公告本

900563-01(MaS/ka)

申請日期	89.12.7.
案號	89126047
類別	H04M 1/08

（以上各欄由本局填註）

A4
C4

493335

發明 ~~新型~~ 專利說明書

一、發明 ~~新型~~ 名稱	中文	資料再生裝置
	英文	DATA REPRODUCING DEVICE
二、發明 ~~創作~~ 人	姓名	1.長谷部高行 TAKAYUKI HASEBE 2.畠山卓久 TAKAHISA HATAKEYAMA 3.利根川忠明 TADAAKI TONEGAWA 4.穴澤健明 TAKEAKI ANAZAWA
	國籍	日本國
	住、居所	1.至 2.地址同 日本國神奈川縣川崎市中原區上小田中4丁目1番1號 富士通股份有限公司內 c/o FUJITSU LIMITED 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa Japan 3.日本國東京都小平市上水本町五丁目20番1號 日立製作所股份有限公司半導體組內 c/o Semiconductor & Integrated Circuits, HITACHI, LTD. 20-1, Josuihoncho 5-chome Kodaira-shi, Tokyo Japan 4.日本國東京都港區赤坂四丁目14番14號 日本哥倫比亞股份有限公司內 c/o NIPPON COLUMBIA CO., LTD 14-14, Akasaka 4-chome Minato-ku, Tokyo Japan
三、申請人	姓名（名稱）	1.富士通股份有限公司 FUJITSU LIMITED 2.日立製作所股份有限公司 HITACHI, LTD. 3.日本哥倫比亞股份有限公司 NIPPON COLUMBIA CO., LTD. 4.三洋電機股份有限公司 SANYO ELECTRIC CO., LTD.
	國籍	日本國
	住、居所（事務所）	1.日本國神奈川縣川崎市中原區上小田中4丁目1番1號 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa Japan 2.日本國東京都千代田區神田駿河台四丁目6番地 6, Kanda Surugadai 4-chome Chiyoda-ku, Tokyo Japan 3.日本國東京都港區赤坂四丁目14番14號 14-14, Akasaka 4-chome Minato-ku, Tokyo Japan 4.日本國大阪府守口市京阪本通2丁目5番5號 5-5, Keihan-Hondori 2-chome, Moriguchi-shi, Osaka Japan
	代表人姓名	1.秋草直之 NAOYUKI AKIKUSA 2.庄山悅彥 ETSUHIKO SHOYAMA 3.篠原忠彥 TADAHIKO SHINOHARA 4.桑野幸德 YUKINORI KUWANO

裝 訂 線

申請日期	
案號	
類別	

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	
	英文	
二、發明創作人	姓名	5.堀吉宏 YOSHIHIRO HORI 6.日置敏昭 TOSHIAKI HIOKI 7.金森美和 MIWA KANAMORI 8.吉川隆敏 TAKATOSHI YOSHIKAWA 9.武村浩司 HIROSHI TAKEMURA
	國籍	日本國
	住、居所	5.至 9.地址同 日本國大阪府守口市京阪本通2丁目5番5號 三洋電機股份有限公司內 c/o SANYO ELECTRIC CO., LTD. 5-5, Keihan-Hondori 2-chome Moriguchi-shi, Osaka Japan
三、申請人	姓名（名稱）	
	國籍	
	住、居所（事務所）	
	代表人姓名	

裝 訂 線

（由本局填寫）

承辦人代碼：	
大　　類：	
IPC分類：	

A6
B6

本案已向：

日本　國（地區）　申請專利，申請日期：　　案號：　　，☑有　☐無主張優先權

1999 年 12 月 7 日　特願平 11-347904(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

A7
B7

五、發明說明（1）

技術領域

本發明係關於一種對可保護複製的資訊的著作權行動電話機等之終端機配送資訊用的資料分配送信系統中的資料再生裝置。

背景技術

近年來，隨著網際網路等之資訊通信網等的進步，各使用者可透過使用行動電話等的個人端終端機，輕易地對網路資訊進行存取作業。

在該種資訊通信網中，係以數位信號傳送資料。因而，即使各使用者在複製例如如上述之資訊通信網中所傳送的音樂或影像資料之情況，亦可在幾乎不會因該種的複製而產生音質或畫質劣化之情形下，進行資料之複製。

換句話說，在該種資訊通信網上傳輸音樂資料或圖像資料等的著作權人有著作權的內容資料，且未採取適當的著作權保護措施時，顯然著作權人之權利有受到侵害之虞。

另一方面，當以著作權保護之目的為最優先考量，而不透過急速擴大之數位資訊通信網進行內容資料之分配送信時，基本上，對於可在複製資料時徵收一定之著作權費的著作權人而言反而不利。

然而，在透過如上述之數位資訊通信網而進行音樂資料等的內容資料之分配送信時，各使用者，再將如此分配送信之資料記錄在任何的記錄裝置之後，即可利用再生裝置予以再生。

五、發明說明（ 2 ）

此種記錄裝置，可採用例如記憶卡等可進行電性之資料寫入及抹除的媒體。

而且，用以再生內容資料的裝置，在使用其用於接受該種資料之分配送信的行動電話機本身時，或記錄裝置如記憶卡等可從用以接受分配送信之裝置中自由裝卸時，亦可使用專用的再生裝置。

此情況，為了要保護著作權人之權利，而有必要在記錄媒體中施行如下保密對策，即未經著作權人之允許，就無法從該記錄媒體中自由地將所接收的內容資料移轉至其他的記錄媒體等中。

為了提高此種系統的保密性，就有必要在構成系統之機器間，或在該機器之內部任何可由外部存取之區域所進行的資料之授受上，充分考慮認證處理或密碼化處理等。

另一方面，會有此種的認證處理或密碼化處理大過繁複，以致於利用正規的機器再生內容資料供視聽之用時，光是到可開始再生的時間就長到無法接受之問題。

發明之揭示

本發明之目的在於提供一種用以再生經分配送信而保持於記錄裝置內之內容資料的再生裝置，該資料再生裝置係具備有可保護該裝置免於被使用者以外的人擅自對該內容資料進行存取的機能。

本發明之另一目的在於提供一種可提高資料分配送信系統之保密，且可迅速開始內容資料之再生處理的資料再生裝置。

五、發明說明（3）

為了達成該目的，本發明之資料再生裝置，係用以將密碼化內容資料解碼而後進行內容資料之再生者，此裝置係具有資料儲存部及資料再生部。

資料儲存部，係保持密碼化內容資料及用以解碼密碼化內容資料的授權鑰(license key)，並使授權鑰以密碼化的狀態輸出，且可相對於資料再生裝置自由裝拆。資料再生部係用以接收資料儲存部的輸出，而再生密碼化內容資料。資料再生部，包含有第一解碼處理部、第二解碼處理部及認證鑰保持部。第一解碼處理部，係根據來自資料儲存部的密碼化授權鑰，以第一解碼鑰進行解碼處理而抽出授權鑰。第二解碼處理部，係接受從資料儲存部讀出的密碼化內容資料，再利用第一解碼處理部的輸出進行解碼而抽出內容資料。認證鑰保持部，係利用公開認證鑰將認證資料予以密碼化及保持俾可對資料儲存部輸出。資料儲存部，包含有第三解碼處理部及控制電路。第三解碼處理部，係用以將利用公開認證鑰密碼化且由資料再生部提供的認證資料予以解碼及抽出。控制電路，係根據利用第三解碼處理部而抽出的認證資料進行認證處理。控制電路，係在與複數個密碼化內容資料之再生動作共通之預定期間內進行認證處理之至少一部分者。

較佳者，預定期間係指在資料再生裝置為活動期間內，資料儲存部被裝設在資料再生部內之後的期間。

或是，預定期間係指在資料儲存部裝設在資料再生裝置內之狀態下使再生裝置活動之後的期間。

五、發明說明（4）

因而，使用本案之資料再生裝置的分配送信系統中，藉由在複數個再生處理中使資料再生裝置與記憶卡之相互認證處理之一部分共有化，即可迅速進行個別的再生動作。

圖式之簡單說明

第1圖係概略說明本發明之資料分配送信系統之整體構成的概念圖。

第2圖係說明第1圖所示之資料分配送信系統中所使用之通信用的資料、資訊等的特性說明圖。

第3圖係顯示授權伺服器10之構成的概略方塊圖。

第4圖係顯示行動電話機100之構成的概略方塊圖。

第5圖係顯示記憶卡110之構成的概略方塊圖。

第6圖係用以說明實施例1之行動電話機100中之再生初始化對話的流程圖。

第7圖係用以說明實施例1之行動電話機100中之再生音樂之再生動作的流程圖。

第8圖係用以說明實施例1之資料分配送信系統中之分配送信動作的第一流程圖。

第9圖係用以說明實施例1之資料分配送信系統中之分配送信動作的第二流程圖。

第10圖係用以說明實施例1之資料分配送信系統中之分配送信動作的第三流程圖。

第11圖係用以說明實施例1之二個記憶卡間之移動動作的第一流程圖。

五、發明說明（ 5 ）

第12圖係用以說明實施例1之二個記憶卡間之移動動作的第二流程圖。

第13圖係用以說明實施例1之二個記憶卡間之移動動作的第三流程圖。

第14圖係說明用於實施例2之資料分配送信系統中之通信用之資料、資訊等的特性圖

第15圖係顯示實施例2之二個記憶卡114之構成的方塊圖。

第16圖係用以說明實施例2之資料分配送信系統中之內容購入時所產生之分配送信動作的第一流程圖。

第17圖係用以說明實施例2之資料分配送信系統中之內容購入時所產生之分配送信動作的第二流程圖。

第18圖係用以說明實施例2之資料分配送信系統中之內容購入時所產生之分配送信動作的第三流程圖。

第19圖係用以說明使用實施例2之記憶卡時之再生對話時各部之動作的流程圖。

第20圖係用以說明實施例2之二個記憶卡間之移動動作的第一流程圖。

第21圖係用以說明實施例2之二個記憶卡間之移動動作的第二流程圖。

第22圖係用以說明實施例2之二個記憶卡間之移動動作的第三流程圖。

第23圖係說明實施例3之資料分配送信系統中所使用之通信用資料、資訊等之特性的圖。

五、發明說明（ 6 ）

第 24 圖係顯示實施例 3 之授權伺服器 11 之構成的圖。

第 25 圖係顯示行動電話機 103 之構成的概略方塊圖。

第 26 圖係用以說明實施例 3 之資料分配送信系統中之內容購入時所產生之分配送信動作的第一流程圖。

第 27 圖係用以說明實施例 3 之資料分配送信系統中之內容購入時所產生之分配送信動作的第二流程圖。

第 28 圖係用以說明實施例 3 之資料分配送信系統中之內容購入時所產生之分配送信動作的第三流程圖。

第 29 圖係用以說明使用實施例 3 之記憶卡時之再生對話時各部之動作的流程圖。

第 30 圖係用以說明實施例 3 之二個記憶卡間之移動動作的第一流程圖。

第 31 圖係用以說明實施例 3 之二個記憶卡間之移動動作的第二流程圖。

第 32 圖係用以說明實施例 3 之二個記憶卡間之移動動作的第三流程圖。

實施發明之最佳形態

以下，參照圖式說明本發明的實施例。

[實施例 1]

第 1 圖係用以概略說明本發明之資料分配送信系統之整體構成的概念圖。

另外，以下雖係舉透過行動電話網將音樂資料分配送信至各使用者的資料分配送信系統之構成為例而加以說

五、發明說明（ 7 ）

明，但是在以下之說明即可明白，本發明並非被限定於該種情況，亦可適用於透過其他的資訊通信網，發送其他的內容資料，例如圖像資料、影像資料、教材資料、朗讀(聲音)資料、遊戲程式等的內容之情況。

參照第1圖，用以管理有著作權之音樂資訊的授權伺服器10，係依預定之密碼方式將音樂資料(以下亦稱為內容資料)予以密碼化之後，對作為發送資料之分配送信載體(carrier)20的行動電話公司提供該種的密碼化內容資料。另一方面，認證伺服器12，係進行要求內容資料之分配送信並進行存取的使用者的行動電話機或記憶片是否為正規機器的認證。

分配送信載體20，係透過自己的行動電話網，而將來自各使用者之分配送信要求(request)轉送至授權伺服器10。授權伺服器10，係當有分配送信要求時，就會透過認證伺服器12確認使用者之行動電話機及記憶卡為正規機器，且在進一步將被要求之內容資料予以密碼化之後透過分配送信載體20之行動電話網，對各使用者之行動電話機發送內容資料。

第1圖中，例如在使用者1之行動電話機100上，形成裝設有可裝卸自如的記憶卡110之構成。記憶卡110，係接受由行動電話機100所接收的密碼化內容資料，並就上述分配送信時所進行的密碼化加以解碼之後，提供至行動電話機100中的音樂再生部(未圖示)。

更且，例如使用者1，可透過連接行動電話機100之

五、發明說明（ 8 ）

耳機 130 等「再生」上述之內容資料，而聽取音樂。

以下，係合併該種的授權伺服器 10、認證伺服器 12 與分配送信載體(行動電話公司)20，統稱為分配送信伺服器 30。

又，將該種的分配送信伺服器 30 對各行動電話機等所進行之傳輸內容資料的處理稱為「分配送信」。

藉由形成該種構成，首先，形成未購入正規之行動電話機及正規之記憶卡的使用者，很難接受及再生來自分配送信伺服器 30 之分配送信資料的構成。

而且，在分配送信載體 20 中，若分配送信載體 20 藉由每次發送例如 1 首曲子份之內容資料時就預先計數該次數，將使用者每次接收內容資料時所需的著作權費當作行動電話機之通話費加以徵收，如此著作權人即可輕易確保著作權費。

而且，該種的內容資料之分配送信，由於可透過所謂行動電話網的封閉式系統進行，所以與網際網路等之開放式系統相較，則比較具有容易採取著作權保護對策之優點。

此時，例如具有記憶卡 112 之使用者 2 利用自己的行動電話機 102，即可直接從分配送信伺服器 30 接受內容資料之分配送信。然而，當使用者 2 直接從分配送信伺服器 30 接收具有相當龐大之資訊量的內容資料等時，有時為了接收該資料而需要花費比較長的時間。在此種情況，若可從已接收該內容資料之分配送信的使用者 1 事先複製該內

五、發明說明（9）

容資料的話，則可提高對使用者的便利性。

然而，從著作權人之權利保護的觀點來看，在系統構成上係不允許內容資料被放任自由複製的。

如第1圖所示，將使用者1所接收的內容資料之內容資料本身予以複製，而將為了令使用者1所持有之該內容資料能再生所需要的再生資訊(再生所需要的權利)對使用者2移動之動作稱為音樂資料之「移動」。在此時，透過行動電話機100及102，即使在記憶卡110與112之間被密碼化的內容資料及再生所需要的資訊(再生資訊)移動。在此，所謂「再生資訊」，係如後面說明所示，具有可解碼按照預定之密碼化方式而被密碼化之內容資料的授權鑰(lisence key)、與作為與著作權保護相關之資訊的授權ID或關於存取再生的限制資訊等之授權資訊。

相對於「移動」，將只進行內容資料本身之複製的動作稱為「複製」。由於複製中未附帶再生資訊，所以使用者2無法再生該內容資料。在此雖未說明，但是前述使用者2利用只包含授權鑰之再生資訊之新的接收資料，即可再生該內容資料。

藉由該種構成，即可就一旦從分配送信伺服器30接收到的內容資料在接收者側進行彈性利用。

行動電話機100及102為PHS(個人手機)時，由於可進行所謂收發機(transceiver)模式之通話，所以利用該種機能，即可在使用者1與使用者2之間進行資訊之移動。

在第1圖所示之構成中，為了可在使用者側再生經密

五、發明說明（10）

碼化而分配送信的內容資料，而在系統上所需要者，係為實現：第一、用以發送通信中之密碼鑰的方式，第二、將內容資料予以密碼化的方式，以及第三、用以防止如此所分配送信之內容資料之擅自複製之資料保護的構成。

在本發明之實施例中，將說明特別是在產生分配送信及再生之各對話時，可充實對該等內容資料之移動目的地的認證及檢查機能，同時可縮短內容再生電路(例如，行動電話機)中之內容資料再生時間的構成。

[系統之鑰匙及資料之構成]

第2圖係說明在第1圖所示之資料分配送信系統中所使用之通信用之關於密碼的鑰匙(key)及分配送信之資料等的特性圖。(本文中所謂之鑰或鑰匙係指資訊處理上的一種碼)。

首先，由分配送信伺服器所分配送信的資料Data，係為音樂資料等的內容資料。內容資料Data，係如後面所說明般，係以至少施予可利用授權鑰Kc予以解碼之密碼化之密碼化內容資料{Data}Kc的形式，由分配送信伺服器30對使用者發布。

另外，以下有關{Y}X之表記，係顯示將資料Y變換成可利用鑰匙X解碼之密碼。

更且，可從分配送信伺服器30，發布內容資料、及關於內容資料或關於對伺服器之存取之作為普通文字資料的附加資訊Data-inf。亦即，在附加資訊Data-inf上，包含有用以特定內容資料之曲名等內容資料的資訊、或分配送

五、發明說明（11）

信伺服器30用以特定係為哪一個伺服器的資訊等。

其次，關於內容資料之密碼化或解碼•再生處理、或作為內容再生電路之行動電話機或作為記錄裝置之記憶卡之認證的鑰匙，有如下幾種。

亦即，如上所述，分別設有用以將內容資料予以密碼化及解碼的授權鑰Kc；用以進行內容再生電路(行動電話機100)認證的公開密碼鑰KPp(n)；以及用以進行記憶卡之認證的公開密碼鑰KPmc(m)。

經公開密碼鑰KPp(n)及KPmc(m)密碼化的資料，係可分別利用內容再生電路(行動電話機100)之固有的秘密解碼鑰Kp(n)及記憶卡固有的秘密解碼鑰Kmc(m)予以解碼。該等固有的秘密解碼鑰，係依行動電話機之種類及記憶卡之種類而有不同的內容。在此，行動電話機或記憶卡之種類，係根據製造該等之廠商的種類、或製造時期(製造批號)之差異等而規定，自然數n係表示用以區別各記憶卡及內容再生電路(行動電話機)之種類的號碼。另外，將共有公開密碼鑰KPmc(m)及KPp(n)的單位稱為等級(class)。

更且，與內容再生電路共通之秘密鑰，係存在有主要為授權鑰Kc或用在對於後面說明之內容再生電路之限制資訊等之取得的秘密鑰Kcom、及在分配送信系統整體中共通運用的認證鑰KPma。秘密鑰Kcom，由於係共通鑰方式中之解碼鑰，所以在分配送信伺服器中，該秘密鑰Kcom係保持作為密碼鑰。

又，秘密鑰Kcom，並不限定於共通鑰方式中之解碼

五、發明說明（12）

鑰，即使作為公開鑰方式中之秘密鑰 Kcom 亦可有同樣構成。此時，分配送信伺服器中之密碼鑰以保有與解碼鑰非對稱之公開密碼鑰 Kpcom 之方式構成即可。

另外，在上述之每一記憶卡及內容再生電路上所設定的公開密碼鑰 KPmc(m)及 KPp(n)，係可以認證資料 {KPmc(n)}KPma 及{KPp(n)}KPma 之形式，於輸出時分別記錄在記憶卡及行動電話機中。另外，認證資料係在利用作為認證鑰之認證鑰 KPma 予以解碼時，可從該解碼結果中確認認證資料之正當性的鑰匙，換言之，係用於承認公開密碼鑰的鑰匙。另外，用以製作認證資料之密碼，係利用與認證鑰成對的非對稱之秘密鑰來進行。

更且，用以控制構成系統之機器，即作為內容再生電路之行動電話機 100 或記憶卡 110 之動作的資訊，係存在有：利用者在購入授權鑰等時，用以指定其購入條件之從行動電話機 100 向分配送信伺服器 30 發送的購入條件資訊 AC；按照購入條件資訊 AC，從分配送信伺服器 30 向記憶卡 110 發送，表示對記憶卡 100 之存取次數予以限制等的存取限制資訊 AC1；以及從分配送信伺服器 30 向行動電話機 100 發送，表示內容再生電路之再生條件之限制的內容再生電路限制資訊 AC2。所謂內容再生電路之再生條件，係指例如在分配送信廉價或免費之樣品以作為新曲之宣傳促銷(promotion)時，只有各內容資料之開端的預定時間允許再生等的條件之意。

用以管理記憶卡 100 內之資料處理的鑰匙，係存在

五、發明說明（13）

有：在每一個如記憶卡之媒體上之公開密碼鑰 KPm(i)(i：自然數)；以及可將由公開密碼鑰 KPm(i)所密碼化的資料予以解碼之每一記憶卡上所固有的秘密解碼鑰 Km(i)。在此，自然數 i，係表示用以區別各記憶卡的號碼。

更且，在如第 1 圖所示之資料分配送信系統中，作為資料通信時所使用的鑰匙(key)等有以下幾種。

亦即，記憶卡外與記憶卡間之資料授受中用以保密的密碼鑰，係可採用於每次進行再生資訊之分配送信、再生及移動時在分配送信伺服器 30、行動電話機 100 或 102、記憶卡 110 或 112 中所生成的共通鑰 Ks1~Ks4。

在此，共通鑰 Ks1~Ks4，係在每次進行行動電話機或記憶卡間之作為通信單位或作為存取單位之「對話」時所產生的固有的共通鑰，以下亦將該等共通鑰 Ks1~Ks4 稱為「對話鑰」。

該等的對話鑰 Ks1~Ks4，藉由在每一通信對話中具有固有的值，即可依分配送信伺服器、行動電話機及記憶卡加以管理。

具體而言，對話鑰 Ks1，係分配送信伺服器內之授權伺服器在每次進行分配送信對話時產生者。對話鑰 Ks2，係記憶卡在每次進行分配送信對話及移動(接收側)對話時產生者；而對話鑰 Ks3，係同樣在記憶卡中每次進行再生對話及移動(發送側)對話時產生者。對話鑰 Ks4，係在行動電話機中每次進行再生對話時產生者。在各對話中，藉由接收發送該等對話鑰，接收其他機器所生成的對話鑰，

五、發明說明（14）

並依該對話鑰執行密碼化之後進行授權鑰等的發送，即可提高對話中的保密強度。

更且，在分配送信伺服器與行動電話機之間所授受的資料，係有供系統識別內容資料之內容ID，或用以特定授權之發行係於何時對誰進行之作為管理碼的授權ID，或在每一分配送信對話中生成，作為用以特定各分配送信對話之碼的授權ID等。

[授權伺服器10之構成]

第3圖係顯示第1圖所示之授權伺服器10之構成的概略方塊圖。

授權伺服器10，係包含有：用以保持按照預定之方式而將音樂資料(內容資料)予以密碼化的資料、或授權ID等分配送信資料的資訊資料庫304；用以保持每一使用者開始存取內容資料後之收費資訊的收費資料庫302；透過資料匯流排BS1接受來自資訊資料庫304及收費資料庫302之資料，以進行預定之處理的資料處理部310；以及透過通信網，在分配送信載體20與資料處理部310之間進行資料授受的通信裝置350。

資料處理部310，係包含有：分配送信控制部315，按照資料匯流排BS1上之資料，控制資料處理部310之動作；對話鑰產生部316，由分配送信控制部315所控制，用以在進行分配送信對話時產生對話鑰Ks1；解碼處理部312，透過通信裝置350及資料匯流排BS1接受由記憶卡及行動電話機送來，且藉由解碼而被密碼化成可了解其正

五、發明說明（15）

當性之認證資料{KPmc(n)}KPma及{KPp(n)}KPma，而進行對認證鑰Kpma的解碼處理；密碼化處理部318，使用解碼處理部312所得的公開密碼鑰KPmc(n)使對話鑰產生部316所生成的對話鑰Ks1密碼化，再將之輸出至資料匯流排BS1；以及解碼處理部320，在各使用者中利用資料匯流排BS1接受依對話鑰Ks1而被密碼化之後所發送的資料，以進行解碼處理。

資料處理部310，更包含有：用以將再生電路共通之秘密鑰Kcom保持作為密碼鑰的Kcom保持部322；密碼化處理部324，利用再生電路共通之密碼鑰KPcom將分配送信控制部315所提供的授權鑰Kc及再生電路控制資訊AC2予以密碼化；密碼化處理部326，利用解碼處理部320所得之記憶卡固有的公開密碼鑰KPm(i)將密碼化處理部324所輸出的資料予以密碼化；以及密碼化處理部328，利用解碼處理部320所提供的對話鑰Ks2進一步將密碼化處理部326之輸出予以密碼化然後輸出至資料匯流排BS1。

另外，在授權伺服器10中，雖已說明利用共通鑰方式中之密碼鑰Kcom作為密碼鑰的構成，但是在公開鑰方式中，行動電話機側具備有秘密解碼鑰Kcom時，係將與秘密解碼鑰Kcom成非對稱且可由秘密解碼鑰Kcom解碼的公開密碼鑰Kpcom保持於Kcom保持部322中。

[行動電話機100之構成]

第4圖係用以說明第1圖所示之行動電話機100之構成的概略方塊圖。

五、發明說明（16）

在行動電話機100中，表示等級的自然數n，係設為n=1。

行動電話機100，係包含有：用以接收經由行動電話網而無線傳輸之信號的天線1102；接收來自天線1102之信號並將之轉換成基頻信號，或調變來自行動電話機之資料並將之提供至天線1102的收發部1104；用以進行行動電話機100之各部資料授受的資料匯流排BS2；以及透過資料匯流排BS2控制行動電話機100之動作的控制器1106。

行動電話機100，更包含有：用以將外部之指示提供至行動電話機100的觸鍵(touch key)部1108；將控制器1106等所輸出的資訊提供至使用者以作為視覺資訊的顯示器1110；在通常的通話動作中，根據透過資料匯流排BS2而提供的接收資料再生聲音的聲音再生部1112；用以進行與外部間之資料授受的連接器1120；以及用以將來自連接器1120之資料轉換成可提供至資料庫BS2之信號，或將來自資料匯流排BS2之資料轉換成可提供至連接器1120之信號的外部介面部1122。

行動電話機100，更包含有：可裝拆自如的記憶卡110，其係用以記憶來自分配送信伺服器30之內容資料(音樂資料)及用於解碼化處理；記憶體介面1200，用以控制記憶卡110與資料匯流排BS2間之資料授受；以及認證資料保持部1500，用以保持可利用認證鑰KPma將每一行動電話機之等級中設定的公開密碼鑰KPp(1)密碼化成可解

五、發明說明（17）

碼狀態的資料。

行動電話機100，更包含有：Kp保持部1502，用以保持作為行動電話機(內容再生電路)固有的秘密解碼鑰之Kp(n)(n=1)；解碼處理部1504，依秘密解碼鑰Kp(1)而解碼接收自資料匯流排BS2的資料以得到記憶卡所產生之對話鑰Ks3；對話鑰產生部1508，在進行使記憶卡110中所儲存之內容資料再生的再生對話時，在與記憶卡110之間利用亂數等產生將資料匯流排BS2上所進行的資料予以密碼化的對話鑰Ks4；密碼化處理部1506，利用解碼處理部1504所得的對話鑰Ks3將所生成的對話鑰Ks4予以密碼化並輸出至資料匯流排BS2；以及解碼處理部1510，利用對話鑰Ks4將資料匯流排BS2上之資料予以解碼，並輸出{Kc//AC2}Kcom。

行動電話機100，更包含有：用以保持共通設定於內容再生電路內之秘密鑰Kcom的Kcom保持部1512；解碼處理部1514，利用秘密鑰Kcom將解碼處理部1510所輸出之{Kc//AC2}Kcom予以解碼而輸出授權鑰Kc及再生電路控制資訊AC2；解碼處理部1516，接收來自資料匯流排BS2之密碼化內容資料{Data}Kc，並利用從解碼處理部1514取得之授權鑰Kc使之解碼以輸出內容資料；接受解碼處理部1516之輸出以再生內容資料的音樂再生部1518；接受音樂再生部1518與音樂再生部1112之輸出，且按照動作模式而選擇性的輸出之切換部1525；以及接受切換部1525之輸出，而與耳機130連接的連接端子1530。

五、發明說明（18）

在此，由解碼處理部 1514 所輸出的再生電路控制資訊 AC2，係透過資料匯流排 BS2 提供至控制器 1106。

另外，在第 4 圖中，為了簡化說明，用以構成行動電話機之方塊中只記載關於本發明之音樂資料之分配送信及再生的方塊，而關於行動電話機本來具備的通話機能之方塊則省略一部分。

[記憶卡 110 之構成]

第 5 圖係說明第 4 圖所示之記憶卡 110 之構成的概略方塊圖。

如已說明般，公開密碼鑰 KPm(i)及與之對應的秘密解碼鑰 Km(i)，雖然在每一記憶卡中係為固有的值，但是在記憶卡 100 中，該自然數係設為 i=1。又，記憶卡之種類(等級)中固有的公開密碼鑰及秘密解碼鑰，雖設有 KPmc(n)及 Kmc(n)，但是在記憶卡 100 中，自然數 n 係以 n=1 來表示。

記憶卡 110，係包含有：用以保持{KPmc(1)}KPma 以作為認證資料的認證資料保持部 1400；用以保持針對記憶卡之每一種類而設定之作為固有的解碼鑰之 Kmc(1)的 Kmc 保持部 1402；用以保持每一記憶卡所固有的秘密解碼鑰 Km(1)的 Km(1)保持部 1421；以及用以保持可將依秘密解碼鑰 Km(1)而被密碼化的資料予以解碼之公開密碼鑰 KPm(1)的 KPm(1)保持部 1416。在此，認證資料保持部 1400，係將針對記憶卡之每一種類(等級)而設定的公開密碼鑰 KPmc(1)密碼化成可利用認證鑰 Kpma 予以解碼之狀

五、發明說明（19）

態並加以保持。

記憶卡 110，更包含有：在與記憶體介面 1200 之間透過端子 1202 授受信號的資料匯流排 BS3；以及解碼處理部 1404，從記憶體介面 1200 提供至資料匯流排 BS3 的資料中，接收來自 Kmc(1)保持部 1402 之記憶卡之每一種類所固有的秘密解碼鑰 Kmc(1)且將分配送信伺服器 30 在分配送信對話中所生成的對話鑰 Ks1 或其他的記憶卡在移動對話中所生成的對話鑰 Ks3 輸出至接點 Pa；解碼處理部 1408，從 KPma 保持部 1414 接收認證鑰 KPma，且以認證鑰 Kpma 進行對來自資料匯流排 BS3 之資料的解碼處理，然後將解碼結果透過資料匯流排 BS4 輸出至控制器 1420 與密碼化處理部 1410；以及密碼化處理部 1406，利用經由切換開關 1442 而選擇性提供的鑰匙，將經由切換開關 1444 而選擇性提供的資料予以密碼化並輸出至資料匯流排 BS3。

記憶卡 110，更包含有：在分配送信、再生及複製之各對話中產生對話鑰 Ks2 或 Ks3 的對話鑰產生部 1418；密碼化處理部 1410，利用透過解碼處理部 1408 而得到的公開密碼鑰 KPp(n)或 KPmc(n)將對話鑰產生部 1418 所輸出的對話鑰 Ks3 予以密碼化並送出至資料匯流排 BS3；以及解碼處理部 1412，接受來自 BS3 之依對話鑰 Ks2 或 Ks3 而被密碼化的資料而後利用得自對話鑰產生部 1418 之對話鑰 Ks2 或 Ks3 予以解碼，並將解碼結果送出至資料匯流排 BS4。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

五、發明說明（20）

記憶卡 110，更包含有：密碼化處理部 1424，在移動(移動端)對話中利用其他的記憶卡公開密碼鑰 KPm(i)(i≠1)將資料匯流排 BS4 上的資料予以密碼化；解碼處理部 1422，利用與公開密碼鑰 KPm(1)成對的記憶卡 110 固有的秘密解碼鑰 Km(1)將資料匯流排 BS4 上的資料予以解碼；以及記憶體 1415，用以儲存接收自資料匯流排 BS4 之由公開密碼鑰 KPm(1)所密碼化之再生資訊(授權鑰 Kc、內容 ID、授權 ID、存取限制資訊 AC1、再生電路控制資訊 AC2)，及儲存來自資料匯流排 BS3 之密碼化內容資料{Data}Kc 及附加資訊 Data-inf。

記憶卡 110，更包含有：授權資訊保持部 1440，用以保持藉由解碼處理部 1422 而得到的授權 ID、內容 ID 及存取限制資訊 AC1；以及控制器 1420，透過資料匯流排 BS3 進行與外部間的資料授受，並接受與資料匯流排 BS4 之間的再生資訊等，以控制記憶卡 110 之動作。

另外，在第 5 圖中，以實線圍住的區域 TRM，係在記憶卡 110 內，組入當進行來自外部之不當的開封處理等時，會因內部資料之抹除或內部電路之破壞，而不能對第三者讀出存在於該區域內之電路內之資料等的模組 TRM。此種模組，一般而言，係為抗拆封模組(Tamper Resistant Module)。

當然，亦可為包含記憶體 1415，且組入模組 TRM 內的構成。然而，藉由形成如第 5 圖所示的構成，則由於保持於記憶體 1415 中之資料，皆為被密碼化的資料，所以第

五、發明說明（21）

三者只有在該記憶體1415中之資料，並無法從內容資料中再生音樂，且由於沒有必要在高價之抗拆封模組內設置記憶體1415，所以有可減低製造成本的優點。

[再生動作]

(再生初始化對話)

其次，說明在行動電話機100內，用以從保持於記憶卡110內的密碼化內容資料再生音樂，並輸出至外部的再生動作(以下，亦稱為再生對話)。

第6圖係用以說明進行行動電話機100與記憶卡110之相互認證處理之一部分以作為初始化處理(亦稱為再生初始化對話)之再生初始化對話各部之動作的流程圖。

如以下說明，i)在行動電話機100上裝設有記憶卡110之狀態下，當投入行動電話機100之電源時，或ii)在對行動電話機100投入電源的狀態下，將記憶卡110插入行動電話機100時，或iii)在分配送信對話等或移動對話等時生成有新的對話鑰之情況下，一次進行再生初始化對話之處理，且藉由使行動電話機100與記憶卡110之相互認證處理之一部分，在複數個再生處理中共有化，即可迅速進行各個的再生動作。

參照第6圖，在上述之定時點，利用行動電話機100之控制器1106的控制，當再生初始化對話開始時(步驟S200)，行動電話機100，會從認證資料保持部1500，將可以認證鑰KPma予以解碼的認證資料{KPp(1)}KPma輸出至資料匯流排BS2(步驟S202)。

五、發明說明（22）

認證資料{KPp(1)}KPma，可透過資料匯流排 BS2 及記憶體介面 1200 而傳送至記憶卡 110。

在記憶卡 110 中，透過端子 1202 而傳輸至資料匯流排 BS3 的認證資料{KPp(1)}KPma，係被取入解碼處理部 1408。解碼處理部 1408，係從 KPma 保持部 1414 接受認證鑰 KPma，以進行資料匯流排 BS3 之資料的解碼處理。當該經由 KPma 而被密碼化的公開密碼鑰 KPp(1)正式被登錄，且施予正式的密碼化時，亦即，可利用認證鑰 KPma 而解碼化，且可辨識解碼時所產生的附屬資料時，會受理已解碼的 KPp(1)。另一方面，在無法解碼時，或是無法辨識在解碼處理中所產生之附屬資料時，就不受理所得的資料(步驟 S243)。

控制器 1420，係在可利用解碼處理部 1408 而受理行動電話機 100 之內容再生電路所固有的公開密碼鑰 KPp(1)時，會判斷所發送而來的公開密碼鑰 KPp(1)，是否為該資料分配送信系統所承認之賦予內容再生電路的公開密碼鑰，並前進至下一個步驟 S210(步驟 S206)。另一方面，在未被受理時，就判斷為來自非承認之機器的不正當存取，並結束處理(步驟 S240)。

在公開密碼鑰 KPp(1)被受理時，控制器 1420，會透過資料匯流排 BS4 對對話鑰產生部 1418，下達生成再生對話之對話鑰 Ks3 的指示。經由對話鑰產生部 1418 而生成的對話鑰 Ks3，係送至密碼化處理部 1410。密碼化處理部 1410，係依經由解碼處理部 1408 而得到的行動電話機 100

五、發明說明（23）

之公開密碼鑰 KPp(1)將對話鑰 Ks3 予以密碼化，且將密碼化資料{Ks3}Kp(1)輸出至資料匯流排 BS3(步驟 S210)。

行動電話機 100，係透過端子 1202 及記憶體介面 1200，而接受資料匯流排 BS4 上之密碼化資料{Ks3}Kp(1)。密碼化資料{Ks3}Kp(1)，可由解碼處理部 1504 予以解碼，並受理在記憶卡 110 所生成的對話鑰 Ks3(步驟 S212)，而結束再生初始化對話(步驟 S213)。

如此，記憶卡 110 具有再生時用以輸出資料之作為輸出目的地的內容再生電路(行動電話機 100)，且接受認證資料，而在確認行動電話機 100 為正規的再生機器後，為了要確保與已確認之對方的連接狀態，而送出一個對話固有的對話鑰 Ks3。接受對話鑰 Ks3 之行動電話機 100 及送出對話鑰 Ks3 之記憶卡 110，會在保持該對話鑰 Ks3，並謀求共有化之後具備於再生中。

(再生處理)

第 7 圖係用以說明接在第 6 圖之再生初始化對話之後之再生處理的流程圖。

當依來自行動電話機 100 之觸鍵部 1108 等的行動電話使用者 1 之指示，而生成再生要求(步驟 S201)時，行動電話機 100 之控制器 1106，會按照再生要求之生成，而透過資料匯流排 BS2 對對話鑰產生部 1508，下達產生再生對話中會在行動電話機 100 中生成的對話鑰 Ks4 之指示。所生成的對話鑰 Ks4 係送至密碼化處理部 1506，而以透過解碼處理部 1504 而得到的對話鑰 Ks3 加以密碼化的{Ks4}Ks3

五、發明說明（24）

會輸出至資料匯流排 BS2(步驟 S214)。

被密碼化的對話鑰{Ks4}Ks3，係透過記憶體介面 1200 而傳送至記憶卡 110。在記憶卡 110 中，係以解碼處理部 1412 將傳送至資料匯流排 BS3 之經過密碼化的對話鑰{Ks4}Ks3 予以解碼，並受理在行動電話機 100 中所生成的對話鑰 Ks4(步驟 S216)。

受理對話鑰 Ks4 之後，控制器 1420 會確認授權資訊保持部 1440 內所對應之具有內容 ID 的存取限制資訊 AC1(步驟 S218)。

在步驟 S218 中，藉由確認作為關於對記憶體之存取限制之資訊的存取限制資訊 AC1，而在立即成為不可再生的狀態時就結束再生對話(步驟 S240)，而在可再生但是再生次數有所限制時就更新存取限制資訊 AC1 之資料且在更新可再生次數之後前進至下一個步驟(步驟 S220)。另一方面，在不以存取限制資訊 AC1 限制再生次數時，就跳過步驟 S220，且存取限制資訊 AC1 無須更新而將處理移行至下一個步驟 S222。

又，在授權保持部 1440 內，在所要求的曲子之該內容 ID 不存在而判斷處於不可再生之狀態時，即結束再生對話(步驟 S240)。

在步驟 S218 中，當判斷在該再生對話中為可再生時，就可執行用以取得記錄於記憶體中的再生要求曲子之授權鑰 Kc 及再生電路控制資訊 AC2 之解碼處理。具體而言，解碼處理部 1454，係按照控制器 1420 之指示，利用記憶

五、發明說明（25）

卡 110 所固有的秘密解碼鑰 Km(1)，將從記憶體 1415 讀出並送至資料匯流排 BS4 之密碼化資料{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)予以解碼。藉此，即可取得可利用秘密解碼鑰 Kcom 予以解碼的密碼化資料{Kc//AC2}Kcom(步驟 S222)。

所得的密碼化資料{Kc//AC2}Kcom，係透過切換開關 1444 之接點 Pd 而送至密碼化處理部 1406。密碼化處理部 1406，係利用通過切換開關 1442 之接點 Pb 而從解碼處理部 1412 接受的對話鑰 Ks4，進一步將從資料匯流排 BS4 接受的密碼化資料{Kc//AC2}Kcom 予以密碼化，再將{{Kc//AC2}Kcom}Ks4 輸出至資料匯流排 BS3(步驟 S224)。

輸出至資料匯流排 BS3 之密碼化資料，係透過記憶體介面 1200 而送出至行動電話機 100。

行動電話機 100 中，係利用解碼處理部 1510 而進行對通過記憶體介面 1200 傳送至資料匯流排 BS2 之密碼化資料{{Kc//AC2}Kcom}Ks4 的解碼處理，並受理經密碼化之授權鑰 Kc 及再生電路控制資訊 AC2 的{Kc//AC2}Kcom (步驟 S226)。解碼處理部 1514，係利用接收自 Kcom 保持部 1512 之與再生電路共通之秘密解碼鑰 Kcom，將密碼化資料{Kc//AC2}Kcom 予以解碼，並受理授權鑰 Kc 及再生電路控制資訊 AC2(步驟 S228)。解碼處理部 1514，係將授權鑰 Kc 傳送至解碼處理部 1516，及將再生電路控制資訊 AC2 輸出至資料匯流排 BS2。

控制器 1106，係透過資料匯流排 BS2，受理再生電路

五、發明說明（26）

控制資訊 AC2 以進行可否再生之確認(步驟 S230)。

在步驟 S230 中，當依再生電路控制資訊 AC2 而判斷不可再生時，再生對話就會被結束(步驟 S240)。

另一方面，當可再生時，就從記憶卡 110 將記錄於記憶體內之所要求曲子的密碼化的內容資料{Data}Kc 輸出至資料匯流排 BS3，並經由記憶體介面 1200 傳輸至行動電話機 100(步驟 S232)。

在行動電話機 100 中，係利用解碼處理部 1516 中的授權鑰 Kc 將從記憶卡 210 輸出並傳輸至資料匯流排 BS2 的密碼化內容資料{Data}Kc 予以解碼，即可獲得被普通文字化的內容資料 Data(步驟 S234)。被解碼之普通文字內容資料 Data 係可藉由音樂再生部 1518 使之再生成音樂，並透過混合部 1525 及端子 1530 而向外部輸出被再生的音樂藉以結束處理(步驟 S240)。

如此，藉由從再生對話的處理中分離出再生初始化對話，並以複數個曲子來共有再生初始化對話，即可對使用者之再生要求迅速開始進行音樂之再生。

更且，由於係在每一再生中產生對話鑰 Ks4，並使用對話鑰 Ks4 對於從記憶卡 110 至內容再生電路(行動電話機 100)之授權鑰 Kc 的發送施予密碼化，所以即使接著同一曲子而再生亦形成同一資料無須通過記憶體介面 1200 的構成。故而，比起不分離出再生初始化對話，而依再生處理之情況，從再生初始化對話開始再生的情況，保密強度不會降低。

附件1

A7
B7

P0.7月6日修正補充

五、發明說明(27)

在再生對話方面，在來自再生初始化對話之一系列的動作中，取送行動電話機及記憶卡中分別生成的密碼鑰，並執行使用相互接受之密碼鑰的密碼化，以將該密碼化資料發送至對方。結果，即使在分配送信對話中之密碼化資料的各自收發中，亦可進行相互認證，且可確保資料分配送信系統之保密。

[分配送信動作]

其次，參照流程圖詳細說明本發明實施例之資料分配送信系統之各對話中的動作。

第8圖、第9圖及第10圖係用以說明實施例1之資料分配送信系統中之購入內容時所發生之分配送信動作(以下，亦稱為分配送信對話)的第一、第二及第三流程圖。

在第8圖至第10圖中，說明使用者1使用記憶卡110，透過行動電話機100自分配送信伺服器30接受內容資料之分配送信時的動作。

首先，由使用者1從其行動電話機100透過觸鍵部1108之按鍵的操作等，提出分配送信要求(步驟S100)。

在記憶卡100中，可按照該分配送信要求，而由認證資料保持部1400輸出認證資料{KPmc(1)}KPma(步驟S102)。

行動電話機100，係除了記憶卡110所受理的認證資料{KPmc(1)}KPma之外，亦對分配送信伺服器30發送行動電話機100本身之認證資料{KPp(1)}KPma、與內容ID、授權購入條件資料AC(步驟S104)。

煩請委員明示P0.年7月6日所提之修正本有無變更實質內容是否准予修正。

經濟部智慧財產局員工消費合作社印製

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 28 ）

在分配送信伺服器 30 中，係自行動電話機接收內容 ID、認證資料{KPmc(1)}KPma、認證資料{KPp(1)}KPma、授權購入條件資料 AC(步驟 S106)，且在解碼處理部 312 中利用認證鑰 KPma 執行解碼處理。當利用認證鑰 KPma 加以密碼化之公開密碼鑰 KPp(1)、KPmc(1)被正式登錄，且施予正式的密碼化時，就受理作為記憶卡 110 之公開密碼鑰之 KPmc(1)、作為行動電話機 100 之公開密碼鑰的 KPp(1)。另一方面，當未被正式登錄時，就不受理未被登錄之公開密碼鑰 KPp(1)、KPmc(1) (步驟 S108)。

分配送信控制部 315，係根據已受理之公開密碼鑰 KPmc(1)及 KPp(1)，對認證伺服器 12 進行詢問(步驟 S110)，若該等的公開密碼鑰在步驟 S108 受理，且為正式被登錄的鑰匙時，就判斷為有效，並移行至下一個處理(步驟 S112)，而當該等的公開密碼鑰未被受理，或即使有被受理但為未被登錄的鑰匙時，就判斷為無效，並結束處理(步驟 S170)。

在此，亦可形成在認證鑰 KPma 之解碼處理中，進行公開密碼鑰 KPp(1)或 KPmc(1)之正當性的認證時，附隨於公開密碼鑰 KPp(1)或 KPmc(1)之各個，而密碼化成認證書可由認證鑰 Kpma 所解碼並發送至分配送信伺服器 30 的構成。

又，亦可形成不對認證伺服器 12 詢問，認證資料{KPmc(1)}KPma 及{KPp(1)}KPma，由於係分別以認證鑰 KPma 予以解碼，而施予可判斷其正當性之密碼化，所以

五、發明說明（29）

授權伺服器 10 之分配送信控制部 315 可從認證鑰 KPma 之解碼結果中獨自進行認證的構成。

詢問的結果，當辨識為有效時，則分配送信控制部 315，就會生成如下用以指定分配送信對話之交易(transaction)ID (步驟 S112)。

接著，對話產生器 316，就會生成分配送信用的對話鑰 Ks1。對話鑰 Ks1，係利用藉由解碼處理部 312 而得之對應於記憶卡 110 的公開密碼鑰 KPmc(1)，以密碼化處理部 318 予以密碼化(步驟 S114)。

交易 ID 與被密碼化之對話鑰{Ks1}Kmc(1)，可經由資料匯流排 BS1 及通信裝置 350 而輸出至外部(步驟 S116)。

行動電話機 100，當接收交易 ID 及已被密碼化之對話鑰{Ks1}Kmc(1)時(步驟 S118)，在記憶卡 110 中，解碼處理部 1404，係可透過記憶體介面 1200，將提供至資料匯流排 BS3 之資料，藉由利用保持於保持部 1402 內之記憶卡 110 所固有的秘密解碼鑰 Kmc(1)進行解碼處理，而藉此解碼及抽出對話鑰 Ks1 (步驟 S120)。

控制器 1420，係當確認在分配送信伺服器 30 生成的對話鑰 Ks1 之受理時，對對話鑰產生部 1418，指示在記憶卡中進行分配送信對話時所生成的對話鑰 Ks2 之生成動作。在分配送信對話中，由於會在記憶卡 110 之對話鑰產生部 1418 上產生新的對話鑰，所以在再生初始化對話中所保持的對話鑰 Ks3 可改寫成對話鑰 Ks2。

密碼化處理部 1406，係利用通過切換開關 1442 之接

五、發明說明（30）

點 Pa 而由解碼處理部 1404 所提供的對話鑰 Ks1，以將藉由切換開關 1444 之接點 Pc 來切換切換開關 1446 之接點所提供的對話鑰 Ks2 及公開密碼鑰 KPm(1)予以密碼化，並將{Ks2//KPm(1)}Ks1 輸出至資料匯流排 BS3(步驟 S122)。

輸出至資料匯流排 BS3 之資料{Ks2//KPm(1)}Ks1，係從資料匯流排 BS3 經由端子 1202 及記憶體介面 1200 送至行動電話機 100，並自行動電話機 100 送至分配送信伺服器 30(步驟 S124)。

分配送信伺服器 30，係接收密碼化資料{Ks2//KPm(1)}Ks1，在解碼處理部 320 中執行利用對話鑰 Ks1 之解碼處理，以受理在記憶卡 110 生成之對話鑰 Ks2 及記憶卡 110 所固有的的公開密碼鑰 KPm(1)(步驟 S126)。

更且，分配送信控制部 315，係按照步驟 S106 中取得的內容 ID 及授權購入條件資料 AC，以生成授權 ID、存取限制資訊 AC1 及再生電路控制資訊 AC2(步驟 S130)。更且，利用資訊資料庫 304 取得用以解碼密碼化內容資料的授權鑰 Kc(步驟 S132)。

參照第 9 圖，分配送信控制部 315，係將已取得的授權鑰 Kc 及再生電路控制資訊 AC2 提供至密碼化處理部 324。密碼化處理部 324，係將從 Kcom 保持部 322 取得之內容再生電路共通的秘密解碼鑰 Kcm 當作密碼鑰，以將授權鑰 Kc 及再生電路控資訊 AC2 予以密碼化(步驟 S134)。

密碼化處理部 324 所輸出之密碼化資料{Kc//AC2}Kcom、分配送信控制部 315 所輸出之授權 ID、內容 ID 及

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

五、發明說明（31）

存取限制資訊 AC1，係由密碼化處理部 326，利用由解碼處理部 320 所得之記憶卡 110 所固有的公開密碼鑰 KPm(1)而加以密碼化(步驟 S136)。

密碼化處理部 328，係接受密碼化處理部 326 之輸出，且利用在記憶卡 110 中生成的對話鑰 Ks2 而進行密碼化。由密碼化處理部 328 所輸出的密碼化資料{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)}Ks2，係經由資料匯流排 BS1 及通信裝置 350 而送至行動電話機 100(步驟 S138)。

如此，存取在發送伺服器 30 及記憶卡 110 中生成的對話鑰，以執行使用互相接收的密碼鑰之密碼化，並藉由將該密碼化資料送至對方，則即使在各自之密碼化資料的收發中亦可進行事實上之相互認證，且可提高資料分配送信系統的保密性。

行動電話機 100，係接收已被傳送之密碼化資料{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)}Ks2 (步驟 S140)，而在記憶卡 110 中，透過記憶卡介面 1200，利用解碼化處理部 1412 將提供至資料匯流排 BS3 之接收資料予以解碼。亦即，解碼處理部 1412，使用由對話鑰產生部 1418 所提供的對話鑰 Ks2 將資料匯流排 BS3 之接收資料予以解碼並輸出至資料匯流排 BS4。

在此階段，在資料匯流排 BS4 上，輸出有可利用保持於 Km(1)保持部 1421 之秘密解碼鑰 Km(1)予以解碼的{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)。該

五、發明說明（32）

{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)，係記錄在記憶體 1415 中(步驟 S144)。

更且，在解碼處理部 1422 中，授權 ID、內容 ID 及存取限制資訊 AC1，係藉由執行記憶卡 112 中所固有之秘密解碼鑰 Km(1)的解碼處理，而經由資料匯流排 B4 而記錄在授權資訊保持部 1440 內(步驟 S148)。

更且，授權 ID、內容 ID 及存取限制資訊 AC1，係記錄在授權資訊保持裝置 1440 內(步驟 S150)。

在步驟 S150 之前的處理正常結束的階段，就會從行動電話機 100 對分配送信伺服器 30 提出內容資料之分配送信要求(步驟 S152)。

分配送信伺服器 30，係接受內容資料之分配送信要求，從資訊資料庫 304，取得密碼化內容資料{Data}Kc 及附加資料 Data-inf，並透過資料匯流排 BS1 及通信裝置 350 將該等的資料輸出(步驟 S154)。

行動電話機 100，係接收{Data}Kc//Data-inf，並受理密碼化內容資料{Data}Kc 及附加資訊 Data-inf(步驟 S156)。密碼化內容資料{Data}Kc 及附加資訊 Data-inf，係經由記憶體介面 1200 及端子 1202 而傳輸至記憶卡 110 之資料匯流排 BS3。在記憶卡 110 中，已接收之密碼化內容資料{Data}Kc 及附加資訊 Data-inf 係以原狀記錄在記憶體 1415 內(步驟 S158)。

更且，當從記憶卡 110 至分配送信伺服器 30，傳送分配送信受理之通知(步驟 S160)，且在分配送信伺服器 30

五、發明說明（33）

接收分配送信受理時(步驟 S162)，隨著將收費資料儲存至收費資料庫 302 內等，而可執行分配送信結束之處理(步驟 S164)，並結束整體的處理(步驟 S170)。

另一方面，行動電話機 100 開始進行再生處理之再生初始化對話。以後之處理，係進行與第 6 圖所示之再生初始化對話相同的處理。步驟 S172、S174、S176、S178、S180，分別相當於第 6 圖中之步驟 S202、S204、S206、S208、S210。

如此，分配送信對話中之行動電話機 100，當結束分配送信之內容資料的記錄時就會立即具備於再生中並執行再生初始化對話，藉此使用者就可在經由觸鍵部 1108 輸入再生以前結束再生初始化對話，而對使用者之再生要求，可在保持保密強度的基礎上，迅速再生內容資料並開始進行音樂之再生。

更且，由於只有在對分配送信要求確認行動電話機 100 之內容再生部及記憶卡 110 所發送來的公開密碼鑰 Kp(1)、Kmc(1)為有效之後，才分配發送內容資料，所以可對不正當的機器禁止分配送信動作，更且，由於係在進行使用依接收側之鑰匙而定的密碼化之後進行資料之收發，所以可確保分配送信中之保密強度。

[移動動作]

其次，說明在二個記憶卡間進行內容資料之移動的處理。

第 11 圖、第 12 圖及第 13 圖，係用以說明在二個記憶

五、發明說明（ 34 ）

卡 110 及 112 之間透過行動電話機 100 及 102 以進行內容資料及鑰匙等之移動處理的第一、第二及第三流程圖。

在第 10 至 12 圖中，使用以識別行動電話機 100 及記憶卡 110 之種類的自然數 n 皆為 1，使用以識別行動電話機 102 及記憶卡 112 之種類的自然數 n 皆為 2。並使用以識別記憶卡 110 及 112 之自然數 i 分別為 i=1 及 i=2。

第 10 至 12 圖中，行動電話機 100 及記憶卡 110 係為發送側，行動電話機 102 及記憶卡 112 係為接收側。又，行動電話機 102，亦裝設有與記憶卡 110 相同構成的記憶卡 112。以下，就記憶卡 112 之各構成部分，使用與記憶卡 110 所對應之部分相同的元件編號加以說明。

參照第 10 圖，首先，使用者從作為發送側之使用者 1 的行動電話機 100，藉由觸鍵部 1108 之按鍵的操作等，提出內容移動要求(步驟 S300)。

所生成的移動要求，係透過作為接收側之使用者 2 的行動電話機 120 而傳輸至記憶卡 112。在記憶卡 112 中，可從認證資料保持部 1500 中輸出經過對應於記憶卡 112 之公開密碼鑰 KPmc(2)解碼的認證資料{KPmc(2)}KPma (步驟 S302)。

記憶卡 112 之認證用資料{KPmc(2)}KPma，係從使用者 2 之行動電話機 120 發送，並經由使用者 1 之行動電話機 110 而由記憶卡 110 接收(步驟 S304)。

在記憶卡 110 中，利用解碼處理部 1408 執行解碼處理。當以 KPma 加以密碼化的公開密碼鑰 KPma(2)正式被

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（35）

登錄，且施予正式之密碼化時，亦即可利用認證鑰 KPma 而解碼，且可辨識解碼時所產生之附屬的資料時，就受理已解碼的 KPmc(2)以作為記憶卡 110 的公開密碼鑰。另一方面，在無法解碼時，或是無法辨識信號處理中所產生之附屬資料時，就不受理所得的資料(步驟 S306)。

控制器 1420，在利用解碼處理部 1408 受理記憶卡 112 之內容中所固有之公開密碼鑰 KPma(2)時，所發送來的公開密碼鑰 KPma(2)，經該資料分配送信系統判斷為賦與被承認之記憶卡的公開密碼鑰時，就前進至下一個步驟 S312(步驟 S308)。另一方面，在未被受理時，就判斷為來自非承認之機器的不正當存取，而結束處理(步驟 S360)。

當認證結果為有效時，控制器 1420，就對對話鑰產生部 1418，指示在移動對話時發送側所產生的對話鑰 Ks3 之輸出動作。在移動對話時之接收側，由於會在記憶卡 110 之對話鑰產生部 1418 上產生新的對話鑰，所以在再生初始化對話中所保持的對話鑰 Ks3 就可改寫成對話鑰 Ks2。對話鑰產生部 1418 所生成的對話鑰 Ks3，係傳輸至密碼化處理部 1410。密碼化處理部 1410，更進一步在步驟 S306 中接受解碼處理部 1408 所解碼的記憶卡 112 之秘密密碼鑰 KPmc(2)，並依 KPmc(2)而將對話鑰 Ks3 予以密碼化。藉此，被密碼化的對話鑰{Ks3}Kmc(2)可輸出至資料匯流排 BS3(步驟 S314)。

輸出至資料匯流排 BS3 的{Ks3}Kmc(2)，可經由記憶體介面 1200、行動電話機 100 及行動電話機 120 而傳輸至

五、發明說明（36）

記憶卡 112。

記憶卡 112，係接受由記憶卡 110 輸出之{Ks3}Kmc(2)，並由解碼處理部 1404 執行對應記憶卡 112 之秘密解碼鑰 Kmc(2)的解碼處理，以受理發送側之記憶卡 110 所生成的對話鑰 Ks3(步驟 S316)。

記憶卡 112 之控制器 1420，係按照對話鑰 Ks3 之受理，而對對話鑰產生部 1418，指示在移動對話中接收側產生的對話鑰 Ks2 之生成動作。在移動對話中之接收側，由於會在記憶卡 110 中之對話鑰產生部 1418 上產生新的對話鑰，所以在再生初始化對話中所保持的對話鑰 Ks3 就可改寫成對話鑰 Ks2。所生成的對話鑰 Ks2，係經由切換開關 1446 中之接點 Pf 及切換開關 1444 中之接點 Pc 而傳輸至密碼化處理部 1406。

密碼化處理部 1406，係從解碼處理部 1404 接受在步驟 S316 所得的對話鑰 Ks3，並利用對話鑰 Ks1 將經由切換開關 1444 之接點 Pc 與切換開關 1446 之接點 Pf 與 Pe 之切換而得的對話鑰 Ks2 與公開密碼鑰 KPm(2)予以密碼化，並將{Ks2//KPm(2)}Ks3 輸出至資料匯流排 BS3(步驟 S318)。

輸出至資料匯流排 BS3 之密碼化資料{Ks2//KPm(2)}Ks3，係經由行動電話機 102 及 100 傳輸至記憶卡 110 之資料匯流排 BS3。

在記憶卡 110 中，利用解碼處理部 1412 並使用對話鑰 Ks3 將傳輸至資料匯流排 BS3 的密碼化資料予以解碼，以

五、發明說明（37）

受理關於記憶卡 112 之對話鑰 Ks2 及公開密碼鑰 KPm(2)(步驟 S322)。

記憶卡 110 之控制器 1420，係按照對話鑰 Ks2 及公開密碼鑰 KPm(2)之受理，而執行授權資訊保持部 1440 內之存取限制資訊 AC1 的確認(步驟 S322)。當確認存取限制資訊 AC1 之結果為非經授權之移動時，就在該階段結束移動對話(步驟 S360)。

另一方面，當確認存取限制資訊 AC1 之結果為允許移動時，就將處理移行至下一個步驟 S322，而控制器 1420，會從授權資訊保持部 1440 中取得所對應之內容 ID 及授權 ID，並更新授權保持部 1440 內之存取限制資訊，及記錄以後之再生及移動的禁止(步驟 S324)。對應於此，在再生對話及移動對話中確認該存取限制資訊 AC1 之後進行處理，並禁止以後之再生及移動對話。

更且，控制器 1420，對記憶體 1415 指示對應於移動內容的對話鑰 Kc 及關於再生資訊的密碼化資料{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)之輸出動作。由記憶體 1415 所輸出的密碼化資料{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)，可利用解碼處理部 1422 使之解碼化，而可在資料匯流排 BS4 上獲得{Kc//AC2}Kcom(步驟 S326)。

在步驟 S324 中從授權資訊保持部取得的授權 ID、內容 ID 及存取限制資訊 AC1、及在步驟 S326 中取得的{Kc//AC2}Kcom，可從資料匯流排 BS4 取入密碼化處理部

五、發明說明（38）

1424 中而予以密碼化。密碼化處理部 1424，係依在步驟 S320 中由解碼處理部 1412 所得的記憶卡 112 固有之公開密碼鑰 KPm(2)，將該等的資料予以密碼化，以生成 {{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)(步驟 S328)。

輸出至資料匯流排 BS4 之密碼化資料{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)，係可通過切換開關 1444 中之接點 Pd 而傳輸至密碼化處理部 1406 中。密碼化處理部 1406，係透過切換開關 1442 之接點 Pb 而接受解碼處理部 1412 所得之記憶卡 112 的對話鑰 Ks2，並依對話鑰 Ks2 而將從接點 Pd 接受的資料予以密碼化。

密碼化處理部 1406，係將{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)}Ks2 輸出至資料匯流排 BS3(步驟 S330)。在步驟 S330 中輸出至資料匯流排 BS3 的密碼化資料，係透過行動電話機 100 及 102，而傳輸至作為移動對話之接收側的記憶卡 112 中。

在記憶卡 112 中，係利用解碼處理部 1412 中對話鑰產生部 1418 所生成的對話鑰 Ks2 而執行解碼，並受理{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)}Ks2(步驟 S332)。

所受理的{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)，係以經公開密碼鑰 KPma(2)加以密碼化的狀態記錄(步驟 S334)。

更且，在解碼處理部 1422 中，藉由執行記憶卡 112 中

五、發明說明（39）

所固有之秘密解碼鑰 Km(2)的解碼處理，即可受理授權 ID、內容 ID 及存取限制資訊 AC1(步驟 S336)。

所受理之授權 ID、內容 ID 及存取限制資訊 AC1，係經過資料匯流排 BS4 而記錄在授權資訊保持部 1440 內(步驟 S338)。

如此，藉由正常結束步驟 S338 之前的處理，即可響應移動授權鑰 Kc 之密碼化資料及分配送信資訊，而透過行動電話機 102 進一步進行內容資料之複製要求(步驟 S340)。

內容資料之複製要求係經由行動電話機 100 而傳送至記憶卡 110，並響應於此，而從記憶卡 110 中之記憶體 1415 輸出所對應的密碼化內容資料{Data}Kc 與附加資訊 Data-inf 至資料匯流排 BS3(步驟 S342)。輸出至資料匯流排 BS3 之該等的資料，係經由記憶體介面 1200、行動電話機 100 及行動電話機 102 而傳送至記憶卡 112，並記錄在記憶卡 112 中之記憶體 1415 內(步驟 S344)。

當結束密碼化內容資料{Data}Kc 及附加資訊 Data-inf 之記錄時，可透過行動電話機 102 傳送移動受理(步驟 S346)。

藉此，若在記憶卡 112 及所對應之行動電話機 102 中正常執行再生對話的話，則可利用行動電話機 102 根據記錄於記憶卡 112 內之內容資料而聽取音樂。

在發送側之行動電話機 100 中，接收由行動電話機 102 所發送的移動受理(步驟 S348)，並接受使用者從鍵輸入部

五、發明說明（ 40 ）

1108輸入的內容資料之抹除或保持之任一種的指示(步驟S350)。

因而，藉由從鍵輸入部1108指示內容資料之抹除，即可在記憶卡110內之記憶體1415中，抹除所對應之{Data}Kc及附加資訊Data-inf(步驟S354)。另一方面，在指示內容資料之保持時，步驟S354就可跳過，而移動處理可在該階段結束(步驟S356)。

在正常進行移動對話時之移動處理結束步驟S356之後，或是移動對話因認證等而中止時，程序就會從步驟S308及S322跳至下一個步驟S358。

另外，記錄於授權保持部1440內之對應的內容ID等的再生資訊，由於可在步驟S324中更新存取限制資訊AC1，並禁止再生對話及移動對話，所以會變成與抹除相同的狀態。對於記錄有在該狀態下的再生資訊之記憶體組(bank)，在接受對新的內容資料之再生資訊時的分配送信或移動時，允許在其上覆寫。在步驟S324中，即使全部抹除該記憶體組內之資料亦可獲得相同的效果。

更且，在將密碼化內容資料記錄在記憶體1415內的狀態下，若重新存取分配送信伺服器30，並只接受再生資訊之分配送信的話，則又可再生密碼化內容資料，並聽取音樂。只有再生資訊之分配送信處理雖未在流程中圖示，但是在分配送信對話之第9圖及第10圖中由於係為不進行關於密碼化內容資料之授受的步驟S152、S154、S156、S158之處理，所以不重覆說明。

五、發明說明（41）

行動電話機 100，係當在步驟 S356 結束移動處理時，就對記憶卡 110 輸出認證用的資料[KPp(1)]KPma(步驟 S358)。

記憶卡 110，係接受來自行動電話機 100 的資料[KPp(1)]KPma，而解碼處理部 1408 利用鑰匙 Kpma 進行解碼，藉以受理鑰匙 KPp(1)(步驟 S360)。

在記憶卡 110 中，係根據控制器 1420 所受理的鑰匙 KPp(1)而進行行動電話機 100 的認證(步驟 S362)。

行動電話機 100，在步驟 S356 中結束移動結束處理時，會在其與記憶卡 110 之間，開始再生初始化對話。以後，由於步驟 S358、S360、S362、S364、S366，分別相當於第 6 圖中之步驟 S202、S204、S206、S208、S210，所以不重覆說明。最後在行動電話機 100 之再生初始化對話結束時結束行動電話機 100 之處理(步驟 S390)。

另一方面，行動電話機 102，當在步驟 S346 中發送移動受理時，會在其與記憶卡 110 之間，開始再生初始化對話。以後，由於步驟 S348、S350、S352、S354、S356，分別相當於第 6 圖中之步驟 S202、S204、S206、S208、S210，所以不重覆說明。最後在行動電話機 102 之再生初始化對話結束時結束行動電話機 102 之處理(步驟 S390)。

如此，移動對話中之發送側的行動電話機 100 及接收側的行動電話機 102，當結束因移動所致之內容資料的授受時就會立即具備於再生中並執行再生初始化對話，藉此各自的使用者就可在透過各自的行動電話機之觸鍵部

五、發明說明（42）

1108指示再生以前結束再生初始化對話，而對使用者之再生要求，可在保持保密強度的基礎上，迅速再生內容資料並開始進行音樂之再生。

更且，由於發送側記憶卡110對於移動要求，只有在確認接收側之記憶卡112所發送來的公開密碼鑰Kmc(2)為有效的情形下，才移動授權鑰等的再生資訊，所以可禁止向不正當的記憶體的移動，更且，由於係在使用依接收側而定的鑰匙進行密碼化的情形下進行資料之收發，所以可確保移動中之保密強度。

[實施例2]

在實施例2之資料分配送信系統中，與實施例1之資料分配送信系統的構成不同，如以下說明般，其特徵點係在將以密碼鑰與解碼鑰為非對稱之公開密碼化方式中之公開鑰密碼鑰Km(1)予以密碼化之後所分配送信的密碼化授權鑰等的資料{{Kc//AC2}Kcom//授權ID//內容ID//AC1}Km(1)利用鑰匙Km(1)予以解碼後再利用本身為對稱型鑰匙之記憶卡固有的秘密共通鑰K(i)予以重新密碼化之後，儲存在記憶體1415內者。

亦即，實施例2之資料分配送信系統，不同點係具備記憶卡114以取代第5圖所說明之實施例1之資料分配送信系統所具有的記憶卡110。

第14圖係說明在實施例2之資料分配送信系統中所使用之通信用的資料、資訊等特性圖，係與實施例1之第2圖做對比的圖。但是，在第14圖中，與第2圖之情況比較，

五、發明說明（43）

如上述般，由於係只有在設有本身為對稱型鑰匙之記憶卡固有的秘密共通鑰 K(i)的構成上不同，所以不重覆其說明。

第 15 圖係顯示實施例 2 之記憶卡 114 之構成的方塊圖，且與實施例 1 做對比的圖。

參照第 15 圖，記憶卡 114 與第 5 圖所示之實施例 1 的記憶卡 110 相較，不同點在於更包含有：用以保持記憶卡固有的秘密共通鑰 K(1)的 K(1)保持部 1450；利用秘密共通鑰 K(1)將資料匯流排 BS4 上的資料予以密碼化的密碼化處理部 1452；以及利用秘密共通鑰 K(1)以將資料匯流排 BS4 上的資料予以解碼的解碼處理部 1454。

其他點，由於與實施例 1 之記憶卡 110 的構成相同，所以在同一部分上附記相同的符號而不重覆其說明。

第 16 圖、第 17 圖及第 18 圖係用以說明實施例 2 之資料分配送信系統中之內容購入時所產生的分配送信動作之第一、第二及第三流程圖，且與實施例 1 之第 8 圖、第 9 圖及第 10 圖做對比的圖。

在第 16 至 18 圖中，係說明使用者 1，藉由使用記憶卡 114，透過行動電話機 100 從分配送信伺服器 30 中接受內容資料之分配送信時的動作。

在此，與實施例 1 之記憶卡 110 之情況的分配送信處理不同點，係在於利用步驟 S144 之處理，在記憶卡 114 受理資料{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)之後，依控制器 1420 之指示，資料{{Kc//AC2}Kcom//授

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 44 ）

權 ID//內容 ID//AC1}Km(1)，會在解碼處理部 1422 中，依秘密解碼鑰 Km(1)而解碼，且可受理資料{Kc//AC2}Kcom、授權 ID、內容 ID 及存取限制資訊 AC1(步驟 S146')。更且，如此所受理的{Kc//AC2}Kcom、授權 ID、內容 ID 及 AC1，係以密碼化處理部 1452 利用記憶卡 114 固有的秘密共通鑰 K(1)加以密碼化，而將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}K(1)記錄在 TRM 區域外之記憶體 1415 內(步驟 S148')。

在以上之分配送信處理中，係在步驟 S146 中，以秘密解碼鑰 Km(1)將{Kc//AC2}Kcom、授權 ID、內容 ID 及 AC1 予以解碼之後，在步驟 S148'中，再以秘密共通鑰 K(1)加以密碼化之後儲存在記憶體 1415 內者，其理由如下。

就非對稱鍵之公開鑰方式的公開密碼鑰 KPm(1)與秘密解碼鑰 Km(1)之組合而言，解碼處理所需要的時間可能變大。

因此，依可高速解碼之共通鑰方式的記憶卡固有之秘密共通鑰 K(1)，重新將該等的資料予以密碼化，即可在對應於密碼化內容資料之內容資料的再生處理中，使作為再生處理所需要之資訊的授權鑰 Kc 及對再生限制資訊 AC1 之解碼處理高速化。

更且，藉由如此變更資料發送時之鑰匙、及儲存於記憶卡內時之鑰匙，亦可提高保密強度。

在此，如上述之公開鑰方式，有 RAS 密碼方式(Rivest-Shamir-Adleman cryptosystem)或橢圓曲線密碼化

五、發明說明（45）

方式，而共通鑰密碼方式，則有資料加密標準(DES，Data Encryption Standard)的密碼方式等。

另外，以上之說明中，雖係就利用全部密碼鑰與解碼鑰為對稱之共通鑰方式的秘密共通鑰K(1)，將根據密碼鑰與解碼鑰為非對稱之公開密碼化方式中的鑰匙KPm(1)/Km(1)之密碼化資料予以重新密碼化的構成加以說明，但是例如針對設於記憶卡110之TRM區域內之授權資訊保持部1440中所保持的授權ID、內容ID及存取限制資訊AC1，不進行重新密碼化，且不儲存在記憶體1415中，而針對資料{Kc//AC2}Kcom，則以秘密共通鑰K(1)重新密碼化之後儲存在記憶體1415內的構成。

其他點，由於與實施例1之分配送信動作相同，所以在同一處理上附記相同的符號並省略其說明。

第19圖係用以說明使用實施例2之記憶卡114時之再生對話時的各部之動作的流程圖。

在此，實施例2之記憶卡114，亦與實施例1之記憶卡110相同，為可進行再生初始對話之處理者。

與第10圖所示之實施例1之記憶卡110時的分配送信處理不同處，係在記憶卡114中，形成在第19圖之步驟S222'之處理中，解碼處理部1454會按照控制器1420之指示，利用K(1)保持部1451所保持的秘密鑰K(1)，將從記憶體1415讀出至資料匯流排BS4的密碼化資料{{Kc//AC2}Kcom//授權ID//內容ID//AC1}K(1)予以解碼的構成。

其他點，由於與實施例1之再生動作相同，所以在同

五、發明說明（46）

一處理上附記相同的符號並省略其說明。

[移動動作]

第20圖、第21圖及第22圖，係用以說明實施例2之移動動作的第一、第二及第三流程圖。

又，實施例2之記憶卡的移動動作，基本上亦與實施例1之移動動作相同。

相對於實施例1之記憶卡110與112之間的移動動作，實施例2之記憶卡114與116之間的移動動作所不同的步驟為步驟S326'、S334'及S336'。在步驟S326'中，控制器1420，係對記憶體1415指示對應於移動內容之對話鑰Kc及關於再生資訊之密碼化資料{{{Kc//AC2}Kcom//授權ID//內容ID//AC1}K(1)之輸出，由記憶體1415所輸出的密碼化資料{{{Kc//AC2}Kcom//授權ID//內容ID//AC1}K(1)，係可藉由解碼處理部1454而利用秘密共通鑰K(1)予以解碼化，且在資料匯流排BS4上獲得{Kc//AC2}Kcom。

在步驟S334'中，係在解碼處理部1422上利用記憶卡116固有的秘密解碼鑰Km(2)將在步驟S332中所受理的{{Kc//AC2}Kcom//授權ID//內容ID//AC1}Km(2)予以解碼，並將{Kc//AC2}Kcom、授權ID、內容ID及存取限制資訊AC1輸出至資料匯流排BS4。

在步驟S336'中，係將在步驟S334'中輸出至資料匯流排BS4的{Kc//AC2}Kcom、授權ID、內容ID及存取限制資訊AC1，再次利用秘密共通鑰K(2)以密碼處理部1452

五、發明說明（47）

加以密碼化之後經過資料匯流排 BS4 而記錄在記憶體 1415 上。

其他點，由於與實施例 1 之移動動作相同，所以在同一處理上附記相同的符號而不重覆其說明。

藉由如以上之構成，即可更加迅速開始再生，同時可強化對內容資料之保密。

另外，實施例 1 及 2 中的處理只有記憶卡內之處理不同，而記憶卡外部之資料的密碼化則相同。有關移動動作方面亦可以目前所說明之實施例 1 與 2 之任一種組合當作發送側與接受側之組合來進行移動。

故而，記憶卡 110 及 114，係具有互換性的記憶卡。

[實施例 3]

在實施例 3 之資料分配送信系統中，與實施例 1 之資料分配送信系統的構成不同，其特徵點在係在分配送信伺服器及行動電話機之內容再生電路中不使用內容再生電路共通之秘密鑰 Kcom 的密碼化及解碼處理。

亦即，實施例 3 之資料分配送信系統，不同點係在於具備有授權伺服器 11 以取代第 3 圖中所說明之實施例 1 之資料分配送信系統所具有的分配送信伺服器 30 內的授權伺服器 10。又，實施例 3 之資料分配送信系統中之行動電話機的構成，可採用行動電話機 103 之構成，以取代第 4 圖中所說明之行動電話機 100 的構成。

第 23 圖係用以說明在實施例 3 之資料分配送信系統中，所使用之通信用的資料、資訊等的特性圖，且係與實

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（48）

施例1之第2圖做對比的圖。但是，在第23圖，與第2圖之情況相較，由於只有形成省略秘密解碼鑰Kcom之構成不同所以不重覆其說明。

第24圖係顯示實施例3之資料分配送信系統之授權伺服器11之構成的概略方塊圖。

授權伺服器11，與授權伺服器10相較，不同點在於不具備再生電路共通之秘密解碼鑰Kcom保持部322、及將秘密鑰Kcom作為密碼鑰以進行密碼化的密碼化處理部324。亦即，在分配送信伺服器31中，分配送信控制部315所輸出的授權鑰Kc及再生電路控制資訊AC2，係直接傳送至密碼化處理部326。有關其他電路構成及動作由於與第3圖所示之授權伺服器10相同所以不重覆其說明。

以後，合併授權伺服器11、認證伺服器12及分配送信載體20而統稱為分配送信伺服器30。

第25圖係顯示實施例3之資料分配送信系統中所使用之行動電話機103之構成的概略方塊圖。

參照第25圖，行動電話機103，與實施例1之第4圖中所說明的行動電話機100之構成相較，不同點在於不具備有用以保持再生電路共通之秘密鑰Kcom的Kcom保持部1512與利用秘密鑰Kcom進行解碼處理之解碼處理部1514。

亦即，在行動電話機103中，對應於不在分配送信伺服器31中實施利用秘密鑰Kcom之密碼化處理，由於可藉由利用對話鑰Ks4進行解碼處理之解碼處理部1510直接

五、發明說明（ 49 ）

獲得授權鑰 Kc，所以形成直接將授權鑰 Kc 提供至解碼處理部 1510 的構成。有關其他的電路構成及動作由於與行動電話機 100 之情況相同所以不重覆說明。

又，有關在實施例 3 之資料分配送信系統中所使用的記憶卡，由於與第 5 圖所示之記憶卡 110 為相同的構成所以不重覆說明。

其次，以流程圖就省略了利用再生電路共通之秘密鑰 Kcom 之密碼化處理後之分配送信及再生之各對話中的動作差異加以說明。

第 26 圖、第 27 圖及第 28 圖，係用以說明實施例 3 之資料分配送信系統中之分配送信動作的第一、第二及第三流程圖。在第 26 至 28 圖中，係就與第 8 至 10 圖中之實施例 1 之資料分配送信系統中之分配送信動作的流程不同的部分加以說明。

參照第 26 至 28 圖，步驟 S132 之前的處理，係與第 9 圖所說明之流程圖相同。

如利用第 24 圖所作的說明，在步驟 S132 中獲得的授權鑰 Kc 及再生電路控制資訊 AC2，由於無須施予利用秘密鑰 Kcom 之密碼化即可以記憶體 110 固有之公開密碼鑰 KPm(1)加以密碼化，所以可省略步驟 S134。

以下，係接在步驟 S132 之後，執行步驟 S136a~S148a，以取代步驟 S136~S148。在步驟 S136a~S148a 之各個步驟中，不同點係以 Kc//AC2 之形式直接處理授權鑰 Kc 及再生電路控制資訊 AC2，以取代在步驟 S136~S148 中所處理

五、發明說明（50）

的{Kc//AC2}Kcom。有關其他的密碼化及解碼處理由於與第9圖中已說明者相同所以不重覆說明。

第29圖係用以說明實施例3之資料分配送信系統中之再生動作的流程圖。在實施例3中，再生初期對話，亦可進行與實施例1相同的處理。

參照第29圖，在實施例3之資料分配送信系統中之再生動作中，與第6圖所示之實施例1之資料分配送信系統中之再生動作相較，不同點在於執行步驟S222a~S226a，以取代步驟S222~S226。在步驟S222a~S226a之各個步驟中，不同點係以Kc//AC2之形式直接處理授權鑰Kc及再生電路控制資訊AC2，以取代在步驟S222~S226中所處理的{Kc//AC2}Kcom。有關其他的密碼化及解碼處理由於與第10圖中已說明者相同所以不重覆說明。更且，又，授權鑰Kc及再生電路控制資訊AC2，由於無須施予利用秘密解碼鑰Kcom之密碼化而可利用記憶卡110固有之公開密碼鑰Km(1)予以密碼化，所以可省略步驟S228。有關其他的步驟由於與第10圖相同所以不重覆說明。

第30圖、第31圖及第32圖，係用以說明實施例3之移動動作的第一、第二及第三流程圖。

在行動電話機103及具有與之同等構成的行動電話機105之間的移動動作中，授權鑰Kc及再生電路控制資訊AC2，除了不施予利用秘密鑰Kcom之密碼化之外，其餘與實施例1之動作相同。換句話說，步驟S326~336除了改為步驟S326a~336a之點外，皆與實施例1之動作相同，

五、發明說明（51）

所以不重覆其說明。

藉由如此的構成，即使形成不在內容再生電路(行動電話機)進行利用共通之秘密解碼化鑰Kcom之在授權伺服器11中的密碼化處理及在行動電話機中之解碼處理的構成，亦可構建享有與實施例1之資料分配送信系統相同效果的資料分配送信系統。

更且，同樣地，即使在實施例2之資料分配送信系統中，亦可形成不在分配送信伺服器及行動電話機中使用再生電路共通之秘密鑰Kcom之密碼化及解碼處理的構成。又，再生裝置，亦可非為行動電話機，且沒有要接受分配送信之必要性。

雖已詳細說明顯示本發明，但是此只為其例示用而已，並非為限定，可明確了解到本發明之精神及範圍只受到隨附之申請專利範圍所示者限定。

元件符號說明

1、2	使用者	10	授權伺服器
12	認證伺服器	20	分配送信載體
30	分配送信伺服器	100,102	行動電話機
110,112	記憶卡	130	耳機
302	收費資料庫	304	資訊資料庫
306	管理資料庫	310	資料處理部
312、320、1404、1408、1422、1504、1510、1514、1516	解碼處理部		
315	分配送信控制部	316、1418、1508	對話鑰產生部
318、324、326、328、1406、1410、1424、1506	密碼化處理部		

A7
B7

五、發明說明（52）

322、1512	Kcom 保持部	350	通信裝置
1102	天線	1104	收發部
1106	控制器	1108	觸鍵部
1110	顯示器	1112	聲音再生部
1120	連接器	1122	外部介面部
1200	記憶體介面	1400	認證資料保持部
1402	Kmc(1)保持部	1415	記憶體
1416	KPm(1)保持部	1420	控制部
1440	授權資訊保持部	1444	切換開關
1500	認證資料保持部	1502	Kp 保持部
1518	音樂再生部	1525	切換部
1530	連接端子		

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

A5
B5

四、中文發明摘要（發明之名稱：　　）

資料再生裝置

行動電話機(100)，係將經分配送信之密碼化內容資料及密碼化授權鑰儲存在記憶卡(110)內。行動電話機(100)與記憶卡(110)，係在電源投入時一起進行互相認證處理之一部分。由記憶卡(110)讀出之密碼化授權鑰(Kc)，就對話鑰(Ks4)而言可由第一解碼處理部(1510)加以解碼，另就系統共通鑰(Kcom)而言可由第二解碼處理部(1514)加以解碼並抽出。第三解碼處理部(1516)，係利用授權鑰(Kc)將從記憶卡(110)讀出之密碼化內容資料予以解碼，以再生內容資料(Data)。

英文發明摘要（發明之名稱：　　）

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

90 7 6 修正補充
年 月 日

第 89126047 號專利申請案

申請專利範圍修正本

(90 年 7 月 6 日)

1. 一種資料再生裝置，其係將密碼化內容資料解碼之後用以進行內容資料之再生者，具有：

資料儲存部(110)，保持用以解碼前述密碼化內容資料及前述密碼化內容資料之授權鑰，並以使前述授權鑰密碼化的狀態輸出，且可相對於前述資料再生裝置自由裝拆；

資料再生部，接受來自前述資料儲存部之輸出，用以再生前述密碼化內容資料；以及

第一控制部(1106)，用以控制前述資料儲存部與前述資料再生部間之資料的授受動作，

前述資料再生部，包含有：

第一解碼處理部(1510,1514,1516)，用以接受從前述資料儲存部讀出的前述授權鑰與前述密碼化內容資料，並利用前述授權鑰將前述密碼化內容資料予以解碼而抽出內容資料；以及

認證鑰保持部(1500)，利用公開認證鑰將認證資料予以密碼化及保持俾可對前述資料儲存部輸出，

前述資料儲存部，包含有：

第二解碼處理部(1408)，用以將利用前述公開認證鑰予以密碼化且由前述資料再生部提供的前述認證資料予以解碼及抽出；以及

第二控制電路(1420)，根據利用前述第二解碼處理部而抽出的前述認證資料進行認證處理，而

前述第一控制電路，係以在與複數個前述密碼化內容資料之再生動作共通的預定期間內進行前述認證處理的方式進行控制者。

2. 如申請專利範圍第1項之資料再生裝置，其中前述資料儲存部，係可相對於前述資料再生裝置自由裝拆的記憶卡。

3. 如申請專利範圍第1項之資料再生裝置，其中前述預定期間，係指在前述資料再生裝置為活動期間內，前述資料儲存部被裝設在前述資料再生部內之後的期間。

4. 如申請專利範圍第1項之資料再生裝置，其中前述預定期間，係指在前述資料儲存部裝設在前述資料再生裝置內之狀態下使前述再生裝置活動之後的期間。

5. 如申請專利範圍第1項之資料再生裝置，其中前述資料再生部，更包含有：

對話鑰產生部(1508)，用以生成每次對前述資料儲存部進行取得前述密碼化內容資料之存取時皆更新的對話鑰；以及

第一密碼化處理部(1506)，利用可在前述資料儲存部中解碼之第一密碼鑰以使前述對話鑰密碼化並將之送至前述資料儲存部，

前述資料儲存部，輸出以可利用第一解碼鑰予以解碼的方式加以密碼化，並進而以前述對話鑰加以密碼化

的前述授權鑰，

前述第一解碼處理部，具有：

第二解碼處理部(1510)，用以利用前述對話鑰將接收自前述資料儲存部之經過可利用前述第一解碼鑰予以解碼的方式加以密碼化，更進一步經過前述對話鑰加以密碼化後的前述授權鑰予以解碼；以及

第三解碼處理部(1514)，接受前述第二解碼處理部之輸出，且利用前述第一解碼鑰予以解碼，用以抽出前述授權鑰者。

6. 如申請專利範圍第5項之資料再生裝置，其中前述第一解碼鑰，係對應前述資料再生裝置及前述資料儲存部而預先被決定的鑰匙。

7. 如申請專利範圍第5項之資料再生裝置，其中前述第一控制電路，係用以控制在與複數個前述密碼化內容資料之再生動作共通之前述預定的期間內將前述對話鑰提供至前述資料儲存部。

8. 如申請專利範圍第1項之資料再生裝置，其中前述資料再生部，更包含有：

對話鑰產生部(1508)，用以生成每次對前述資料儲存部進行取得前述密碼化內容資料之存取時皆更新的對話鑰；以及

第一密碼化處理部(1506)，利用可在前述資料儲存部中解碼之第一密碼鑰以使前述對話鑰密碼化並將之送至前述資料儲存部，

前述第一解碼處理部，具有第二解碼處理部(1510)，用以利用前述對話鑰將經前述對話鑰加以密碼化後之從前述資料儲存部接收的前述授權鑰予以解碼。

9. 如申請專利範圍第8項之資料再生裝置，其中前述第一控制電路，係用以控制在與複數個前述密碼化內容資料之再生動作共通之前述預定的期間內將前述對話鑰提供至前述資料儲存部。

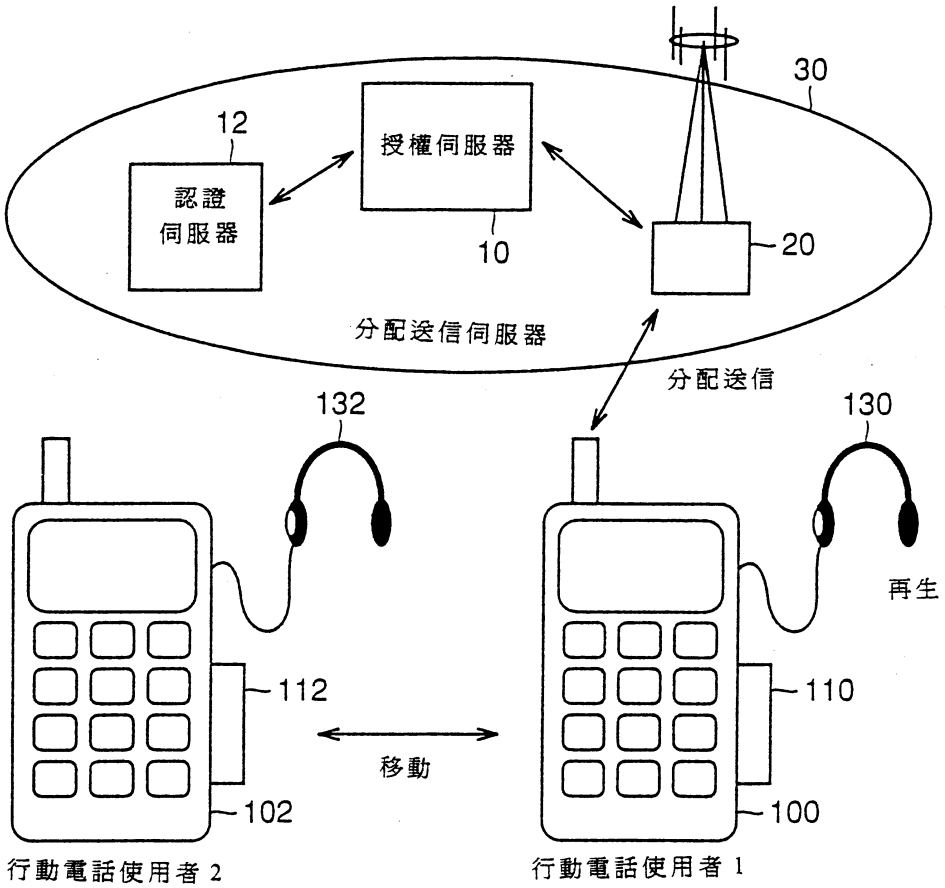
10. 如申請專利範圍第7項之資料再生裝置，其中前述預定期間，係指在前述資料再生裝置為活動期間內，前述資料儲存部被裝設在前述資料再生部內之後的期間。

11. 如申請專利範圍第9項之資料再生裝置，其中前述預定期間，係指在前述資料再生裝置為活動期間內，前述資料儲存部被裝設在前述資料再生部內之後的期間。

12. 如申請專利範圍第7項之資料再生裝置，其中前述預定期間，係指在前述資料儲存部裝設在前述資料再生裝置內之狀態下使前述再生裝置活動之後的期間。

13. 如申請專利範圍第9項之資料再生裝置，其中前述預定期間，係指在前述資料儲存部裝設在前述資料再生裝置內之狀態下使前述再生裝置活動之後的期間。

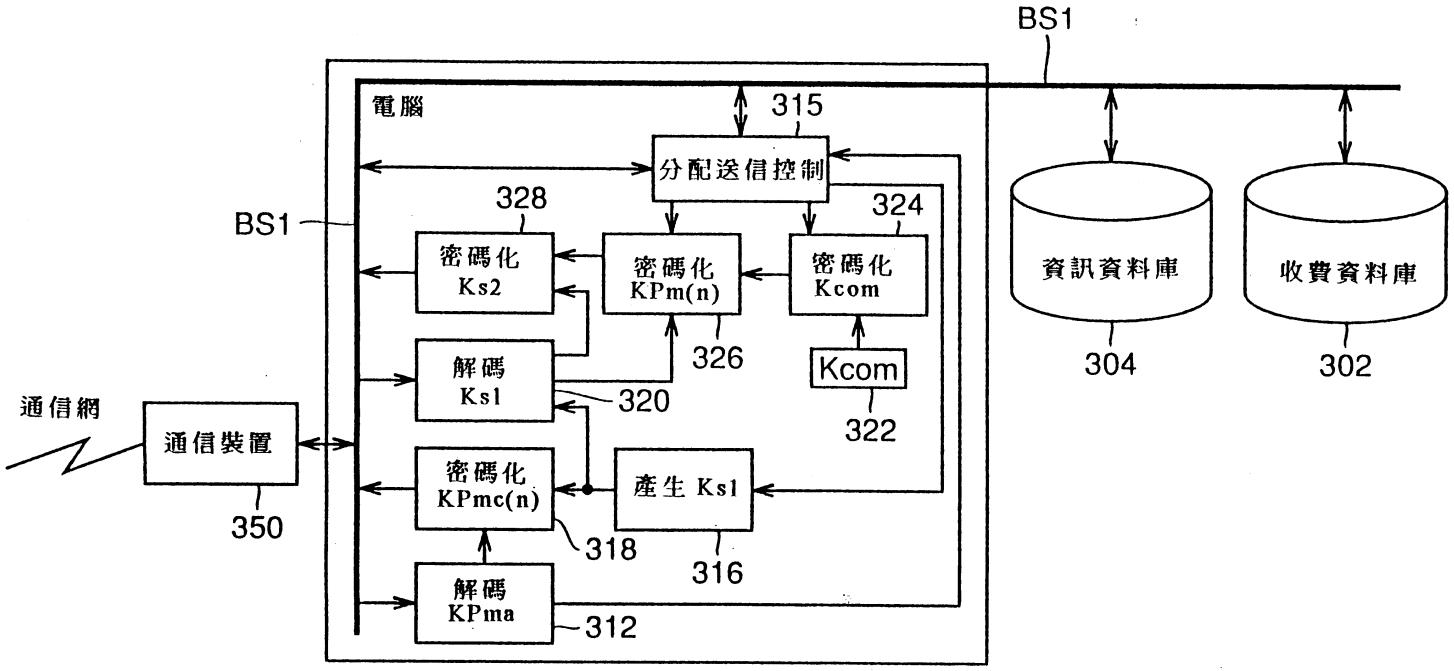
891×6047


30
12
授權伺服器
認證
伺服器
10
20
分配送信伺服器
分配送信
132
130
再生
112
110
移動
102
100
行動電話使用者 2
行動電話使用者 1

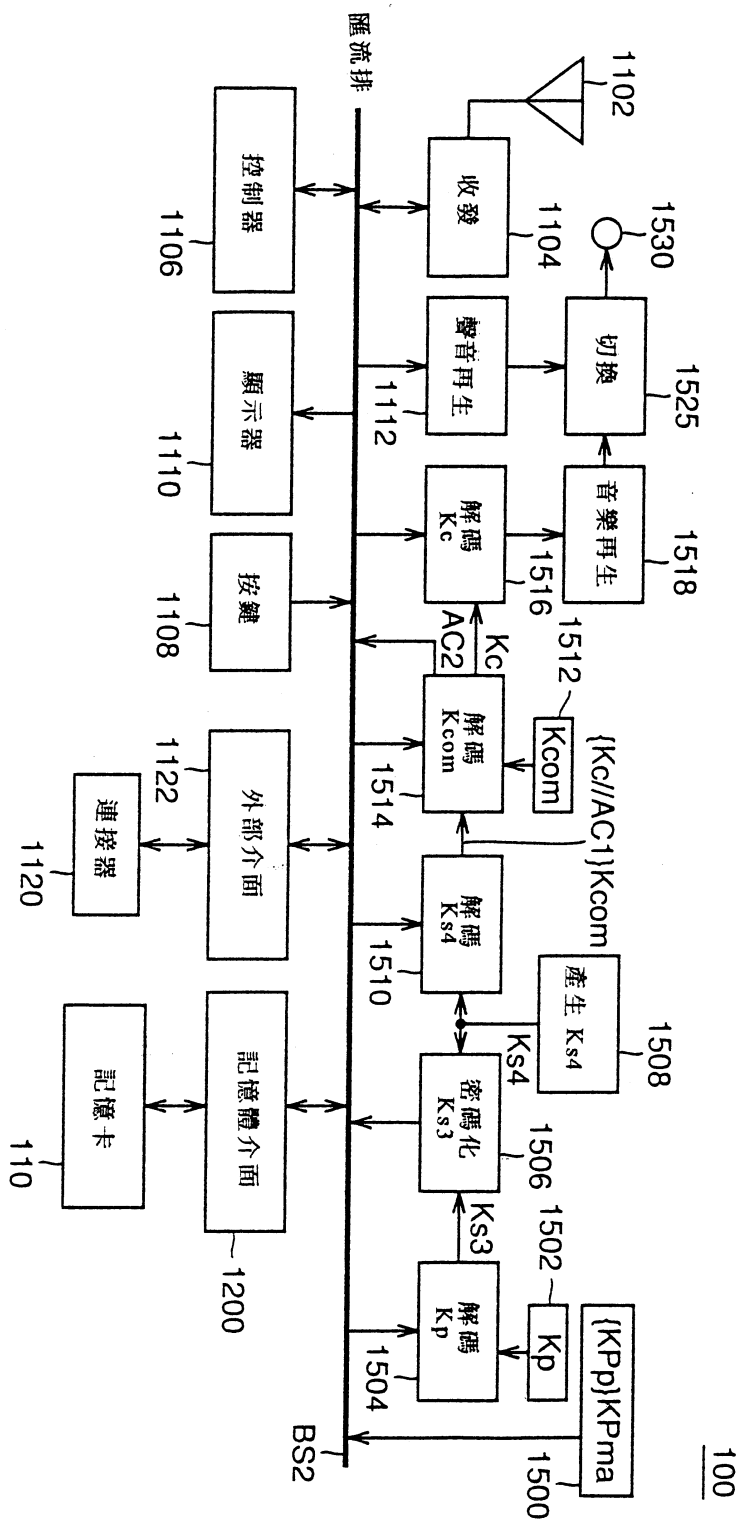
第 1 圖

名稱	機能・特徵	保持・產生處
Data	內容資料，以{Data}Kc 之形式發布以作爲施予可以Kc 解碼之密碼化內容資料	分配送信伺服器
Data-inf	附加資訊，關於內容資料之著作相關或伺服器存取相關等的普通文字資訊	分配送信伺服器
Kc	授權鑰 用以將密碼化內容資料予以解碼的解碼鑰	分配送信伺服器
Kp(n)/Kmc(n)	內容再生電路/記憶卡之等級中所固有的秘密解碼鑰n 爲用以識別等級的識別子	行動電話機記憶卡
KPp(n)/KPmc(n)	可以 Kp(n)/Kmc(n)予以解碼之非對稱的公開密碼化鑰， 以{KPp(n)}KPma/{KPmc(n)}KPma 之形式輸出時記錄， 在解碼時，生成用以顯示被解碼之公開密碼鑰KPp(n)/KPmc(n)之正當性的附隨資訊。 n 爲用以識別等級的識別子	行動電話機記憶卡
Kcom	再生電路共通之秘密解碼鑰，用於被密碼化之Kc,AC2 之解碼(亦可爲非對稱之分配送信伺服器KPcom/再生電路 Kcom)	分配送信伺服器行動電話機
KPma	認證鑰	分配送信伺服器
AC	對於來自利用者側之授權的購入條件(機能限定，授權數等)	行動電話機
AC1	對於記憶體之存取的限制資訊	分配送信伺服器
AC2	再生電路中之控制資訊	分配送信伺服器
Km(i)	每一個記憶卡中所固有的解碼鑰(i 爲用以識別卡片之識別子)	記憶卡
KPm(i)	可以 Km(i)予以解碼的非對稱之公開密碼鑰	記憶卡
Ks1	在每一分配送信對話中所產生的對話固有之共通鑰	分配送信伺服器
Ks2	在每一分配送信/移動(接收)對話時所產生的對話固有之共通鑰	記憶卡
Ks3	在每一再生/移動(發送側)對話中所產生的對話固有之共通鑰	記憶卡
Ks4	在每一再生對話中所產生的對話固有之共通鑰	行動電話機
內容 ID	用以識別內容資料 Data 之碼	分配送信伺服器
授權 ID	可特定授權之發行的管理碼(亦可考慮包含內容 ID 加以識別)	分配送信伺服器
交易 ID	可特定在每一分配送信對話中所生成之分配送信對話的碼(亦可與授權 ID 兼用)	分配送信伺服器

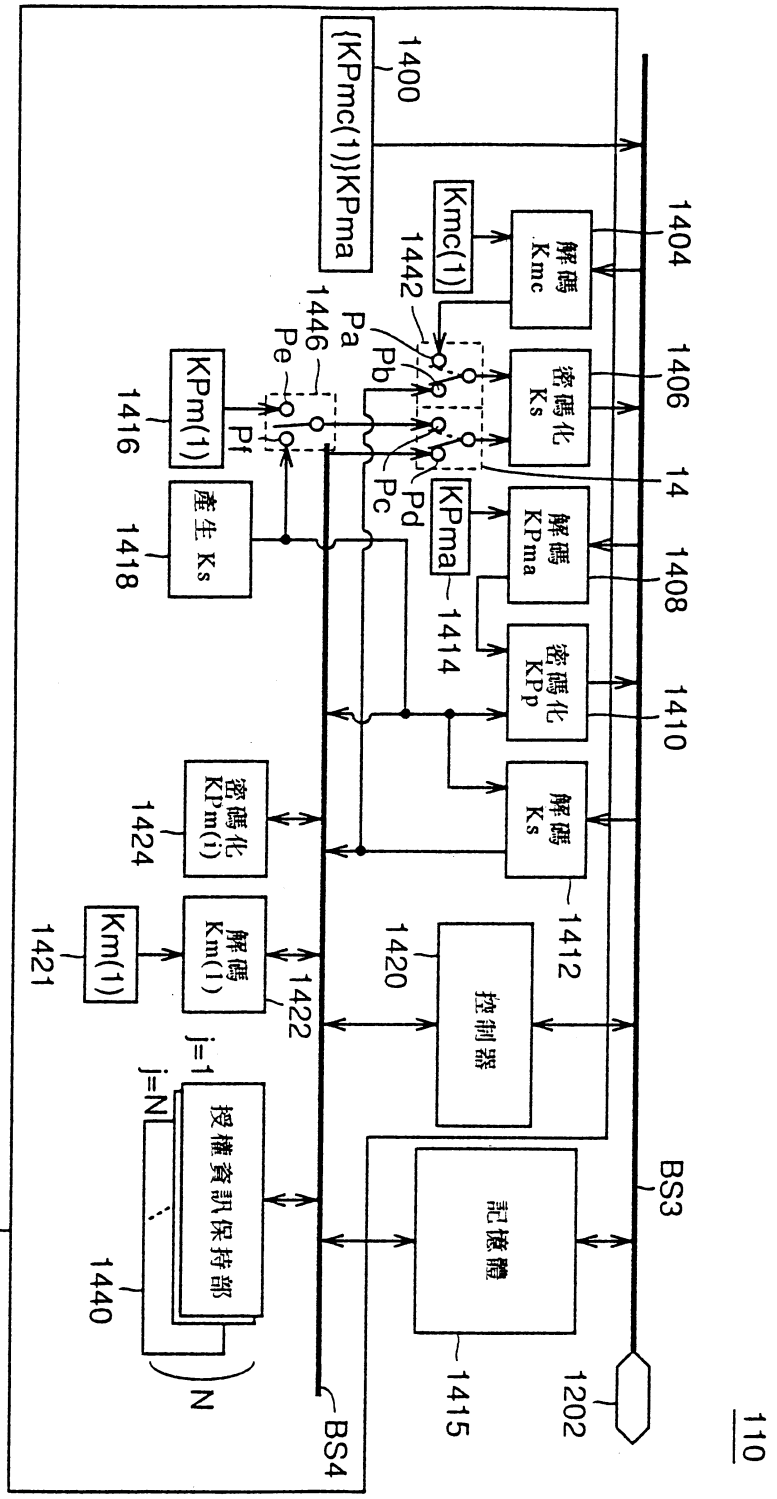
第 2 圖


BS1
電腦
315
分配送信控制
328
324
BS1
密碼化
Ks2
密碼化
KPm(n)
密碼化
Kcom
326
解碼
Ks1
320
Kcom
322
通信網
通信裝置
350
密碼化
KPmc(n)
318
產生 Ks1
316
解碼
KPma
312
資訊資料庫
304
收費資料庫
302

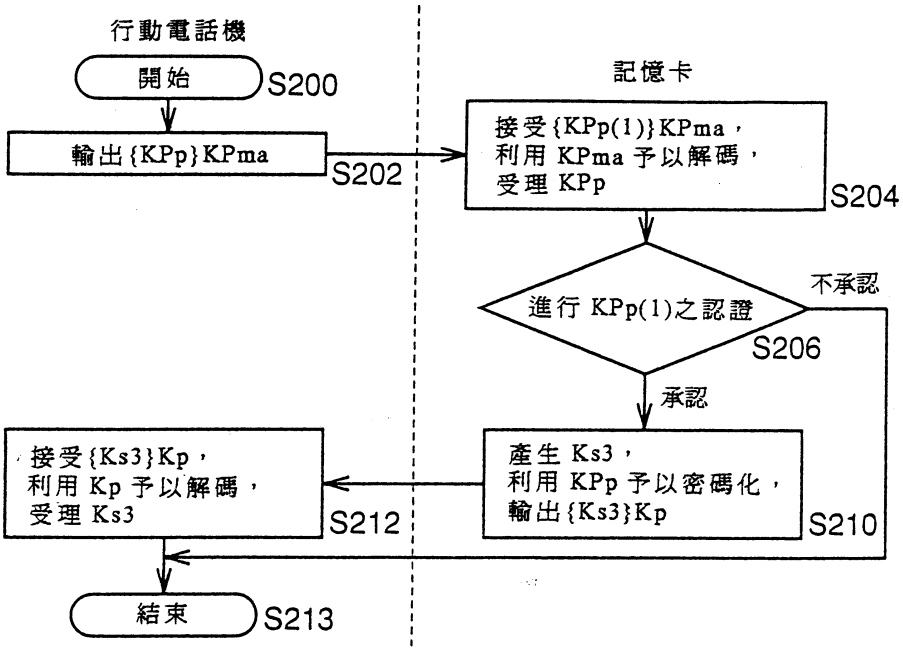
第 3 圖


100
匯流排
1102
1530
收發
1104
控制器
1106
顯示器
1110
按鍵
1108
聲音再生
1112
切換
1525
音樂再生
1518
解碼 Kc
1516
解碼 Kcom
1512
Kcom
{Kc//AC1}Kcom
解碼 Ks4
1514
1510
產生 Ks4
1508
密碼化 Ks3
1506
Ks4
Ks3
解碼 Kp
1502
Kp
{KPp}KPma
1500
1504
BS2
Kc
AC2
外部介面
1122
連接器
1120
記憶體介面
1200
記憶卡
110

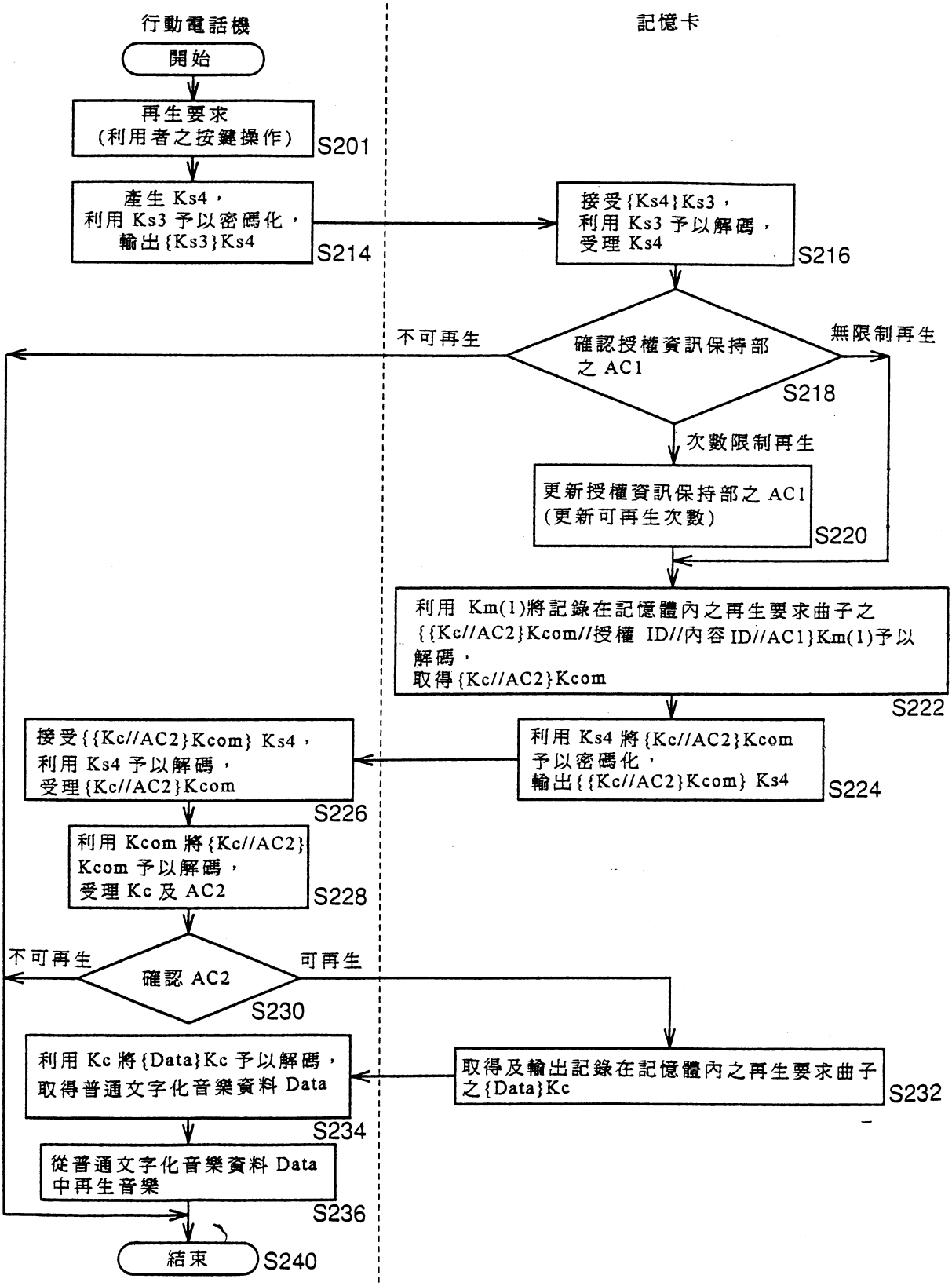
第 4 圖


110
1400
{KPmc(1)}KPma
Kmc(1)
1442
解碼 Kmc
1404
密碼化 Ks
1406
解碼 KPma
14
密碼化 KPp
1408
解碼 Ks
1410
KPma
1414
1412
Pa
Pb
Pc
Pd
Pe
Pf
1446
KPm(1)
1416
產生 Ks
1418
密碼化 KPm(i)
1424
解碼 Km(1)
1422
Km(1)
1421
控制器
1420
記憶體
1415
授權資訊保持部
1440
j=1
j=N
N
1202
BS3
BS4
TRM

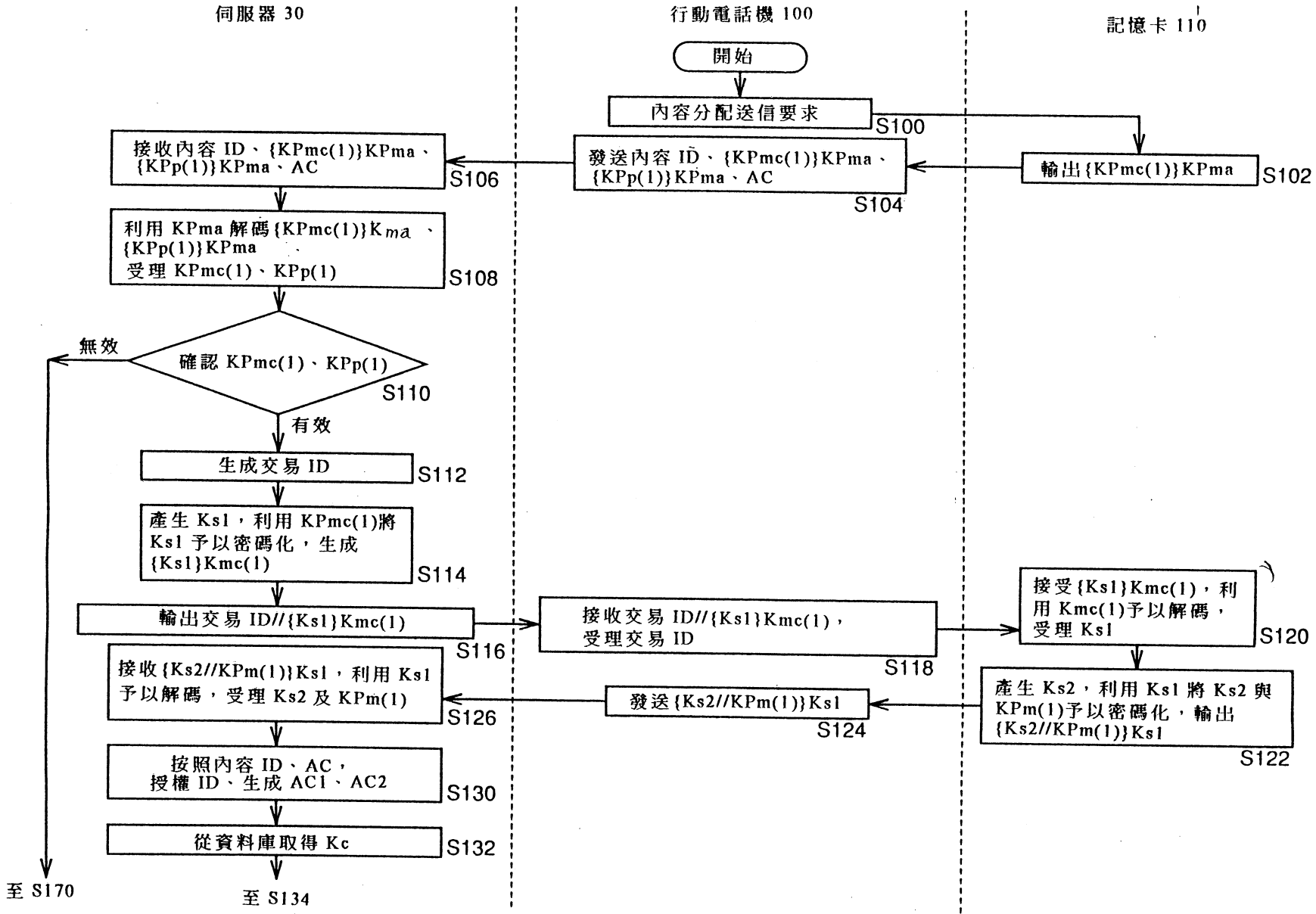
第 5 圖


行動電話機
開始
S200
輸出{KPp}KPma
S202
記憶卡
接受{KPp(1)}KPma，
利用 KPma 予以解碼，
受理 KPp
S204
進行 KPp(1)之認證
S206
不承認
承認
產生 Ks3，
利用 KPp 予以密碼化，
輸出{Ks3}Kp
S210
接受{Ks3}Kp，
利用 Kp 予以解碼，
受理 Ks3
S212
結束
S213

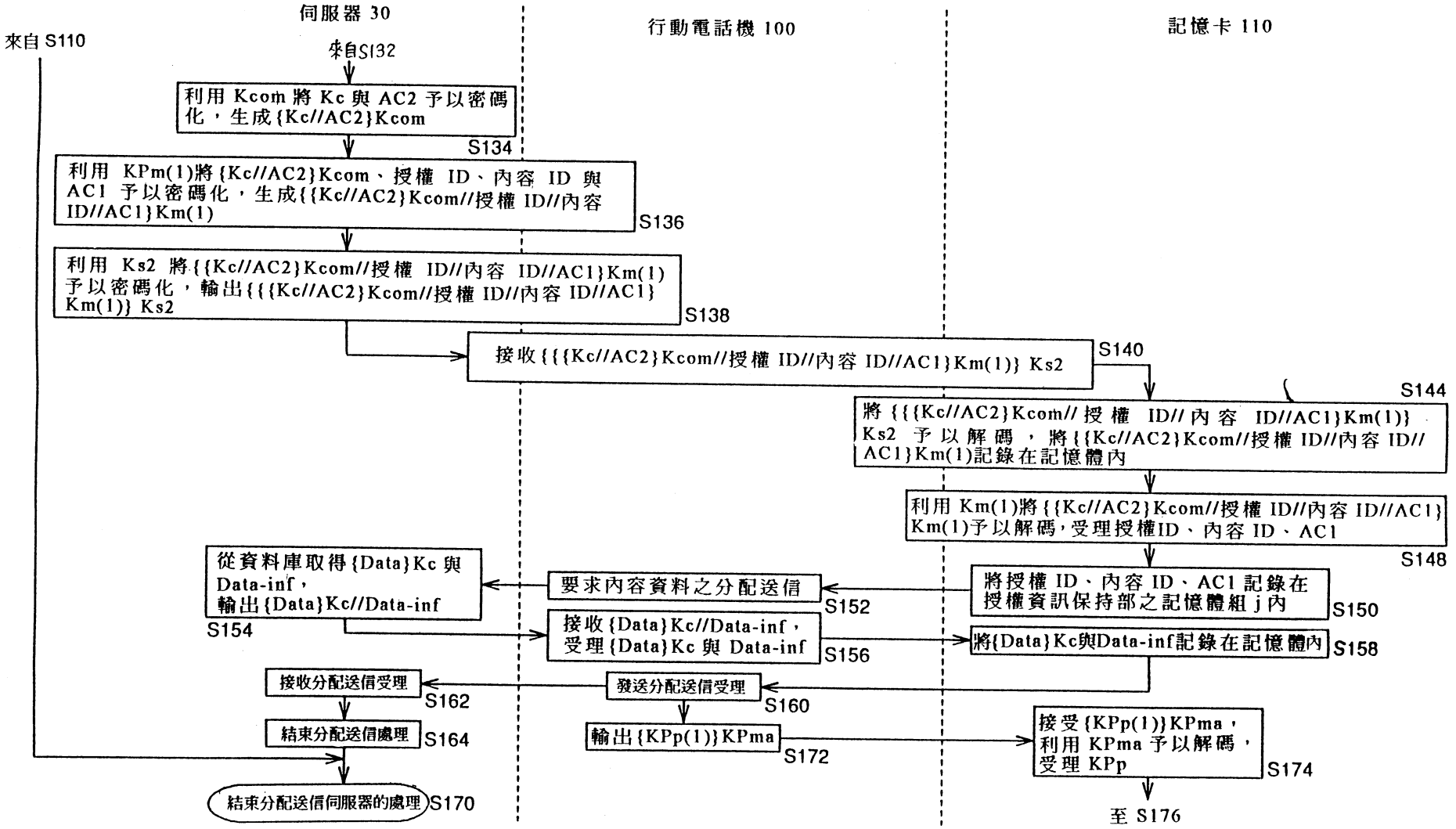
第 6 圖


行動電話機
記憶卡
開始
再生要求
(利用者之按鍵操作)
S201
產生 Ks4，
利用 Ks3 予以密碼化，
輸出{Ks3}Ks4
S214
接受{Ks4}Ks3，
利用 Ks3 予以解碼，
受理 Ks4
S216
確認授權資訊保持部
之 AC1
S218
不可再生
無限制再生
次數限制再生
更新授權資訊保持部之 AC1
(更新可再生次數)
S220
利用 Km(1)將記錄在記憶體內之再生要求曲子之
{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)予以
解碼，
取得{Kc//AC2}Kcom
S222
利用 Ks4 將{Kc//AC2}Kcom
予以密碼化，
輸出{{Kc//AC2}Kcom} Ks4
S224
接受{{Kc//AC2}Kcom} Ks4，
利用 Ks4 予以解碼，
受理{Kc//AC2}Kcom
S226
利用 Kcom 將{Kc//AC2}
Kcom 予以解碼，
受理 Kc 及 AC2
S228
確認 AC2
S230
不可再生
可再生
取得及輸出記錄在記憶體內之再生要求曲子
之{Data}Kc
S232
利用 Kc 將{Data}Kc 予以解碼，
取得普通文字化音樂資料 Data
S234
從普通文字化音樂資料 Data
中再生音樂
S236
結束
S240

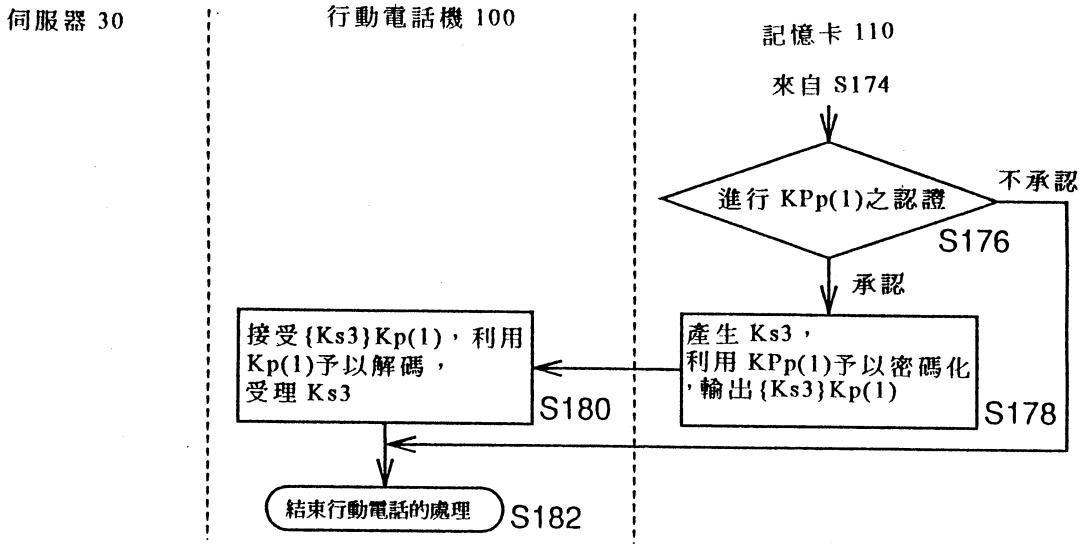
第 7 圖


伺服器 30
行動電話機 100
記憶卡 110
開始
內容分配送信要求
S100
輸出{KPmc(1)}KPma
S102
發送內容 ID、{KPmc(1)}KPma、{KPp(1)}KPma、AC
S104
接收內容 ID、{KPmc(1)}KPma、{KPp(1)}KPma、AC
S106
利用 KPma 解碼{KPmc(1)}Kma、{KPp(1)}KPma
受理 KPmc(1)、KPp(1)
S108
確認 KPmc(1)、KPp(1)
S110
無效
有效
至 S170
生成交易 ID
S112
產生 Ks1，利用 KPmc(1)將 Ks1 予以密碼化，生成{Ks1}Kmc(1)
S114
輸出交易 ID//{Ks1}Kmc(1)
S116
接收交易 ID//{Ks1}Kmc(1)，受理交易 ID
S118
接受{Ks1}Kmc(1)，利用 Kmc(1)予以解碼，受理 Ks1
S120
產生 Ks2，利用 Ks1 將 Ks2 與 KPm(1)予以密碼化，輸出{Ks2//KPm(1)}Ks1
S122
發送{Ks2//KPm(1)}Ks1
S124
接收{Ks2//KPm(1)}Ks1，利用 Ks1 予以解碼，受理 Ks2 及 KPm(1)
S126
按照內容 ID、AC，授權 ID、生成 AC1、AC2
S130
從資料庫取得 Kc
S132
至 S134

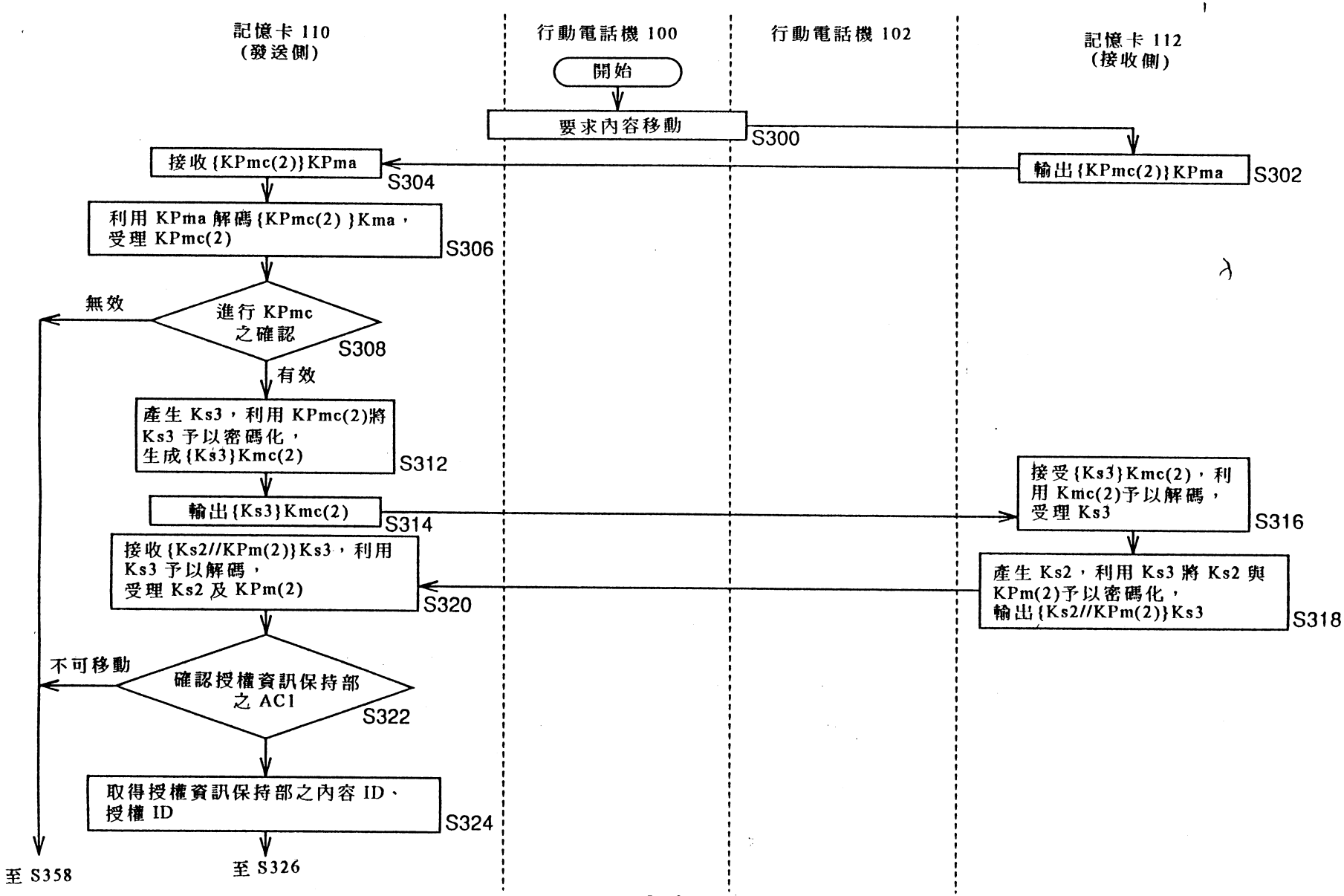
第 8 圖


伺服器 30
行動電話機 100
記憶卡 110
來自 S110
來自S132
利用 Kcom 將 Kc 與 AC2 予以密碼化，生成{Kc//AC2}Kcom
S134
利用 KPm(1)將{Kc//AC2}Kcom、授權 ID、內容 ID 與 AC1 予以密碼化，生成{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)
S136
利用 Ks2 將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)予以密碼化，輸出{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)} Ks2
S138
接收{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)} Ks2
S140
S144
將{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)} Ks2 予以解碼，將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)記錄在記憶體內
利用 Km(1)將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)予以解碼，受理授權ID、內容 ID、AC1
S148
將授權 ID、內容 ID、AC1 記錄在授權資訊保持部之記憶體組 j 內
S150
要求內容資料之分配送信
S152
從資料庫取得{Data}Kc 與 Data-inf，輸出{Data}Kc//Data-inf
S154
接收{Data}Kc//Data-inf，受理{Data}Kc 與 Data-inf
S156
將{Data}Kc與Data-inf記錄在記憶體內
S158
發送分配送信受理
S160
接收分配送信受理
S162
結束分配送信處理
S164
輸出{KPp(1)}KPma
S172
接受{KPp(1)}KPma，利用 KPma 予以解碼，受理 KPp
S174
至 S176
結束分配送信伺服器的處理
S170

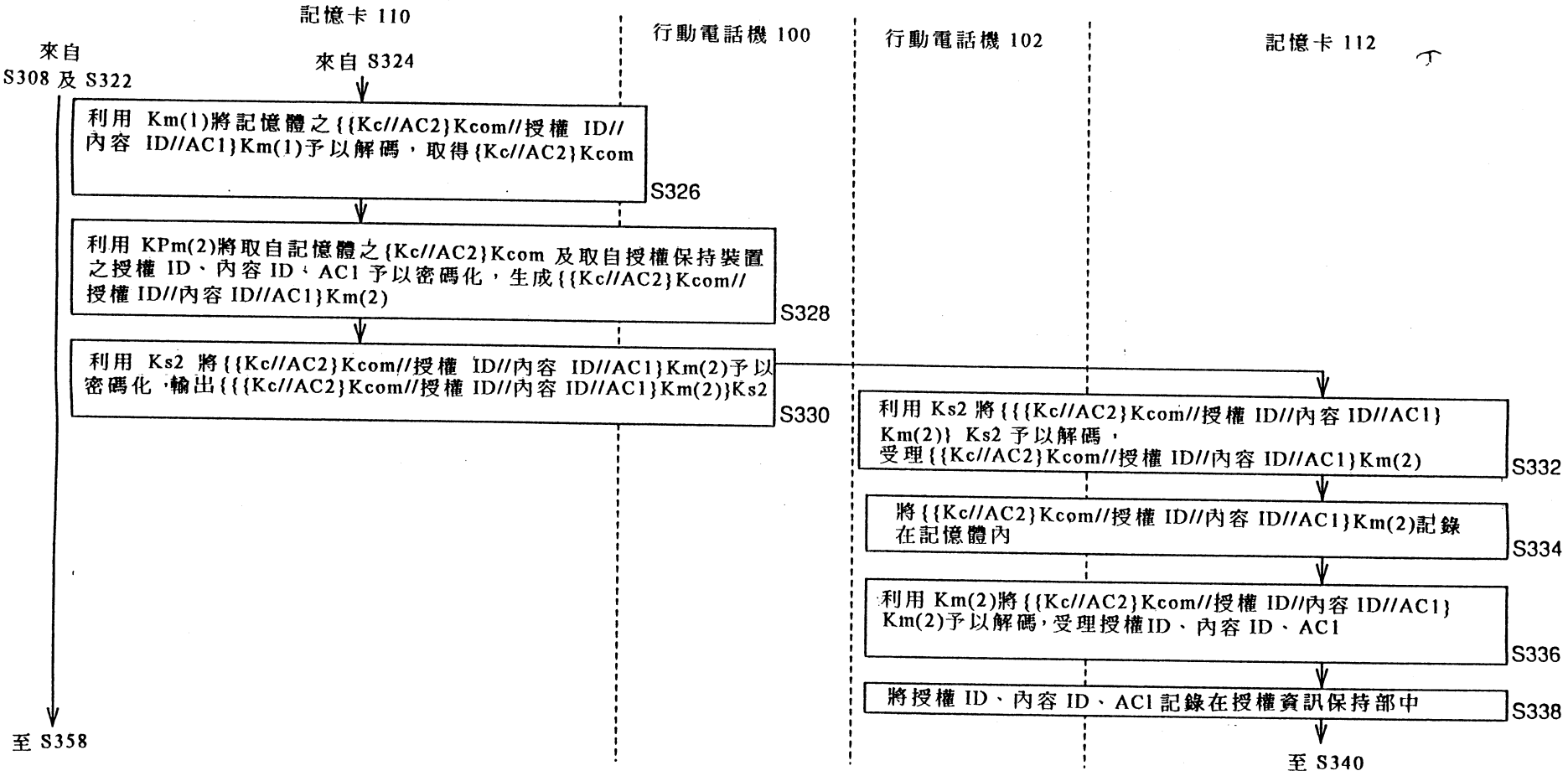
第 9 圖


伺服器 30
行動電話機 100
記憶卡 110
來自 S174
進行 KPp(1)之認證
S176
不承認
承認
產生 Ks3，
利用 KPp(1)予以密碼化
，輸出{Ks3}Kp(1)
S178
接受{Ks3}Kp(1)，利用
Kp(1)予以解碼，
受理 Ks3
S180
結束行動電話的處理
S182

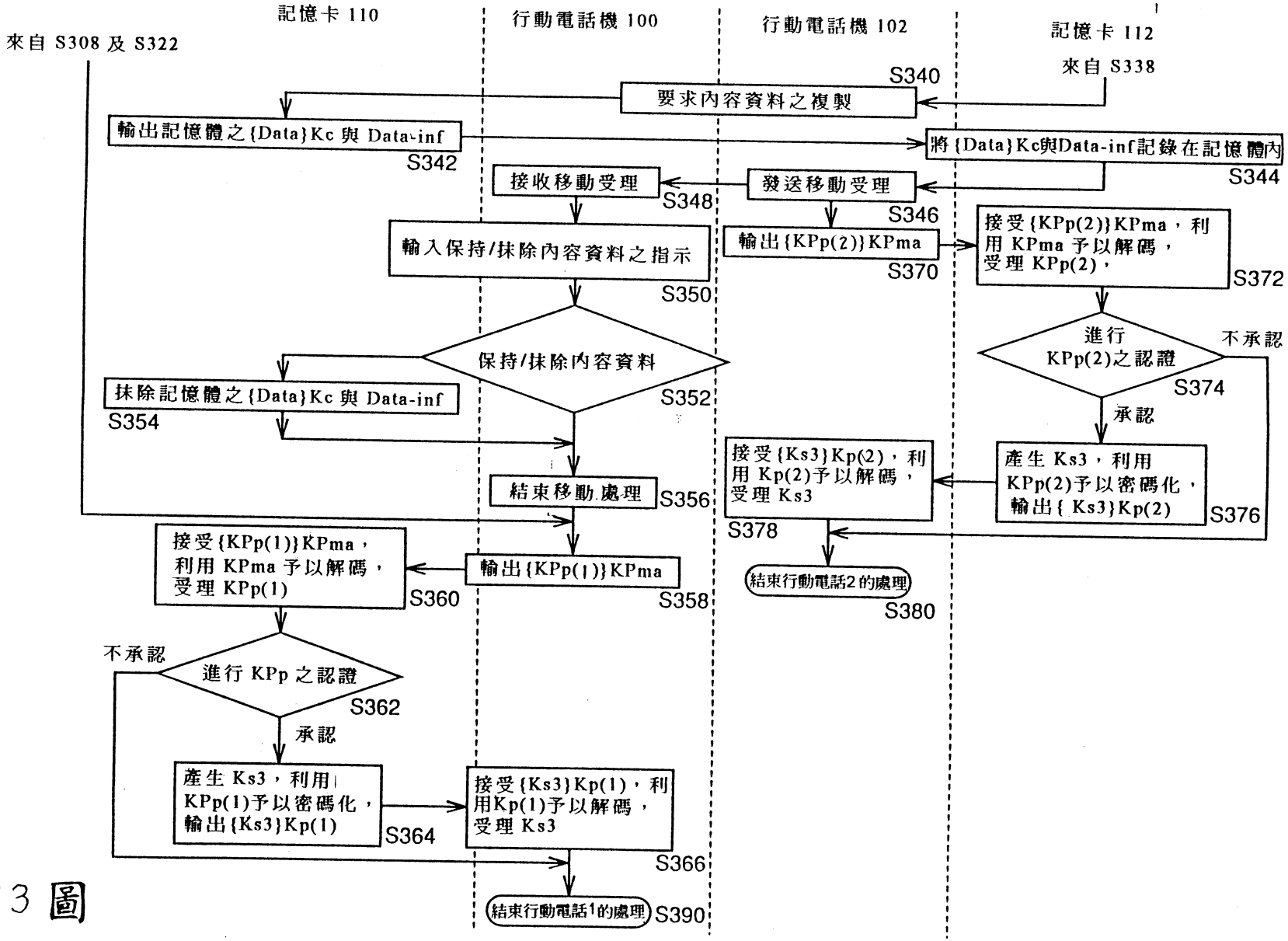
第10圖


記憶卡 110
(發送側)
行動電話機 100
行動電話機 102
記憶卡 112
(接收側)
開始
要求內容移動
S300
輸出{KPmc(2)}KPma
S302
接收{KPmc(2)}KPma
S304
利用 KPma 解碼{KPmc(2) }Kma，
受理 KPmc(2)
S306
進行 KPmc
之確認
S308
無效
有效
產生 Ks3，利用 KPmc(2)將
Ks3 予以密碼化，
生成{Ks3}Kmc(2)
S312
輸出{Ks3}Kmc(2)
S314
接受{Ks3}Kmc(2)，利
用 Kmc(2)予以解碼，
受理 Ks3
S316
產生 Ks2，利用 Ks3 將 Ks2 與
KPm(2)予以密碼化，
輸出{Ks2//KPm(2)}Ks3
S318
接收{Ks2//KPm(2)}Ks3，利用
Ks3 予以解碼，
受理 Ks2 及 KPm(2)
S320
確認授權資訊保持部
之 AC1
S322
不可移動
取得授權資訊保持部之內容 ID、
授權 ID
S324
至 S358
至 S326

第11圖


記憶卡 110
行動電話機 100
行動電話機 102
記憶卡 112
來自 S308 及 S322
來自 S324
利用 Km(1)將記憶體之{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)予以解碼，取得{Kc//AC2}Kcom
S326
利用 KPm(2)將取自記憶體之{Kc//AC2}Kcom 及取自授權保持裝置之授權 ID、內容 ID、AC1 予以密碼化，生成{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)
S328
利用 Ks2 將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)予以密碼化，輸出{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)}Ks2
S330
至 S358
利用 Ks2 將{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)} Ks2 予以解碼，受理{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)
S332
將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)記錄在記憶體內
S334
利用 Km(2)將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)予以解碼，受理授權ID、內容 ID、AC1
S336
將授權 ID、內容 ID、AC1 記錄在授權資訊保持部中
S338
至 S340

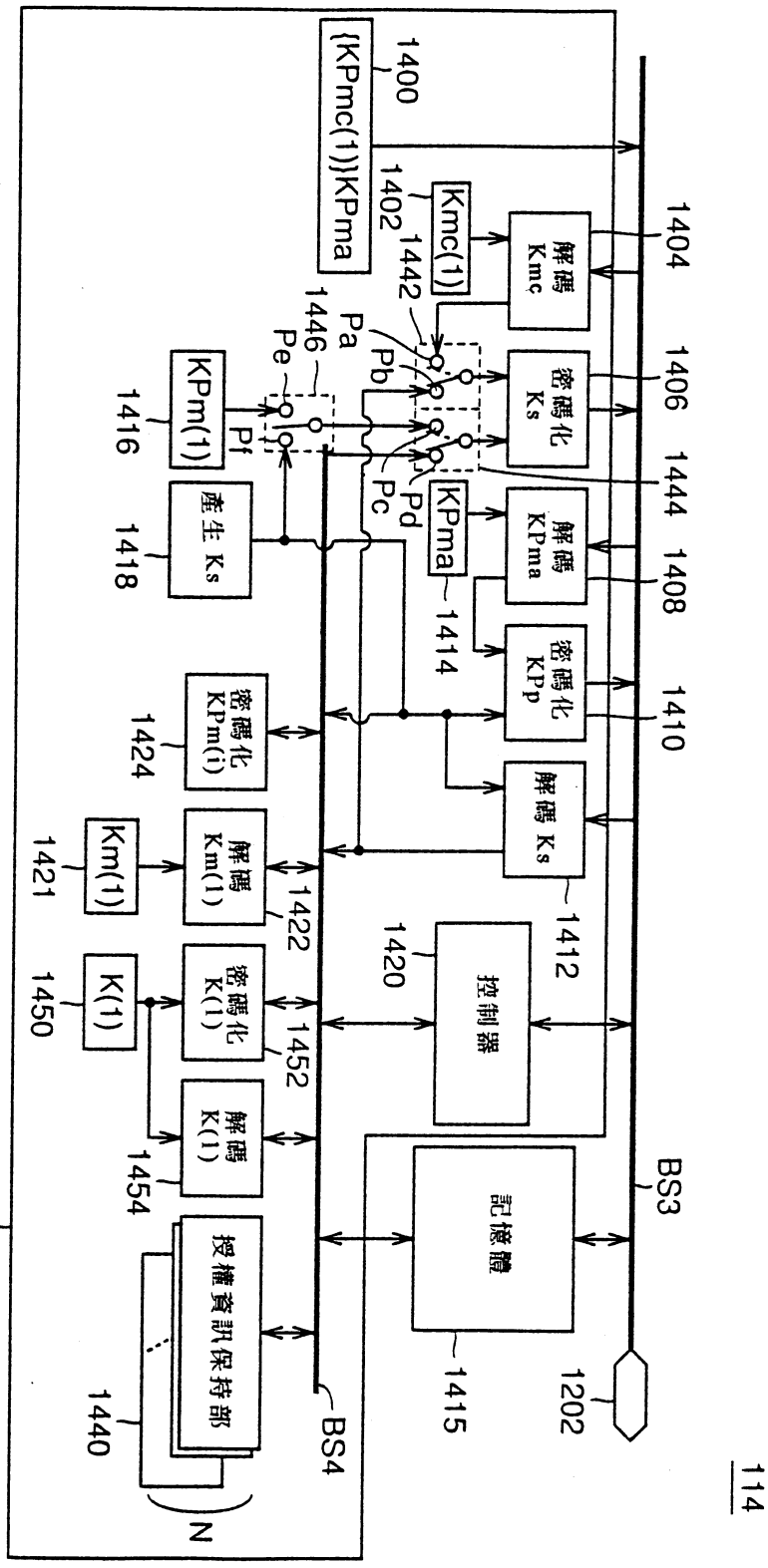
第12圖


記憶卡 110
行動電話機 100
行動電話機 102
記憶卡 112
來自 S308 及 S322
來自 S338
S340
要求內容資料之複製
輸出記憶體之{Data}Kc 與 Data-inf
S342
將{Data}Kc與Data-inf記錄在記憶體內
S344
接收移動受理
S348
發送移動受理
S346
輸入保持/抹除內容資料之指示
S350
輸出{KPp(2)}KPma
S370
接受{KPp(2)}KPma，利用 KPma 予以解碼，受理 KPp(2)，
S372
進行 KPp(2)之認證
S374
不承認
承認
保持/抹除內容資料
S352
抹除記憶體之{Data}Kc 與 Data-inf
S354
產生 Ks3，利用 KPp(2)予以密碼化，輸出{ Ks3}Kp(2)
S376
接受{Ks3}Kp(2)，利用 Kp(2)予以解碼，受理 Ks3
S378
結束移動處理 S356
結束行動電話2的處理
S380
接受{KPp(1)}KPma，利用 KPma 予以解碼，受理 KPp(1)
S360
輸出{KPp(1)}KPma
S358
不承認
進行 KPp 之認證
S362
承認
產生 Ks3，利用 KPp(1)予以密碼化，輸出{Ks3}Kp(1)
S364
接受{Ks3}Kp(1)，利用Kp(1)予以解碼，受理 Ks3
S366
結束行動電話1的處理 S390

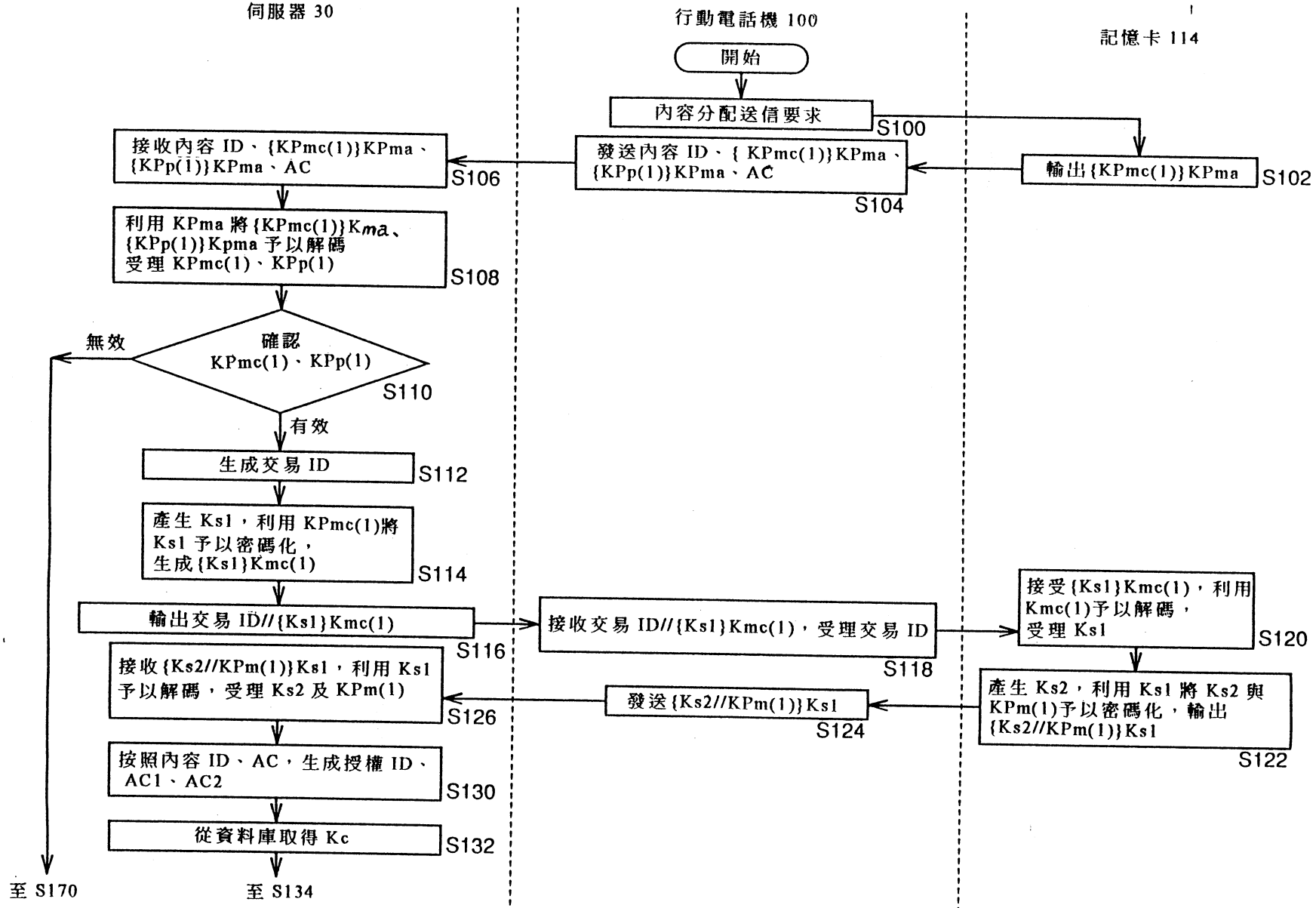
第13圖

名稱	機能・特徵	保持・產生處
Data	內容資料，以{Data}Kc 之形式發布以作爲施予可以 Kc 解碼之密碼化內容資料	分配送信伺服器
Data-inf	附加資訊，關於內容資料之著作相關或伺服器存取相關等的普通文字資訊	分配送信伺服器
Kc	授權鍵 用以將密碼化內容資料予以解碼的解碼鑰	分配送信伺服器
Kp(n)/Kmc(n)	內容再生電路/記憶卡之等級中所固有的秘密解碼鑰 n 爲用以識別等級的識別子	行動電話機 記憶卡
KPp(n)/KPmc(n)	可以 Kp(n)/Kmc(n)予以解碼之非對稱的公開密碼化鑰， 以{KPp(n)}KPma/{KPmc(n)}KPma 之形式輸出時記錄， 在解碼時，生成用以顯示被解碼之公開密碼鑰 KPp(n)/KPmc(n)之正當性的附隨資訊。 n 爲用以識別等級的識別子	行動電話機 記憶卡
Kcom	再生電路共通之秘密解碼鑰，用於被密碼化之 Kc,AC2 之解碼(亦可爲非對稱之分配送信伺服器 KPcom/再生電路 Kcom)	分配送信伺服器 行動電話機
KPma	認證鑰	分配送信伺服器
AC	對於來自利用者側之授權的購入條件(機能限定，授權數等)	行動電話機
AC1	對於記憶體之存取的限制資訊	分配送信伺服器
AC2	再生電路中之控制資訊	分配送信伺服器
Km(i)	每一個記憶卡中所固有的解碼鑰(i 爲用以識別卡片之識別子)	記憶卡
KPm(i)	可以 Km(i)予以解碼的非對稱之公開密碼鑰	記憶卡
K(i)	對稱型之記憶體固有的秘密鑰(i 爲用以識別卡片之識別子)	記憶卡
Ks1	在每一分配送信對話中所產生的對話固有之共通鑰	分配送信伺服器
Ks2	在每一分配送信/移動(接收)對話時所產生的對話固有之共通鑰	記憶卡
Ks3	在每一再生/移動(發送側)對話中所產生的對話固有之共通鑰	記憶卡
Ks4	在每一再生對話中所產生的對話固有之共通鑰	行動電話機
內容 ID	用以識別內容資料 Data 之碼	分配送信伺服器
授權 ID	可特定授權之發行的管理碼(亦可考慮包含內容 ID 加以識別)	分配送信伺服器
交易 ID	可特定在每一分配送信對話中所生成之分配送信對話的碼 (亦可與授權 ID 兼用)	分配送信伺服器

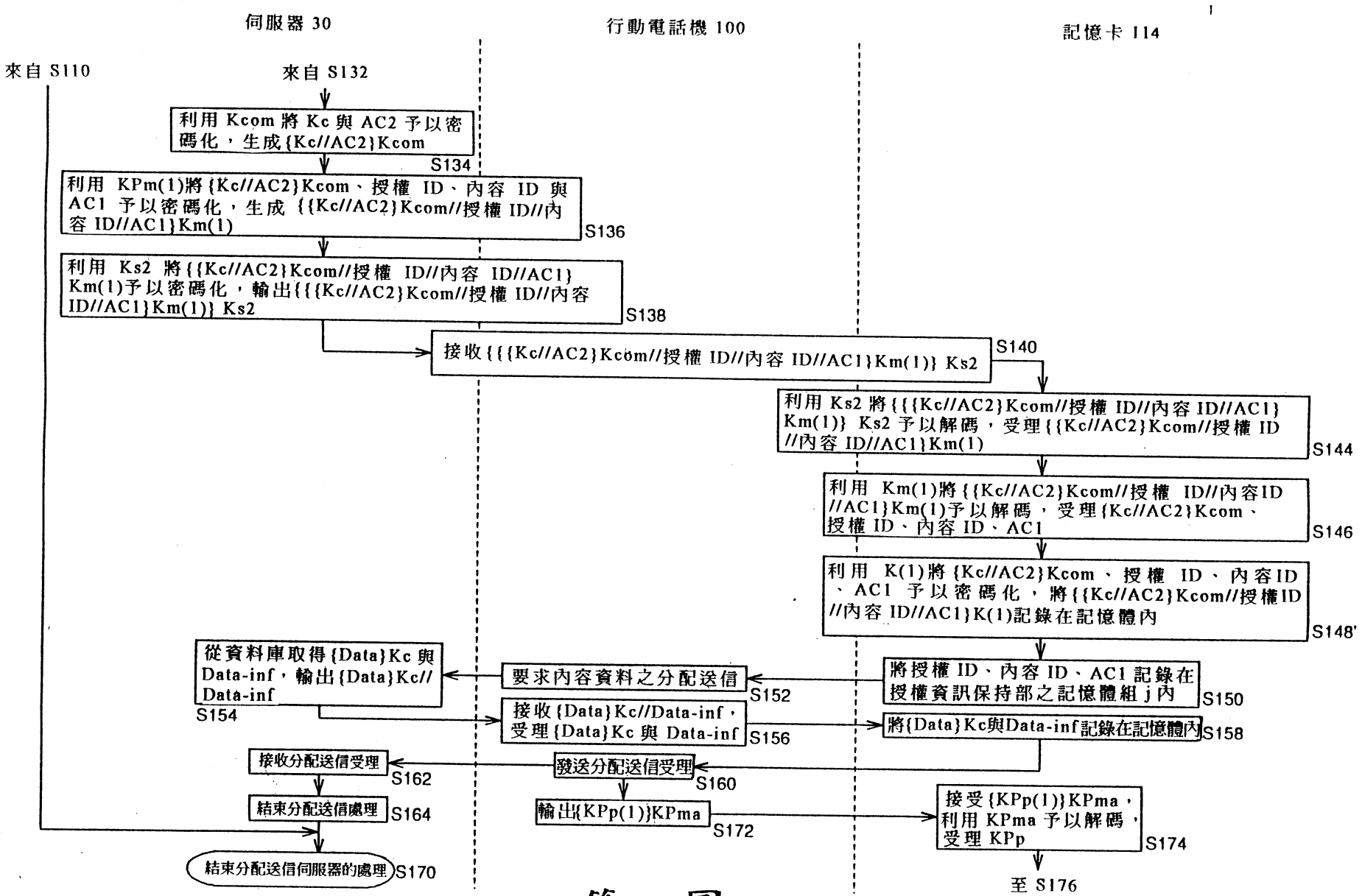
第14圖


114
1202
BS3
BS4
TRM
1400
{KPmc(1)}KPma
1402
Kmc(1)
1442
解碼 Kmc
1404
密碼化 Ks
1406
解碼 KPma
1444
密碼化 KPp
1408
解碼 Ks
1410
KPma
1414
1412
控制器
1420
記憶體
1415
Pa
1446
Pe
Pb
Pf
Pd
Pc
KPm(1)
1416
產生 Ks
1418
密碼化 KPm(i)
1424
解碼 Km(1)
1422
Km(1)
1421
密碼化 K(1)
1452
K(1)
1450
解碼 K(1)
1454
授權資訊保持部
1440
N

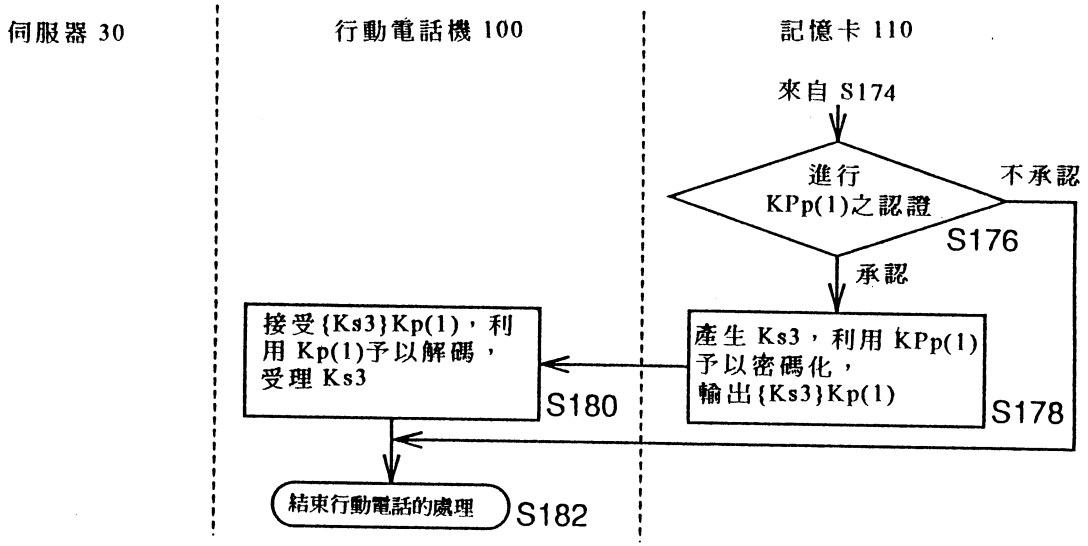
第15圖


伺服器 30
行動電話機 100
記憶卡 114
開始
內容分配送信要求
S100
輸出{KPmc(1)}KPma
S102
發送內容 ID、{ KPmc(1)}KPma、{KPp(1)}KPma、AC
S104
接收內容 ID、{KPmc(1)}KPma、{KPp(1)}KPma、AC
S106
利用 KPma 將{KPmc(1)}Kma、{KPp(1)}Kpma 予以解碼
受理 KPmc(1)、KPp(1)
S108
確認
KPmc(1)、KPp(1)
S110
無效
有效
至 S170
生成交易 ID
S112
產生 Ks1，利用 KPmc(1)將 Ks1 予以密碼化，
生成{Ks1}Kmc(1)
S114
輸出交易 ID//{Ks1}Kmc(1)
S116
接收交易 ID//{Ks1}Kmc(1)，受理交易 ID
S118
接受{Ks1}Kmc(1)，利用 Kmc(1)予以解碼，
受理 Ks1
S120
產生 Ks2，利用 Ks1 將 Ks2 與 KPm(1)予以密碼化，輸出{Ks2//KPm(1)}Ks1
S122
發送{Ks2//KPm(1)}Ks1
S124
接收{Ks2//KPm(1)}Ks1，利用 Ks1 予以解碼，受理 Ks2 及 KPm(1)
S126
按照內容 ID、AC，生成授權 ID、AC1、AC2
S130
從資料庫取得 Kc
S132
至 S134

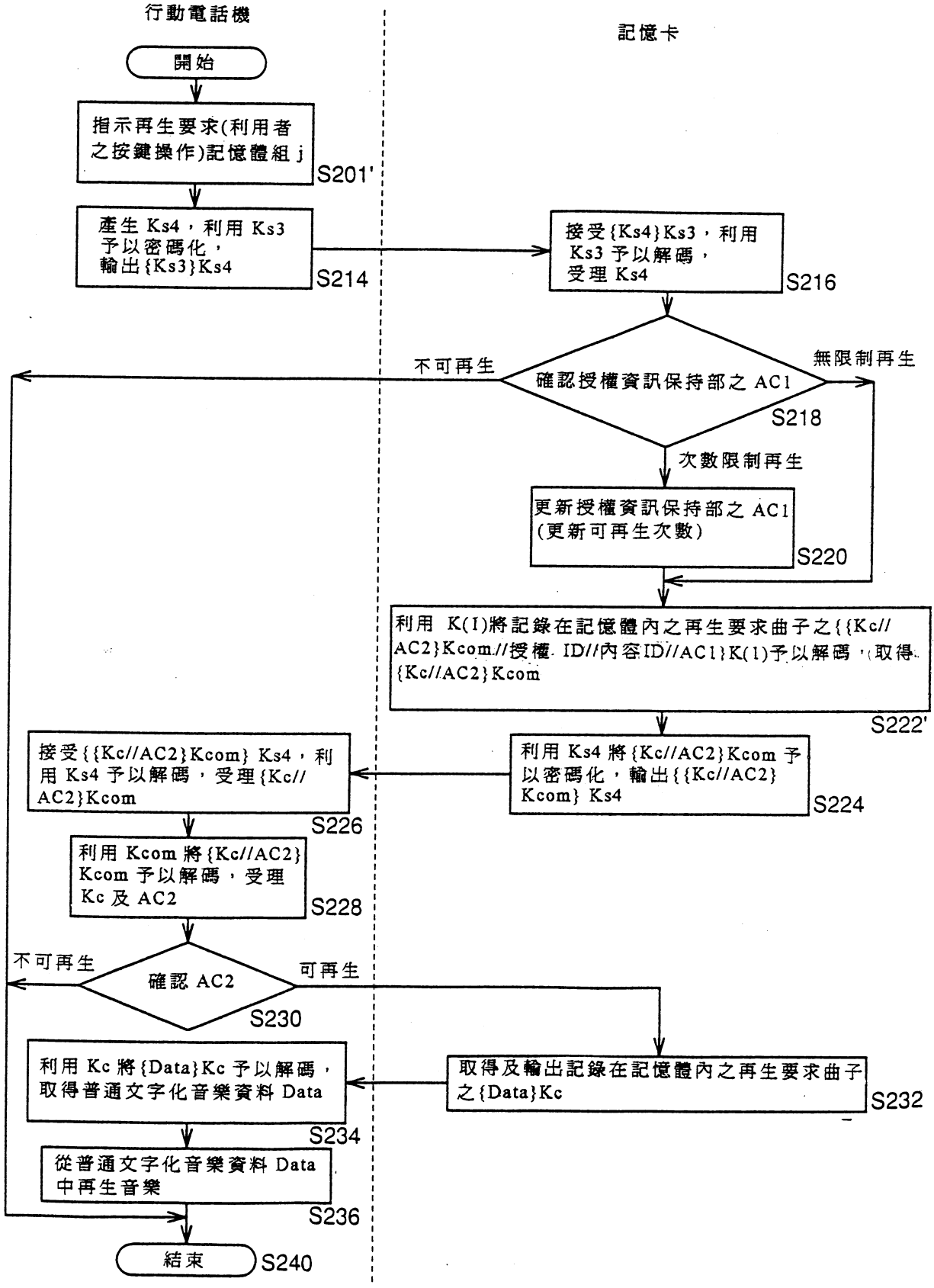
第16圖


伺服器 30
行動電話機 100
記憶卡 114
來自 S110
來自 S132
利用 Kcom 將 Kc 與 AC2 予以密碼化，生成{Kc//AC2}Kcom
S134
利用 KPm(1)將{Kc//AC2}Kcom、授權 ID、內容 ID 與 AC1 予以密碼化，生成 {{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)
S136
利用 Ks2 將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)予以密碼化，輸出{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)} Ks2
S138
接收{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)} Ks2
S140
利用 Ks2 將{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)} Ks2 予以解碼，受理{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(1)
S144
利用 Km(1)將{{Kc//AC2}Kcom//授權 ID//內容ID//AC1}Km(1)予以解碼，受理{Kc//AC2}Kcom、授權 ID、內容 ID、AC1
S146
利用 K(1)將{Kc//AC2}Kcom、授權 ID、內容ID、AC1 予以密碼化，將{{Kc//AC2}Kcom//授權ID//內容 ID//AC1}K(1)記錄在記憶體內
S148'
從資料庫取得{Data}Kc 與 Data-inf，輸出{Data}Kc//Data-inf
S154
要求內容資料之分配送信
S152
將授權 ID、內容 ID、AC1 記錄在授權資訊保持部之記憶體組 j 內
S150
接收{Data}Kc//Data-inf，受理{Data}Kc 與 Data-inf
S156
將{Data}Kc與Data-inf記錄在記憶體內
S158
接收分配送信受理
S162
發送分配送信受理
S160
結束分配送信處理
S164
輸出{KPp(1)}KPma
S172
接受{KPp(1)}KPma，利用 KPma 予以解碼，受理 KPp
S174
結束分配送信伺服器的處理
S170
至 S176

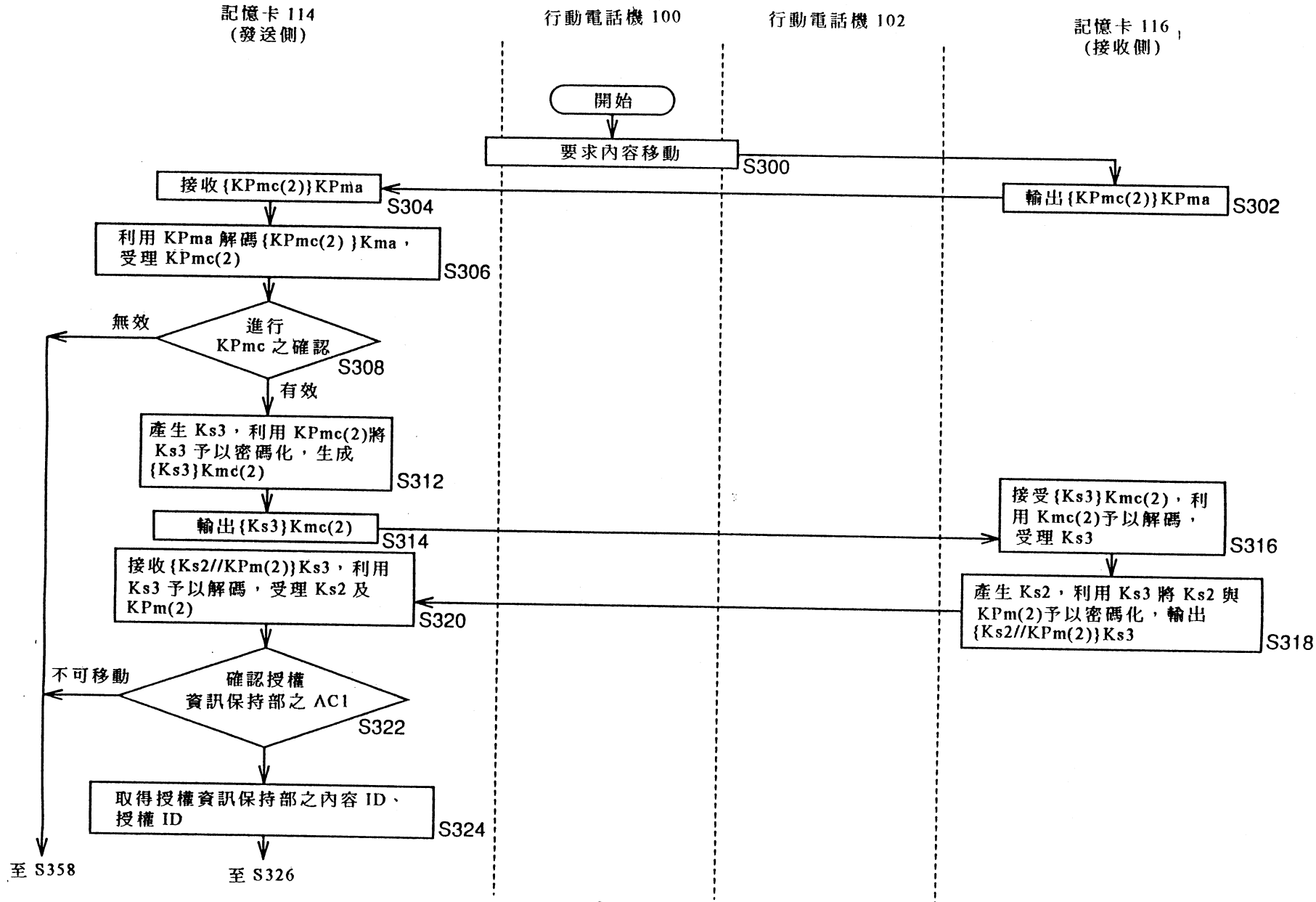
第17圖


伺服器 30
行動電話機 100
記憶卡 110
來自 S174
進行
KPp(1)之認證
S176
不承認
承認
產生 Ks3，利用 KPp(1)
予以密碼化，
輸出{Ks3}Kp(1)
S178
接受{Ks3}Kp(1)，利
用 Kp(1)予以解碼，
受理 Ks3
S180
結束行動電話的處理
S182

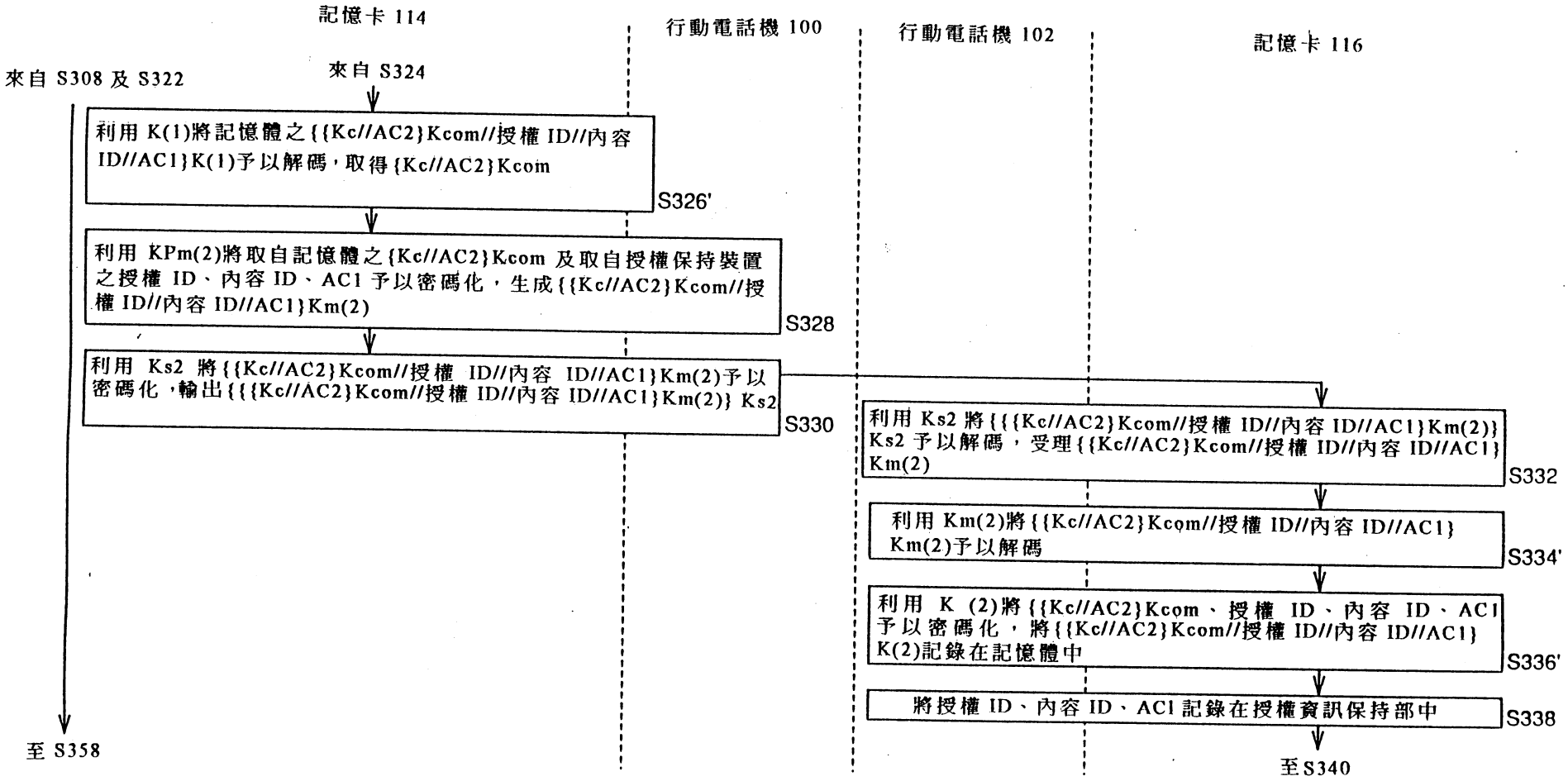
第18圖


行動電話機
記憶卡
開始
指示再生要求(利用者之按鍵操作)記憶體組 j
S201'
產生 Ks4，利用 Ks3 予以密碼化，輸出{Ks3}Ks4
S214
接受{Ks4}Ks3，利用 Ks3 予以解碼，受理 Ks4
S216
確認授權資訊保持部之 AC1
S218
不可再生
無限制再生
次數限制再生
更新授權資訊保持部之 AC1 (更新可再生次數)
S220
利用 K(I)將記錄在記憶體內之再生要求曲子之{{Kc//AC2}Kcom//授權 ID//內容ID//AC1}K(1)予以解碼，取得{Kc//AC2}Kcom
S222'
利用 Ks4 將{Kc//AC2}Kcom 予以密碼化，輸出{{Kc//AC2}Kcom} Ks4
S224
接受{{Kc//AC2}Kcom} Ks4，利用 Ks4 予以解碼，受理{Kc//AC2}Kcom
S226
利用 Kcom 將{Kc//AC2}Kcom 予以解碼，受理 Kc 及 AC2
S228
確認 AC2
S230
不可再生
可再生
取得及輸出記錄在記憶體內之再生要求曲子之{Data}Kc
S232
利用 Kc 將{Data}Kc 予以解碼，取得普通文字化音樂資料 Data
S234
從普通文字化音樂資料 Data 中再生音樂
S236
結束
S240

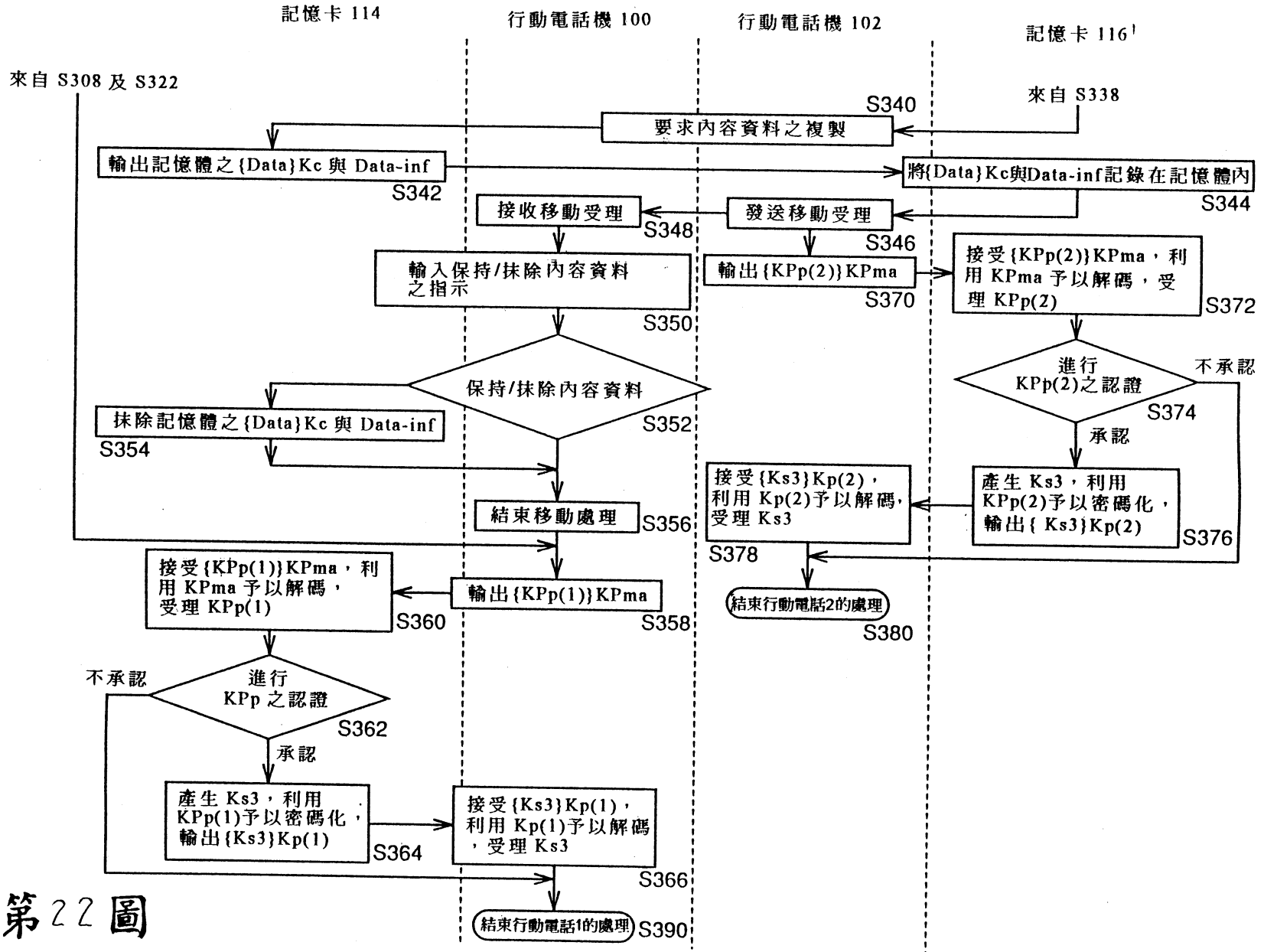
第19圖


記憶卡 114
(發送側)
行動電話機 100
行動電話機 102
記憶卡 116
(接收側)
開始
要求內容移動
S300
輸出{KPmc(2)}KPma
S302
接收{KPmc(2)}KPma
S304
利用 KPma 解碼{KPmc(2) }Kma，
受理 KPmc(2)
S306
進行
KPmc 之確認
S308
無效
有效
產生 Ks3，利用 KPmc(2)將
Ks3 予以密碼化，生成
{Ks3}Kmc(2)
S312
輸出{Ks3}Kmc(2)
S314
接受{Ks3}Kmc(2)，利
用 Kmc(2)予以解碼，
受理 Ks3
S316
產生 Ks2，利用 Ks3 將 Ks2 與
KPm(2)予以密碼化，輸出
{Ks2//KPm(2)}Ks3
S318
接收{Ks2//KPm(2)}Ks3，利用
Ks3 予以解碼，受理 Ks2 及
KPm(2)
S320
確認授權
資訊保持部之 AC1
S322
不可移動
取得授權資訊保持部之內容 ID、
授權 ID
S324
至 S358
至 S326

第20圖


記憶卡 114
行動電話機 100
行動電話機 102
記憶卡 116
來自 S308 及 S322
來自 S324
利用 K(1)將記憶體之{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}K(1)予以解碼，取得{Kc//AC2}Kcom
S326'
利用 KPm(2)將取自記憶體之{Kc//AC2}Kcom 及取自授權保持裝置之授權 ID、內容 ID、AC1 予以密碼化，生成{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)
S328
利用 Ks2 將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)予以密碼化，輸出{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)} Ks2
S330
至 S358
利用 Ks2 將{{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1}Km(2)} Ks2 予以解碼，受理{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1} Km(2)
S332
利用 Km(2)將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1} Km(2)予以解碼
S334'
利用 K (2)將{{Kc//AC2}Kcom、授權 ID、內容 ID、AC1 予以密碼化，將{{Kc//AC2}Kcom//授權 ID//內容 ID//AC1} K(2)記錄在記憶體中
S336'
將授權 ID、內容 ID、AC1 記錄在授權資訊保持部中
S338
至S340

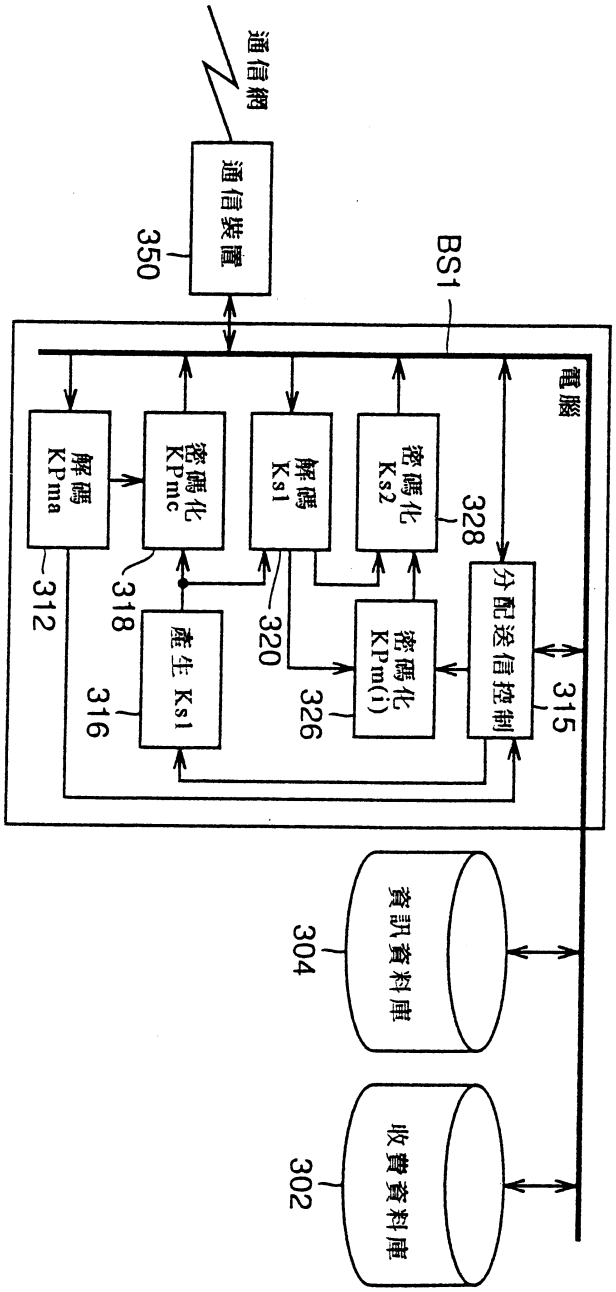
第21圖


記憶卡 114
行動電話機 100
行動電話機 102
記憶卡 116'
來自 S308 及 S322
來自 S338
S340
要求內容資料之複製
輸出記憶體之{Data}Kc 與 Data-inf
S342
將{Data}Kc與Data-inf記錄在記憶體內
S344
接收移動受理
S348
發送移動受理
S346
輸入保持/抹除內容資料之指示
S350
輸出{KPp(2)}KPma
S370
接受{KPp(2)}KPma，利用 KPma 予以解碼，受理 KPp(2)
S372
保持/抹除內容資料
S352
進行 KPp(2)之認證
S374
不承認
承認
抹除記憶體之{Data}Kc 與 Data-inf
S354
接受{Ks3}Kp(2)，利用 Kp(2)予以解碼，受理 Ks3
S378
產生 Ks3，利用 KPp(2)予以密碼化，輸出{ Ks3}Kp(2)
S376
結束移動處理
S356
接受{KPp(1)}KPma，利用 KPma 予以解碼，受理 KPp(1)
S360
輸出{KPp(1)}KPma
S358
結束行動電話2的處理
S380
不承認
進行 KPp 之認證
S362
承認
產生 Ks3，利用 KPp(1)予以密碼化，輸出{Ks3}Kp(1)
S364
接受{Ks3}Kp(1)，利用 Kp(1)予以解碼，受理 Ks3
S366
結束行動電話1的處理
S390

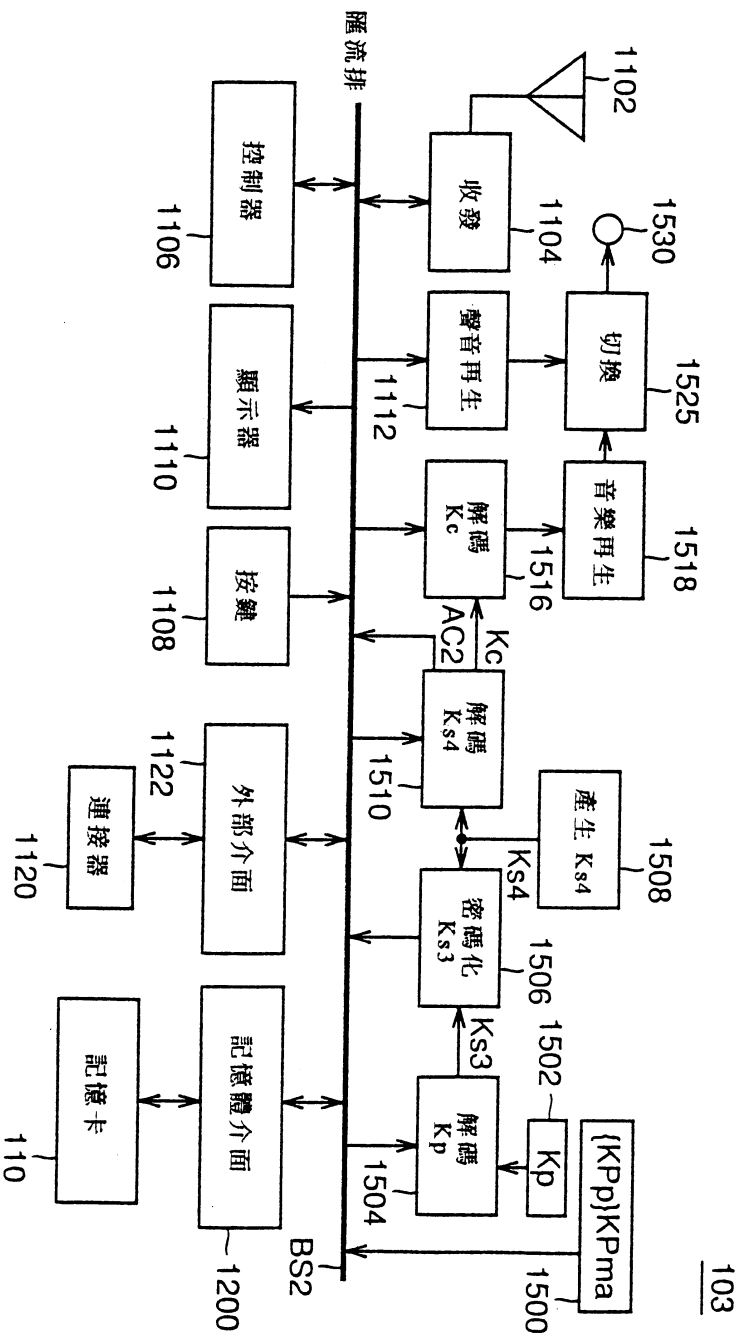
第22圖

名稱	機能・特徵	保持・產生處
Data	內容資料，以{Data}Kc 之形式發布以作爲施予可以 Kc 解碼之密碼化內容資料	分配送信伺服器
Data-inf	附加資訊，關於內容資料之著作相關或伺服器存取相關等的普通文字資訊	分配送信伺服器
Kc	授權鍵 用以將密碼化內容資料予以解碼的解碼鑰	分配送信伺服器
Kp(n)/Kmc(n)	內容再生電路/記憶卡之等級中所固有的秘密解碼鑰 n 爲用以識別等級的識別子	行動電話機 記憶卡
KPp(n)/KPmc(n)	可以 Kp(n)/Kmc(n)予以解碼之非對稱的公開密碼化鑰，以{KPp(n)}KPma/{KPmc(n)}KPma 之形式出庫時記錄，在解碼時，生成用以顯示被解碼之公開密碼鑰 KPp(n)/KPmc(n)之正當性的附隨資訊。 n 爲用以識別等級的識別子	行動電話機 記憶卡
KPma	認證鑰	分配送信伺服器
AC	對於來自利用者側之授權的購入條件(機能限定，授權數等)	行動電話機
AC1	對於記憶體之存取的限制資訊	分配送信伺服器
AC2	再生電路中之控制資訊	分配送信伺服器
Km(i)	每一個記憶卡中所固有的解碼鑰(i 爲用以識別卡片之識別子)	記憶卡
KPm(i)	可以 Km(i)予以解碼的非對稱之公開密碼鑰	記憶卡
Ks1	在每一分配送信對話中所產生的對話固有之共通鑰	分配送信伺服器
Ks2	在每一分配送信/移動(接收)對話時所產生的對話固有之共通鑰	記憶卡
Ks3	在每一再生/移動(發送側)對話中所產生的對話固有之共通鑰	記憶卡
Ks4	在每一再生對話中所產生的對話固有之共通鑰	行動電話機
內容 ID	用以識別內容資料 Data 之碼	分配送信伺服器
授權 ID	可特定授權之發行的管理碼(亦可考慮包含內容 ID 加以識別)	分配送信伺服器
交易 ID	可特定在每一分配送信對話中所生成之分配送信對話的碼 (亦可與授權 ID 兼用)	分配送信伺服器

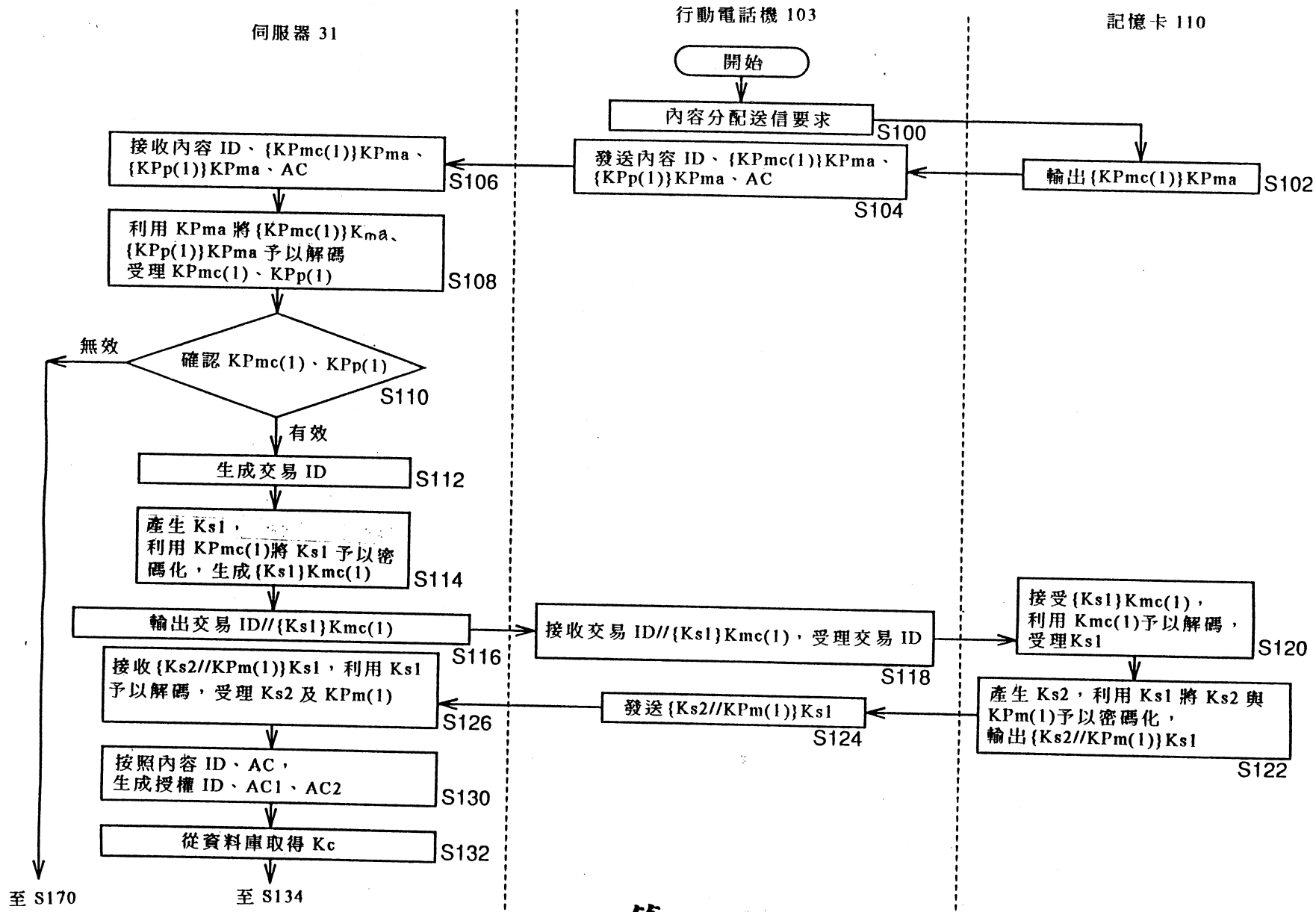
第23圖


通信網
通信裝置
350
BS1
電腦
解碼 KPma
312
密碼化 KPmc
318
解碼 Ks1
320
密碼化 Ks2
328
分配送信控制
315
產生 Ks1
316
密碼化 KPm(i)
326
資訊資料庫
304
收費資料庫
302
11

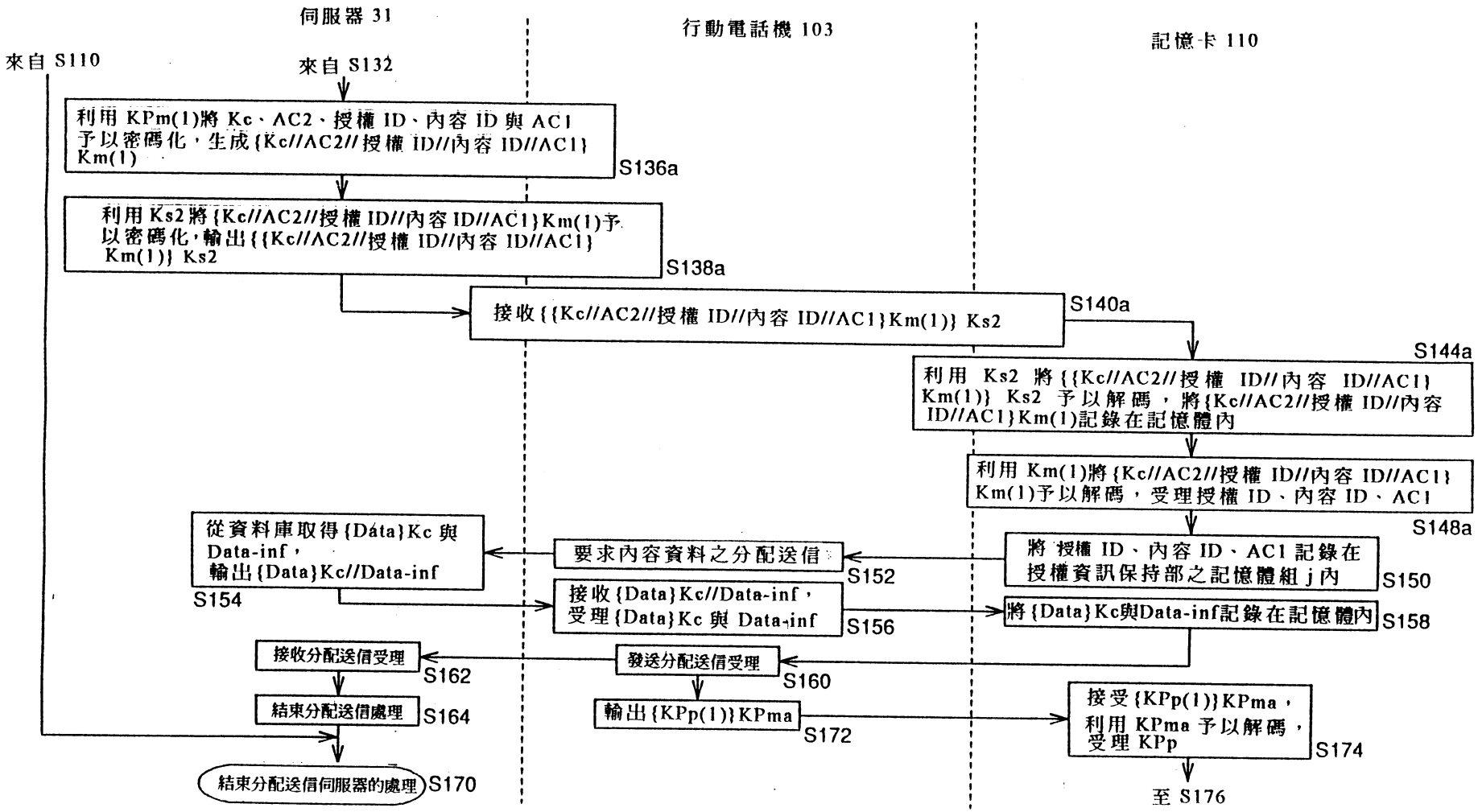
第24圖


103
匯流排
1102
收發
1104
控制器
1106
顯示器
1110
按鍵
1108
聲音再生
1112
切換
1525
音樂再生
1518
1530
解碼 Kc
1516
Kc
AC2
解碼 Ks4
1510
產生 Ks4
1508
Ks4
密碼化 Ks3
1506
Ks3
解碼 Kp
1504
1502
Kp
{KPp}KPma
1500
BS2
外部介面
1122
連接器
1120
記憶體介面
1200
記憶卡
110

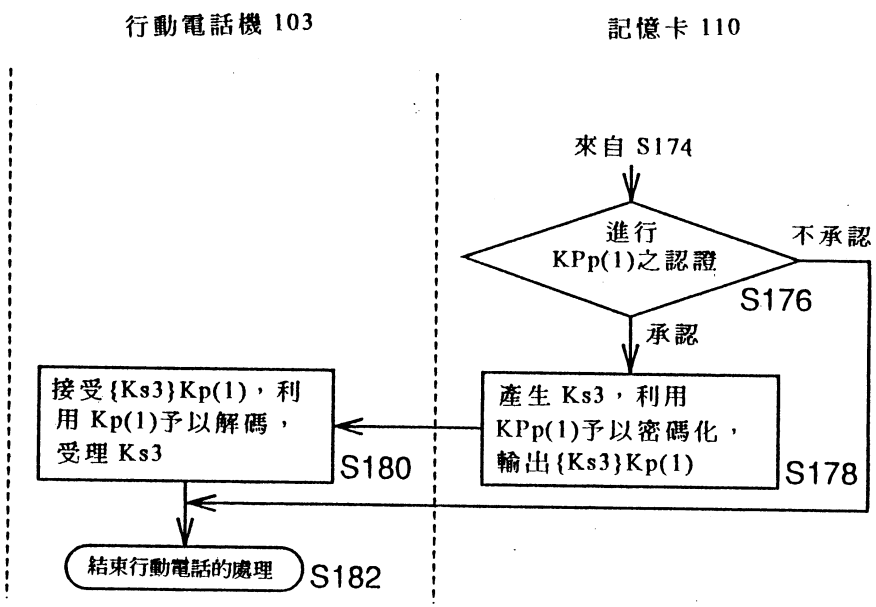
第25圖


伺服器 31
行動電話機 103
記憶卡 110
開始
內容分配送信要求
S100
輸出{KPmc(1)}KPma
S102
發送內容 ID、{KPmc(1)}KPma、{KPp(1)}KPma、AC
S104
接收內容 ID、{KPmc(1)}KPma、{KPp(1)}KPma、AC
S106
利用 KPma 將{KPmc(1)}Kma、{KPp(1)}KPma 予以解碼受理 KPmc(1)、KPp(1)
S108
確認 KPmc(1)、KPp(1)
S110
無效
有效
至 S170
生成交易 ID
S112
產生 Ks1，利用 KPmc(1)將 Ks1 予以密碼化，生成{Ks1}Kmc(1)
S114
輸出交易 ID//{Ks1}Kmc(1)
S116
接收交易 ID//{Ks1}Kmc(1)，受理交易 ID
S118
接受{Ks1}Kmc(1)，利用 Kmc(1)予以解碼，受理Ks1
S120
產生 Ks2，利用 Ks1 將 Ks2 與 KPm(1)予以密碼化，輸出{Ks2//KPm(1)}Ks1
S122
發送{Ks2//KPm(1)}Ks1
S124
接收{Ks2//KPm(1)}Ks1，利用 Ks1 予以解碼，受理 Ks2 及 KPm(1)
S126
按照內容 ID、AC，生成授權 ID、AC1、AC2
S130
從資料庫取得 Kc
S132
至 S134

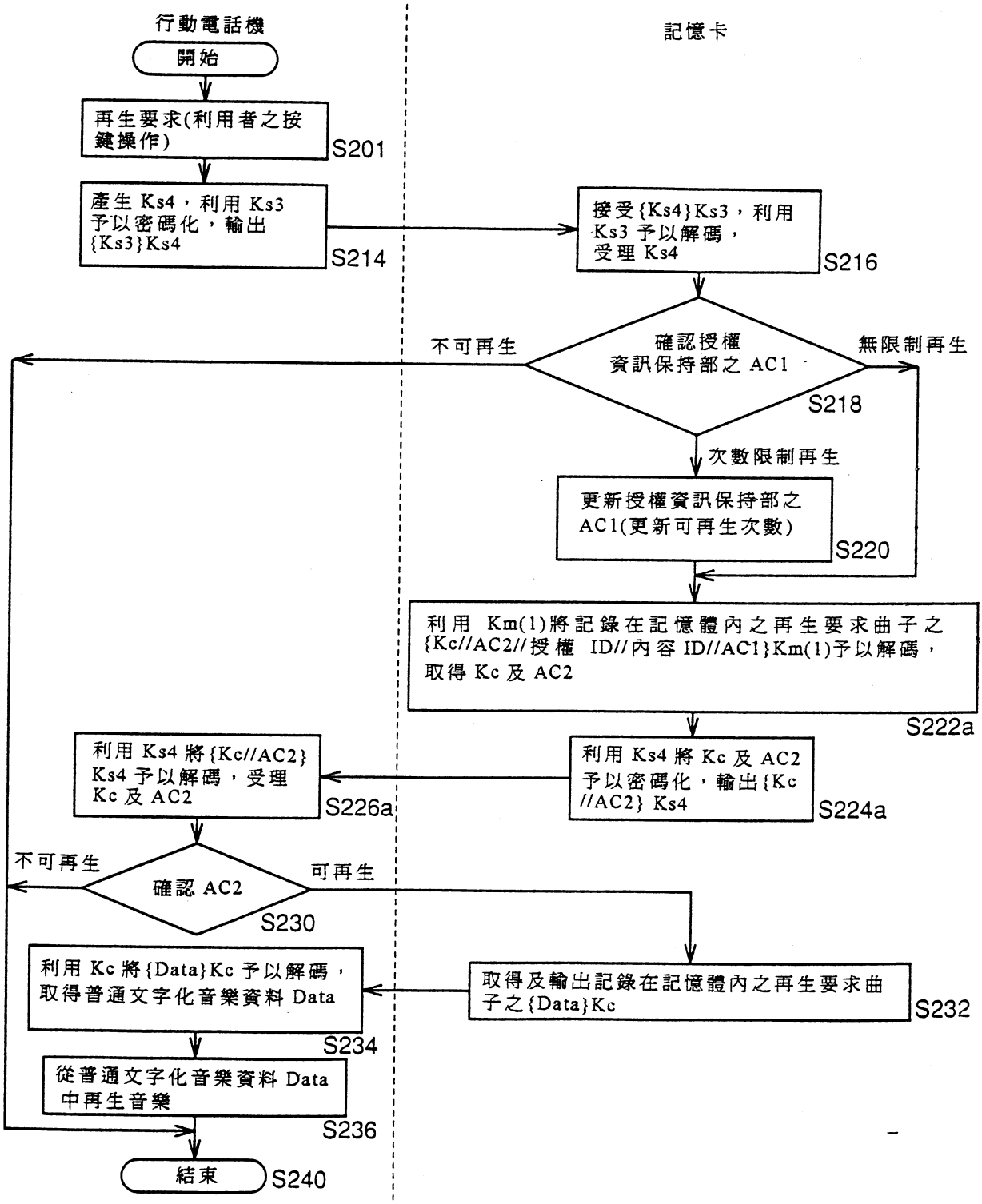
第26圖


伺服器 31
行動電話機 103
記憶卡 110
來自 S110
來自 S132
利用 KPm(1)將 Kc、AC2、授權 ID、內容 ID 與 AC1 予以密碼化，生成{Kc//AC2//授權 ID//內容 ID//AC1} Km(1)
S136a
利用 Ks2 將{Kc//AC2//授權 ID//內容 ID//AC1}Km(1)予以密碼化，輸出{{Kc//AC2//授權 ID//內容 ID//AC1} Km(1)} Ks2
S138a
接收{{Kc//AC2//授權 ID//內容 ID//AC1}Km(1)} Ks2
S140a
S144a
利用 Ks2 將{{Kc//AC2//授權 ID//內容 ID//AC1} Km(1)} Ks2 予以解碼，將{Kc//AC2//授權 ID//內容 ID//AC1}Km(1)記錄在記憶體內
利用 Km(1)將{Kc//AC2//授權 ID//內容 ID//AC1} Km(1)予以解碼，受理授權 ID、內容 ID、AC1
S148a
將 授權 ID、內容 ID、AC1 記錄在授權資訊保持部之記憶體組 j 內
S150
要求內容資料之分配送信
S152
從資料庫取得{Data}Kc 與 Data-inf，輸出{Data}Kc//Data-inf
S154
接收{Data}Kc//Data-inf，受理{Data}Kc 與 Data-inf
S156
將{Data}Kc與Data-inf記錄在記憶體內
S158
發送分配送信受理
S160
接收分配送信受理
S162
結束分配送信處理
S164
輸出{KPp(1)}KPma
S172
接受{KPp(1)}KPma，利用 KPma 予以解碼，受理 KPp
S174
至 S176
結束分配送信伺服器的處理
S170

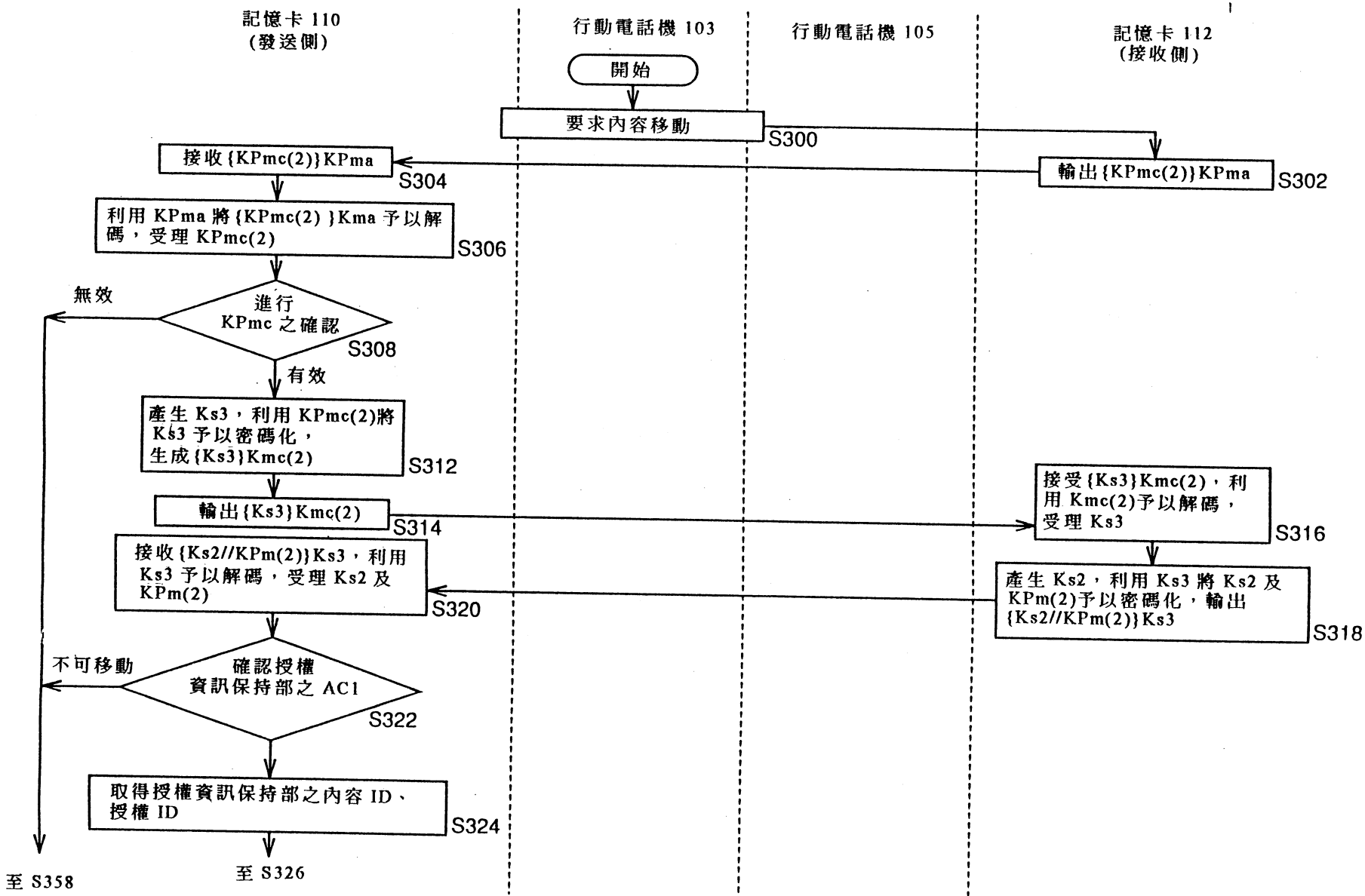
第27圖


伺服器 31
行動電話機 103
記憶卡 110
來自 S174
進行
KPp(1)之認證
不承認
S176
承認
產生 Ks3，利用
KPp(1)予以密碼化，
輸出{Ks3}Kp(1)
S178
接受{Ks3}Kp(1)，利
用 Kp(1)予以解碼，
受理 Ks3
S180
結束行動電話的處理
S182

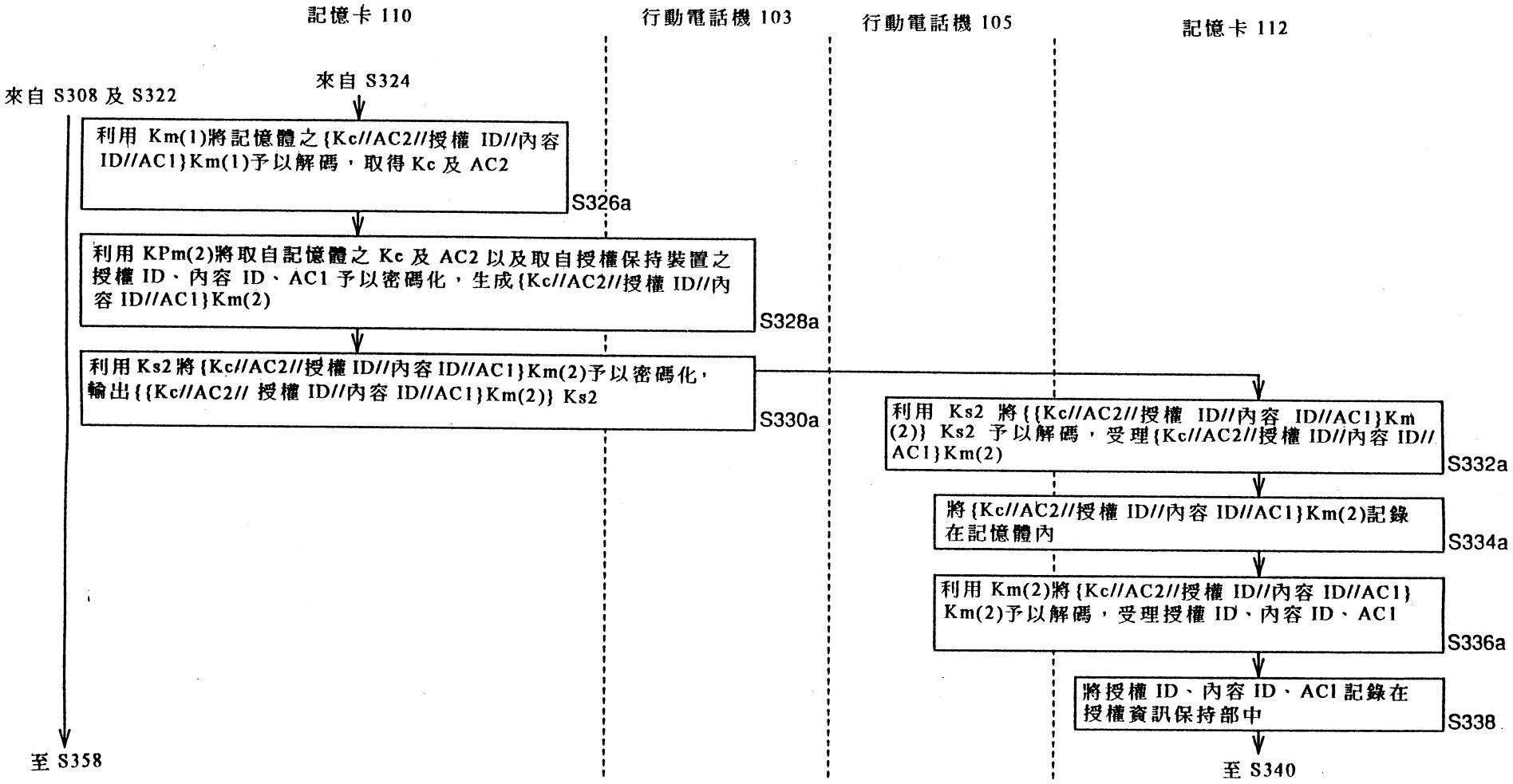
第28圖


行動電話機
記憶卡
開始
再生要求(利用者之按鍵操作)
S201
產生 Ks4，利用 Ks3 予以密碼化，輸出 {Ks3}Ks4
S214
接受{Ks4}Ks3，利用 Ks3 予以解碼，受理 Ks4
S216
確認授權資訊保持部之 AC1
S218
不可再生
無限制再生
次數限制再生
更新授權資訊保持部之 AC1(更新可再生次數)
S220
利用 Km(1)將記錄在記憶體內之再生要求曲子之{Kc//AC2//授權 ID//內容 ID//AC1}Km(1)予以解碼，取得 Kc 及 AC2
S222a
利用 Ks4 將 Kc 及 AC2 予以密碼化，輸出{Kc//AC2} Ks4
S224a
利用 Ks4 將{Kc//AC2} Ks4 予以解碼，受理 Kc 及 AC2
S226a
確認 AC2
S230
不可再生
可再生
取得及輸出記錄在記憶體內之再生要求曲子之{Data}Kc
S232
利用 Kc 將{Data}Kc 予以解碼，取得普通文字化音樂資料 Data
S234
從普通文字化音樂資料 Data 中再生音樂
S236
結束
S240

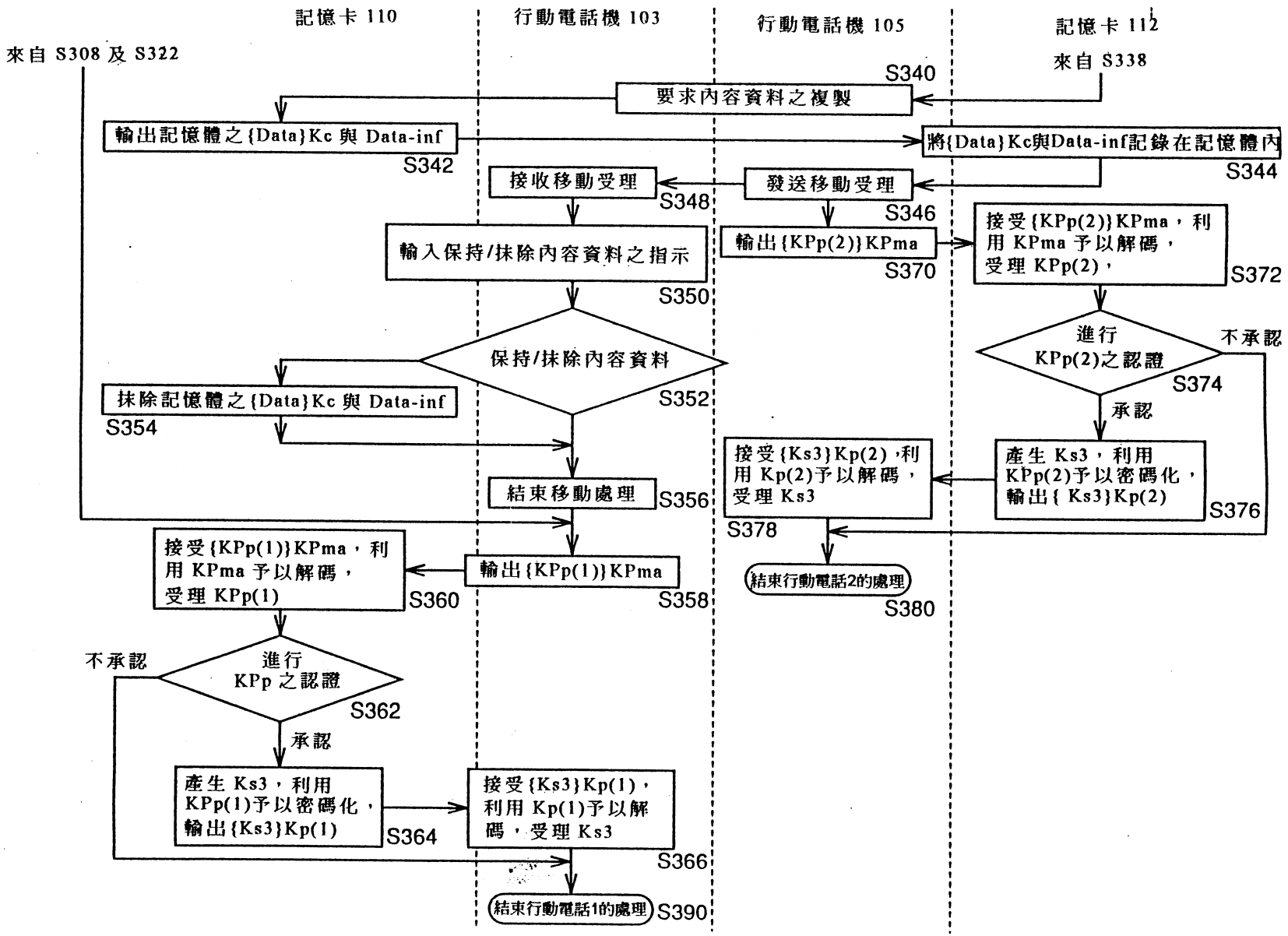
第29圖


記憶卡 110
(發送側)
行動電話機 103
行動電話機 105
記憶卡 112
(接收側)
開始
要求內容移動
S300
輸出{KPmc(2)}KPma
S302
接收{KPmc(2)}KPma
S304
利用 KPma 將{KPmc(2) }Kma 予以解碼，受理 KPmc(2)
S306
進行 KPmc 之確認
S308
無效
有效
產生 Ks3，利用 KPmc(2)將 Ks3 予以密碼化，生成{Ks3}Kmc(2)
S312
輸出{Ks3}Kmc(2)
S314
接受{Ks3}Kmc(2)，利用 Kmc(2)予以解碼，受理 Ks3
S316
產生 Ks2，利用 Ks3 將 Ks2 及 KPm(2)予以密碼化，輸出{Ks2//KPm(2)}Ks3
S318
接收{Ks2//KPm(2)}Ks3，利用 Ks3 予以解碼，受理 Ks2 及 KPm(2)
S320
確認授權資訊保持部之 AC1
S322
不可移動
取得授權資訊保持部之內容 ID、授權 ID
S324
至 S358
至 S326

第30圖


記憶卡 110
行動電話機 103
行動電話機 105
記憶卡 112
來自 S308 及 S322
來自 S324
利用 Km(1)將記憶體之{Kc//AC2//授權 ID//內容 ID//AC1}Km(1)予以解碼，取得 Kc 及 AC2
S326a
利用 KPm(2)將取自記憶體之 Kc 及 AC2 以及取自授權保持裝置之授權 ID、內容 ID、AC1 予以密碼化，生成{Kc//AC2//授權 ID//內容 ID//AC1}Km(2)
S328a
利用 Ks2 將{Kc//AC2//授權 ID//內容 ID//AC1}Km(2)予以密碼化，輸出{{Kc//AC2// 授權 ID//內容 ID//AC1}Km(2)} Ks2
S330a
至 S358
利用 Ks2 將{{Kc//AC2//授權 ID//內容 ID//AC1}Km(2)} Ks2 予以解碼，受理{Kc//AC2//授權 ID//內容 ID//AC1}Km(2)
S332a
將{Kc//AC2//授權 ID//內容 ID//AC1}Km(2)記錄在記憶體內
S334a
利用 Km(2)將{Kc//AC2//授權 ID//內容 ID//AC1}Km(2)予以解碼，受理授權 ID、內容 ID、AC1
S336a
將授權 ID、內容 ID、AC1 記錄在授權資訊保持部中
S338
至 S340

第31圖


記憶卡 110
行動電話機 103
行動電話機 105
記憶卡 112
來自 S308 及 S322
來自 S338
S340
要求內容資料之複製
輸出記憶體之{Data}Kc 與 Data-inf
S342
將{Data}Kc與Data-inf記錄在記憶體內
S344
接收移動受理
S348
發送移動受理
S346
輸入保持/抹除內容資料之指示
S350
輸出{KPp(2)}KPma
S370
接受{KPp(2)}KPma，利用 KPma 予以解碼，受理 KPp(2)，
S372
保持/抹除內容資料
S352
進行 KPp(2)之認證
S374
不承認
承認
抹除記憶體之{Data}Kc 與 Data-inf
S354
接受{Ks3}Kp(2)，利用 Kp(2)予以解碼，受理 Ks3
S378
產生 Ks3，利用 KPp(2)予以密碼化，輸出{ Ks3}Kp(2)
S376
結束移動處理
S356
結束行動電話2的處理
S380
接受{KPp(1)}KPma，利用 KPma 予以解碼，受理 KPp(1)
S360
輸出{KPp(1)}KPma
S358
不承認
進行 KPp 之認證
S362
承認
產生 Ks3，利用 KPp(1)予以密碼化，輸出{Ks3}Kp(1)
S364
接受{Ks3}Kp(1)，利用 Kp(1)予以解碼，受理 Ks3
S366
結束行動電話1的處理
S390

第32圖