁有者。

10. 如申請專利範圍第9項之方法，其特徵是從該第一資料載體的至少該獨特辨識符號產生之獎酬代碼值被傳送到該服務中心以便收集獲得獎酬的利益。

11. 如申請專利範圍第1或2項之方法，其特徵是使用光碟-尤其是可記錄及/或可再寫入光碟(CD)或數位視訊光碟(DVD)-當作資料載體。

12. 如申請專利範圍第1或2項之方法，其特徵是該使用者資料是音訊資料、視訊資料、或軟體。

13. 如申請專利範圍第1項之方法，其特徵是該服務中心使用該被儲存的資訊以僅授予該第二資料載體對該使用者資料之該副本的存取權。

14. 一種對儲存在第一資料載體上之使用者資料做超分送

六、申請專利範圍

防護的系統，該系統包括：

a)播放器與記錄器，用來將該使用者資料從該第一資料載體複製到第二資料載體，並儲存超分送資料於該第二資料載體上；

b)傳送裝置，用來將被儲存的超分送資料傳送到服務中心；及

c)服務中心，用來對該第二資料載體上的該使用者資料之該副本授予存取權，

其中該播放器被提供以從來自該第一與第二資料載體的至少該等獨特載體辨識符號決定一代碼值，且該記錄器被提供以儲存至少該代碼值與該第一資料載體之該獨特辨識符號於該第二資料載體上。

15. 一種播放器，供使用於如申請專利範圍第14項之系統中，以讀取儲存於一第一資料載體上之使用者資料，其特徵在於該播放器被提供以從來自該第一資料載體的至少一獨特載體辨識符號以及一第二資料載體的至少一獨特載體辨識符號決定一代碼值。

16. 一種記錄器，供使用於如申請專利範圍第14項之系統中，用來將儲存於一第一資料載體上之使用者資料記錄到一第二資料載體上，並儲存超分送資料於該第二資料載體上，其特徵在於該記錄器被提供以進一步將該第一資料載體的至少一獨特載體辨識符號以及一代碼值記錄到該第二資料載體上，其中代碼值係由該第一資料載體的至少該獨特載體辨識符號以及該第二資料載體的一

六、申請專利範圍

獨特載體辨識符號所決定。

17. 一種儲存使用者資料與超分送資料之資料載體，該資料載體使用於如申請專利範圍第1項之超分送防護方法內，超分送資料包括：

a)辨識資料載體之獨特載體辨識符號；

b)辨識儲存在資料載體上之使用者資料的資料辨識符號；

c)被用以提供超分送功能的超分送辨識符號；及

d)對使用者資料及/或超分送資料做加密的一個或更多個金鑰。


原版
超分送辨識符號
資產金鑰
...
金鑰鎖櫃
標題辨識符號
UDI-RO
致能金鑰區段
實體碟片標記

圖 3A

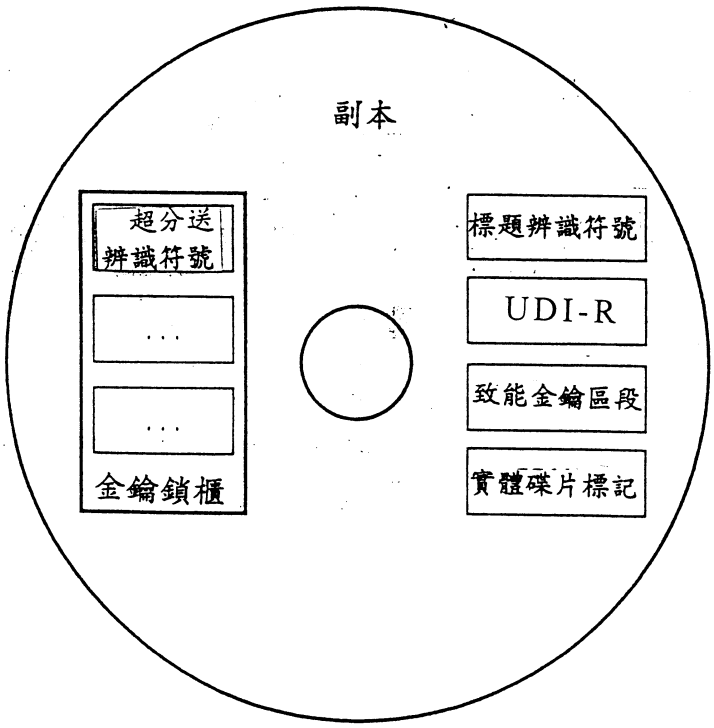
副本
超分送辨識符號
...
...
金鑰鎖櫃
標題辨識符號
UDI-R
致能金鑰區段
實體碟片標記

圖 3B