合格本

申請日期	89.3.2
案號	89103694
類別	G06K 9/36, H03M 7/30

（以上各欄由本局填註）

A4
C4

530267

發明 新型 專利說明書

一、發明 新型 名稱	中文	電子內容傳送系統之多媒體播放機
	英文	"MULTIMEDIA PLAYER FOR AN ELECTRONIC CONTENT DELIVERY SYSTEM"
二、發明 創作 人	姓名	1.喬治 格列高里 葛魯斯　2.馬可 M. 赫塔多 3.肯尼斯 路易斯 米爾斯堤　4.伊德葛 當斯
	國籍	1-4.均美國
	住、居所	1.美國佛羅里達州聚光點市東北24大道4310號 2.美國佛羅里達州波卡拉頓市西北28大道4720號 3.美國佛羅里達州波音頓海灘市美琪路9927號 4.美國佛羅里達州福特勞德達爾市東北第58街2740號
三、申請人	姓名（名稱）	美商萬國商業機器公司
	國籍	美國
	住、居所（事務所）	美國紐約州阿蒙市新果園路
	代表人姓名	傑拉德 羅森賽

（由本局填寫）

承辦人代碼：	
大　　類：	
ＩＰＣ分類：	

A6
B6

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有　□無主張優先權
美國	1998年12月10日	09/208,774	□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

A7
B7

五、發明說明（ 1 ）

相關申請案之對照

本申請案是1998年10月22日(目前日期爲_____)提出申請的申請案09/177,096之分案申請案，而該申請案09/177,096是1998年8月13日(目前日期爲_____)提出申請的申請案09/133,519之部份繼續申請案。本申請案特此引用先前申請案09/177,096之整個揭示事項以供參照。此外，本申請案主張在技術上與連同本申請案讓渡給國際商務機器股份有限公司(IBM)的下列申請案相關的主題之權項。

內部案號	申請案序號	發明名稱	發明人
SE9-98-006		Secure Electronic Content Management	Kenneth L. Milsted George Gregory Gruse Marco M. Hurtado Edgar Downs Cesar Medina
SE9-98-007		Multimedia Player Toolkit	George Gregory Gruse John J. Dorak, Jr. Kenneth L. Milsted
SE9-98-008		Multimedia Content Creation System	Kenneth L. Milsted Qing Gong Edgar Downs
SE9-98-010		Key Management System for End-User Digital Player	Jeffrey B. Lotspiech Marco M. Hurtado George Gregory Gruse Kenneth L. Milsted
SE9-98-011		Multi-media player for an Electronic Content Delivery System	Marco M. Hurtado George Gregory Gruse Edgar Downs Kenneth L. Milsted
SE9-98-013		A method to identify CD content	Kenneth L. Milsted Craig Kindell Qing Gong

五、發明說明（ 2 ）

SE9-98-014		Toolkit for delivering electronic content from an Online store	Richard Spagna Kenneth L. Milsted David P. Lybrand Edgar Downs
SE9-98-015		A method and apparatus to automatically create encode digital content	Kenneth L. Milsted Kha Kinh Nguyen Qing Gong
SE9-98-016		A method and apparatus to indicate an encoding rate for digital content	Kenneth L. Milsted Qing Gong

發明背景

1．發明領域

所揭示的本發明在廣義上係有關電子商務(electronic commerce)之領域，尤係有關一種經由諸如網際網路及全球資訊網等的全球性通訊網路而安全傳送諸如印刷媒體、電影、電玩、及音樂等數位資產並管理該等數位資產的權利之系統及相關工具程式。

2．相關技術說明

使用諸如網際網路等的全球性配送系統來配送諸如音樂、電影、電腦程式、圖片、電玩、及其他內容之趨勢持續在成長。在此同時，有價數位內容的所有人及出版商已減緩了接受利用網際網路來配送數位資產，其原因有數個。第一個原因是：所有人恐懼未經授權的複製、或數位內容的剽竊。數位內容的電子式傳送消除了剽竊的數個障礙。電子式配送消除的一個障礙是對實體可記錄媒體(例

五、發明說明（ 3 ）

如軟碟或光碟)本身的需求。雖然將數位內容複製到實體媒體時，在使用空白錄音帶或可記錄光碟的許多情形中之成本少於一美元，但是總是要耗用金錢。然而，在電子式配送的情形中，不再需要實體媒體。因爲係以電子方式配送內容，所以實體媒體的成本不是一個因素。第二個障礙是內容本身的格式，亦即以一類比格式儲存的內容相對於以一數位格式儲存的內容。當以影印方式複製諸如印刷圖片等的以一類比格式儲存之內容時，拷貝的品質低於原始的品質。每一次後續的複製一份拷貝(有時被稱爲一代)之品質又比原始的品質再低一些。當以數位方式儲存圖片時，就不會發生品質的降低。每一份拷貝及每一代的拷貝都如原始圖片一般的清晰及鮮明。由於完美的數位拷貝加上以極低成本利用電子方式配送內容及經由網際網路而廣泛地配送內容之整合效應，所以使未經授權的拷貝之剽竊及配送變得較爲容易。只要按下鍵盤的幾個鍵，非法複製者即可經由網際網路而傳送數百份甚至數千份完美複製的數位內容。因此，目前需要確保以電子方式配送的數位資產的保護及安全性。

數位內容提供者希望建立一種可保護內容所有人權利的安全之數位內容全球性配送系統。建立一數位內容配送系統的問題包括開發用於數位內容電子式配送、權利管理、及資產保護之系統。以電子方式配送的數位內容包括諸如印刷媒體、電影、電玩、程式、電視、多媒體、及音樂等內容。

五、發明說明（ 4 ）

部署一電子式配送系統時，使數位內容提供者能夠經由立即的銷售回報及電子式對帳而迅速得到付款，並經由內容的重新發行而得到第二份的收益來源。因爲電子式數位內容配送系統不會受到實體庫存缺貨或退貨的影響，所以數位內容提供者及零售商可以有更低的成本及更高的利潤率。數位內容提供者可協助新的配送通路或強化現有的配送通路以更快的時效分送庫存。可利用電子式配送系統的交易資料來取得與客户購買模式有關的資訊，並用來提供與電子式行銷計畫及促銷有關的立即回饋。爲了達到這些目標，數位內容提供者需要使用一種電子式配送模式，使範圍寬廣的使用者及企業可以取得數位內容，同時確保了數位資產的保護及計費。

諸如即時音訊系統(real audio)、AT&T 的 A2B、Liquid Audio Pro Corp. 的 Liquid Audio Pro、Audio Soft 的 City Music Network、及其他系統等的在市場上可取得的數位內容電子式配送系統提供了經由有擔保及無擔保式電子網路而傳送數位資料。使用有擔保式電子網路時，大幅降低了數位內容提供者將數位資料配送到廣泛的閱聽者之要求。使用諸如網際網路及全球資訊網等無擔保式網路時，可利用加密法而使數位內容安全地送抵使用者。然而，一旦在使用者的機器上將經過加密的數位內容解密時，則使用者易於對該數位內容作未經授權的再度傳播。因此，目前需要一種安全的數位內容電子式配送系統，該系統提供了對數位資產的保護，並確保：縱使在將數位內容配送到消費

五、發明說明（ 5 ）

者及企業之後，也能保護內容提供者的權利。因此，權利管理需要能夠進行安全配送、合約授權、及數位資產使用的控制。

數位內容所有人已減緩接受電子式配送的另一個理由是這些數位內容所有人希望維持及促進現有的配銷通路。大多數內容所有人係經由零售商銷售。在音樂市場中，這些美國的零售商包括Tower Records、Peaches、Blockbuster、Circuit City、及其他的零售商。許多這些零售商都設有網站，可讓網際網路使用者經由網際網路選購，且可以電子郵件寄給使用者供其選購。音樂網站包括@tower、Music Boulevard、及Columbia House。使用電子式配送時，可能使這些零售商店之間無法差異化，且與內容所有人之間無法差異化，尤其在全球資訊網上時更是如此。因此，目前需要對諸如圖片、電玩、音樂、程式、及視訊產品等的電子內容零售商於其經由電子式配送而銷售音樂時提供一種相互之間且與內容所有人之間差異化的方式。

內容所有人準備其數位內容，以便經由諸如電子商店等的配銷網站而進行電子式配送。在網際網路上的各電子商店或經由其他線上服務的各電子商店想要經由其產品線及產品促銷而在相互之間差異化。傳統的商店(亦即類比於電子商店的非電子式且非線上的商店)利用產品促銷、產品業務員、產品樣本、自由退貨政策、及其他促銷計畫，使其與競爭者之間差異化。然而，在內容提供者對數位內容有加上使用條件的線上世界中，電子商店進行差異化的

五、發明說明（ 6 ）

能力可能受到嚴重的限制。此外，縱使可改變使用條件，電子商店也面臨了處理與來自內容提供者的數位內容相關聯的中介資料(metadata)以便用電子方式促銷及銷售產品之困難工作。當電子商店處理中介資料時，需要管理數種需要。第一，電子商店需要自內容提供者接收與數位內容相關聯的中介資料。大部分的時間可能係以加密方式傳送此種中介資料的一部分，因而內容提供者必須建立一種機制，以便將經過加密的內容解密。第二，電子商店可能希望在自內容提供者接收內容之前，或在電子商店接收內容之後，預覽來自內容提供者的內容，以便有助於產品行銷、產品定位、及其他與內容有關的促銷考慮點。第三，電子商店需要提取某些用於諸如圖形及藝人等促銷材料之中介資料。電子商店通常將此種促銷材料直接用於線上促銷。第四，電子商店可能希望修改某些容許的使用條件，以便產生不同的數位內容產品線，而使其與其他電子商店之間有差異化。第五，電子商店可能需要將諸如網址等的某些地址插入中介資料，或改變中介資料中的某些地址，以便使採購者自動向一帳款代收機構付款，而不必向該電子商店付款。第六，電子商店可能需要產生授權許可，以便容許在符合使用條件的情形下使用有著作權的數位內容。例如，該授權許可可能同意對該數位內容進行次數有限制的拷貝。授權許可必須能反映所同意的條款。

有鑑於所有這些要求，爲了處理與數位內容相關的中介資料，許多電子商店撰寫自訂規格的軟體程式，以便處理

五、發明說明（ 7 ）

這些要求。開發這些自訂規格的軟體程式所需的時間、成本、及測試可能是相當多的。因此，目前需要一種對這些要求的解決方案。

數位內容所有人已減緩了接納電子式配送的另一原因是準備用於電子式配送的內容之困難。目前許多內容提供者在其產品目錄中有數千甚至數萬的產品內容。在一音樂市場的實例中，一內容所有人對單一錄音母帶同時有數種不同的格式(例如CD、錄音帶、及MD)不是太奇怪的。此外，一單一格式可能針對一特定的配銷通路，而將一錄音母帶重新製作母帶或重新混音。舉例而言，針對廣播電台播放的混音可能不同於針對舞曲用音軌所作的混音，也可能不同於一般消費者可購得的 CD 之混音。盤點及追蹤這些不同的混音版本可能是相當累贅的。此外，許多錄音母帶所有人經常以各種後續出版系列之方式重新發行舊的錄音，例如以"精選集"之方式，或編排成電影原聲帶及其他出版系列之方式、或其他編排方式重新發行。當以數位方式提供更多的內容時，將內容重新混音並編碼以供電子式配送的需求也成長了。內容所有人經常需要利用舊的錄音格式作為指引，引便選擇正確的錄音母帶，並將這些錄音重新處理及編碼，以便經由電子式配送而發行。想要將其舊的格式用於協助其重新發行舊的錄音以供電子式配送的內容提供者尤其適用上述的情形。內容提供者將搜尋資料庫，以便匹配內容名稱、藝人、及錄音，而設定編碼參數。此種以人工方式搜尋錄音內容目錄資料庫的程序不是

五、發明說明（ 8 ）

沒有缺點的。一種缺點即是需要讓作業人員以人工方式搜尋一資料庫，並適當地設定處理參數。另一種缺點即是作業人員在自一資料庫選擇資料時可能發生抄寫錯誤的機率。因此，目前需要將一種可自動擷取諸如音訊等內容之相關聯的資料及錄音母帶。

內容所有人經由一種稱爲編碼的程序而準備其供電子式配送之數位內容。編碼涉及內容的取得、在該內容係以一種類比格式呈現時對該內容進行的數位化、及對該內容的壓縮。該壓縮程序可讓數位內容以更有效率的方式經由網路傳送並儲存在可記錄媒體，這是因爲傳送或儲存的資料量減少了。然而，壓縮也不是沒有缺點的。大部分的壓縮都涉及某些資訊的失掉，因而被稱爲耗損式壓縮(lossy compression)。內容提供者必須決定採用何種壓縮演算法及所需的壓縮水準。例如，在音樂中，數位內容或歌曲可能視音樂類型的不同而有相當不同的特徵。針對某一類型而選擇的壓縮演算法及壓縮水準可能對另一音樂類型並不是最佳的選擇。內容提供者可能發現壓縮演算法及壓縮水準的某些組合相當適用於諸如古典音樂等的某一音樂類型，但對諸如重金屬音樂等的另一音樂類型就無法得到令人滿意的結果。此外，錄音工程師經常必須對音樂進行等化，執行動態範圍調整，並執行其他的預先處理及處理設定，以便確保所編碼的音樂類型將產生所需的結果。此種固定必須以人工方式設定這些編碼參數之需要，例如針對每一數位內容設定等化位準及動態範圍設定值之需要可能

五、發明說明（ 9 ）

是累贅的。再回到該音樂的例子，一個內容系列涵蓋多種音樂類型的音樂內容提供者將必須以人工方式選擇待編碼的每一首歌曲或每一組歌曲、及所需的編碼參數組合。因此，目前需要一種無須以人工方式選擇編碼處理參數之方式。

壓縮內容的程序可能需要大量專用的計算資源，特別是諸如完整長度的電影等較大內容的項目。壓縮演算法供應商提供與其壓縮技術相關聯的各種取捨及優點。這些取捨包括：壓縮內容所需的時間長度及計算資源；自原始內容得到的壓縮量；播放所需的位元傳輸速率；壓縮後內容之效能品質；以及其他因素。當一編碼程式採用一多媒體檔作爲輸入，並產生一編碼後輸出檔，但並無進程或狀態的過渡期間指示時，採用此種編碼程式時將發生問題。此外，在許多情形中，利用其他的程式來呼叫或管理一個並無進程的過渡期間指示之編碼程式。此時將使呼叫的應用程式無法量度已編碼的內容量爲指定要編碼的完整選擇之百分率。在該呼叫的程式正嘗試安排數個不同的程式立即執行時，上述的情形將發生問題。此外，在已選擇要編碼的內容批次且內容提供者想要決定編碼程序的進度時，前文所述的情形是相當累贅的。因此，目前需要一種可解決這些問題的方式。

數位內容提供者已減緩了採用電子式配送的又一理由爲：其內容缺少針對電子傳送式內容而在使用者裝置上產生數位播放機之標準。內容提供者、電子商店、或電子式

五、發明說明（ 10）

配送鏈中的其他成員可能想要在諸如個人電腦系統、視訊轉換器(set-top boxes)、及手持式裝置等的各種裝置上提供自訂規格的播放機。目前需要一種可在一防篡改環境(亦即一種在一第三者正在播放時可阻止對內容作未經授權的存取之環境)中處理數位內容的解密之一組工具程式。此外，需要一組工具程式使一使用者得以管理一本機數位內容庫，但該組工具程式不讓該使用者存取非其所購買的內容以供使用。

若要得知與保護數位內容的背景有關之進一步資訊，請參閱下列三種來源。AT&T Labs(Florham Park, N.J.) 的 Jack Lacy、James Synder、David Maher所著的"Music on the Internet and the Intellectual Property Protection Problem"，可進入網址 http://www.a2bmusic.com/about/papers/musicipp.htm 於線上閱讀該論文。InterTrust Technologies Corp.(Sunnyvale, CA)的 Olin Sibert、David Bernstein、及 David Van Wie 所著的論文 "Securing the Content, Not the Wire for Information Commerce"中述及一種稱爲DigiBox的密碼保護容器物件，可進入網址 http://www.intertrust.com/architecture/stc.html於線上閱讀該論文。以及一IBM White Paper "Cryptolope Container Technology"，可進入網址 http:///cyptolope.ibm.com/white.htm 於線上閱讀該論文。

發明概述：

目前需要克服上述的各項缺點，並提供一種用於一電子內容傳送系統之多媒體播放機。本發明的一實施例提供了

五、發明說明（ 11）

一種播放已在一系統上壓縮過且利用一第一加密金鑰加密過的數位內容資料之方法。根據該方法，係利用一對應於該第一加密金鑰的第一解密金鑰將至少部分的該內容資料解密。將該解密的內容資料解壓縮，以便產生解壓縮的內容資料，並播放該解壓縮的內容資料。在一較佳方法中，擷取分別儲存在該系統上的一第二解密金鑰之多個區段，且利用該第二解密金鑰將該第一解密金鑰解密。在該等實施例中，可利用該第一解密金鑰將先前利用該第一加密金鑰加密的資料解密，且可利用該第二解密金鑰將先前利用該第二加密金鑰加密的資料解密。此外，在各實施例中，一加密金鑰及其對應的解密金鑰可以是對稱金鑰(亦即相同的金鑰)或一金鑰對(例如一公開金鑰及其對應的私人金鑰)。

本發明的另一實施例提供了一種用來播放已壓縮過且利用一第一加密金鑰加密過的數位內容之數位內容播放機。該數位內容播放機包含：一解密器，用以利用一對應於該第一加密金鑰的第一解密金鑰將至少部分的該內容資料解密；一解壓縮器，用以將該解密的內容資料解壓縮；以及一播放機，用以播放或記錄該解壓縮的內容資料。在一較佳的播放機中，該解密器擷取分別儲存在電腦系統上的一第二解密金鑰之多個區段，且利用該第二解密金鑰將該第一解密金鑰解密。

簡而言之，根據本發明，揭示了一種安全地將資料提供給一使用者的系統之方法及裝置。將資料加密，以便只能

五、發明說明（ 12）

夠利用一資料解密金鑰將該資料解密，其中係利用一第一公開金鑰將該資料解密金鑰加密，且該使用者的系統可存取該加密的資料，該方法包含下列步驟：將該加密的資料解密金鑰傳送到一擁有對應於該第一公開金鑰的一第一私人金鑰之交換所；利用該第一私人金鑰將該資料解密金鑰解密；利用一第二公開金鑰將該資料解密金鑰重新加密；將該重新加密的資料解密金鑰傳送到該使用者的系統，而該使用者的系統擁有一對應於該第二公開金鑰之第二私人金鑰；以及利用該第二私人金鑰將該重新加密的資料解密金鑰解密。

附圖簡述

圖1是根據本發明的一安全數位內容電子式配送系統概觀之方塊圖。

圖2是根據本發明的一例示安全容器物件(Secure Container；簡稱SC)及相關聯的圖形表示法之方塊圖。

圖3是根據本發明的一安全容器物件(SC)的加密程序概觀之方塊圖。

圖4是根據本發明的一安全容器物件(SC)的解密程序概觀之方塊圖。

圖5是根據本發明的圖1所示安全數位內容配送系統的權利管理架構各層概觀之方塊圖。

圖6是內容配送及授權許可控制於應用於圖5所示授權許可控制層時的一概觀之方塊圖。

圖7示出根據本發明的圖1所示工作流程管理工具程式之

五、發明說明（ 13）

一例示使用者介面。

圖8是對應於根據本發明的圖7所示使用者介面的工作流程管理程式的主要工具程式、元件、及程序之方塊圖。

圖9是根據本發明的圖1所示一電子數位內容商店的主要工具程式、元件、程序之方塊圖。

圖10是根據本發明的圖1所示使用者裝置的主要組件及程序之方塊圖。

圖11是計算根據本發明的內容預先處理及壓縮工具程式的一編碼速率因數的一方法之流程圖。

圖12是自動擷取根據本發明的圖8所示自動中介資料取得工具程式的額外資訊的一方法之流程圖。

圖13是自動設定根據本發明的圖8所示預先處理及壓縮工具程式的預先處理及壓縮參數的一方法之流程圖。

圖14示出根據本發明而將內容下載到一個圖15所示本機內容庫的播放應用程式之使用者介面螢幕。

圖15是在根據本發明的圖9所示使用者裝置上執行的一播放應用程式的主要元件及程序之方塊圖。

圖16示出根據本發明的圖15所示播放應用程式之一例示使用者介面螢幕。

圖17是自動擷取根據本發明的圖8所示自動中介資料取得工具程式的額外資訊的一替代實施例之流程圖。

一實施例之詳細說明

現在提供本發明的一目錄，以便協助讀者迅速找到本實施例中之不同的各節。

五、發明說明（ 14）

I. 安全數位內容電子式配送系統

A. 系統概述

1. 權利管理

2. 量度(Metering)

3. 開放性架構

B. 系統功能組成部分

1. 內容提供者

2. 電子數位內容商店

3. 中間市場夥伴

4. 交換所

5. 使用者裝置

6. 傳輸基礎建設

C. 系統使用

II. 密碼觀念及其在安全數位內容電子式配送系統上的應用

A. 對稱演算法

B. 公共金鑰演算法

C. 數位簽名

D. 數位證明書

E. SC(s)圖形表示法指南

F. 一安全容器物件加密實例

III. 安全數位內容電子式配送系統流程

IV. 權利管理架構模型

A. 架構層功能

B. 功能分割及流程

五、發明說明（ 15）

1. 內容格式化層

2. 內容使用控制層

3. 內容識別層

4. 授權許可控制層

C. 內容配送及授權許可控制

V. 安全容器物件結構

A. 一般性結構

B. 權利管理語言語法及語意

C. 安全容器物件流程及處理概述

D. 中介資料安全容器物件620格式

E. 報價安全容器物件641格式

F. 交易安全容器物件640格式

G. 訂單安全容器物件650格式

H. 授權許可安全容器物件660格式

I. 內容安全容器物件格式

VI. 安全容器物件包封及打開

A. 概述

B. 材料表(Bill Of Material；簡稱BOM)

C. 金鑰說明部份

VII. 交換所

A. 概述

B. 權利管理程序

C. 特定國家參數

D. 稽核記錄及追蹤

五、發明說明（ 16）

E. 結果回報

F. 帳單開立及付款驗證

G. 重新傳輸

VIII. 內容提供者

A. 概述

B. 工作流程管理程式

1. 產品等候動作/資訊程序

2. 新內容要求程序

3. 自動中介資料取得程序

4. 手動式中介資料輸入程序

5. 使用條件程序

6. 受監控的發行程序

7. 中介資料SC(s)產生程序

8. 浮水印程序

9. 預先處理及壓縮程序

10. 內容品質管制程序

11. 加密程序

12. 內容SC(s)產生程序

13. 最後品質保證程序

14. 內容傳播程序

15. 工作流程規則

C. 中介資料同化及輸入工具程式

1. 自動中介資料取得工具程式

2. 手動式中介資料輸入工具程式

五、發明說明（ 17）

3. 使用條件工具程式

4. 中介資料SC(s)之各組成部分

5. 受監控的發行工具程式

D. 內容處理工具程式

1. 浮水印工具程式

2. 預先處理及壓縮工具程式

3. 內容品質管制工具程式

4. 加密工具程式

E. 內容SC(s)產生工具程式

F. 最後品質保證工具程式

G. 內容傳播工具程式

H. 內容促銷網站

I. 內容網站代管(Content Hosting)

1. 代管內容網站

2. 安全數位內容電子式配送系統提供的代管內容網站111

IX. 電子數位內容商店

A. 概述-對多個電子數位內容商店之支援

B. 點對點電子數位內容配送服務

1. 整合要求

2. 內容取得工具程式

3. 交易處理模組

4. 通知介面模組

5. 帳戶對帳工具程式

五、發明說明（ 18）

C. 廣播電子數位內容配送服務

X. 使用者裝置

A. 概述

B. 應用程式安裝

C. 安全容器物件處理器

D. 播放應用程式

1. 概述

2. 使用者介面元件

3. 拷貝/播放管理元件

4. 解密1505、解壓縮1506、及播放元件

5. 資料管理1502及資料庫存取元件

6. 應用程式間通訊元件

7. 其他雜項元件

8. 一般性播放應用程式

I. 安全數位內容電子式配送系統

A. 系統概述

安全數位內容電子式配送系統是一種技術平台，包含將數位內容及與數位內容相關的內容安全地傳送到一使用者用户端裝置並對該等內容進行權利管理所需之之技術、規格、工具程式、及軟體。使用者裝置包含個人電腦系統、視訊轉換器(IRDs)、及網際網路裝置。這些裝置可將該內容拷貝到該內容所有人許可的外部媒體或可攜式消費家電裝置。術語數位內容(Digital Content)或內容(Content)意指以數位格式儲存的資訊及資料，包括：圖片、電影、視訊

五、發明說明（ 19）

節目、音樂、程式、多媒體、及電玩。

該技術平台規定如何準備數位內容、如何經由點對點或廣播基礎建設(例如纜線、網際網路、衛星、及無線電)而安全地配送、如何授權給使用者裝置、以及如何防止未經授權的拷貝或播放。此外，該技術平台之架構可在諸如浮水印、壓縮/編碼、加密、及其他安全演算法等的各種技術隨著時間而有所進展時，整合或移植該等技術。

安全數位內容電子式配送系統之基本組成部分包括：(1)對內容所有人的所有權保護之權利管理；(2)交易計次以便進行立即且精確的報酬給付；以及(3)一種開放性且文件記載詳盡的架構，可讓內容提供者準備內容，並可讓該內容經由多種網路基礎建設而安全配送，以便在任何符合標準的播放機上播放。

1.權利管理

係經由分佈在該系統的各工作組成部分之間的一組功能而實施該安全數位內容電子式配送系統中之權利管理。其主要功能包括：授權許可及控制，使該內容只能被取得一授權許可的得到授權之中間人或最終使用者解碼；以及根據採購或授權許可的條款，例如根據容許拷貝次數、播放次數、或授權許可有效的時間間隔或期限，而對內容的使用進行控制及強制執行。權利管理的次要功能爲起動一裝置，用以識別未經授權的內容拷貝之起源，以便對抗剽竊。

係利用一種交換所(Clearinghouse)實體及安全容器物件(Secure Container；簡稱SC)技術而實施授權許可及控制。

五、發明說明（ 20）

交換所在驗證過已成功完成一授權許可交易之後，即使中間人或最終使用者可以將內容解碼，藉此而提供授權許可。安全容器物件係用來在各系統組成部分之間配送加密的內容及資訊。SC是一種加密的資訊或內容載體，該載體利用加密、數位簽名、及數位證明書，而使電子資訊及內容不會受到未經授權的攔截或修改。該SC亦可驗證數位內容的可信賴性及完整性。這些權利管理功能的優點在於：電子數位內容配送基礎建設並不一定要是安全的或可信賴的。因此，可經由諸如全球資訊網及網際網路等的網路基礎建設而傳輸。這是由於係在安全容器物件內將內容加密，且該內容的儲存及配送係與該內容的解密及使用隔離。只有具有解密金鑰的使用者可將加密的內容解密，且交換所只針對經過授權且適當的使用要求發出解密金鑰。交換所將不批准未知或未經授權者的額外要求、或不符內容所有人設定的內容使用條件的要求。此外，如果在內容的傳輸期間一SC被篡改，則交換所中之軟體決定該SC被篡改或被偽造，並拒絕接受該交易。

係經由在一最終使用者裝置上執行的最終使用者播放應用程式(195)而起動內容使用的控制。該應用程式將一數位碼嵌入每一份的內容，該數位碼規定可容許的拷貝及播放次數。利用數位浮水印技術來產生該數位碼，使其他的最終使用者播放應用程式(195)無法得知該數位碼，並使該數位碼可抗拒更改的嘗試。在一替代實施例中，只是將該數位碼保存爲與內容(113)相關聯的使用條件之一部

五、發明說明（ 21）

分。當在一符合標準的最終使用者裝置中存取數位內容(113)時，最終使用者播放應用程式(195)讀取該浮水印，以便檢查使用限制，並在需要時更新該浮水印。如果對該內容所要求的使用不符使用條件，例如拷貝次數用完了，則最終使用者裝置將不執行該要求。

數位浮水印也提供了識別經過授權的或未經授權的內容拷貝的來源之方式。內容所有人將一起始浮水印嵌入內容中，以便識別內容所有人、指定著作權資訊、規定配送地理區、及加入其他相關的資訊。將一第二浮水印嵌入最終使用者裝置上的內容，以便識別內容購買者(或授權許可)及最終使用者裝置、指定購買或授權許可條件及日期、及加入任何其他相關的資訊。

因爲浮水印變成內容中不可分的一部分，所以不論拷貝是經過授權的或未經授權的，該等內容中都必然載有這些浮水印。因此，不論將內容儲存在何處，也不論內容的來源爲何，數位內容都必然包含與該內容的來源及容許使用有關的資訊。可利用該資訊來對抗內容的非法使用。

2.量度

交換所保留經由該交換所而批准金鑰交換的所有交易之記錄，作爲其權利管理功能的一部分。該記錄可量度授權許可及原始的使用條件。可將該交易記錄以立即或定期之方式回報給諸如內容所有人或內容提供者、零售商、及其他相關夥伴等的各負責方，以便有助於以電子方式進行交易付款的對帳、及其他的用途。

五、發明說明（ 22）

3.開放性架構

該安全數位內容電子式配送系統是一種開放性架構，該架構具有公佈的規格及介面，而有助於廣泛地在是市場中實施並接受該系統，並同時維護內容所有人的權利保護。該系統架構的彈性及開放性亦可使該系統在各種技術、傳輸基礎建設、及裝置進入市場時，能夠隨著時間而有所進展。

該架構在有關內容的本質及其格式方面具有開放性。該架構支援音訊、程式、多媒體、視訊、或其他類型的內容之配送。該內容可以是諸如用於數位音樂的線性PCM等的一原生格式，也可以是經過諸如濾波、壓縮、或預強調/解強調等的額外預先處理或編碼而得到的一格式。該架構對於各種加密及浮水印技術都具有開放性。該架構可以選擇特定的技術以適應不同的內容類型及格式，並可導入或採用新開發出的技術。此種彈性可讓內容提供者在安全數位內容電子式配送系統內選擇及升級其用於資料壓縮、加密、及格式化所用的技術。

該架構也對不同的配送網路及配送模式具有開放性。該架構支援經由低速網際網路連線或高速衛星及纜線網路而進行的內容配送，並可配合點對點或廣播模型。此外，該架構被設計成可在其中包括低成本消費家電裝置的多種裝置上實施最終使用者裝置中之功能。此種裝置可讓內容提供者及零售商經由多種服務類型而將內容提供給中間人或最終使用者，並可讓使用者購買內容或取得內容的授權許可，播放該內容，並將該內容記錄在各種符合標準的播放

五、發明說明（ 23）

裝置。

B.系統功能組成部分

現在請參閱圖1，圖中示出根據本發明的一安全數位內容電子式配送系統100概觀之方塊圖。安全數位內容電子式配送系統100包含數個其中包含一端到端解決方案之業務組成部分，這些業務組成部分包括：內容提供者101或數位內容所有人、電子數位內容商店103、中間市場夥伴(圖中未示出)、交換所105、代管內容網站111、傳輸基礎建設107、及最終使用者裝置109。每一這些業務組成部分都利用到安全數位內容電子式配送系統100的各種組成部分。下文中將對與電子內容113配送有關的這些業務組成部分及系統組成部分作高階的說明。

1.內容提供者101

內容提供者101或內容所有人是原始內容113的所有人、及(或)被授權將獨立內容113作成套件以供進一步配銷之配銷商。內容提供者101可直接利用其權利，或將內容113授權給電子數位內容商店103、或中間市場夥伴(圖中未示出)，且通常回收與電子商務收益相關的內容使用付款。內容提供者101的例子包括Sony、Time-Warner、MTV、IBM、Microsoft、Turner、Fox、及其他內容提供者。

內容提供者101使用作爲安全數位內容電子式配送系統100的一部分而提供之各工具程式，以便準備其內容113及相關的資料以供配送。一工作流程管理程式154安排所要處理的內容113之時程，並在該內容113經過內容113準備

五、發明說明（24）

及套件組成的各步驟時，追蹤該內容113，以便保持優異的品質保證。在整份本文件中，術語中介資料意指與內容113相關的資料，且在本實施例中並不包括內容113本身。舉例而言，某一首歌曲的中介資料可能是歌曲名稱或歌曲的消費點數，但並非該歌曲的錄音。內容113將包含錄音。一中介資料同化及輸入工具程式161係用來自內容提供者資料庫160提取中介資料，或提取內容提供者以一指定格式提供的資料(在一音樂的實例中，爲諸如CD名稱、藝人名稱、歌曲名稱、及CD圖片等內容113之資訊)，並將這些資料組成套件以供電子式配送。也利用中介資料同化及輸入工具程式161來輸入內容113之使用條件。使用條件中的資料可包括拷貝限制規則、批發價、以及任何必要的業務規則。利用一浮水印工具程式來隱藏內容113中用來識別內容所有人、處理日期、及其他相關資料等的資料。在內容113是音訊的一實施例中，利用一音訊預先處理工具程式來調整內容113或其他音訊的動態範圍，及(或)等化內容113，以便得到最佳的壓縮品質，並壓縮到所需的壓縮等級，且將內容113加密。這些工具程式具有適應性，以遵循數位內容壓縮/編碼、加密、及格式化方法在技術上的進展，而讓內容提供者101在市場上出現新的工具程式時，可利用最佳的工具程式。

SC包封工具程式將加密的內容113、數位內容相關資料或中介資料、及加密金鑰包封在各SCs(將於下文中說明之)中，並儲存在一代管內容網站及(或)促銷網站，以供電子

五、發明說明（ 25）

式配送。代管內容網站可設於內容提供者101或設於多個場所，其中包括電子數位內容商店103及中間市場夥伴(圖中未示出)的場所。因爲內容113及金鑰(將於下文中說明之)係在各SCs中加密及包封，所以電子數位內容商店103或人和其他網站代管業者無法在不經過交換所批准且通知內容提供者101的情形下直接存取解密後的內容113。

2.電子數位內容商店103

電子數位內容商店103是經由諸如以內容113爲主題的銷售計畫或內容113的電子式促銷等多種服務或應用而行銷內容113之實體。電子數位內容商店103管理其服務的設計、開發、業務運作、結帳、促銷、及銷售。線上電子數位內容商店103的例子爲提供軟體的電子式下載之網站。

電子數位內容商店103在其服務的範圍內，執行了安全數位內容電子式配送系統100的某些功能。電子數位內容商店103集合來自內容提供者101之資訊，將內容及中介資料包封在額外的SCs中，並將這些SCs傳送到消費者或企業，作爲一服務或應用的一部分。電子數位內容商店103利用安全數位內容電子式配送系統100提供的工具程式，而協助其完成下列事項：中介資料提取、次要使用條件、SC的包封、及電子內容交易的追蹤。該次要使用條件資料可包括諸如內容113購買價格、計次付費價格、複製授權及目標裝置類型、或可用時間限制等的零售業務報價資料。

一旦一電子數位內容商店103完成一最終使用者對電子

五、發明說明（ 26）

內容113的一有效要求之後，該電子數位內容商店103即負責授權交換所105將內容113的解密金鑰發給該客户。該電子數位內容商店也授權包含內容113的SC之下載。該電子數位內容商店可選擇將包含數位內容的各SCs放在其本身的網站，及(或)可選擇利用另一代管內容網站的網站代管及配送設施。

電子數位內容商店可利用安全數位內容電子式配送系統100而針對最終使用者可能提出的疑問或問題提供客户服務，電子數位內容商店103也可將其客户服務支援外包給交換所105。

3.中間市場夥伴(圖中未示出)

在一替代實施例中，可利用安全數位內容電子式配送系統100將內容113提供給被稱爲中間市場夥伴的其他企業。這些夥伴可包括提供非電子服務的數位內容相關公司，例如配銷內容113的電視台或視訊俱樂部、電台或唱片俱樂部等。這些夥伴亦可包括諸如錄音室、複製公司、製作人等處理材料作爲錄音製作或行銷一部分的其他受託者。這些中間市場夥伴需要交換所105的批准，以便將內容113解密。

4.交換所105

交換所105對與在一SC中加密的內容113的銷售及(或)容許使用提供授權許可及記錄保存。當交換所105自一中間人或最終使用者接收到一個對內容113的一解密金鑰之要求時，交換所105即確認所要求資訊的完整性及可信賴

五、發明說明（ 27）

性；驗證一電子數位內容商店或內容提供者101已授權該要求；以及驗證所要求的使用符合內容提供者101所規定的內容使用條件。一旦滿足這些驗證之後，交換所105即將包封在一授權許可SC的內容113解密金鑰傳送到提出要求的最終使用者。該金鑰被加密成只有經過授權的使用者才能擷取該金鑰。如果最終使用者的要求是無法驗證的、不完整的、或未經授權的，則交換所105拒絕對解密金鑰的要求。

交換所105保存所有交易的記錄，並可以立即、定期、或侷限某些交易之方式將這些記錄回報給諸如電子數位內容商店103及內容提供者101等各負責方。此種回報是一種可將內容113的銷售資訊通知內容提供者101且電子數位內容商店103可得到以電子方式配送到其客户的稽核報告之一種方式。如果交換所105偵測到一SC中的資訊已洩漏出去或不符內容使用條件，則交換所105亦可通知內容提供者101及(或)電子數位內容商店103。係針對資料收集儲存及報告產生，而設計交換所105資料庫的交易記錄及儲存能力。

在另一實施例中，交換所105可提供客户支援及交易例外狀況的處理，例如退款、傳輸失敗、及購買爭端。交換所105可以一獨立實體之方式運作，而作爲權利管理及量度之一受託管理人。交換所於需要時也提供開立帳單及結算的服務。電子交換所的例子包括Secure-Bank.com、及由Visa/Mastercard所成立的安全電子交易(Secure Electronic

五、發明說明（ 28）

Transaction；簡稱SET)。在一實施例中，交換所105是最終使用者裝置109可連線到的網站。在另一實施例中，交換所105是電子數位內容商店103的一部分。

5.最終使用者裝置109

最終使用者裝置109可以是包含符合安全數位內容電子式配送系統100規格的一最終使用者播放應用程式195(將於下文中說明之)之任何播放裝置。些裝置包括個人電腦系統、視訊轉換器(IRDs)、及網際網路裝置。可在軟體及(或)消費電子裝置硬體中實施最終使用者播放應用程式195。除了執行播放、記錄、及內容庫管理功能以外，最終使用者播放應用程式195也執行SC處理，而起動最終使用者裝置109中之權利管理。最終使用者裝置109管理包含數位內容的各SCs之下載及儲存；要求並管理自交換所105接收經過加密的數位內容金鑰；處理每次拷貝或播放數位內容時的浮水印；根據數位內容的使用條件而管理所作拷貝(或刪除拷貝)的次數；以及在容許時執行拷貝到一外部媒體或可攜式消費電子裝置。該可攜式消費電子裝置可執行一部分的最終使用者播放應用程式195功能，以便處理浮水印中嵌入的內容使用條件。在本文全文中，術語最終使用者及最終使用者裝置係用來意指在一最終使用者裝置109上的使用或執行。

6.傳輸基礎建設107

安全數位內容電子式配送系統100與連接電子數位內容商店103及最終使用者裝置109的傳輸網路無關。安全數位

五、發明說明（29）

內容電子式配送系統100支援諸如網際網路等點對點配送模式、及諸如數位廣播電視等廣播配送模式。

縱然使用相同的工具程式及應用程式來取得、包封、及追蹤經由各種傳輸基礎建設107的內容113交易，但是可根據所選擇的基礎建設及配送模式，而改變將服務提供給客戶的表現方式及方法。所傳輸內容113的品質可能也有所不同，這是因爲高頻寬的傳輸基礎建設能夠以比較低頻寬的傳輸基礎建設更可接受的回應時間傳輸高品質的數位內容。可調整針對一點對點配送模式而設計的服務應用程式，以便也可支援一廣播配送模式。

C.系統使用

安全數位內容電子式配送系統100可安全地將高品質的電子式內容113傳送到消費者或企業的最終使用者裝置109，以便管制及追蹤內容113的使用。

可利用新的及現有的配送通路，而在各種消費者及企業對企業服務中部署安全數位內容電子式配送系統100。每一特定的服務可使用一種不同的金融模式，且可經由安全數位內容電子式配送系統100的各權利管理而執行該金融模式。可利用交換所105的權利管理及最終使用者播放應用程式195的防止拷貝特殊功能，而實施諸如批發或零買、計次付費使用、訂用服務、拷貝/無拷貝限制、或重新配送等模式。

安全數位內容電子式配送系統100可讓電子數位內容商店103及中間市場夥伴於創造用來銷售內容113的服務時，

五、發明說明（31）

位元流密碼(stream cipher)。位元流密碼係一次在單一資料位元上運算。RSA資料安全聲稱：在RC4中，每一輸出位元組需要八到十六個機器運算。

IBM設計了一種稱爲SEAL的快速演算法。SEAL是一種位元流演算法，該演算法使用一可變長度的金鑰，且係針對32位元的處理器而最佳化。SEAL在每個資料位元組中需要大約五個基本的機器指令。如果已將所使用的160位元金鑰預先處理到內部表中，則採用50百萬赫的486 CPU之電腦係以每秒7.2百萬位元組的速率執行SEAL程式碼。

Microsoft在其CryptoAPI文件的概論中報告了加密效能標準檢查程式的結果。在一採用Pentium 120百萬赫CPU且作業系統爲Windows NT 4.0的電腦上執行的一個使用Microsoft的CryptoAPI之應用程式得到了下列的結果。

密碼	金鑰長度	金鑰建立時間	加密速度
DES	56	460	1,138,519
RC2	40	40	286,888
RC4	40	151	2,377,723

B.公共金鑰演算法

在安全數位內容電子式配送系統100中，係利用公共金鑰將各對稱金鑰及其他小資料片段加密。公共金鑰演算法使用兩個金鑰。這兩個金鑰在數學上是相關的，因而利用一個金鑰加密的資料可以利用另一金鑰解密。金鑰的所有人將一個金鑰保密(祕密金鑰(private key))，並公開分送第二金鑰(公共金鑰)。

五、發明說明（32）

爲了確保一個利用公共金鑰演算法的機密訊息的安全性，必須使用接收者的公共金鑰將該訊息加密。只有擁有相關聯的祕密金鑰的接收者可將該訊息解密。也利用公共金鑰演算法來產生數位簽名。祕密金鑰係用於此種用途。下節將提供與數位簽名有關的資訊。

最常用的公共金鑰演算法是RSA公共金鑰密碼。RSA公共金鑰密碼已成爲業界中公共金鑰事實上的標準。在加密及數位簽名上也相當好用的其他演算法包括ElGamal及Rabin。RSA是一種可變金鑰長度的密碼。

對稱金鑰演算法比公共金鑰演算法快速許多。在軟體中，DES的速度大致爲RSA的至少100倍。因此，並不將RSA用來將大量的資料加密。RSA資料安全報告在一使用90百萬赫Pentium CPU的機器上，RSA資料安全的工具程式套件BSAFE 3.0在祕密金鑰運算(利用祕密金鑰進行的加密或解密)中具有下列的產生速率：在512位元模數下爲每秒21.6千位元，而在1024位元模數下爲每秒7.4千位元。

C.數位簽名

在安全數位內容電子式配送系統100中，SC(s)的發出者在該SC(s)上數位方式簽名，而保護SC(s)的完整性。一般而言，爲了產生一訊息的數位簽名，一訊息所有人首先計算訊息摘要(將於下文中說明之)，然後利用該所有人的祕密金鑰將該訊息摘要加密。將該訊息連同其簽名而配送。該訊息的任何接收者可首先可利用該訊息所有人的公共金鑰將該簽名解密，以便恢復該訊息摘要，而驗證數位簽

五、發明說明（ 33 ）

名。該接收者然後計算所接收訊息的摘要，並將該摘要與所恢復的摘要比較。如果在配送的過程中，該訊息並未被改變，則所計算的摘要與所恢復的摘要必須相同。

在安全數位內容電子式配送系統100中，因爲SC(s)包含數個資料部分，所以爲每一部分計算一摘要，且爲該等序連部分的摘要計算一總結摘要。係利用該SC(s)發出者的祕密金鑰將該總結摘要加密。經過加密的總結摘要即是該發出者的SC(s)數位簽名。各部分摘要及該數位簽名係包含在SC(s)的本體中。SC(s)的接收者利用所接收的數位簽名及部分摘要，而驗證該SC(s)及其各組成部分之完整性。

利用一種單向雜亂演算法(hash algorithm)計算一訊息摘要。一雜亂演算法取得一可變長度的輸入訊息，並將該輸入訊息轉換成一固定長度的字串，亦即訊息摘要。單向雜亂演算法只在一個方向上運算。亦即，易於計算一輸入訊息的摘要，但是非常難以(計算上的不可行)自其摘要產生輸入訊息。因爲該單向雜亂函數的特性，我們可將一訊息摘要視爲該訊息的指紋。

最常見的單向雜亂函數是來自RSA資料安全的MD5、及美國國家技術及標準協會(National Institute of Technology and Standards；簡稱NITS)設計的SHA。

D.數位證明書

數位證明書係用來證明或驗證已傳送一經數位簽名的訊息的人員或實體之身分。證明書是一種由一將一公共金鑰與一人員或實體結合的認證中心(certification authority)發

五、發明說明（ 34 ）

出的數位文件。該證明書包括公共金鑰、人員或實體的名稱、到期日、認證中心的名稱、及其他資訊。該證明書也包含該認證中心之數位簽名。

當一實體(或人員)傳送一份以其公共金鑰簽署並伴隨有其數位證明書之訊息時，訊息的接收者利用來自該證明書的實體名稱來決定是否要接受該訊息。

在安全數位內容電子式配送系統100中，除了最終使用者裝置109發出的以外的每一SC(s)都包含該SC(s)的產生者之證明書。因爲許多最終使用者並不需要取得一證明書或握有由非眞實認證中心所發出的證明書，所以最終使用者裝置109並不需要將證明書包含在其SC(s)中。在安全數位內容電子式配送系統100中，交換所105可選擇將證明書發出到電子數位內容商店103。因而可讓最終使用者裝置109獨立驗證安全數位內容電子式配送系統100已授權電子數位內容商店103。

E.SC(s)圖形表示法指南

本文件使用圖示而以圖形來代表SC(s)，圖中示出加密部分、非加密部分、加密金鑰、及證明書。現在請參閱圖2，該圖示出SC(s) 200的一例示圖示。下列符號係用於SC(s)的圖示。金鑰201是一公共金鑰或祕密金鑰。諸如交換所CLRNGH的金鑰之齒孔指示該金鑰之所有人。鑰把內的PB指示該金鑰是一公共金鑰，因而該金鑰201是一交換所的公共金鑰。鑰把內的PV指示該金鑰是一祕密金鑰。菱形是一最終使用者數位簽名202。首字指示該祕密金鑰

五、發明說明（35）

係用來產生簽名，因而EU係指示如下表所示的最終使用者之數位簽名。對稱金鑰203係用來將內容加密。一加密對稱金鑰物件204包含一個以一CLRNGH的PB加密的對稱金鑰203。長方形上方邊界的金鑰是用來將物件加密的之金鑰。該長方形之內的符號或文字指示該加密物件(在該例中爲一對稱金鑰)。圖中示出另一加密物件，該加密物件在此實例中爲一交易識別碼加密物件205。內容授權管理的使用條件206將於下文中說明。SC(s) 200包含以一最終使用者數位簽名202簽名的若干使用條件206、交易識別碼加密物件205、一應用程式識別碼加密物件207、以及加密對稱金鑰物件204。

下表示出用來識別SC(s)的簽名者之首字。

首字	組成部分
CP	內容提供者 101
MS	電子數位內容商店 103
HS	代管內容網站 111
EU	最終使用者裝置 109
CH	交換所 105
CA	認證中心(圖中未示出)

F.一安全容器物件加密實例

下表及圖提供了用來產生資訊並自SC(s)取得資訊的加密及解密程序之一概觀。在該程序概觀中產生及解密的SC(s)是一個一般性SC(s)。該SC(s)並不代表安全數位內容電子式配送系統100中的權利管理所用的任何特定SC(s)類型。該程序包含圖3中針對加密程序而示出之步驟。

圖3所示加密程序之流程

五、發明說明（ 36 ）

步驟　程序

301　傳送者產生一隨機對稱金鑰，並利用該對稱金鑰將內容加密。

302　傳送者利用一雜亂演算法執行該加密的內容，以便產生內容摘要。

303　傳送者利用接收者的公共金鑰將該對稱金鑰加密。PB RECPNT意指接收者的公共金鑰。

304　傳送者利用步驟302所用的相同雜亂演算法執行加密的對稱金鑰，以便產生對稱金鑰摘要。

305　傳送者利用步驟302所用的相同雜亂演算法執行該內容摘要及該對稱金鑰摘要之序連，以便產生SC(s)摘要。

306　傳送者利用該傳送者的祕密金鑰將該SC(s)摘要加密，以便產生該SC(s)之數位簽名。PV SENDER意指該傳送者的祕密金鑰。

307B　傳送者產生一SC(s)檔案，該SC(s)檔案包含加密的內容、加密的對稱金鑰、內容摘要、對稱金鑰摘要、傳送者的證明書、及SC(s)簽名。

307A　傳送者在開始安全的通訊之前，必須先自一認證中心取得證明書。該認證中心將該傳送者的公共金鑰及該傳送者的名稱包含在該證明書中，並在該證明書上簽認。PV CAUTHR意指該認證中心的祕密金鑰。傳送者將SC(s)傳輸到接收者。

圖4所示解密程序之流程

五、發明說明（ 37 ）

步驟　程序

408　接收者接收SC(s)，並準備其各組成部分。

409　接收者利用認證中心的公共金鑰將傳送者證明書中之數位簽名解密，而驗證該數位簽名。如果該證明書的數位簽名是有效的，則接收者自該證明書取得該傳送者的公共金鑰。

410　接收者利用該傳送者的公共金鑰將SC(s)數位簽名解密。因而恢復SC(s)摘要。PB SENDER意指該傳送者的公共金鑰。

411　接收者利用該傳送者用來計算SC(s)摘要的同一雜亂演算法來執行所接收的內容摘要及加密的金鑰摘要之序連。

412　接收者將所計算的SC(s)摘要與自該傳送者數位簽名恢復的SC(s)摘要比較。如果兩者相同，則接收者確認所接收的摘要並未被變更，並繼續進行解密程序。如果兩者不同，則接收者捨棄該SC(s)，並通知該傳送者。

413　接收者利用步驟411中所用的相同雜亂演算法執行加密的對稱金鑰，以便計算對稱金鑰摘要。

414　接收者將所計算的對稱金鑰摘要與該SC(s)中接收的對稱金鑰摘要比較。如果兩者相同，則接收者知道加密的對稱金鑰並未被改變。接收者繼續進行解密程序。如果兩者不同，則接收者捨棄該SC(s)，並通知該傳送者。

五、發明說明（ 38 ）

415 接收者利用步驟411中所用的相同雜亂演算法執行加密的內容，以便計算內容摘要。

416 接收者將所計算的內容摘要與該SC(s)中接收的內容摘要比較。如果兩者相同，則接收者知道加密的內容並未被改變。接收者繼續進行解密程序。如果兩者不同，則接收者捨棄該SC(s)，並通知該傳送者。

417 接收者利用該接收者的祕密金鑰將該加密的對稱金鑰解密。因而恢復該對稱金鑰。PV RECPNT意指該接收者的祕密金鑰。

418 接收者利用對稱金鑰將加密的內容解密，因而恢復該內容。

III. 安全數位內容電子式配送系統流程

安全數位內容電子式配送系統100包含該系統的不同參與者所使用的數個組成部分。這些參與者包括內容提供者101、電子數位內容商店103、經由最終使用者裝置109的最終使用者、及交換所105。一高階系統流程係用來作爲安全數位內容電子式配送系統100的一概觀。當內容流經系統100時，下文所概述的該流程追蹤該內容。此外，該流程概述各參與者使用的步驟，以便進行購買交易，因而將內容113解密及使用。系統流程所作的某些假設包括：

- 這是用於一數位內容服務的系統流程(一個人電腦的點對點介面)。
- 內容提供者101以PCM未壓縮格式(以音樂音訊舉例)傳送音訊數位內容。

五、發明說明（ 39 ）

- 內容提供者101在一符合ODBC的資料庫中設有中介資料，或內容提供者101將資料直接輸入內容資訊處理子系統，或將以規定的ASCII檔案格式提供資料。
- 電子數位內容商店執行金融結算。
- 內容113係放在一單一代管內容網站111。

熟悉本門技術者當可了解，可改變這些假設，以便適應諸如音樂、視訊、及程式等數位內容、以及電子式配送系統廣播的精確本質。

下列流程係示於圖 1 。

步驟　程序

121　內容提供者101提供一未壓縮的PCM音訊檔作爲內容113。將該音訊檔的檔案名稱連同內容提供者101的內容113之特有識別碼輸入工作流程管理程式154。

122　內容資訊處理子系統利用內容提供者101的內容113之特有識別碼、及資料庫映射樣板所提供的資訊，而自內容提供者的資料庫160獲得中介資料。

123　內容提供者101在整個取得及準備程序中，利用工作流程管理工具程式154來指引內容流程。

124　將內容113的使用條件輸入內容資訊處理子系統，且可以人工或自動方式執行上述步驟。該資料包括拷貝限制規則、及需要的任何其他的業務規則。所有的中介資料輸入可以與資料的音訊處理同時發生。

125　利用浮水印工具程式將資料隱藏在內容113中，而內容提供者101必須以該浮水印工具程式來識別該

五、發明說明（40）

內容。不論內容來自何處(此例爲內容提供者101)，也不論內容提供者101指定的任何其他資訊，都可包含浮水印資料。

- 內容處理工具程式125針對所支援的不同壓縮等級，而執行內容113需要的等化、動態範圍調整、及重新抽樣。
- 利用內容處理工具程式125將內容113壓縮成所需的壓縮層級。然後可播放內容113，以便驗證該壓縮產生了所需的內容113品質等級。在必要時，可視需要而多次執行等化、動態範圍調整、壓縮、及播放品質檢查。
- SC包封工具程式利用一對稱金鑰將內容113及一部分的中介資料加密。該工具程式然後利用交換所105的公共金鑰將該金鑰加密，以便產生一加密的對稱金鑰。在不包含內容113的安全性資料的情形下，可將該金鑰傳送到任何場所，這是因爲可將該金鑰解密的唯一實體即是交換所105。

126 SC包封工具程式152然後將加密的對稱金鑰、中介資料、及與內容113有關的其他資訊包封在一中介資料SC中。

127 然後將加密的內容113及中介資料包封到一內容SC。此時完成了對內容113及中介資料的處理。

128 然後利用內容傳播工具程式(圖中未示出)將中介資

五、發明說明（41）

料SC(s)傳送到內容促銷網站156。

129 內容傳播工具程式將內容SC(s)傳送到代管內容網站111。該代管內容網站可設於內容提供者101、交換所105、或代管內容網站專用的一特殊場所。該網站的網址是被加入中介資料SC的中介資料。

130 內容促銷網站156將加入系統100的新內容113通知電子數位內容商店103。

131 電子數位內容商店103然後利用內容取得工具程式下載對應於其想要銷售的內容113之中介資料SCs。

132 電子數位內容商店103將利用該內容取得工具程式自中介資料SC(s)抽取其想要在其網站上促銷內容113的任何資料。在必要時，存取該中介資料的這些部分可以是安全的且要收費的。

133 利用該內容取得工具程式輸入該電子數位內容商店103專用的內容113使用條件。這些使用條件包括在內容113的不同壓縮等級下之零售價格及拷貝/播放限制。

134 SC包封工具程式將電子數位內容商店103專用的使用條件及原始的中介資料SC(s)包封到一報價SC。

135 在更新電子數位內容商店103之後，上網的最終使用者即可購得內容113。

136 當一最終使用者找到其想要購買的內容113時，該最終使用者點選一內容圖像，並將該內容項目加入其購貨車中，而該購貨車是由電子數位內容商店

五、發明說明（42）

103所維護。當該最終使用者完成選購時，該最終使用者將購買要求傳送到電子數位內容商店103以供處理。

137 電子數位內容商店103然後聯繫信用卡清算機構，以便用其目前與信用卡清算機構往來的相同方式要求持有該資金。

138 一旦該電子數位內容商店103自信用卡清算機構接收到傳回的信用卡授權號碼之後，該電子數位內容商店103即將該號碼儲存在一資料庫，並利用SC包封工具程式建立一交易SC。該交易SC包含該最終使用者已購買的內容113之所有報價SCs、一個可追蹤到該電子數位內容商店103之交易識別碼、識別該最終使用者之資訊、壓縮等級、所購買歌曲的使用條件及價格表。

139 然後將該交易SC傳送到最終使用者裝置109。

140 當該交易SC到達最終使用者裝置109時，該交易SC起動最終使用者播放應用程式195，而該最終使用者播放應用程式195則開啓該交易SC，並得知該最終使用者的購買。最終使用者播放應用程式195然後開啓個別的報價SCs，且在一替代實施例中可將一估計下載時間通知該使用者。最終使用者播放應用程式195然後要求該使用者指定其想要下載內容113的時間。

141 最終使用者播放應用程式195將根據最終使用者要

五、發明說明（43）

求的下載時間而醒來，並建立一個包含內容113的加密對稱金鑰、交易識別碼、及最終使用者資訊等資訊的訂單SC，而開始下載程序。

142 然後將該訂單SC傳送到交換所105以供處理。

143 交換所105接收到該訂單SC，開啓該訂單SC，並驗證資料並未被篡改。交換所105確認該最終使用者購買的使用條件。這些使用條件必須符合內容提供者101所規定的使用條件。然後將該資訊記錄在一資料庫。

144 一旦完成了所有的檢查之後，利用交換所105的祕密金鑰將加密的對稱金鑰解密。然後利用該最終使用者的公共金鑰將該對稱金鑰加密。然後利用SC包封工具程式將該新的加密對稱金鑰包封到一授權許可SC。

145 然後將該授權許可SC傳送到該最終使用者。

146 當最終使用者裝置109接收到該授權許可SC時，即將該授權許可SC儲存在記憶體中，直到下載內容SC爲止。

147 最終使用者裝置109要求代管內容網站111傳送對應於該授權許可SC的所購買內容113。

148 內容113被傳送到最終使用者裝置109。於接收到內容113時，最終使用者裝置109利用該對稱金鑰將內容113解密。

IV.權利管理架構模型

五、發明說明（44）

A.架構層功能

圖5是安全數位內容電子式配送系統100的權利管理架構之方塊圖。在架構上，有四層代表安全數位內容電子式配送系統100：授權許可控制層501、內容識別層503、內容使用控制層505、及內容格式化層507。本節中將說明每一層的整體功能目標、及每一層的個別主要功能。每一層的功能係完全獨立於其他各層的功能。在廣義的限制之內，可以類似的功能取代一層中之功能，而不會影響到其他層的功能。一層的輸出顯然需要滿足相鄰層可接受的格式及語意。

授權許可控制層501確保：

- 使數位內容於配送過程中不會受到非法攔截及篡改；
- 內容113係來自一合法的內容所有人，並經由一授權配銷商(例如電子數位內容商店103)而配送；
- 數位內容購買者具有一經適當授權的應用程式；
- 在購買者或最終使用者取得內容113的一份拷貝之前，該購買者先付款給該配銷商；以及
- 保留一份交易記錄以供回報之用。

內容識別層503可驗證著作權及內容購買者之身分。內容的著作權資訊及內容購買者的身分可以對內容113的任何經授權的或未經授權的拷貝進行來源追蹤。因此，內容識別層503提供了一種對抗盜版之方式。

內容使用控制層505確保內容113的拷貝係根據商店使用條件519而用於購買者的裝置。商店使用條件519可指定內

五、發明說明（45）

容113被容許的播放及本機拷貝次數，並可指定是否可將內容113記錄到一外部可攜式裝置。內容使用控制層505中之功能追蹤內容的拷貝/播放使用，並更新拷貝/播放狀態。

內容格式化層507可讓內容113的格式自內容所有人的設施中之原生表示法轉換成一種與安全數位內容電子式配送系統100的服務特殊功能及配送裝置一致的形式。該轉換處理可包括壓縮編碼及其相關聯的預先處理，例如頻率等化及振幅動態範圍調整。對於是音訊的內容113而言，在購買者端上，也需要處理所接收的內容113，以便得到一種適於播放的格式，或傳輸到一可攜式裝置。

B.功能分割及流程

權利管理架構模式係示於圖5，且該圖示出將各架構層對映到構成安全數位內容電子式配送系統100的各工作組成部分、及每一層中的重要功能。

1.內容格式化層507

與內容格式化層507相關聯的一般性功能是在內容提供者101上的內容預先處理502及壓縮511、以及最終使用者裝置109上的內容解碼513及解壓縮515。預先處理的需要及特定功能之例子係如前文所述。利用內容壓縮511來減少內容113的檔案大小及其傳輸時間。適用於內容113類型的任何壓縮演算法及傳輸媒體可用於安全數位內容電子式配送系統100。對於音樂而言，MPEG 1/2/4、Dolby AC-2及AC-3、Sony適應性變換碼(Adaptive Transform Coding；簡稱ATRAC)、及低位元傳輸速率演算法是某些一般使用的

五、發明說明（46）

壓縮演算法。係以壓縮形式將內容113儲存在最終使用者裝置109，以便減少儲存容量的要求。於實際播放時將內容113解壓縮。易於實際播放時執行解碼。於後文中討論到內容使用控制層505時將說明編碼之目的及類型。

2.內容使用控制層505

內容使用控制層505容許對最終使用者裝置109上的內容113使用所施加的條件或限制進行規範及強制執行。這些條件可規定內容113被容許的播放次數、是否容許內容113的後續拷貝、後續拷貝的次數、以及是否可將內容113拷貝到一外部可攜式裝置。內容提供者101設定容許的使用條件517，並將該使用條件517以一SC的形式(請參閱討論授權許可控制層501的該節)傳送到電子數位內容商店103。電子數位內容商店103可增添或縮小使用條件517，只要該使用條件517不使內容提供者101所設定的原始條件失效即可。電子數位內容商店103然後將(一SC中)所有的商店使用條件519傳送到最終使用者裝置109及交換所105。交換所105在授權將內容113釋出到最終使用者裝置109之前，先執行使用條件確認521。

最終使用者裝置109中之內容使用控制層505執行內容使用條件517的強制執行。首先，於接收到內容113拷貝時，最終使用者裝置109中之內容識別層503以一個代表起始拷貝/播放許可的拷貝/播放碼523標示該內容113。播放應用程式195然後在將該內容113儲存在最終使用者裝置109之前，先以密碼方式將內容113編碼。播放應用程式195爲

五、發明說明（47）

每一內容項目產生一編碼金鑰，並將該金鑰加密，且將該金鑰隱藏在最終使用者裝置109中。然後每當最終使用者裝置109存取內容113以便進行拷貝或播放時，最終使用者裝置109在容許將內容113解碼並執行播放或拷貝之前，先驗證該拷貝/播放碼。最終使用者裝置109也適當地更新內容113的原始拷貝中的任何新後續拷貝中的拷貝/播放碼。係在已被壓縮的內容113上執行拷貝/播放編碼。亦即，在嵌入該拷貝/播放碼之前，無須先將內容113解壓縮。

最終使用者裝置109使用一授權許可浮水印527將該拷貝/播放碼嵌入內容113內。只有可識別嵌入演算法及相關聯編碼金鑰的最終使用者播放應用程式195可讀取或修改所嵌入的資料。閱聽人無法看到或無法聽到該資料；亦即，該資料並未對內容113之品質造成可感知的降低。自浮水印經歷過內容處理、資料壓縮、數位至類比及類比至數位轉換、及正常內容處理所導入的信號品質降低的數個步驟以來，浮水印仍然以其中包括類比表示法的任何表示形式而保留在內容113中。在一替代實施例中，並不使用一授權許可浮水印527將該拷貝/播放碼嵌入內容113內，最終使用者播放應用程式195反而使用安全儲存的使用條件519。

3.內容識別層503

作爲內容識別層503的一部分，內容提供者101也使用一授權許可浮水印527將諸如內容識別碼、內容所有人、及其他資訊(例如出版日期及地理配送區)等的資料嵌入內容113中。本發明中將該浮水印稱爲著作權浮水印529。於接

五、發明說明（48）

收到時，最終使用者裝置109將內容113的拷貝加上內容購買者名稱及交易識別碼535(請參閱下文中之授權許可控制層501該節)及諸如授權許可日期及使用條件517等的其他資訊之浮水印。在本發明終將該浮水印稱爲授權許可浮水印。經過授權或未經授權取得的且經過可保有內容品質的音訊處理之任何內容113拷貝都載有著作權浮水印及授權許可浮水印。內容識別層503可嚇阻盜版。

4.授權許可控制層501

授權許可控制層501使內容113不會受到未經授權的攔截，並確保只以個別的方式將內容釋出給一個具有經適當授權的最終使用者裝置109且與一經授權的電子數位內容商店103完成一授權許可購買交易之最終使用者。授權許可控制層501以雙重加密531保護內容113。係利用一個內容提供者101產生的加密對稱金鑰將內容113加密，且係利用交換所的公共金鑰621將該對稱金鑰加密。只有交換所105可在開始時恢復該對稱金鑰。

授權許可控制係將交換所105設計成"受託方"。在授與授權許可要求537的許可(亦即將內容113的對稱金鑰623釋出給最終使用者裝置109)之前，交換所105先驗證：交易541及授權許可543已完成且爲可信的；電子數位內容商店103已自安全數位內容電子式配送系統100取得銷售電子內容113的授權；以及最終使用者繼而一經適當授權的應用程式。稽核/回報545可產生報告，並與安全數位內容電子式配送系統100中經授權的其他各方分享授權許可交易資訊。

五、發明說明（49）

係利用SC處理533實施授權許可控制。利用SC(s)將加密的內容113及資訊配送給各系統作業組成部分(下文中將述及與SC(s)詳細結構有關的更多資訊)。SC是一種使用密碼的資訊載體，該資訊載體使用密碼加密、數位簽名、及數位證明書，使電子資訊及內容113不會受到未經授權的攔截及修改。SC亦可對電子資料進行可信賴性的驗證。

授權許可控制要求內容提供者101、電子數位內容商店103、及交換所105具有自用來鑑定這些組成部分的有聲譽認證中心所發出之眞實加密數位證明書。最終使用者裝置109並不需要具有數位證明書。

C.內容配送及授權許可控制

圖6是內容配送及授權許可控制於應用於圖5所示授權許可控制層時的一概觀之方塊圖。該圖示出電子數位內容商店103、最終使用者裝置109、及交換所105係經由網際網路而互連且在這些組成部分之間使用單向(點對點)傳輸之情形。內容提供者101與電子數位內容商店103間之通訊亦可經由網際網路或其他網路。現在假設最終使用者裝置109與電子數位內容商店103間之內容購買商務交易係基於標準的網際網路全球資訊網協定。作爲全球資訊網型互動的一部分，最終使用者選擇所要購買的內容113，提供個人及金融資訊，並同意購買的條件。電子數位內容商店103可利用諸如安全電子交易(SET)等的協定自一受讓機構取得付款授權。

圖6中也假設電子數位內容商店103根據標準全球資訊網

五、發明說明（ 50 ）

通訊協定而已將最終使用者播放應用程式195下載到一最終使用者裝置109。該架構要求電子數位內容商店103將一特有的應用程式識別碼指定給下載的播放應用程式195，並要求最終使用者裝置109儲存該識別碼，以供爾後的應用程式授權許可驗證(請參閱下文)。

整體授權許可流程開始於內容提供者101。內容提供者101利用一個在當地產生的加密對稱金鑰將內容113加密，並利用交換所105的公共金鑰621將對稱金鑰623加密。在一替代實施例中，並不在當地產生該對稱金鑰，而是將該對稱金鑰自交換所105傳送到內容提供者101。內容提供者101產生一個圍繞加密的內容113之內容SC(s) 630、一個圍繞加密的對稱金鑰623之中介資料SC(s) 620、商店使用條件519、以及與資訊相關聯的其他內容113。每一內容113物件都有一個中介資料SC(s) 620及一個內容SC(s) 630。內容113物件可以是同一首歌的一壓縮等級，或者內容113物件可以是專輯上的每一首歌，或者內容113物件可以是整張專輯。對於每一內容113物件而言，中介資料SC(s) 620亦載有與內容使用控制層505相關聯的商店使用條件519。

在步驟601中，內容提供者101將中介資料SC(s) 620配送到一個或多個電子數位內容商店103，並在步驟602中將內容SC(s) 630配送到一個或多個代管內容網站。每一電子數位內容商店103又產生一報價SC(s) 641。該報價SC(s) 641通常包含與中介資料SC(s) 620相同的許多資訊，其中包括內容提供者101的數位簽名624、及內容提供者101的數位

五、發明說明（51）

證明書(圖中未示出)。如前文所述，電子數位內容商店103可增添或縮小內容提供者101開始時所指定的(由內容使用控制層處理的)商店使用條件519。亦可選擇以內容提供者101的數位簽名624簽認內容SC(s) 630及(或)中介資料SC(s) 620。

在步驟603中完成了最終使用者裝置109與電子數位內容商店103間的內容購買交易之後，電子數位內容商店103在步驟604中產生一交易SC(s) 640，並將該交易SC(s) 640傳送到最終使用者裝置109。該交易SC(s) 640包含一特有交易識別碼535、購買者的名稱(亦即最終使用者)(圖中未示出)、最終使用者裝置109之公共金鑰661、及與所購買的內容113相關聯之報價SC(s) 641。圖6所示之交易資料642代表交易識別碼535及最終使用者名稱(圖中未示出)。係利用交換所105的公共金鑰621將交易資料642加密。亦可選擇利用電子數位內容商店103的一數位簽名643簽認交易SC(s) 640。

在步驟605中，於接收到交易SC(s) 640(及包含在交易SC(s) 640之報價SC(s) 641)，在最終使用者裝置109上執行的最終使用者播放應用程式195利用一訂單SC(s) 650向交換所105要求授權許可。訂單SC(s) 650包含：來自報價SC(s) 641之加密後對稱金鑰623及商店使用條件519、來自交易SC(s) 640之加密後交易資料642、以及來自最終使用者裝置109之加密後應用程式識別碼551。在另一實施例中，係利用最終使用者裝置109之一數位簽名652簽認訂單SC(s) 650。

五、發明說明（52）

自最終使用者裝置109接收到訂單SC(s) 650時，交換所105驗證下列事項：

1. 電子數位內容商店103自安全數位內容電子式配送系統100取得授權(存在於交換所105之資料庫160)；
2. 訂單SC(s) 650並未被變更；
3. 交易資料642及對稱金鑰623是完整的及可信的；
4. 最終使用者裝置109所購買的電子商店使用條件519與內容提供者101設定的使用條件517一致；以及
5. 應用程式識別碼551具有一有效結構，且係由一經過授權的電子數位內容商店103提供該應用程式識別碼551。

如果該驗證是成功的，則在步驟606中交換所105將對稱金鑰623及交易資料642解密，並建立授權許可SC(s) 660，且將該授權許可SC(s) 660傳送到最終使用者裝置109。該授權許可SC(s) 660載有對稱金鑰623及交易資料642，且係利用最終使用者裝置109的公共金鑰661將對稱金鑰623及交易資料642加密。如果任何驗證並未成功，則交換所105拒絕授權給最終使用者裝置109，並通知最終使用者裝置109。交換所105亦立即將該驗證失敗的訊息通知電子數位內容商店103。在一替代實施例中，交換所105以其數位簽名663簽認授權許可SC(s) 660。

在接收到授權許可SC(s) 660之後，最終使用者裝置109將先前自交換所105接收的對稱金鑰623及交易資料642解密，並在步驟607中向一代管內容網站111要求內容SC(s)

五、發明說明（53）

630。在步驟608中內容SC(s) 630到達時，最終使用者裝置109在步驟609中利用對稱金鑰623將內容113解密，並將內容113及交易資料642傳送到其他層，以便進行前文中參照圖5所述的授權許可浮水印嵌入、拷貝/播放編碼、亂序編碼、及進一步的內容113處理。

最後，在步驟610中，交換所105定期將總結交易報告傳送到內容提供者101及電子數位內容商店103，以供稽核及追蹤之用。

V.安全容器物件結構

A.一般性結構

安全容器物件(SC)是一種包含數個組成部分之結構，這些組成部分合而界定了一個單位的內容113、或一交易的一部分，這些組成部分也界定了諸如使用條件、中介資料、及加密方法等相關資訊。SC(s)被設計成使資訊的完整性、完成性、及可信賴性可以被驗證。可將SC(s)中的某些資訊加密，因而只有在取得適當的授權之後，才可存取這些資訊。

SC(s)包含至少一個材料表(Bill Of Materials；簡稱BOM)組成部分，該組成部分具有與SC(s)有關的資訊記錄、及與SC(s)中包含的每一組成部分有關的資訊記錄。針對每一組成部分，利用諸如MD-5等的一雜亂演算法計算一訊息摘要，然後將該訊息摘要包含在該組成部分的BOM記錄中。將該等組成部分的摘要序連在一起，且利用這些摘要計算另一摘要，然後利用產生該SC(s)的實體的祕密金鑰

五、發明說明（54）

將該另一摘要加密，以便產生一數位簽名。接收該SC(s)的各方可利用該數位簽名來驗證所有的摘要，並因而確認該SC(s)及所有該SC(s)的各組成部分之完整性及完成性。

可包含下列資訊作爲BOM中之記錄及每一組成部分之記錄。SC(s)類型決定需要包含哪些記錄：

- SC(s)版本
- SC(s)識別碼
- SC(s)類型(例如報價、訂單、交易、內容、中介資料或促銷、及授權許可)
- SC(s)的發行人
- 產生SC(s)的日期
- SC(s)的到期日
- 交換所的網址
- 用於所包含各組成部分的摘要演算法之描述(系統預設爲MD-5)
- 用於數位簽名加密的演算法之描述(系統預設爲RSA)
- 數位簽名(所包含各組成部分的所有序連摘要之加密後摘要)

SC(s)可包含一個以上的BOM。例如，一報價SC(s) 641包含原始的中介資料SC(s) 620組成部分(其中包括其BOM)、電子數位內容商店103所增添的額外資訊、以及一個新的BOM。中介資料SC(s) 620 BOM之一記錄係包含在報價SC(s) 641之BOM中。該記錄包含中介資料SC(s) 620 BOM的一摘要，該摘要可用來確認中介資料SC(s) 620之完

五、發明說明（ 55 ）

整性，因而亦可利用中介資料SC(s) 620 BOM中儲存的各組成部分摘要值來確認中介資料SC(s) 620中包含的該等組成部分之完整性。中介資料SC(s) 620的各組成部分在爲報價SC(s) 641而產生的該新BOM中並無任何記錄。只有電子數位內容商店103及中介資料SC(s) 620 BOM所增添的各組成部分在該新BOM中有記錄。

SC(s)亦可包含一金鑰描述組成部分。金鑰描述組成部分包含一些記錄，這些記錄包含與該SC(s)中各加密組成部分有關的下列資訊：

- 加密組成部分之名稱。
- 當將該組成部分解密時該組成部分所用的名稱。
- 將該組成部分加密所用的加密演算法。
- 指示用來將該組成部分加密的公共加密金鑰之一金鑰識別碼、或於解密時用來將該加密組成部分解密之一加密的對稱金鑰。
- 用來將該對稱金鑰加密之加密演算法。當該金鑰描述組成部分中之記錄包含一個用來將該加密組成部分加密之加密的對稱金鑰時，才有本欄位。
- 用來將該對稱金鑰加密的該公共加密金鑰之一金鑰識別碼。只有在該金鑰描述組成部分中之記錄包含一加密的對稱金鑰、及用來將該加密部分加密的對稱金鑰之加密演算法識別碼時，才有本欄位。

如果SC(s)並未包含任何加密組成部分，則並無任何金鑰描述組成部分。

五、發明說明（ 56 ）

B.權利管理語言語法及語意

權利管理語言包含若干參數，可將值指定給該等參數，以便在購買內容113之後，規定對一最終使用者於使用內容113時的限制。對內容113使用的限制是使用條件517。每一內容提供者101針對其每一內容113項目規定使用條件517。電子數位內容商店103解譯中介資料SC(s) 620中之使用條件517，並利用該資訊提供其想要對其客户報價的選項，且利用該資訊增添內容113之零售資訊。在一最終使用者選擇所要購買的一內容113項目之後，最終使用者裝置109要求根據商店使用條件519的內容113授權。在交換所105將一授權許可SC(s) 660傳送到該最終使用者之前，交換所105先驗證該商店使用條件。所要求的條件519係與內容提供者101在中介資料SC(s) 620中規定的容許使用條件517一致。

當一最終使用者裝置109接收所購買的內容113時，利用浮水印工具程式將商店使用條件519編碼到該內容113中，或編碼到安全儲存的使用條件519中。在最終使用者裝置109上執行的最終使用者播放應用程式195確保編碼到內容113的商店使用條件519被強制執行。

下列是在內容113是音樂的一實施例中商店使用條件519的一些例子：

- 可將歌曲錄音。
- 可播放歌曲若干次。

C.安全容器物件流程及處理概述

五、發明說明（57）

內容提供者101建立中介資料SC(s) 620，並利用中介資料SC(s) 620來界定諸如歌曲等的內容113。內容113本身並不包含在這些SC(s)中，這是因爲內容113的容量通常對於電子數位內容商店103及最終使用者是太大了，而無法只爲了存取描述性中介資料而有效率地下載容器物件。SC(s)反而包含一個指向內容113的一外部通用資源位標(Uniform Resource Locators；簡稱URL)。SC(s)亦包含：提供與內容113有關的描述性資訊之中介資料、以及在諸如音樂的情形中爲CD封面圖片及(或)在歌曲內容113的情形中爲數位音訊片段之任何其他相關聯之資料。

電子數位內容商店103下載其得到授權的中介資料SC(s) 620，並建立報價SC(s) 641。總之，報價SC(s) 641包含來自中介資料SC(s) 620的某些組成部分及BOM、以及電子數位內容商店103加入的額外資訊。於建立報價 SC(s) 641時，產生該報價SC(s) 641的一個新BOM。電子數位內容商店103也利用中介資料SC(s) 620自這些中介資料提取中介資料資訊，而在其網站上建立HTML網頁，用以將內容113的描述提供給最終使用者，因而最終使用者可能購買內容113。

報價SC(s) 641中由電子數位內容商店103加入的資訊通常是用來縮小在中介資料SC(s) 620中指定的使用條件517之選擇、以及諸如商店的圖形影像檔及商店的網站的網址之促銷資料。中介資料SC(s)620中之一報價SC(s) 641樣板指示：電子數位內容商店103可取代報價SC(s) 641中的哪些資訊；電子數位內容商店103需要哪些額外資訊(在需要

五、發明說明（58）

額外資訊的情形）；以及在嵌入的中介資料SC(s) 620中要保留哪些組成部分。

當一最終使用者決定向一電子數位內容商店103購買內容113時，將報價SC(s) 641包含在一交易SC(s) 640中。電子數位內容商店103建立一交易SC(s) 640，並爲所購買的每一內容113項目包含報價SC(s) 641，且將該交易SC(s) 640傳送到最終使用者裝置109。最終使用者裝置109接收交易SC(s) 640，並確認交易SC(s) 640及所包含報價SC(s) 641之完整性。

最終使用者裝置109爲所購買的內容113項目建立一訂單SC(s) 650。自報價SC(s) 641、交易SC(s) 640、及最終使用者裝置109的組態檔包含資訊。以一次一個之方式將訂單SC(s) 650傳送到交換所105。接收訂單SC(s) 650的交換所105之網址係被包含作爲中介資料SC(s) 620的BOM中之一個記錄，且交換所105之網址又係包含在報價SC(s) 641中。

交換所105驗證並處理訂單SC(s) 650，以便將一授權許可浮水印527及存取所購買內容113所需的所有資訊提供給最終使用者裝置109。交換所105的一個功能即是將來自報價SC(s) 641的浮水印指令解密並將來自內容SC(s) 630的內容113解密所需的對稱金鑰623解密。一個加密的對稱金鑰623記錄實際包含一個以上的實際加密之對稱金鑰623。在執行該加密之前，內容提供者101可先選擇將其名稱附加在實際對稱金鑰623之後。將內容提供者101的名稱連同對稱金鑰623一起加密時，可在安全性上對抗仿冒內容提供者

五、發明說明（ 59 ）

101利用合法SC(s)建立其本身的中介資料SC(s) 620及內容SC(s) 630。交換所105驗證連同對稱金鑰623而加密的內容提供者101名稱符合SC(s)證明書中該內容提供者101的名稱。

如果交換所105需要對浮水印指令進行任何改變，則交換所105將對稱金鑰623解密，然後修改浮水印指令，並利用一個新對稱金鑰623再度將這些浮水印指令加密。然後利用最終使用者裝置109的公共金鑰661重新將該對稱金鑰623加密。交換所105也將SC(s)中的其他對稱金鑰623解密，並利用最終使用者裝置109的公共金鑰661再度將這些對稱金鑰623加密。交換所105建立一個包含新加密的對稱金鑰623及更新後浮水印指令之授權許可SC(s) 660，並回應訂單SC(s) 650，而將該授權許可SC(s) 660傳送到最終使用者裝置109。如果訂單SC(s) 650的處理並未成功地完成，則交換所105將一報告授權程序失敗的HTML網頁或等效資訊送回到最終使用者裝置109。

一授權許可SC(s) 660將存取一內容113項目所需的每一資訊提供給一最終使用者裝置109。最終使用者裝置109向代管內容網站111要求適當的內容SC(s) 630。內容提供者101建立內容SC(s) 630，且內容SC(s) 630包含加密的內容113及中介資料部分。最終使用者播放應用程式195利用來自授權許可SC(s) 660的對稱金鑰623將內容113、中介資料、及浮水印指令解密。然後將浮水印指令附加到內容113，並對內容113進行亂序編碼，且將編碼後的內容113

五、發明說明（ 60 ）

儲存在最終使用者裝置109。

D.中介資料安全容器物件620格式

下表示出包含在一中介資料SC(s) 620的各組成部分。組成部分(Parts)行中的每一欄都是與BOM在一起的SC(s)中包含的各別物件(例外爲以[]字元包圍的組成部分名稱)。BOM存有SC(s)中包含的每一組成部分之一記錄。組成部分存在(Part Exists)行指示該組成部分本身實際上包含在SC(s)中，且摘要(Digest)行指示是否針對該組成部分而計算一訊息摘要。當一SC(s)係包含在其他的SC(s)時(由相關聯的樣板決定)，某些組成部分並不會傳播，但是整個原始的BOM則會傳播。因爲交換所105需要整個BOM來驗證原始SC(s)中之數位簽名，所以才執行上述步驟。

下表的金鑰描述部分行界定SC(s)的金鑰描述部分中包含的記錄。金鑰描述部分中的記錄界定與加密金鑰相關的資訊、以及用來將SC(s)內的組成部分加密或將另一SC(s)內的組成部分加密之演算法。每一記錄包含加密的組成部分名稱、及(在必要時)一個指向另一包含該加密的組成部分的SC(s)之網址。結果名稱(Result Name)行界定被指定給接密後的組成部分之名稱。加密演算法(Encrypt Alg)行界定用來將組成部分加密的加密演算法。金鑰識別碼/加密金鑰(Key Id/Enc Key)行界定用來將組成部分加密的加密金鑰之一識別碼、或用來將組成部分加密的加密對稱金鑰623位元串之一64基編碼。對稱金鑰演算法(Sym Key Alg)行是一可選用的參數，而當前一行是一加密的對稱金鑰623

五、發明說明（61）

時，該參數界定用來將對稱金鑰623加密的加密演算法。對稱金鑰識別碼(Sym Key ID)行是當金鑰識別碼/加密金鑰行是一加密的對稱金鑰623時用來將對稱金鑰623加密的加密金鑰之一識別碼。

組成部分	BOM		金鑰描述部分				
	組成部分存在	摘要	結果名稱	加密演算法	金鑰識別碼/加密金鑰	對稱金鑰演算法	對稱金鑰識別碼
[內容網址]			輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
[中介資料網址]			輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
	SC版本						
	SC識別碼						
	SC類型						
	SC發行人						
	日期						
	到期日						
	交換所網址						
	摘要演算法識別碼						
	數位簽名演算法識別碼						
內容識別碼	是	是					
中介資料	是	是					
使用條件	是	是					
SC樣板	是	是					
浮水印指令	是	是	輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
金鑰描述部分	是	是					
交換所證明書	是	否					
證明書	是	否					
	數位簽名						

下文中將說明用於上述中介資料SC(s)表之術語：

五、發明說明（62）

- [內容網址]-金鑰描述部分中的一記錄中之一參數。這是指向與該中介資料SC(s) 620相關聯的內容SC(s) 630中的加密內容113之一網址。該中介資料SC(s) 620本身並不包含該加密內容113。
- [中介資料網址]-金鑰描述部分中的一記錄中之一參數。這是指向與該中介資料SC(s) 620相關聯的內容SC(s) 630中的加密中介資料之一網址。該中介資料SC(s) 620本身並不包含該加密的中介資料。
- 內容識別碼-界定一個指定給一內容113項目的一特有識別碼之組成部分。如果中介資料SC(s) 620對照到一個以上的內容113項目，則有一個以上的內容識別碼包含在該組成部分中。
- 中介資料-包含與一內容113項目相關的資訊(例如在一歌曲情形中的藝人及CD封面圖片)之組成部分。可以有多個中介資料組成部分，可將某些中介資料組成部分加密。中介資料組成部分的內部結構係取決於內含的中介資料之類型。
- 使用條件-包含用來描述將要對一最終使用者或內容113的使用施加的使用選項、規則、及限制的資訊之組成部分。
- SC(s)樣板-界定用來描述建立報價、訂單、及授權許可SC(s) 660的必要及選用資訊的樣板之組成部分。
- 浮水印指令-一個包含用來在內容113中實施浮水印的加密指令及參數之組成部分。交換所105可修改浮水

五、發明說明（63）

印指令，並將浮水印指令送回到最終使用者裝置109內的授權許可SC(s) 660。金鑰描述部分中有一記錄，用以界定用來將浮水印指令加密的加密演算法、於將浮水印指令解密時所使用的輸出組成部分名稱、用來將浮水印指令加密的加密對稱金鑰623位元串之一64基編碼、用來將對稱金鑰623加密之加密演算法、以及將對稱金鑰623解密所需的公共金鑰之識別碼。

- 交換所證明書-一認證中心或交換所105發出的證明書，該證明書包含交換所105的簽認公共金鑰621。可能有一個以上的證明書，在此種其情形中，係使用一階層式結構，其中最高層的證明書包含用來開啓次一層級證明書之公共金鑰，依此類推，直到到達最低層級的證明書，而該最低層級的證明書包含交換所105之公共金鑰621。
- 證明書-一認證中心或交換所105發出的證明書，該證明書包含產生SC(s)的實體之簽認公共金鑰621。可能有一個以上的證明書，在此種其情形中，係使用一階層式結構，其中最高層的證明書包含用來開啓次一層級證明書之公共金鑰，依此類推，直到到達最低層級的證明書，而該最低層級的證明書包含SC(s)產生者之公共金鑰621。
- SC版本-由SC包封工具程式指定給SC(s)之一版本編號。
- SC識別碼-由產生SC(s)的實體指定給該SC(s)之一特

五、發明說明（64）

有識別碼。

- SC類型-指示SC(s)的類型(例如中介資料、報價、訂單等)。
- SC發行人-指示產生SC(s)之實體。
- 產生日-產生SC(s)的日期。
- 到期日-SC(s)到期且不再有效的日期。
- 交換所網址-最終使用者播放應用程式195應與之互動以便取得存取內容113的適當授權之交換所105位址。
- 摘要演算法識別碼-用來計算各組成部分的摘要的演算法之識別碼。
- 數位簽名演算法識別碼-用來將序連的組成部分摘要之摘要加密之一識別碼。
- 數位簽名-利用產生SC(s)的實體的公共金鑰加密的各序連組成部分摘要之一摘要。
- 輸出部分-當將一加密的組成部分解密時指定給輸出部分之名稱。
- RSA及RC4-用來將對稱金鑰623及資料部分加密的系統預設加密演算法。
- 加密對稱金鑰-於解密時用來將一SC(s)組成部分解密的一加密金鑰位元串之一64基編碼。
- CH公共金鑰-指示交換所105的公共金鑰621係用來將資料加密之一識別碼。

E.報價安全容器物件641格式

下表示出包含在報價SC(s) 641的各組成部分。除了某些

五、發明說明（ 65 ）

中介資料組成部分以外的各組成部分、以及來自中介資料SC(s) 620之BOM亦係包含在報價SC(s) 641中。

組成部分	BOM 組成部分存在	摘要	金鑰描述部分 結果名稱	加密演算法	金鑰識別碼/加密金鑰	對稱金鑰演算法	對稱金鑰識別碼
[內容網址]			輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
[中介資料網址]			輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
	SC版本						
	SC識別碼						
	SC類型						
	SC發行人						
	日期						
	到期日						
	交換所網址						
	摘要演算法識別碼						
	數位簽名演算法識別碼						
內容識別碼	是	是					
中介資料	有些	是					
使用條件	是	是					
SC樣板	是	是					
浮水印指令	是	是	輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
金鑰描述部分	是	是					
交換所證明書	是	否					
證明書	是	否					
	數位簽名						

報價SC組成部分

	SC版本	
	SC識別碼	
	SC類型	
	SC發行人	
	日期	
	到期日	
	摘要演算法識別碼	
	數位簽名演算法識別碼	
中介資料SCBOM	是	是
額外及取代的欄位	是	是
電子數位內容	是	是
商店證明書	是	是
	數位簽名	

（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（66）

下文將說明一些用於上文所述報價SC(s) 641但先前並未在另一SC(s)中說明的術語：

- 中介資料SC(s) BOM-來自原始中介資料SC(s) 620之BOM。報價SC(s) 641 BOM包含中介資料SC(s) 620 BOM之摘要。
- 額外及取代的欄位-被電子數位內容商店103取代的使用條件資訊。交換所105利用所接收的SC(s)樣板確認該資訊，以便確定電子數位內容商店103所取代的任何使用條件是在其授權的範圍內。
- 電子數位內容商店證明書-交換所105利用其祕密金鑰簽名並提供給電子數位內容商店103的證明書。最終使用者播放應用程式195利用該證明書驗證電子數位內容商店103是內容113的一合法配銷商。最終使用者播放應用程式195及交換所105可利用交換所105的公共金鑰621將該證明書的簽名解密，而驗證電子數位內容商店103是一授權配銷商。最終使用者播放應用程式195在本機保留一份其於安裝時所接收作爲起始設定的一部分之交換所105公共金鑰621。

F.交易安全容器物件640格式

下表示出包含在交易SC(s) 640中的各組成部分、以及其BOM與金鑰描述部分。

五、發明說明（67）

組成部分	BOM 組成部分存在	摘要	金鑰描述部分 結果名稱	加密演算法	金鑰識別碼/加密金鑰	對稱金鑰演算法	對稱金鑰識別碼
	SC版本						
	SC識別碼						
	SC類型						
	SC發行人						
	日期						
	到期日						
	摘要演算法識別碼						
	數位簽名演算法識別碼						
交易識別碼	是	是	輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
最終使用者識別碼	是	是	輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
最終使用者公共金鑰	是	是					
報價SC(s)	是	是					
內容使用之選擇	是	是					
顯示之HTML	是	是					
金鑰描述部分	是	是					
電子數位內容商店證明書	是	否					
	數位簽名						

下文將說明一些用於上文所述交易SC(s) 640但先前並未在另一SC(s)中說明的術語：

- 交易識別碼535-被電子數位內容商店103指定而唯一識別交易之一識別碼。
- 最終使用者識別碼-最終使用者於進行購買選擇並提供信用卡資訊時電子數位內容商店103所取得的最終使用者指示碼。
- 最終使用者之公共金鑰-交換所105用來將對稱金鑰623重新加密的最終使用者之公共金鑰661。於購買交易時，最終使用者的公共金鑰661被傳送到電子數位內容商店103。
- 報價SC(s)-所購買的內容113項目之報價SC(s) 641。
- 內容使用之選擇-最終使用者所購買的每一內容113項

五、發明說明（ 68 ）

目之一使用條件陣列。

- 要顯示的HTML-於接收到交易SC(s) 640時或在最終使用者裝置109與交換所105進行互動時最終使用者播放應用程式195在網際網路瀏覽器視窗中顯示的一個或多個HTML網頁。

當最終使用者裝置109接收一交易SC(s) 640時，可執行下列步驟，以便驗證SC(s)之完整性及可信賴性：

1. 利用交換所105之公共金鑰621驗證電子數位內容商店103證明書之完整性。在接收到交換所105的公共金鑰621作爲最終使用者播放應用程式195的安裝程序時起始設定的一部分之後，將該公共金鑰621儲存在最終使用者裝置109。
2. 利用來自電子數位內容商店103證明書的公共金鑰來驗證SC(s)之數位簽名643。
3. 驗證該SC(s)各組成部分的雜亂函數。
4. 驗證交易SC(s) 640中包含的每一報價SC(s) 641之完整性及可信賴性。

G.訂單安全容器物件650格式

下表示出包含在訂單SC(s) 650中的各組成部分、以及其BOM與金鑰描述部分。這些組成部分將資訊提供給交換所105，以供解密及驗證之用，或由交換所105確認這些組成部分。這些組成部分及來自報價SC(s) 641之BOM亦係包含在訂單SC(s) 650。中介資料SC(s) BOM的組成部分存在行中之某些字串指示該等組成部分中之某些組成部分並未包

五、發明說明（ 69 ）

含在訂單SC(s) 650。亦可在不作任何改變的情形下包含來自中介資料SC(s) 620之BOM，因而交換所105可確認中介資料SC(s) 620及其各組成部分之完整性。

組成部分	BOM 組成部分存在	摘要	金鑰描述部分 結果名稱	加密演算法	金鑰識別碼/加密金鑰	對稱金鑰演算法	對稱金鑰識別碼
中介資料SC(s)組成部分							
[內容網址]			輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
[中介資料網址]			輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
	SC(s)版本						
	SC(s)識別碼						
	SC(s)類型						
	SC(s)發行人						
	日期						
	到期日						
	交換所網址						
	摘要演算法識別碼						
	數位簽名演算法識別碼						
內容識別碼	是	是					
中介資料	有些	是					
使用條件	是	是					
SC(s)樣板	是	是					
浮水印指令	是	是	輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
金鑰描述部分	是	是					
交換所證明書	是	否					
證明書	是	否					
	數位簽名						
報價SC(s)組成部分							
	SC(s)版本						
	SC(s)識別碼						
	SC(s)類型						
	SC(s)發行人						
	日期						
	到期日						
	摘要演算法識別碼						
	數位簽名演算法識別碼						
中介資料SC(s)BOM	是	是					
額外及取代的欄位	是	是					
電子數位內容商店證明書	是	否					
證明書	是	否					
	數位簽名						

五、發明說明（ 70 ）

交易 SC(s)組成部分

	SC(s)版本						
	SC(s)識別碼						
	SC(s)類型						
	SCs()發行人						
	日期						
	到期日						
	摘要演算法識別碼						
	數位簽名演算法識別碼						
交易識別碼	是	是	輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
最終使用者識別碼	是	是	輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
最終使用者公共金鑰	是	是					
報價 SC(s)	一個報價 SC(s)	是					
內容使用之選擇	是	是					
在瀏覽器視窗中顯示之 HTML	是	是					
金鑰描述部分	是	是					
電子數位內容商店證明書	是	是					
	數位簽名						

訂單 SC(s)組成部分

	SC(s)版本				
	SC(s)識別碼				
	SC(s)類型				
	SCs()發行人				
	日期				
	到期日				
	摘要演算法識別碼				
	數位簽名演算法識別碼				
報價 SC(s) BOM	是	是			
交易 SC(s) BOM	是	是			
加密信用卡資訊	是	是	輸出部份	RSA	CH公共金鑰
金鑰描述部分	是	是			
	數位簽名				

下文將說明一些用於上文所述訂單SC(s) 650但先前並未在另一SC(s)中說明的術語：

- 交易 SC(s) BOM-原始交易 SC(s) 640 中之 BOM。訂單 SC(s) 650 BOM 包含交易 SC(s) 640 BOM 的摘要。
- 加密信用卡資訊-用來將購買金額記帳到一信用卡或借方卡的最終使用者之選用加密資訊。當產生報價 SC(s) 641 的電子數位內容商店 103 並不處理向客戶開

五、發明說明（71）

立帳單時，需要該資訊，在此種情形中，交換所105可處理向客户開立帳單。

H.授權許可安全容器物件660格式

下表示出包含在授權許可SC(s) 660之各組成部分、及其BOM。如金鑰描述部分所示，交換所105已利用最終使用者的公共金鑰661將浮水印指令解密所需的對稱金鑰623、內容113、及內容113中介資料重新加密。當最終使用者裝置109接收到授權許可SC(s) 660時，最終使用者裝置109將對稱金鑰623解密，並利用解密後的對稱金鑰623存取授權許可SC(s) 660及內容SC(s) 630之各加密組成部分。

組成部分	BOM 組成部分存在	摘要	金鑰描述部分 結果名稱	加密演算法	金鑰識別碼/加密金鑰	對稱金鑰演算法	對稱金鑰識別碼
[內容網址]			輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
[中介資料網址]			輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
	SC(s)版本						
	SC(s)識別碼						
	SC(s)類型						
	SC(s)發行人						
	日期						
	到期日						
	摘要演算法識別碼						
	數位簽名演算法識別碼						
內容識別碼	是	是					
使用條件	是	是					
交易資料	是	是					
浮水印指令	是	是	輸出部分	RC4	加密對稱金鑰	RSA	CH公共金鑰
金鑰描述部分	是	是					
證明書	是	否					
	數位簽名						

下文將說明一些用於上文所述授權許可SC(s) 660但先前並未在另一SC(s)中說明的術語：

- 最終使用者公共金鑰-指示最終使用者的公共金鑰661係用來將資料加密之一識別碼。

五、發明說明（72）

- 訂單SC(s) 650識別碼-自訂單SC(s) 650 BOM取得的SC(s)識別碼。
- 證明書廢止清單-先前由交換所105發出並簽名但目前不再有效的證明書識別碼之一可選用清單。具有一個廢止清單中包含的一證明書可驗證的簽名之任何SC(s)都是無效的SC(s)。最終使用者播放應用程式195將一份交換所105的證明書廢止清單儲存在最終使用者裝置109。當接收到一廢止清單時，如果新的廢止清單是更新的版本時，則最終使用者播放應用程式195以該更新的版本取代其本機的拷貝。廢止清單包含一版本編號或一時戳(或以上兩者)，以便決定哪一份清單是最新的。

I.內容安全容器物件格式

下表示出包含在內容SC(s) 630中的各組成部分、及BOM：

組成部分	BOM 組成部分存在	摘要
[內容網址]		
[中介資料網址]		
	SC(s)版本	
	SC(s)識別碼	
	SC(s)類型	
	SC(s)發行人	
	日期	
	到期日	
	交換所105網址	
	摘要演算法識別碼	
	數位簽名演算法識別碼	
內容識別碼	是	是
加密的內容	是	是
加密的中介資料	是	是
中介資料	是	是
證明書	是	否
	數位簽名	

五、發明說明（ 73 ）

下文將說明一些用於上文所述內容SC(s) 630但先前並未在另一SC(s)中說明的術語：

- 加密的內容-一內容提供者101利用一對稱金鑰623加密的內容113。
- 加密的中介資料-與內容113相關聯且係由一內容提供者101利用一對稱金鑰623加密的中介資料。

內容SC(s) 630中並未包含任何金鑰描述部分，這是因爲將加密的組成部分解密的金鑰是在交換所105上建立的授權許可SC(s) 660中。

VI. 安全容器物件的包封及打開

A. 概述

SC(s)包封工具程式是一個具有一應用程式介面(Application Programming Interface；簡稱API)的32位元Windows程式，可在多個或單一程序步驟中呼叫該程式，以便產生一個具有所有指定組成部分之SC(s)。SC(s)包封工具程式151、152、153可在各種硬體平台上支援內容提供者101、交換所105、電子數位內容商店103、及需要SC(s)包封的其他網站上支援Windows程式。一BOM及一或有的金鑰描述部分被產生，並被包含在SC(s)中。一組包封工具程式API可讓呼叫的程式指定所需的資訊，以便產生BOM及金鑰描述部分中之記錄，並將各組成部分包含在SC(s)中。也是由包封工具程式執行各組成部分及對稱金鑰623之加密、以及各摘要及數位簽名之計算。包封工具程式所支援的加密演算法及摘要演算法係包含在包封工具

五、發明說明（74）

程式碼中，或係經由一外部介面而呼叫該加密演算法及摘要演算法。

一API執行用來建立一SC(s)的包封工具程式介面，而該API接受下列參數作爲輸入：

- 各序連結構的一緩衝區之一指標。該緩衝區中的每一結構是對該包封工具程式的一命令、及執行該命令所需的資訊。包封工具程式命令包括：將一組成部分加入具有一相關聯的BOM記錄之SC(s)、將一記錄加入該BOM、以及將記錄加入金鑰描述部分。
- 指示上述緩衝區中包含的序連結構數目之一值。
- BOM組成部分之名稱及位置。
- 每一位元爲供未來使用的一指定旗標或保留旗標之一值。目前界定了下列的旗標：
  - 指示在處理了緩衝區中所有的結構之後是否應將該SC(s)的所有組成部分結合放入單一檔案中。於建立一SC(s)時，將各組成部分結合成單一物件是最後一個步驟。
  - 指示是否在BOM部分中省略了數位簽名。如果該旗標並未被設定，則在將SC(s)結合到一單一物件之前，先計算數位簽名。

在一替代實施例中，若干API執行用來建立一SC(s)的包封工具程式介面，而該等API接受下列參數作爲輸入：

- 首先呼叫一API，以便產生一材料表(BOM)部分，其方式爲傳送一結構之指標，而該結構包含一些用來設定SC(s)起始值的資訊，這些資訊包括SC(s) BOM部

五、發明說明（75）

分中之IP記錄、用於BOM部分的名稱、尋找將被加入的組成部分之一系統預設位置、及一旗標值。該API送回一個用於後續各包封工具程式API之SC(s)識別值(handle)。

- 該包封工具程式具有一個當將一組成部分加入一SC(s)時即使用之API。該API接受一先前包封工具程式API於先前送回的一SC(s)識別值、包含與所加入的組成部分有關的資訊之一結構之一指標、以及一旗標值。與所加入的組成部分有關的資訊包括：該組成部分之名稱及位置、用於該組成部分的BOM之名稱、所加入的該組成部分之類型、該組成部分的一雜亂值、及旗標等。
- 在將所有的組成部分加入該SC(s)之後，呼叫一包封工具程式API，以便將其中包括BOM部分的所有組成部分包封到一單一SC(s)物件中，而該單一SC(s)物件通常是一檔案。該API接受：一先前包封工具程式API於先前送回的一SC(s)識別值、用於經過包封的SC(s)之名稱、一個具有用來簽認該SC(s)的資訊的一結構之指標、以及一旗標值。

包封工具程式或呼叫包封工具程式的實體可利用一SC(s)樣板來建立一SC(s)。SC(s)樣板具有用來指定正在建立的該SC(s)中所需的各組成部分及記錄之資訊。樣板亦可指定用於將對稱金鑰623及各加密組成部分加密的加密方法及金鑰參考位置。

包封工具程式具有一個用來打開一SC(s)之API。打開一

五、發明說明（ 76 ）

SC(s)即是取得一SC(s)並將該SC(s)分開成其個別組成部分之程序。然後可呼叫該包封工具程式，以便將自該SC(s)打開的各加密組成部分解密。

B.材料表(BOM)部分

於建立一SC(s)時，即由包封工具程式產生BOM部分。該BOM是一文字檔，包含與該SC(s)有關的資訊、及與該SC(s)中包含的各組成部分有關之資訊。BOM中的每一記錄是在單一行上，而一新的行則指示一個新的記錄之開始。BOM通常包含：每一組成部分之摘要、以及可用來確認該SC(s)的可信賴性及完整性之一數位簽名。

一BOM內的記錄類型係如下文所示：

IP 一IP記錄包含一組名稱=與SC(s)相關的數值對。下列名稱係保留給SC(s)的一些特性：

V major.minor.fix

V特性指定SC(s)的版本。這是產生SC(s)時所依據的SC(s)規格之版本編號。接續的字串應是major.minor.fix的形式，其中major、minor、及fix分別是主要版本編號、次要版本編號、及修補層級。

ID 值

ID特性是是正在產生該特定SC(s)的實體指定給該SC(s)的一特有值。該文件的一後續版本中將界定該值的格式。

T 值

該T特性指定SC(s)的類型，而此種類型應爲下列所示

五、發明說明（77）

的其中之一：

ORD-一訂單SC(s) 650。

OFF-一報價SC(s) 641。

LIC-一授權許可SC(s) 660。

TRA-一交易SC(s) 640。

MET-一中介資料SC(s) 620。

CON-一內容SC(s) 630。

A值

該A特性識別SC(s)的製作者或發行人。製作者/發行人的身分應是清楚的及(或)登錄到交換所105的。

D 值

該D特性識別SC(s)產生的日期及或有的時間。該值的形式應爲yyyy/mm/dd[@hh:mm[:ss[.fsec]][(TZ)]]，用以代表年/月/日@時/分/秒/十分之一秒(時區)。該值的可選用部分係以[]字元圍住。

E 值

該E特性識別SC(s)終止的日期及或有的時間。該值的形式應與先前所界定的D特性值所用的形式相同。於可能時，應將終止日期/時間與交換所105中存放的日期/時間比較。

CCURL 值

該CCURL特性識別交換所105之網址。該值的形式爲一有效的外部網址。

H 值

五、發明說明（ 78 ）

H特性識別用來計算SC(s)中包含的各組成部分的訊息摘要之演算法。

D　D記錄是一種資料或組成部分資料項記錄，包含用來識別組成部分的類型、組成部分的名稱、組成部分的(或有)摘要、以及該組成部分並未包含在SC(s)的一(或有)指示。在該類型識別碼之後的一負號係用來指示該組成部分並未包含在該SC(s)中。下列是資料或組成部分記錄的保留類型：

K part_name [digest]

指定金鑰描述部分。

C part_name [digest]

指定用來確認數位簽名之證明書。

T part_name [digest]

指定使用條件部分。

YF part_name [digest]

指定報價SC(s) 641的樣板部分。

YO part_name [digest]

指定訂單SC(s) 650的樣板部分。

YL part_name [digest]

指定授權許可SC(s) 660的樣板部分。

ID part_name [digest]

指定被查詢到的內容113項目的內容113之識別碼。

五、發明說明（79）

CH part_name [digest]

指定交換所105證明書部分。

SP part_name [digest]

指定電子數位內容商店103證明書部分。

B part_name [digest]

指定在另一SC(s)的組成部分或組成部分的子集係包含在該SC(s)時該另一SC(s)之一BOM部分。

BP part_name sc_part_name [digest]

指定在另一SC(s)係被包含而作爲該SC(s)的一單一組成部分時該另一SC(s)之一BOM部分。該sc_part_name是包含在該SC(s)中且係由該BOM部分界定的SC(s)組成部分之名稱。與該BOM相同的一BOM亦係包含在由該sc_part_name參數界定的SC(s)中。

D part_name [digest]

指定一資料(或中介資料)部分。

S　S記錄是一個用來界定該SC(s)的數位簽名之一簽名記錄。係亦下文所述方式規定該數位簽名：

S key_identifier signature_string signature_algorithm

該S記錄包含：金鑰識別碼，用以指示該簽名之加密金鑰；簽名位元串，該簽名字串是對數位簽名位元串之64基編碼；以及簽名演算法，用以將摘要加密，以便產生該數位簽名。

C.金鑰描述部分

五、發明說明（ 80 ）

包封工具程式產生金鑰描述部分，以便提供與將加密組成部分解密所需的加密金鑰有關之資訊。可將加密組成部分包含在所建立的該SC(s)中，而加密組成部分也可放在被所建立的SC(s)參照到的其他SC(s)中。金鑰描述部分是一文字檔，包含與加密金鑰及用到加密金鑰的組成部分有關之資訊記錄。金鑰描述部分中的每一記錄是在單行上，而一新行則指示一個新記錄的開始。

下列記錄類型係用於一金鑰描述部分內，且係界定如下：

K encrypted_part_name;result_part_name;part_encryption_algorithm_identifier; public_key_identifier key_encryption_algorithm 及 encrypted_symmetric_key。K記錄指定可包含在該SC(s)中或可包含在該記錄所參照的另一SC(s)中之一加密組成部分。該encrypted_part_name是該SC(s)的一組成部分之名稱、或指向另一SC(s)的加密組成部分之名稱。result_part_name是提供給解密後組成部分之名稱。part_encryption_algorithm_identifier指示用來將該組成部分加密的加密演算法。public_key_identifier是用來將對稱金鑰623加密的金鑰之一識別碼。key_encryption_algorithm_identifier指示用來將對稱金鑰623加密的加密演算法。加密的對稱金鑰是對用來將該組成部分加密的加密對稱金鑰623進行一64基編碼。

五、發明說明（81）

VII.交換所105

A.概述

交換所105負責安全數位內容電子式配送系統100的權利管理功能。交換所105的功能包括：電子數位內容商店103的起動、對內容113權利的驗證、購買交易及相關資訊的完整性及可信賴性確認、將內容加密金鑰或對稱金鑰623配送到最終使用者裝置109、這些金鑰配送的追蹤、以及將交易總結回報到電子數位內容商店103及內容提供者101。最終使用者裝置109利用內容加密金鑰將其通常由一購買交易而自一授權電子數位內容商店103取得權利的內容113解密。在將一內容加密金鑰傳送到一最終使用者裝置109之前，交換所105執行整個驗證程序，以便確認銷售內容113的實體之可信賴性、及最終使用者裝置109對內容113之權利。上述程序要呼叫SC分析工具程式185。在某些組態中，交換所105亦可在其場所代管(co-locating)一個用來執行電子數位內容商店103的信用卡授權及開立帳單功能之系統，而處理內容113的金融結算。交換所105利用諸如ICVerify及Taxware等的OEM套裝軟體來處理信用卡流程及地方營業稅。

電子數位內容商店實施例

一個想要加入安全數位內容電子式配送系統100成爲一內容113經銷商的電子數位內容商店103向提供內容113給安全數位內容電子式配送系統100的一個或多個數位內容提供者101提出要求。只要雙方達成協議，並沒有限定的

五、發明說明（82）

提出要求的程序。在諸如Sony、Time-Warner等音樂內容所有人之數位內容所有人決定讓電子數位內容商店103銷售其內容113時，通常係利用電子郵件聯繫交換所105，要求將該電子數位內容商店103加入安全數位內容電子式配送系統100。數位內容所有人提供電子數位內容商店103的名稱、以及交換所105可能需要用來產生該電子數位內容商店103的數位證明書之任何其他資訊。以一種安全的方式將該數位證明書傳送到該數位內容所有人，該數位內容所有人然後將該數位證明書傳送到該電子數位內容商店103。交換所105維護其已指定的數位證明書之一資料庫。每一證明書包含：一版本編號、一特有序號、簽名演算法、發出者的名稱(交換所105的名稱)、該證明書的有效日期範圍、電子數位內容商店103的名稱、電子數位內容商店103的公共金鑰、以及利用交換所105的祕密金鑰簽認的所有其他資訊之一雜亂碼。具有交換所105的公共金鑰621之各實體可確認該證明書，然後保證一個具有一可利用證明書的公共金鑰確認的簽名之SC(s)是一有效的SC(s)。

在電子數位內容商店103自數位內容所有人接收到交換所105爲其產生的數位證明書、及用來處理SC(s)的必要工具程式之後，即可開始提供最終使用者可購買的內容113之報價。電子數位內容商店103在交易SC(s) 640中加入其證明書，並利用其數位簽名643簽認該SC(s)。最終使用者裝置109首先檢查數位證明書廢止清單，然後利用交換所

五、發明說明（83）

105的公共金鑰621來驗證電子數位內容商店103的數位證明書中之資訊，而驗證該電子數位內容商店103是安全數位內容電子式配送系統100上的內容113之一有效配銷商。交換所105維護一數位證明書廢止清單。可將該廢止清單包含在交換所105產生的一授權許可SC(s) 660中，作爲該SC(s)的一個組成部分。最終使用者裝置109保留一份廢止清單，因而可利用該廢止清單作爲電子數位內容商店103數位證明書確認的一部分。當最終使用者裝置109接收一授權許可SC(s) 660時，即決定該SC(s)中是否包含一新的廢止清單，如果確係如此，則更新最終使用者裝置109上的本機儲存之廢止清單。

B.權利管理程序

報價SC(s)分析

一最終使用者自電子數位內容商店103接收到包含報價SC(s) 641的交易SC(s) 640之後，交換所105自該最終使用者接收一訂單SC(s) 650。訂單SC(s) 650包含：若干包含與內容113及其使用相關的資訊之組成部分、與銷售內容113的電子數位內容商店103有關之資訊、以及與購買內容113的最終使用者有關之資訊。在交換所105開始處理訂單SC(s) 650中的資訊之前，交換所105先執行某些程序，以便確保SC(s)是事實上有效的且並未以任何方式篡改該SC(s)包含的資料。

確認

交換所105驗證數位簽名而開始訂單SC(s) 650的確認，

五、發明說明（84）

交換所105然後驗證訂單SC(s) 650各組成部分的完整性。爲了確認數位簽名，在有簽名的情形下，交換所105首先利用所包含的簽認實體之公共金鑰661將該簽名本身的內容631解密。(該簽認實體可以是內容提供者101、電子數位內容商店103、最終使用者裝置109、或上述各組成部分的任何組合。)交換所105然後計算該SC(s)的各序連組成部分摘要之摘要，並將所計算出的該摘要與該數位簽名的解密後內容113比較。如果這兩個值相符，則該數位簽名是有效的。爲了驗證每一組成部分的完整性，交換所105計算該組成部分的摘要，並將所計算出的該摘要與BOM中的數位值比較。交換所105遵循相同的程序來驗證訂單SC(s) 650內包含的中介資料及報價SC(s) 641部分的數位簽名及組成部分之完整性。

交易及報價SC(s) 641數位簽名的驗證程序也間接地驗證電子數位內容商店103係爲安全數位內容電子式配送系統100所授權。上述程序係基於交換所105是證明書的發出者。此外，交換所105亦可利用電子數位內容商店103的公共金鑰而成功地驗證交易SC(s) 640及報價SC(s) 641之數位簽名，但是只有在簽認該SC(s)的實體具有相關聯的祕密金鑰之所有權時，才能如此進行。請注意，交換所105並不需要設有電子數位內容商店103的本機資料庫，這是因爲該商店係利用交換所的公共金鑰來簽認交易SC(s) 640及報價SC(s) 641之公共金鑰。

交換所105然後確認最終使用者購買的內容113之商店使

五、發明說明（85）

用條件519，以便確保該商店使用條件519係包含在中介資料SC(s) 620中設定的限制之內。如前文所述，中介資料SC(s) 620係包含在訂單SC(s) 650之內。

金鑰處理

在成功地完成訂單SC(s) 650的可信賴性及完整性檢查、電子數位內容商店103的確認、以及商店使用條件519的確認之後，交換所105執行加密後對稱金鑰623及浮水印指令之處理。訂單SC(s) 650的中介資料SC(s) 620部分通常具有數個對稱金鑰623，而這些對稱金鑰623係位於利用交換所105的公共金鑰621加密之金鑰描述部分。於產生中介資料SC(s) 620時，內容提供者101執行對稱金鑰623之加密。

一個對稱金鑰623係用來將浮水印指令解密，且其他的對稱金鑰係用來將內容113及任何加密的中介資料解密。內容113可代表單一首歌曲或一CD上的所有歌曲，所以不同的對稱金鑰623可用於每一首歌曲。浮水印指令係包含在訂單SC(s) 650中的中介資料SC(s) 620部分內。內容113及加密後中介資料是存放在代管內容網站111上的內容SC(s) 630中。內容SC(s) 630內的加密後內容113及中介資料部分之網址及組成部分名稱係包含在訂單SC(s) 650的中介資料SC(s) 620部分之金鑰描述部分。交換所105利用其祕密金鑰將對稱金鑰623解密，然後利用最終使用者裝置109的公共金鑰661將每一該等對稱金鑰加密。係自訂單SC(s) 650擷取最終使用者裝置109之公共金鑰661。新加密的對稱金鑰623係包含在交換所105送回到最終使用者裝置

五、發明說明（86）

109的授權許可SC(s) 660之金鑰描述部分。

在處理對稱金鑰623的這段時間中，交換所105可能想要修改浮水印指令。如果發生此種情形，則在交換所105將對稱金鑰623解密之後，將浮水印指令修改並重新加密。新的浮水印指令被包含在傳送回最終使用者裝置109的授權許可SC(s) 660內，作爲該SC(s)的一個組成部分。

如果授權許可SC(s) 660的所有處理都是成功的，則交換所105將一授權許可SC(s) 660送回到最終使用者裝置109。最終使用者裝置109利用授權許可SC(s) 660資訊下載內容SC(s) 630，並存取加密的內容113及中介資料。最終使用者裝置109亦執行浮水印指令。

如果交換所105無法成功地處理訂單SC(s) 650，則將一HTML網頁送回到最終使用者裝置109，並在網際網路瀏覽器視窗中顯示該HTML網頁。該HTML網頁指示交換所105無法處理該交易的原因。

在一替代實施例中，如果使用者在內容113銷售所設定的發行日之前，已購買了該內容113的一份拷貝，則傳送回不具有對稱金鑰623之授權許可SC(s) 660。在發行日當天或發行日之後，將授權許可SC(s) 660傳送回交換所105，以便接收對稱金鑰623。舉例而言，內容提供者101可讓使用者在一首新歌的發行日之前先下載該首新歌，讓使用者在內容提供者101設定的發行日之前可先下載該歌曲，並準備好播放該歌曲。此種方式可在發行日立即該起內容113，而無須在發行日爲頻寬及下載時間而煩惱。

五、發明說明（87）

C.特定國家參數

交換所105可選擇使用最終使用者裝置109的網域名稱及(或有的)信用卡帳單開立地址來決定最終使用者的國家位置。如果該最終使用者所居住的國家對內容113的銷售有任何限制，則交換所105在將授權許可SC(s) 660傳送到最終使用者裝置109之前，先確保所處理的交易並未違反任何這類限制。也希望電子數位內容商店103執行與交換所105相同的檢查，而加入將內容113配送到各國家的管理。如果電子數位內容商店103並未顧及內容提供者101所設定的特定國家規則，則交換所105執行其所能執行的所有檢查。

D.稽核記錄及追蹤

交換所105針對於內容113購買交易及報告要求交易期間所執行的每一作業維護這些作業的資訊之一稽核記錄150。該資訊可用於諸如安全數位內容電子式配送系統100之稽核、報告的產生、及資料採擷(data mining)等的多種用途。

交換所105也爲電子數位內容商店103維護帳單開立子系統182中的帳户餘額。數位內容所有人將電子數位內容商店103的定價結構提供給交換所105。該資訊可包括電子數位內容商店103必須接受的現行特價、量販折扣、及帳户不足額限制等的資訊。交換所105利用該定價資訊來追蹤電子數位內容商店103的帳户餘額，並確保這些帳户餘額不會超過內容提供者101所設定的不足額限制。

五、發明說明（88）

交換所105通常記錄下列的作業：

- 最終使用者裝置109對授權許可SC(s)660的要求
- 當交換所105處理帳單開立時的信用卡授權號碼
- 將授權許可SC(s) 660傳送到最終使用者裝置109
- 對報告的要求
- 最終使用者通知內容SC(s) 630及授權許可SC(s) 660已接收到且已確認

交換所105通常針對一授權許可SC(s) 660記錄下列資訊：

- 要求的日期及時間
- 購買交易的日期及時間
- 所購買項目之內容識別碼
- 內容提供者101之識別碼
- 商店使用條件519
- 浮水印指令修改
- 電子數位內容商店103所加入的交易識別碼535
- 電子數位內容商店103之識別碼
- 最終使用者裝置109之識別碼
- 最終使用者的信用卡資訊(在交換所105處理帳單開立的情形下)

交換所105通常針對最終使用者信用卡的確認而記錄下列資訊：

- 要求的日期及時間
- 向信用卡收費的金額

五、發明說明（89）

- 所購買項目之內容識別碼
- 電子數位內容商店103所加入的交易識別碼535
- 電子數位內容商店103之識別碼
- 最終使用者之識別碼
- 最終使用者的信用卡資訊
- 自信用卡清算銀行接收的授權號碼

當將一授權許可SC(s) 660傳送到最終使用者裝置109時，交換所105通常記錄下列資訊：

- 要求的日期及時間
- 所購買項目之內容識別碼
- 內容提供者101之識別碼
- 使用條件517
- 電子數位內容商店103所加入的交易識別碼535
- 電子數位內容商店103之識別碼
- 最終使用者之識別碼

當提出對一報告的要求時，通常記錄下列資訊：

- 要求的日期及時間
- 傳送出報告的日期及時間
- 所要求的報告之類型
- 用來產生報告之參數
- 要求報告的實體之識別碼

E.結果回報

交換所105利用其在最終使用者購買交易期間所記錄的資訊來產生報告。內容提供者101及電子數位內容商店103

五、發明說明（90）

可經由一付款驗證介面183向交換所105要求交易報告，因而以上兩者可使其本身的交易資料庫與交換所105記錄的資訊一致。交換所105亦可將定期的報告提供給內容提供者101及電子數位內容商店103。

交換所105界定一安全電子介面，可讓內容提供者101及電子數位內容商店103要求及接收報告。報告要求SC(s)包含一個由交換所105指定給提出要求的實體之證明書。交換所105利用該證明書及該SC的數位簽名來驗證該要求係自一授權實體發出。該要求亦包含諸如界定報告的範圍的持續時間等之參數。交換所105確認該等要求參數，以便確保提出要求者只能接收其容許持有的資訊。

如果交換所105決定報告要求SC(s)是可信賴性的及有效的，則交換所105產生一報告，並將該報告包封到一報告SC(s)，以便傳送到提出該要求的實體。可以自動的方式在指定的時間間隔產生某些報告，並將這些報告儲存在交換所105，因而在接收到一要求時，可立即傳送該等報告。在本文件的後續版本將指定報告中資料的格式。

F.帳單開立及付款驗證

交換所105或電子數位內容商店103可處理內容113的帳單開立。在交換所105處理電子內容113的帳單開立之情形中，電子數位內容商店103將最終使用者的訂單分成電子式商品、及(或有的)實體商品。電子數位內容商店103然後將其中包括最終使用者的帳單開立資訊及需要得到授權的總金額的交易資訊通知交換所105。交換所105授權該最

五、發明說明（91）

終使用者的信用卡，並將一通知送回到電子數位內容商店103。在交換所105對該最終使用者的信用卡授權的同時，電子數位內容商店103可對所購買的任何實體商品向該最終使用者的信用卡收費。在最終使用者裝置109下載某一電子項目之後，即通知交換所105，而可向該最終使用者的信用卡收費。上述步驟即是可在最終使用者裝置109上使用內容113之前由最終使用者裝置109所執行的最後一步驟。

在電子數位內容商店103處理內容113的帳單開立之情形中，在最終使用者裝置109將訂單SC(s) 650傳送到交換所105之前，並不將與交易有關的資訊通知交換所105。在下載每一電子項目之後，仍然由最終使用者裝置109通知交換所105。當交換所105收到通知之後，交換所105將一通知傳送到電子數位內容商店103，使電子數位內容商店103可向該最終使用者的信用卡收費。

G.重新傳輸

安全數位內容電子式配送系統100提供用來處理內容113的重新傳輸之能力。通常係由一客户服務介面184執行該能力。電子數位內容商店103一使用者介面，而最終使用者可依照該使用者介面的指引而起動一重新傳輸。最終使用者連線到購買內容113的電子數位內容商店103網站，以便要求內容113的重新傳輸。

當最終使用者因無法下載內容113或無法使用先前下載的內容113，而對一先前購買的內容113項目要求一份新的

五、發明說明（92）

拷貝時，即執行內容113的重新傳輸。電子數位內容商店103決定該最終使用者是否有資格進行內容113的一重新傳輸。如果該最終使用者有資格進行一重新傳輸，則電子數位內容商店103建立一交易SC(s) 640，該交易SC(s) 640包含所要重新傳輸的內容113項目之報價SC(s) 641。將該交易SC(s) 640傳送到最終使用者裝置109，且由該最終使用者執行與一購買交易相同的各步驟。如果對於要進行重新傳輸的內容113項目最終使用者裝置109要用到金鑰庫中之一亂序編碼的金鑰，則交易SC(s) 640包含用來指示最終使用者裝置109刪除該亂序編碼的金鑰之指令。

在交換所105處理內容113購買的金融結算的情形中，電子數位內容商店103在交易SC(s) 640中加入一旗標，且該旗標係承載於訂單SC 650中而傳送到交換所105。交換所105解譯訂單SC(s) 650中之該旗標，並繼續進行該交易，而不針對內容113的購買而向最終使用者收費。

VIII. 內容提供者

A. 概述

安全數位內容電子式配送系統100中之內容提供者101即是數位內容所有人、或擁有內容113的權利之實體。內容提供者101的任務是準備內容113以供配銷，並使可下載版的內容113之電子數位內容商店103或零售商可得到與內容113有關的資訊。爲了將最高的安全性及權利控制提供給內容提供者101，提供了一系列的工具程式，使內容提供者101得以在其營業場所準備其內容113並將其內容113安

五、發明說明（93）

全地包封到SC(s)，因而當內容113離開內容提供者101的領域時，該內容113是安全的，且未經授權者無法接觸或存取該內容113。此種方式可使內容113自由地經由諸如網際網路等不安全的網路配送，而不必害怕駭客或未經授權者將竊取該內容113。

內容提供者101的工具程式之終極目標在於：準備諸如一歌曲或歌曲系列等的一內容113，並將該內容113包封到內容SC(s) 630，並且將描述該歌曲的資訊、該歌曲的核准使用法(內容使用條件517)、及該歌曲的促銷資訊包封到一中介資料SC(s) 620。爲了達到此一目的，提供了下列一組的工具程式：

- 工作流程管理程式154-安排處理活動的時程，並管理各程序之所需同步。
- 內容處理工具程式155-用來控制其中包括加上浮水印、預先處理(在一音訊的例子中，任何必需的等化、動態範圍調整、或重新取樣)、編碼、及壓縮的內容113檔案準備之一組工具程式。
- 中介資料同化及輸入工具程式161-用來自內容提供者的資料庫160及(或)協力廠商的資料庫或資料輸入檔案收集內容113描述資訊及(或)經由操作者的互動而收集該資訊並提供用來指定內容使用條件517之一組工具程式。亦提供一種用來擷取或提取諸如CDS或DDP檔的數位音訊內容之介面。一品質管制工具程式可用來預覽所準備的內容及中介資料。可進行中介資

五、發明說明（94 ）

料所需的任何修正、或內容的重新提交以供進一步的處理。

- SC(s)包封工具程式152-將所有的內容113及資訊加密及包封，並呼叫SC(s)包封工具程式將該內容113及資訊包封到SC(s)。
- 內容傳播工具程式(圖中未示出)-將SC(s)傳播到諸如代管內容網站111及電子數位內容商店103等的指定配銷中心。
- 內容促銷網站156-儲存中介資料SC(s) 620及或有的額外促銷材料，以供電子數位內容商店103下載。

B.作流程管理程式

該工具程式之目的在於對內容113的處理活動進行時程安排、追蹤、及管理。該應用程式可進行多使用者的存取，並可在內容提供者101的企業內部網路(Intranet)或企業外部網路(extranet)內的遠端位置上進行內容113的時程安排及狀態檢查。此種設計容許進行協力式處理，此時多個個人可以平行之方式對多件內容113進行作業，且可將特定的責任指定給不同的個人，而且這些個人可散佈在世界各地。

現在請參閱圖8，該圖是對應於圖7的工作流程管理程式154的主要程序之方塊圖。圖8所示之主要程序總結了本節中所述工具程式提供的內容113處理功能。工作流程管理程式154負責將工作提供給這些程序，並於完成其現行程序時，將工作導引到下一個需要的程序。係利用一系列的

五、發明說明（95）

應用程式介面(APIs)完成上述步驟，而每一處理工具程式呼叫該等應用程式介面，以便執行下列事項：

- 擷取所要處理的次一工作
- 指示成功地完成一程序
- 指示並未成功地完成一程序及失敗的原因
- 提供一程序的過渡狀態(以便起動一些只需要一相依程序的部分完成之程序)
- 將註釋加入一個指定程序可取得的產品

工作流程管理程式154也具有一使用者介面，而一例示工作流程管理程式使用者介面700係示於圖7，而該使用者介面提供了下列功能：

- 在處理的各階段中可指定並執行系統預設值及條件的規格之一組態設定控制功能
- 讓使用者自行訂定工作流程及自動化處理流程
- 工作的時程安排
- 狀態查詢及報告
- 將一相關聯的工作之註釋或指令加入一個或多個程序
- 工作管理(亦即暫停、解除、移除、改變優先順序(處理的順序))

每一程序具有一個與其相關聯且由工作流程管理工具程式154管理的佇列。向工作流程管理程式154要求工作的所有程序將使工作流程管理程式154於該程序的相關聯佇列中目前並無工作時，將該程序(工具程式)暫停在一等候狀態，或將與該工作有關的且執行該工作的各別程序所需的

五、發明說明（96）

所有資訊送回到該程序。如果一程序被暫停於一等候狀態，則當工作流程管理程式154將一工作置於該程序之佇列時，該程序即恢復處理。

工作流程管理程式154也根據一組指定的規格而管理處理的流程或順序。如果內容提供者101有特殊的處理需求或要設定特定的預設規則，則內容提供者101可自行訂定這些規則。當一程序報告完成了指定給該程序的工作時，該程序即將此種狀態通知工作流程管理程式154，且工作流程管理程式154根據指定的規則而決定要將次一工作放在哪一個佇列中。

亦可在任何處理步驟上，經由程式API，或以人工方式經由工作流程管理程式使用者介面700或處理器介面，而將指示特殊處理指令或注意事項之註釋附加到產品上。

在較佳實施例中，係利用Java來實施工作流程管理程式154中之各程序，但是亦可使用諸如C/C++、組合語言(Assembler)及等效語言等其他的程式語言。我們當了解，下文中針對工作流程管理程式154而說明的各程序可在多種硬體及軟體平台上執行。可以在一電腦可讀取的媒體中的一應用程式之方式配送作爲一完整系統或一完整系統構成程序的部分程序之工作流程管理程式154，而該電腦可讀取的媒體包括(但不限於)諸如網路之電子式配送方式、軟碟、光碟、及抽換式硬碟機。

現在請參閱圖8，圖中示出對應於圖7所示工作流程管理程式154的主要程序之方塊圖。下列各節概述每一程序，

五、發明說明（97）

並說明每一程序所需的資訊或動作。

1.產品等候動作/資訊程序801

一旦可取得程序所需的所有資訊，且工作業已成功地完成了所有相依的程序時，即將工作置於特定的程序佇列。一特殊佇列係存在於工作流程管理程式154，而該特殊佇列係用來存放因缺少資訊或發生了無法進行進一步處理的失敗而目前無法處理的工作。係將這些工作置於產品等候動作/資訊程序801佇列。該佇列中每一工作有相關聯的狀態，用以指示該工作正在等候的動作或資訊、該工作完成的上一程序、以及一旦提供了缺少的或額外的資訊之後或成功地完成了所需的動作之後該工作將要進行的次一程序。

任何程序完成時，將使工作流程管理程式154檢查該佇列，並決定該佇列中是否有任何工作正在等候該程序(動作)的完成、或該程序所提供的資訊。如果確係如此，則將該工作存放在適當的程序佇列中。

2.新內容要求程序802

內容提供者101決定其想要以電子方式銷售及配送的那些產品(例如，一產品可以是一首歌曲或一歌曲集)。工作流程管理程式154的起始功能是使一操作者得以識別這些產品，並將這些產品放置在新內容要求程序802的佇列中。內容提供者101可利用組態設定選項而指定在產品選擇介面上提示哪些資訊。輸入足夠的資訊，以便唯一地識別該產品。亦可選擇包含一些額外的欄位，以便在中介資

五、發明說明（98 ）

料提取的同時，要求以人工方式輸入起動音訊處理階段所需的資訊。如果並未以人工方式提供，則可選擇自系統預設的組態環境中擷取該資訊，或自內容提供者的資料庫160擷取該資訊，且係如同在自動中介資料取得程序803中的情形，係在中介資料處理的第一階段中取得該資訊。內容提供者的資料庫160中的內容113之構造及能力決定內容選擇程序。

如果指定了執行向內容提供者101的資料庫160查詢所需的必要資訊，則由自動中介資料取得程序803處理該工作。在一音樂實施例中，爲了適當安排要進行音訊處理的產品之時程，將指定產品的類型、所需的壓縮等級、以及該音訊的PCM或WAV檔案名稱。可經由一自訂的查詢介面或全球資訊網瀏覽器功能，而輸入該資訊作爲產品選擇程序的一部分，或選擇該資訊。該資訊的規格可安排產品的時程，以便進行內容處理。

該產品選擇使用者介面提供了一選項，使操作者得以指定要將產品釋出以供處理、或暫時保留該產品以等候進一步的資訊輸入。如果保留該產品，則將工作加入新內容要求程序802的佇列中，而等候進一步的動作來完成資料的輸入，及(或)釋出該產品以供處理。一旦釋出該產品之後，工作流程管理程式154即評估所指定的資訊，並決定該工作準備要轉移到哪些程序。

如果提供了適當的資訊而得以自動化地查詢內容提供者101的資料庫160，則將工作放到用於自動中介資料取得程

五、發明說明（99）

序803之佇列。如果並未針對自動中介資料取得程序803而設定資料庫映射表的組態，則將該工作放到用於手動式中介資料輸入程序804之佇列(請參閱自動中介資料取得程序803節中有關資料庫映射表之細節說明)。

如果指定了用於音訊處理的所需一般性資訊、及加入浮水印所需的特定資訊，則將該工作放到用於加入浮水印程序808之佇列(內容處理的第一階段)。如果在釋出工作時失掉了所需的資訊，則將該工作連同用來指示失掉該資訊的狀態放到產品等候動作/資訊程序801之佇列。

如果該狀態指示內容113的檔案名稱遺失，例如在內容113是音訊而PCM或WAV檔遺失的例子中，該狀態可指示需要擷取內容(或自數位媒體進行數位提取)。音訊處理功能要求可經由一標準檔案系統介面而存取歌曲檔。如果歌曲係位於外部媒體或音訊處理工具程式無法直接存取的一檔案系統上，則首先將該等檔案拷貝到一可存取的檔案系統。如果歌曲爲數位格式但係存放在CD或數位錄音帶上，則音訊處理工具程式可存取的一檔案系統提取這些歌曲。一旦可存取這些檔案之後，即利用工作流程管理程式使用者介面700來指定或選擇工作的路徑及檔案名稱，因而在也已指定加入浮水印程序所需的所有其他資訊的情形下，可將該工作釋出到加入浮水印程序。

3.自動中介資料取得程序803

自動中介資料取得程序803執行對內容提供者101的資料庫160或已輸入資料的一階段性資料庫之一系列查詢，嘗

五、發明說明（100）

試以一種自動化的方式取得所能得到的最多產品資訊。在可將各項目放到自動中介資料取得程序803的佇列之前，自動中介資料取得程序803先要求下列資訊：

- 資料庫映射表，該資料庫映射表具有適當的資訊，用以產生對內容提供者101的資料庫160之查詢
- 執行查詢所需的產品資訊
- 用來唯一界定產品之適當產品資訊

對內容提供者101的資料庫160執行一自動化查詢，以便取得處理內容113所需之資訊。例如，如果內容113是音樂，則執行該查詢所需的資訊可以是專輯名稱，或者可以是內容提供者101指定的一UPC、或一特定專輯、或選擇識別碼。在所要取得的資訊中，某些資訊被指定爲必須的(請參閱與自動中介資料取得程序803的該節所述之細節)。如果取得了所有必須的資訊，則隨即將該工作放到使用條件程序805之佇列。如果失掉了任何必須的資訊，則將該歌曲放到手動式中介資料輸入程序804的佇列中。如果產品等候動作/資訊程序801佇列中的任何工作正在等候該步驟中得到的任何資訊，則更新工作狀態，以便指示不再需要等候該資訊。如果該工作不再有任何未解決的需求，則將該工作放到下一個界定的佇列。

4.手動式中介資料輸入程序804

手動式中介資料輸入程序804提供了一種讓操作者可輸入失掉的資訊之方式。該程序並無相依性。一旦指定了所有必須的資訊之後，即將該工作放到使用條件程序805。

五、發明說明（101）

5.使用條件程序805

使用條件程序805可指定產品使用及限制之規格。使用條件程序805可能需要某些中介資料。在完成使用條件規格時，除非要求受監控的發行程序806選項，或者受監控的發行程序806選項被設定爲工作流程管理程式154規則中之預設選項，否則該工作有資格被放到中介資料SC(s)產生程序807之佇列。在此種情形中，該工作被放到受監控的發行程序806之佇列。在放到中介資料SC(s)產生程序807的佇列之前，工作流程管理程式154將首先保證已滿足了各程序的所有相依性(請參閱下文)。如果並非如此，則將該工作放到產品等候動作/資訊程序801之佇列中。

6.受監控的發行程序806

受監控的發行程序806可對數位內容產品指定的資訊進行品質檢查及確認。該程序並無任何相依性。監控者可審查先前在該產品的任何處理階段中附加到該工作之註釋，並採取適當的動作。在審查了所有的資訊及註釋之後，監控者可以有下列的選項：

- 核准發行，並將該產品放到中介資料SC(s)產生程序807之佇列中。
- 修改及(或)加入資訊，並將該產品放到中介資料SC(s)產生程序807之佇列中。
- 將註釋加入該工作中，並將該工作重新放到手動式中介資料輸入程序804之佇列中。
- 加入註釋，並將該工作放到產品等候動作/資訊程序

五、發明說明（102）

801之佇列中。

7.中介資料SC(s)產生程序807

中介資料SC(s)產生程序807將先前收集的所有資訊及中介資料SC(s) 620所需的其他資訊蒐集在一起，並呼叫SC(s)包封程序，以便產生中介資料SC(s) 620。該工具程式需要下列資訊作爲輸入：

- 必須的中介資料
- 使用條件
- 在該產品的所有品質等級的加密階段中使用之加密金鑰

該最後一個相依性要求：相關聯的音訊物件先完成音訊處理階段，然後才可產生中介資料SC(s) 620。在完成中介資料SC(s)產生程序807時，將根據所指定的工作流程規則，而將該工作放到最後品質保證程序813之佇列、或內容傳播程序814之佇列。

8.加入浮水印程序808

加入浮水印程序808將著作權及其他資訊加入內容113。在內容113是一首歌曲的一實施例中，該工具程式需要下列資訊作爲輸入：

- 歌曲檔案名稱(在專輯的情形中爲多個檔案名稱)
- 浮水印指令
- 浮水印參數(將包含在浮水印的資訊)

於完成加入浮水印程序808時，如果可取得預先處理及壓縮程序809所需的輸入，則將該工作放到預先處理及壓縮程序809之佇列，否則將該工作放到產品等候動作/資訊

五、發明說明（103）

程序801之佇列。

9.預先處理及壓縮程序809

預先處理及壓縮程序809將內容113編碼成指定的壓縮等級，以便先執行任何必需的預先處理。將一工作放到該佇列時，實際上產生了多個佇列資料項。係針對所需產品的每一壓縮等級而產生一工作。可以平行方式在多個系統上執行該編碼程序。該工具程式需要下列的輸入：

- 加入浮水印的內容之檔案名稱(在專輯的情形中爲多個檔案名稱)
- 產品的品質等級(可預先設定該品質等級)
- 壓縮演算法(可預先設定該壓縮演算法)
- 產品類型(在預先處理器需要的情形下)

於完成該編碼程序時，如果工作流程規則已有設定，則將工作放到內容品質管制程序810之佇列。如果並非如此，則將這些工作放到加密程序811之佇列。

如果編碼工具程式的協力供應商並未提供一種顯示諸如音訊的內容113中已被處理的百分率之方法，或者並未提供一種指示所選擇的內容113的整個選擇中已被編碼的百分率之方法，則在圖11中示出一種決定圖8所示內容預先處理及壓縮工具程式對數位內容之編碼率。該方法開始時係在步驟1101中選擇所需的編碼演算法及位元傳輸速率。然後在步驟1102中進行查詢，以便決定該演算法及編碼速率是否具有一預先計算的速率因數。該速率因數是用來決定對一特定編碼演算法及一特定位元傳輸速率而進行壓縮

五、發明說明（104）

的速率之因數。如果並未儲存任何先前計算的速率因數，則在一段預定的時間中將內容113的一樣本編碼。在較佳實施例中，該段預定的時間是幾秒鐘。在一段預定的時間中之該編碼速率是用來計算一個新的速率因數R_{NEW}。在步驟1108中，於已知時間長度及所編碼的內容113量時，一新的速率因數R_{NEW}的計算爲R_{NEW}=(所編碼的數位內容長度)/(時間長度)。在步驟1109中，將內容113編碼，並利用先前計算的速率因數R_{NEW}顯示該編碼狀態。然後在步驟1107中儲存該編碼速率因數R_{NEW}，以供未來用於該編碼演算法及編碼位元傳輸速率。在步驟1103中，如果所選擇的演算法具有一個先前計算的速率因數R_{STORED}，則在步驟1104中將內容113編碼，並利用該先前計算的速率因數R_{STORED}顯示進度。在此同時，在步驟1105中爲所選擇的該演算法及位元傳輸速率計算一現行速率因數$R_{CURRENT}$。在步驟1106中，利用該現行速率因數$R_{CURRENT}$來更新所儲存的速率因數R_{NEW}=(R_{STORED}+$R_{CURRENT}$)之平均值。速率因數的此種反覆更新在每一次持續使用一特定編碼演算法及位元傳輸速率時，可使編碼速率的決定變得愈來愈精確。然後在步驟1107中儲存該新的速率R_{NEW}，以供未來使用。如果現行速率因數$R_{CURRENT}$超出先前儲存的速率因數R_{STORED}到一特定範圍或臨界值，則可以不更新R_{STORED}。

然後可提供編碼狀態的顯示。該編碼狀態包括：在現行的編碼速率下，根據編碼速率、及內容113的總檔案長度，而將全部內容113的百分率顯示爲百分率長條。該編

五、發明說明（105）

碼狀態亦可包括剩餘的編碼時間。將內容113之總檔案長度除以所計算的編碼速率$R_{CURRENT}$，即可計算出其餘的編碼時間。可將該編碼狀態傳送到另一個可能用到該呼叫程序之程式。此種方式可協助監督程式對各相依程式進行編碼及批次處理，以便得到更有效率的處理。我們當了解，在一替代實施例中，編碼可包含加入浮水印的步驟。

10.內容品質管制程序810

內容品質管制程序810在功能上類似於受監控的發行程序806。該程序是一可供選用的步驟，可讓使用者確認至目前爲止所執行的內容處理之品質。該程序除了加入浮水印程序808及預先處理及壓縮程序809的編碼部分的完成之外，對其他程序並無相依性。於完成內容品質管制程序810時，可以有下列的選項：

- 可釋出工作，並將這些工作放到加密程序811的佇列。
- 可附加註釋，並可將一個或多個工作重新放到預先處理及壓縮程序809的佇列。

最後一個選項要求歌曲檔的未編碼但加有浮水印之版本保持在可使用的狀態，直到執行過內容品質管制程序810後爲止。

11.加密程序811

加密程序811呼叫適當的安全數位內容電子式配送權利管理功能，以便將每一個加上浮水印的/編碼的歌曲檔加密。該程序除了所有其他音訊處理的完成之外，對其他程

五、發明說明（106）

序並無相依性。於完成加密程序811時，將該工作放到內容SC(s)產生程序812的佇列。

12.內容SC(s)產生程序812

內容SC(s)產生程序812可能需要將某些中介資料檔案包含在內容SC(s) 630中。如果需要內容113以外的檔案，則收集該等檔案，並呼叫SC(s)包封程序，以便爲所產生內容113(例如一首歌)的每一壓縮等級產生一內容SC(s) 630。於完成內容SC(s)產生程序812時，將根據規定的工作流程規則，而將該首歌放到最後品質保證程序813的佇列或內容傳播程序814的佇列。

13.最後品質保證程序813

最後品質保證程序813是一可供選用的步驟，可在相關聯的中介資料與內容SC(s) 630之間進行一交互對照檢查，以便驗證上述兩者之間正確地匹配，並驗證內含的所有資訊及內容113都是正確的。於完成最後品質保證程序813時，將工作放到內容傳播程序814的佇列。如果發現了一問題，則在大多數的情形中將把工作重新放到缺點階段的佇列。在該階段的重作在成本上是高出許多，這是因爲除了修正問題所需的重新處理之外，該產品還必須經過整個的重新加密及重新包封程序。我們強烈建議利用先前的各品質保證階段來保證內容113之品質、以及資訊的正確性及完整性。

14.內容傳播程序814

內容傳播程序814負責將SC(s)傳送到適當的代管網站。

五、發明說明（107）

在成功地傳送SC(s)之後，記錄工作完成狀態，並自佇列中刪除該工作。如果在傳送SC(s)時發生問題，則在一指定次數的重新嘗試之後，在工作流程管理程式154中以旗標將該工作標示爲失敗及發生的錯誤。

15.工作流程規則

圖8所示的工作流程規則係依照下文所述的三種主要系統而作業：

A：工作流程管理程式154

1. 新內容要求程序802
2. 產品等候動作/資訊程序801
3. 最後品質保證程序813
4. 內容傳播(及通知)程序814

B：中介資料同化及輸入工具程式161

1. 自動中介資料取得程序803
2. 手動式中介資料輸入程序804
3. 受監控的發行程序806
4. 中介資料SC(s)產生程序807

C：內容處理工具程式155

1. 加入浮水印程序808(需要著作權資料)
2. 預先處理及壓縮程序809
3. 內容品質管制程序810
4. 加密程序811
5. 內容SC(s)產生程序812

工作流程

A7
B7

五、發明說明（108）

內容113選擇操作者輸入一新產品及，且該將工作開始放到A1的佇列。(新內容要求程序802)

A1: 當內容113選擇操作者將該工作釋出到工作流程管理程式154時，則將該將工作放到B1(自動中介資料取得程序803)的佇列。

A2: 來自步驟B1(自動中介資料取得程序803)，
或步驟B2(手動式中介資料輸入程序804)，
或步驟B3(受監控的發行程序806)
在至步驟Before(中介資料SC(s)產生程序807)的途中
[需要加密金鑰]。

來自步驟Before(中介資料SC(s)產生程序807)
在至步驟A3(最後品質保證程序813)或步驟A4(內容傳播程序814)的途中
[需要內容SC(s) 630]。

來自步驟C1(加入浮水印程序808)
在至步驟C2(預先處理及壓縮程序809)的途中
[需要預先處理及壓縮程序809之中介資料]。

來自步驟C4(加密程序811)
在至步驟C5(內容SC(s)產生程序812)的途中
[需要內容SC(s) 630包封的中介資料]。

來自步驟C5(內容SC(s)產生程序812)
在至步驟A3(最後品質保證程序813)或步驟A4(內容傳播程序814)的途中
[需要中介資料SC(s) 620]。

五、發明說明（109）

A3: 在步驟A3(最後品質保證程序813)之後，
放到佇列B2(手動式中介資料輸入程序804)，
或放到佇列B3(受監控的發行程序806)，
或放到品質保證作業員所要求的佇列。

A4: 在步驟A4(內容傳播程序814)之後，
針對該產品而執行工作流程管理程式154。

B1: 在步驟B1(自動中介資料取得程序803)之後，
如果有步驟C1(加入浮水印程序808)所需的中介資料，則將代表該產品的一資料項放到佇列C1。
(亦執行下列邏輯)
如果失掉了任何必須的中介資料，或者如果有指定給人工中介資料提供者的註釋，則亦將該產品放到佇列B2(手動式中介資料輸入程序804)，
否則如果向該產品要求受監控的發行，則將該產品放到佇列B3(受監控的發行程序806)。
否則如果該產品針對所有要求的品質等級有來自內容處理工具程式155的所有資訊，則將該產品放到佇列Before(中介資料SC(s)產生程序807)，
否則將產品的旗標標示爲需要加密金鑰，並將該產品放到佇列A2(產品等候動作/資訊程序801)。

B2: 在步驟B2(手動式中介資料輸入程序804)的過程中，
如果尚未執行步驟C1(加入浮水印程序808)，且有

五、發明說明（110）

步驟C1所需的中介資料，則將一個代表該產品的資料項放到佇列C1。

(亦執行下列邏輯)

如果已提供了步驟C2(預先處理及壓縮程序809)所需的中介資料，則

(亦執行下列邏輯)

如果有中介資料同化及輸入工具程式161可收集的所有中介資料，則

如果要求該產品的受監控之發行，則將該產品放到佇列B3(受監控的發行程序806)

否則

如果有來自內容處理工具程式155的步驟C4(加密程序811)之所有資訊，則將該產品放到佇列Before(中介資料SC(s)產生程序807

否則將該產品的旗標標示爲需要加密金鑰，並將該產品放到佇列A2(產品等候動作/資訊程序801)。

否則

如果中介資料提供者要求一強制性受監控的發行，則將該產品放到佇列B3(自動中介資料取得程序806)

否則不執行任何事項(將該產品保留在佇列B2(手動式中介資料輸入程序804)。

五、發明說明（111）

B3: 在步驟B3(受監控的發行程序806)的過程中，

如果該作業員正將該產品傳送回步驟B2(手動式中介資料輸入程序804)，則將該產品放到佇列B2。

否則如果該作業員釋出該產品，則

如果有來自內容處理工具程式155的步驟C4(加密程序811)之所有資訊，則將該產品放到佇列Before(中介資料SC(s)產生程序)

否則將該產品的旗標標示爲需要加密金鑰，並將該產品放到佇列A2(產品等候動作/資訊程序801)。

否則將該產品保留在佇列B3(受監控的發行程序806)。

Before: 在步驟Before(中介資料SC(s)產生程序807)之後，

將該產品的旗標標示爲已包封中介資料。

如果已包封所有的(產品/品質等級)關係(tuple)，則

如果內容提供者101的組態規定要對SC(s)進行品保，則將該產品放到佇列A3(最後品質保證程序813)

否則將該產品放到佇列A4(內容傳播程序814)。

否則將該產品的旗標標示爲需要內容113 SC(s)，並將該產品放到佇列A2(產品等候動作/資訊程序801)。

C1: 在步驟C1(加入浮水印程序808)之後，

五、發明說明（112）

如果有步驟C2(預先處理及壓縮程序809)所需的中介資料，則爲每一(產品/品質等級)關係產生一資料項，並將這些資料項放到佇列C2，

否則將該產品的旗標標示爲需要預先處理/壓縮之中介資料，並將該產品放到佇列A2(產品等候動作/資訊程序801)。

C2: 在步驟C2(預先處理及壓縮程序809)之後，

如果內容提供者101的組態規定要進行內容品質管制程序810，則將該(產品/品質等級)關係放到佇列C3(內容品質控制程序810)，

否則將該(產品/品質等級)關係放到佇列C4(加密程序811)。

C3: 在步驟C3(內容品質管制程序810)之後，將該(產品/品質等級)關係放到佇列C4(加密程序811)。

C4: 在步驟C4(加密程序811)之後，

將所需的資訊(亦即程序所產生且用來將內容113加密的對稱金鑰623提供給中介資料同化及輸入工具程式161。

如果有內容SC(s) 630所需的所有中介資料，則將該(產品/品質等級)關係放到佇列C5(內容SC(s)產生程序812)，

否則將該產品的旗標標示爲需要用於內容SC(s)630包封之中介資料，並將該(產品/品質等級)關係放到佇列 A2(產品等候動作/資訊程序

五、發明說明（113）

801)。

C5: 在步驟C5(內容SC(s) 產生程序812)之後，

將品質等級的旗標標示爲已在該品質等級上將內容113包封。

如果已包封該(產品/品質等級)關係，則

如果將該產品的旗標標示爲已包封中介資料，則

如果內容提供者101的組態規定要對SC(s)進行品保，則將該產品放到佇列A3(最後品質保證程序813)

否則將該產品放到佇列A4(內容傳播程序814)

否則將該產品的旗標標示爲需要中介資料SC(s)620，並將該產品放到佇列A2(產品等候動作/資訊程序801)。

否則(尚未包封所有的(產品/品質等級)關係)不執行任何事項(另一(產品/品質等級)關係觸發一行動)。

C.中介資料同化及輸入工具程式

中介資料包含用來描述內容113的資料，例如在音樂的例子中，包含錄音的名稱、藝人、作者/作曲者、製作人、及錄音長度。下列說明係基於內容113爲音樂的情形，但是熟悉本門技術者當可了解，諸如視訊、程式、多媒體、電影、及等效物等的其他內容類型也是在本發明的適用範圍及意義內。

該子系統整合下列資料：內容提供者101提供給電子數

五、發明說明（114）

位內容商店103以便有助於促銷該產品之資料(例如，對於音樂而言，爲該藝人之音樂段落樣本、該藝人之歷史、該錄音出現的專輯清單、與該藝人及(或)產品相關聯的類型)、內容提供者101針對所購買的產品而提供給最終使用者的資料(例如藝人、製作人、專輯封面、音樂長度)、以及內容提供者101想要提供給最終使用者的不同購買選項(使用條件517)。將該等資料包封到一中介資料SC(s)620，並使電子數位內容商店103可取得該等資料。爲了達到此一目的，提供了下列的工具程式：

- 自動中介資料取得工具程式
- 手動式中介資料輸入工具程式
- 使用條件工具程式
- 受監控的發行工具程式

這些工具程式使內容提供者101得以執行前文所述工作流程管理程式154之各程序。在較佳實施例中，本文所述的工具程式係基於Java的一工具程式套件，但是亦可使用諸如C/C++、組合語言及等效程式語言等的其他程式語言。

1.自動中介資料取得工具程式

自動中介資料取得工具程式讓使用者能夠執行前文所述的自動中介資料取得程序803。該自動中介資料取得工具程式係用來存取內容提供者101之資料庫160，並在沒有作業員協助的情形下儘量擷取最多的資料。可以使用組態設定方法將該程序自動化。內容提供者101可修改系統預設

五、發明說明（115）

的中介資料樣板，以便識別內容提供者101想要提供給最終使用者的資料類型(例如作曲家、製作人、伴奏者、音樂長度)、以及內容提供者101提供給電子數位內容商店103的促銷資料(例如，在一音樂的例子中，爲該藝人之音樂段落樣本、該藝人之歷史、該錄音出現的專輯清單、與該藝人相關聯的類型)。系統預設的中介資料樣板包括：最終使用者裝置109所需的資料欄位、可選擇提供給最終使用者裝置109的資料欄位、以及目標針對電子數位內容商店103且係用來促銷藝人、專輯、及(或)單曲的一組樣本資料欄位。

爲了自內容提供者101的資料庫160提取該等樣板資料欄位，自動中介資料取得工具程式使用一個將該類資料(例如作曲者、製作人、藝人的傳記)映射到該資料庫內可找到該資料的位置之映射表。每一內容提供者101都協助指定其環境中之該映射表。

自動中介資料取得工具程式利用內容提供者101的一中介資料樣板及映射表，而自內容提供者101的資料庫160取得所能取得的任何資料。以自動中介資料取得程序803的結果更新每一產品的狀態。失掉任何必須資料的一產品被放到手動式中介資料輸入程序804的佇列，否則可將該產品包封到一中介資料SC(s) 620。

2.手動式中介資料輸入工具程式

手動式中介資料輸入工具程式讓一使用者能夠執行前文所述的手動式中介資料輸入程序804。該手動式中介資料

五、發明說明（116）

輸入工具程式可讓任何經過適當授權的作業員提供失掉的資料。如果該作業員決定無法取得失掉的資料，則該作業員可將一註釋附加到該產品，並要求受監控的發行。內容提供者101可基於品質保證的理由而要求該產品進行受監控的發行。一旦已有所有必須的資料，且並未要求受監控的發行，則可將該產品包封到一中介資料SC(s) 620。

3.使用條件工具程式

使用條件工具程式讓一使用者能夠執行前文所述的使用條件程序805。利用電子式配送之方式提供內容113以供銷售或租用(有限制的使用)之程序涉及一系列的商業決策。內容提供者101決定在何種壓縮等級下提供內容113。然後針對內容113的每一壓縮後編碼版本，規定一個或多個使用條件。每一使用條件針對內容113的使用而規定最終使用者的權力、及對最終使用者的任何限制。

將一部分的內容處理工具程式155及一組使用條件(最終使用者的權利及限制)附加到該產品。

一使用條件規定：

1. 該使用條件適用的內容113之壓縮編碼版本。
2. 該使用條件所涵蓋的使用者類型(例如企業、私人消費者)。
3. 該使用條件係適用於內容113的購買或租用。

對於租用而言：

- 用來限制租用條件的量度單位(例如天數、播放次數)。

五、發明說明（117）

- 超過之後即無法再播放內容113的上述量度單位數。

對於購買而言：

- 容許最終使用者製作可播放拷貝的份數。
- 最終使用者可用來製作這些拷貝的媒體種類(例如可錄製CD(CD-R)、MD、個人電腦)。

4. 可進行購買/租用交易的一段時間(亦即一最終使用者只有在開始供應日之後且在最後供應日之前才能在該使用條件的條款下購買/租用)。
5. 最終使用者可進行該交易(或租用)的國家。
6. 在此使用條件下的購買/租用交易價格。
7. 浮水印參數。
8. 須通知交換所105的事件類型。

一組使用條件的例子

內容提供者101可決定在1997年第四季測試北美市場對重新發行一著名童謠歌者所演唱童謠之接受性。該試銷將以兩種不同的壓縮編碼版本供應該童謠：384Kbps(每秒384千位元)及56Kbps。可購買(可在MD上製作一份拷貝)或租用(二星期)該384Kbps的版本，而只能購買(不得製作拷貝)該56Kbps的版本。任何購買/租用都具有相同的浮水印指令，且內容提供者101要求交換所105記錄所製作的每一份拷貝之份數。因而將產生下文所示之使用條件：

五、發明說明（118）

	使用條件 1	使用條件 2	使用條件 3
壓縮編碼版本	384Kbps	384Kbps	56Kbps
使用者類型	私人消費者	私人消費者	私人消費者
交易類型	購買	租用	購買
供應日期	1 Oct 1997-31 Dec 1997	1 Oct 1997-31 Dec 1997	1 Oct 1997-31 Dec 1997
國家	美國及加拿大	美國及加拿大	美國及加拿大
浮水印	標準	標準	標準
通知事件	拷貝動作	無	無
拷貝次數	1	0	0
拷貝媒體	MD	不適用	不適用
租用時間	不適用	14 天	不適用
價格	價格 1	價格 2	價格 3

4. 中介資料 SC(s) 620 之各組成部分

下文所述是中介資料同化及輸入工具程式161所收集而供包含在中介資料SC(s) 620中的某些種類的資料。嘗試按照功能及目標將資料分類成各SC(s)組成部分。

產品識別碼 [src:content provider;]
[dest:everybody;]

授權者品牌公司 [dest:EMS;end-user;]

被授權者品牌公司 [dest:EMS;end-user;]

該物件(被轉授權者品牌公司)
之來源(發行人) [dest:everybody;]

物件類型(亦即一單一物件或一
陣列的物件)物件識別碼 [dest:everybody;]

國際標準錄音碼(ISRC)

國際標準音樂編號(ISMN)

使用條件(來源：內容提供者；目標：EMS、最終使用者、交換所105)

五、發明說明（119）

購買使用條件(來源：EMS；目標：最終使用者、交換所105)

使用該物件(錄音)的該組使用條件(消費者的限制及權利)

該陣列的使用條件中之一個別資料項

該使用條件適用的內容113之壓縮編碼版本

該使用條件係適用於內容113的購買或租用

對於租用而言：

用來限制租用條件的量度單位(例如天數、播放次數)。

超過之後即無法再播放內容113的上述量度單位數。

對於購買而言：

容許最終使用者製作可播放拷貝的份數。

最終使用者可用來製作這些拷貝的媒體種類(例如可錄製CD(CD-R)、MD、個人電腦)。

可進行購買/租用交易的一段時間(亦即一最終使用者只有在開始供應日之後且在最後供應日之前才能在該使用條件的條款下購買/租用)

最終使用者可進行該交易(或租用)的國家之一指標

在此使用條件下的購買/租用交易價格

加密浮水印指令及參數之一指標

須通知交換所105的事件類型之一指標

購買資料(經過加密；可選用的資訊；來源：EMS；目

五、發明說明（120）

標：最終使用者、交換所105)

購買日期

購買價格

帳單開立名稱及地址

消費者名稱及地址

消費者的國家(最佳推測)

中介資料1(來源：內容提供者；目標：EMS、最終使用者)

一陣列的{

著作權資訊

屬於作曲的

屬於錄音的

歌曲名稱

主要藝人

}

下列事項的一指標{

美術品(例如專輯封面)；

美術品的格式(例如GIF、JPEG)；

}

可選用的資訊：

一陣列的額外資訊{

作曲者

發行人

製作人

伴奏者

五、發明說明（121）

錄音日期

發行日期

歌詞

歌曲名稱(說明)/歌曲長度

該錄音出現的專輯清單

類型

}

中介資料2(來源：內容提供者；目標：EMS)

一陣列的結構，每一結構代表同一錄音的不同品質等級{

該錄音；

該錄音的品質等級；

(可能經過壓縮的)該錄音之長度(以位元組爲單位)；

}

中介資料3(來源：內容提供者；目標：EMS、最終使用者)

可選用的資訊：

促銷材料：

下列藝人促銷材料的一指標{

該藝人網站的一網址；

該藝人的的背景描述；

與藝人有關的訪問(連同該訪問的格式(例如文字、音訊、視訊))；

評論(連同評論的格式(例如文字、音訊、視訊))；

樣本片段(及其格式及壓縮等級)；

最近及即將來臨的音樂會/露面/事件-其日期及位

五、發明說明（122）

置；

}

下列專輯促銷材料之一指標{

樣本片段(及其格式及壓縮等級)；

製作人、及(或)作曲者、及(或)電影/戲劇/演員班底、及(或)專輯的製作等的背景說明；

與非藝人有關的訪問(連同該訪問的格式(例如文字、音訊、視訊))；

評論(連同評論的格式(例如文字、音訊、視訊))；

類型；

}

單曲促銷：

樣本片段(及其格式及壓縮等級)

製作人、及(或)作曲者、及(或)電影/戲劇/演員班底、及(或)單曲的製作等的背景說明。

評論(連同評論的格式(例如文字、音訊、視訊))

5.受監控的發行工具程式

受監控的發行工具程式讓使用者能夠執行前文所述之受監控的發行程序806。被內容提供者101指定爲得到受監控的發行授權之個人可召集一個等候受監控的發行之一產品(亦即在受監控的發行程序806的佇列上等候之一產品)，檢查其內容113及其附加的註釋，並且

核准其內容113，並釋出該產品，以便包封在一中介資料SC(s) 620，

五、發明說明（123）

或

作任何必需的更正，並釋出該產品，以便包封在一中介資料SC(s) 620，或

附加一個規定所要採取的更正行動之註釋，並重新將該產品提交到手動式中介資料輸入程序704。

在另一實施例中，在產生SC(s)之後，有另一個可選用的品質保證步驟，此時可開啓SC(s)的內容113，並檢查該內容113的完整性及正確性，而且在此同時，可對是否要將該產品釋出到零售通路作出最後的核准或拒絕的決定。

D.內容處理工具程式

內容處理工具程式155實際上是用來處理數位內容檔案而產生加上浮水印的、編碼的、及加密的內容之一組軟體工具程式。該等工具程式利用工業標準的數位內容處理工具程式，而在技術有所進展時，可以外掛方式更換加上浮水印、編碼、及加密技術。如果可經由一命令行系統呼叫介面載入所選擇的該工業標準工具程式，並將參數傳送到該工具程式，或提供一可經由一DLL介面而呼叫函式之工具程式套件，則可將內容處理自動化到相當的程度。每一工具程式的一前端應用程式查詢內容處理工具程式155中的適當佇列中是否有下一個可進行的工作，並擷取所需的檔案及參數，然後載入該工業標準的內容處理工具程式，以便執行所需的功能。於完成該工作時，如果該工具程式並未回報終止狀態，則可能需要以人工方式更新該佇列。

現在將說明內容處理工具程式155的一般性版本，但是

五、發明說明（124）

使用者自訂的版本也是可能的。可以Java、C/C++、或任何等效軟體來撰寫內容處理工具程式155。可利用其中包括軟碟、光碟等任何電腦可讀取的裝置或經由一網站而配送內容處理工具程式155。

1.浮水印工具程式

浮水印工具程式讓使用者能夠執行前文所述的加入浮水印程序808。該工具程式利用音訊浮水印技術，將內容113所有人的著作權資訊施加到歌曲檔。內容提供者101及特定的浮水印技術決定了將要被寫出的實際資訊。前端的浮水印工具程式可取得該資訊，因而該浮水印工具程式可適當地將該資訊傳送到加上浮水印函式。此種方式對中介資料同化及輸入工具程式161有了同步的要求，以便保證該中介資料同化及輸入工具程式161先取得該資訊，然後才容許該歌曲的音訊檔被處理。在未取得該浮水印資訊之前，將無法對該歌曲進行音訊處理。

浮水印的施加是音訊處理的第一步驟，這是因爲該步驟是對所創作歌曲的所有編碼之共同步驟。只要該浮水印能夠經過編碼技術的考驗，則只需對每一首歌進行一次的加浮水印程序。

各種加浮水印技術都是習知的且可在市場上取得的。然而，前端的浮水印工具程式可支援各種工業標準的浮水印工具程式。

2.預先處理及壓縮工具程式

預先處理及壓縮工具程式可讓使用者能夠執行前文所述

五、發明說明（125）

之預先處理及壓縮程序809。音訊編碼涉及兩個程序。編碼基本上是對(一音樂內容例子中之)一PCM音訊流施行一有耗損的壓縮演算法。通常可調整編碼器，以便根據所需的音訊品質等級，而產生各種播放位元流傳輸速率。較高的品質將會造成較大的檔案容量，而且因爲高品質的內容113之檔案容量可能會變得太大，所以高品質內容113的下載時間可能變得太長，因而有時會禁止使用標準的28,800 bps的數據機。

因此，內容提供者101可能提供各種數位內容品質以供下載，以便能夠滿足沒有耐心且使用窄頻網路之客戶，這些客戶不想耗用幾個小時等候下載；同時能夠滿足音響迷或使用寬頻網路的客戶，這些客戶或者是只購買高品質的內容113，或具有較高速度的連線。

壓縮演算法在其技術上有所變化，以便產生內容113的較低位元傳輸速率之再生。可以演算法(亦即MPEG、AC3、ATRAC)及壓縮等級來改變該技術。爲了獲得較高的壓縮等級，在將資料傳送到壓縮演算法之前，通常先以最低的抽樣率將該資料重新抽樣。爲了在傳眞度的耗損較小的情形下得到更有效率的壓縮，或者爲了避免某些頻率範圍有極端的信號失落，數位內容有時可能需要對某些頻率的等化位準進行調整，或對錄音的動態範圍進行調整。內容預先處理的要求與壓縮演算法及所需的壓縮等級有直接的相關性。在某些情形中，可成功地利用內容113的型態(例如音樂類型)作爲決定預先處理要求的一基礎，這是因

五、發明說明（126）

爲同一音樂類型內的歌曲通常具有類似的動態範圍。使用某些壓縮工具程式時，這些預先處理的功能是編碼程序的一部分。使用其他的壓縮工具程式時，係在執行壓縮之前，先執行所需的預先處理。

除了供銷售的可下載音訊檔之外，每一首歌曲也具有一低位元傳輸速率(Low Bit Rate；簡稱LBR)編碼片段，可利用一LBR位元流協定而將該首歌曲抽樣。該LBR編碼也是內容處理工具程式155的責任。內容提供者101提供該片段作爲一獨立的PCM檔，或作爲偏移量及長度之參數。

與加浮水印的情形相同，我們希望可經由一DLL或命令行系統呼叫介面而載入編碼工具程式，並傳送所有必須的參數到該等編碼工具程式，以供預先處理及壓縮。例如，如果內容是音樂，且如果決定在執行任何音訊處理之前先自內容提供者的資料庫160取得該歌曲的類型，則可能要求前端編碼工具程式與中介資料同化及輸入工具程式161同步。上述情形係取決於所選擇的編碼工具程式、及該歌曲類型的不確定性。如果內容提供者101對每首歌曲都改變編碼品質等級的選擇，則也在編碼步驟之前先提供該資訊，且該資訊與中介資料同化及輸入工具程式161所產生的中介資料一致。

目前已知有各種高品質的編碼演算法及工具程式。然而，前端編碼工具程式可支援各種工業標準的編碼工具程式。

現在請參閱圖12，圖中示出根據本發明的圖8所示自動

五、發明說明（127）

中介資料取得工具程式的一實施例之流程圖。本程序開始時係自內容提供者101正在檢查的媒體讀取一識別碼。內容的一個例子即是一音樂CD實施例。在一音樂CD實施例中，可取得下列的代碼：通用價格碼(Universal Price Code；簡稱UPC)、國際標準錄音碼(International Standard Recording Code；簡稱ISRC)、國際標準音樂編號(International Standard Music Number；簡稱ISMN)。在步驟1201中，在適當的播放裝置(例如，對音樂CD而言是音樂CD唱盤，對DVD電影而言是DVD影碟機、對DAT數位式錄音帶或等效物而言是DAT錄音機)中讀取內容的識別碼。然後在步驟1202中，利用該識別碼作爲索引而搜尋內容提供者101之資料庫160。在步驟1203中，於資料庫160及任何其他相關的資源中擷取圖8所示工作流程管理程序所需的資訊之全部或部分。該資訊可包括內容113及與內容113相關的中介資料。在步驟1204中，利用所擷取的額外資訊來啓動工作流程管理程式154，以便產生電子內容113。我們當了解，可將諸如數片音樂CD等的數個所選擇媒體放到佇列中，使自動中介資料取得工具程式得以產生一系列的內容，以供電子式配送。例如，可自一系列的CD中產生所有的內容113，或者甚至可自內容提供者101檢視的一片或多片CD的所選出之一些歌曲中產生所有的內容113。

在一替代實施例中，可自動自內容提供者的資料庫160擷取預先處理參數。現在請參閱圖13，圖中示出一種自

五、發明說明（128）

動設定根據本發明的圖8所示預先處理及壓縮工具程式的預先處理及壓縮參數之方法。在該實施例中，內容113是音樂。在步驟1301中，選擇要在內容處理工具程式155中編碼的音樂(內容113)。在步驟1302中，決定所選擇音樂的類型。可以人工方式輸入該音樂類型，或利用諸如自圖12所示程序擷取的額外資料等的其他可用中介資料來決定音樂類型。然後在步驟1303中檢查所選擇的音訊壓縮等級及音訊壓縮演算法。然後在步驟1304中，以音樂類型、壓縮設定值、及壓縮演算法來查詢應在預先處理及壓縮程序809中使用哪些壓縮參數。

3.內容品質管制工具程式

內容品質管制工具程式讓使用者能夠執行前文所述之內容品質管制程序810。該工具程式是一種可供選用的內容處理工具程式，且使品質管制技術員能有機會重新檢查經過編碼及加上浮水印的內容檔案，並根據品質衡量標準而核准或拒絕該等內容檔案。品質管制技術員可將該內容重新編碼，而以人工方式進行預先處理的調整，直到得到適當的品質爲止，或者將該歌曲的旗標標示爲需要重新處理，並附加一個說明問題的註釋。

內容提供者101可將該程序步驟設定爲內容處理工作流程的一個可供選用的步驟或必須的步驟。在包封該內容的所有SC(s)(例如一CD上的各首歌曲之每一SC(s))之後，提供了一個額外的可供選用之最後品質保證程序813步驟，此時可測試內容編碼的品質，但是能夠在加密及包封之前

五、發明說明（129）

早一些發現問題才能更有效率地進行內容處理。因此，非常希望能在該步驟中保證內容的品質，而不是等到最後才完成所有的處理。

4.加密工具程式

加密工具程式讓使用者能夠執行前文所述的加密程序811。內容加密是內容處理工具程式155的最後一個步驟。現在要將先前利用編碼工具程式產生的內容之每一版本加密。加密工具程式是SC(s)包封工具程式的一種功能。呼叫該SC(s)包封工具程式而將歌曲加密，並送回所產生的加密金鑰。隨後將該金鑰放入SC(s)包封工具程式，以便用來產生中介資料SC(s) 620。

E.內容SC(s)產生工具程式

一旦收集了所有的中介資料之後，內容SC(s)產生工具程式根據中介資料的預定用途而將中介資料分成若干類型。這些組的中介資料被寫入檔案中，而放到SC包封工具程式作爲中介資料SC(s) 620的中介資料部分。每一組成部分(檔案)都有特有的處理要求。一旦對相關聯的歌曲進行處理及加密，且決定了目的地(代管內容網站111的網址)之後，即準備產生內容113的內容SC(s) 630。已完成處理且符合所有前文所述要求的內容113係在佇列中等候，以便包封到工作流程管理程式154的包封工具程式之佇列中。

內容SC(s)產生工具程式現在擷取中介資料同化及輸入工具程式161的各先前步驟所產生的所有必須檔案，並呼叫各SC(s)包封工具程式函式，以便產生中介資料SC(s)

五、發明說明（130）

620及內容SC(s) 630。該程序爲每一首歌曲產生一單一中介資料SC(s) 620及多個內容SC(s) 630。例如，如果內容是音樂，則將在針對整首歌曲的各種品質等級進行的音訊處理期間產生的每一音訊檔包封到各別的內容SC(s) 630。傳送爲樣本片段所產生的音訊檔，作爲中介資料SC(s) 620中包含的中介資料檔。

F.最後品質保證工具程式

最後品質保證工具程式讓使用者能夠執行前文所述的最後品質保證程序813。一旦已爲一內容檔案建立了所有的SC(s)之後，即可對該內容進行最後的品質保證檢查。可在內容113準備程序的各階段上執行品質保證。內容提供者101可選擇在完成每一主要步驟時執行品質保證，以避免未來的過量重作，或者可選擇等候到所有的音訊準備程序完成之後，立刻對每一項目執行品質保證。如果選擇後者，則在完成SC(s)產生的時點上執行品質保證。該工具程式可對該首歌曲的每一SC(s)進行開啓、檢查、及音樂播放。

發現任何問題時，縱使是很小的文字改變也要求因SC(s)的內部安全特性而重新建立該SC(s)。爲了避免不必要的重新處理時間，我們強烈建議利用中間的品質保證步驟來保證中介資料的精確性，我們並建議預留該特定的品質保證步驟，用來確認與該歌曲的各SC(s)間之交互參照。如果發現了問題，則品保人員可輸入一個附加到該首歌曲的一問題描述，並將該首歌曲重新放到適當的處理佇列，以

五、發明說明（131）

供重新處理。在工作流程管理程式154中適當地更新狀態，以便指示該歌曲的所有相關組成部分之狀態。如並未發現任何問題，則將內容113標示爲可準備發行。

G.內容傳播工具程式

內容傳播工具程式讓使用者能夠執行前文所述的內容傳播程序814。一旦已核准內容113的發行，則將內容113的SC(s)放到內容傳播程序之佇列。內容傳播工具程式監督該佇列，並根據內容提供者101所提供的組態設定，而執行SC(s)檔案的立即傳輸、或一組SC(s)檔案的批次傳輸。內容提供者101亦可選擇設定內容傳播工具程式的組態，以便自動將所有的SC(s)保存在該佇列中，直到以人工方式將該等SC(s)標示爲可發行爲止。此種方式可讓內容提供者101在內容的預定發行日之前先準備該內容，並保存這些內容，直到內容提供者想要發行諸如新歌、電影、或電玩等的內容爲止。SC(s)亦可根據一指定發行日而控制對內容113之存取，因而內容提供者101實際上無須抑制SC(s)的配送，但是此種人工方式的發行選項亦可用來管理傳輸較大檔案所需的網路頻寬。

當被標示爲可發行時，內容113之內容SC(s) 630係經由FTP而傳送到指定的代管內容網站111。中介資料SC(s) 620係經由FTP而傳送到內容促銷網站156。此時SC(s)逐步進入新的內容113目錄，直到可處理這些SC(s)，並將這些SC(s)整合到內容促銷網站156爲止。

圖17是自動擷取根據本發明的圖8所示自動中介資料取

五、發明說明（132）

得工具程式的額外資訊的一替代實施例之流程圖。該程序類似於前文中參照圖8所述之程序。然而，對受監控的發行程序806的品質檢查及內容品質管制程序809係結合成一個被稱爲品質管制1704的品質檢查。在中介資料SC產生程序807及內容SC產生程序812之前執行品質檢查。在SC產生之前執行品質檢查時，無須打開內容113及相關聯的中介資料SC(s) 620之步驟。此外，在本實施例中，已取消了產品等候動作/資訊程序801的佇列。根據要求何種行動，而將工作放到特定的程序佇列。例如，如果工作要求人工的中介資料，則輸入額外的中介資料，並將該工作放到人工中介資料輸入佇列。此外，也將自動中介資料取得程序803及新內容要求程序合併，以便在中介資料同化及輸入工具程式161及內容處理工具程式155之前發生。最後，重要的是要指出：係在自動中介資料取得程序803時及自動中介資料取得程序803時輸入使用條件804。這是因爲可在自動中介資料取得程序803步驟中自動填入許多使用條件。

H.內容促銷網站

爲了經由數位下載而最有效地傳播內容提供者101爲銷售而提供的資訊，並爲了使電子數位內容商店103取得必要的檔案而得以提供將內容113下載到其客戶，每一內容提供者101應有一個代管此類資訊的網站。此種方式類似於目前某些內容提供者101使其零售商及其他需要此類資訊的夥伴取得促銷內容所用的方法。在此類服務業已存在

五、發明說明（133）

的情形中，可將一額外的部分加入網站中，此時電子數位內容商店103可經由下載而看到一份可供銷售的內容清單。

內容提供者101可完全控制該網站的設計及配置，或者可選擇利用作爲安全數位內容電子式配送系統100的工具程式套件的一部分而提供的一組裝完備可立即啓用的網路伺服器解決方案。爲了針對該服務而實施其本身的設計，內容提供者101只需要將到中介資料SC(s) 620的連結提供給連線到其網站的電子數位內容商店103。利用安全數位內容電子式配送系統100的工具程式套件即可達到上述目的。內容提供者101將自行決定該選擇程序及所要顯示的資訊。

內容促銷網站156處理經由FTP而自內容傳播工具程式接到一新內容目錄的中介資料SC(s) 620。可利用SC(s)預覽工具程式開啓容器物件，以便顯示或提取容器物件的資訊。然後可利用該資訊更新HTML網頁及(或)將資訊加到一個由該服務所維護的可搜尋資料庫。該SC(s)預覽工具程式實際上是電子數位內容商店103用來開啓及處理中介資料SC(s) 620的內容取得工具程式之一子集。然後應將中介資料SC(s) 620檔案移到一個由內容促銷網站156維護的永久性目錄。

一旦將中介資料SC(s) 620整合到內容促銷網站156之後，即可公告可取得該中介資料SC(s) 620。當將一個新的中介資料SC(s) 620加入網站時，內容提供者101可將一通

五、發明說明（134）

知傳送到所有的訂閱電子數位內容商店103，或者內容提供者101可每天(或指定的定期)將這一天(或這段期間)中加入的所有中介資料SC(s) 620作單一的通知。係傳送一包含對照到所加入中介資料SC(s) 620的參數之指定CGI訊息串，而經由一個與電子數位內容商店103網路伺服器的標準HTTP交換而執行該通知。電子數位內容商店103的通知介面模組(將於下文中說明)處理該訊息。

I.內容代管

演藝事業每年產生幾千個諸如CD、電影、及電玩等的內容節目，再加上現有的以萬爲單位的內容節目。安全數位內容電子式配送系統100被設計成可支援目前可自商店取得的所有內容節目。

安全數位內容電子式配送系統100最後每天可下載到客戶的內容節目之數目係以千或萬爲單位。對於大量的內容節目而言，需要大量的頻寬。電腦硬碟儲存空間及頻寬都需要對多個代管內容網站111進行分散式且可擴展的配置。該系統也支援世界各地的客戶。因而需要海外的網站來加速對全球性客戶的配送。

安全數位內容電子式配送系統100上的內容代管被設計成：可讓內容提供者101管理其本身的內容，或共用一組共同的設施或一組設施。

安全數位內容電子式配送系統100上的內容代管包含：多個代管內容網站111，這些代管內容網站111合而包含安全數位內容電子式配送系統100提供的所有內容113；以及

五、發明說明（135）

數個輔助內容網站(圖中未示出)，這些輔助內容網站包含內容提供者101提供的若干現行熱賣產品。代管內容網站111的數目係根據使用該系統的最終使用者數目而改變。輔助內容網站只存有數目有限的歌曲，但是這些網站代表了該系統上所使用的一個相當大百分率的頻寬。當主要網站的容量增加到最大容量點時，即將該等輔助網站上線。輔助網站可位於接近網路接取點(Network Access Point；簡稱NAP)處，以便有助於加速下載時間。亦可將輔助網站置於世界上的不同地理區域，以便加速下載時間。

如果內容提供者101選擇將所有其內容113放在其自身的系統，則可將該網站視爲具有或未具有額外輔助內容網站的單一代管內容網站111。此種方式可讓內容提供者建立其本身的可擴展之分散式系統。在另一實施例中，電子數位內容商店103亦可作爲某些內容113的代管內容網站111。該實施例要求在電子數位內容商店103與內容提供者101之間有特殊的金融協定。

1.代管內容網站

本說明書的內容提供者一節說明的內容傳播工具程式經由FTP或HTTP將內容113加入代管內容網站111，或經由諸如在磁帶、CD-ROM、快閃記憶體、或其他電腦可讀取的媒體上配送內容等的離線裝置而將內容113加入代管內容網站111。內容提供者101產生的中介資料SC(s) 620包含一欄位，用以指示找出內容113的內容SC(s) 630之網址。該網址對應於一代管內容網站111。電子數位內容商店103如

五、發明說明（136）

果得到內容提供者101在報價SC(s) 641中的許可，則可越過該網址。當最終使用者裝置109想要下載內容SC(s) 630時，最終使用者裝置109即連線到代管內容網站111。

最終使用者裝置109將授權許可SC(s) 660傳送到代管內容網站111，而提出對內容SC(s) 630的要求。該授權許可SC(s) 660是交換所105所傳送回的相同授權許可SC(s) 660。可驗證授權許可SC(s) 660的數位簽名，以便決定該授權許可SC(s) 660是否爲一有效的授權許可SC(s)。如果該授權許可SC(s)是一有效的授權許可SC(s)，則開始下載，或可將下載要求轉向到另一代管內容網站111。

2.安全數位內容電子式配送系統100提供的代管內容網站111

對於安全數位內容電子式配送系統100而言，接收對一內容SC(s) 630的起始要求之主要內容網站決定應利用哪一個網站來下載內容113。該網站利用下列資訊作出上述決定：

- 是否有存放所要求內容113之輔助內容網站？（安全數位內容電子式配送系統100所提供的內容113之大部分係只存放在主要網站）；
- 最終使用者裝置109位於哪一地理區？（當最終使用者裝置109提出該要求時，可自該最終使用者裝置109得到此一資訊，並將該資訊放到訂單SC(s) 650中而傳送到交換所105）；
- 是否有適當的輔助網站且在工作中？（輔助網站有時可能是離線的）；

五、發明說明（137）

• 輔助網站的負載爲何？(在一輔助網站忙於處理存取活動的某些情形中，可選擇較不忙碌的另一網站。

在將內容SC(s) 630傳送到最終使用者裝置109之前，先對最終使用者的要求執行分析及驗證。一資料庫存放了曾用來下載內容113的所有授權許可SC(s)之識別碼。可檢查該資料庫，以便確保最終使用者裝置109只對所購買的每一件內容113提出一個要求。此種方式可避免惡意的使用者重複存取代管內容網站111而嘗試減緩代管內容網站111的存取速度，並防止對內容SC(s) 630作未經授權的下載。

係根據客户對個別件的內容113之需求，而定期執行增加或減少將內容113放到輔助內容網站。

內容代管路由器

內容代管路由器(圖中未示出)係設於代管內容網站111中，且接收最終使用者想要下載內容113的所有要求。該內容代管路由器執行對最終使用者要求的驗證檢查，以便確保最終使用者確實已購買了內容113。在一資料庫中維護了各輔助內容網站的狀態，該狀態包括哪些內容113係存放在這些輔助內容網站、及這些輔助內容網站的現行狀態。該現行狀態包括網站上的存取活動量、及一網站是否因維護作業而關閉。

該內容代管路由器的唯一介面是當要求下載內容113時最終使用者裝置109所傳送的授權許可SC(s) 660。授權許可SC(s) 660包含用來指示該使用者被容許下載內容113的資訊。

五、發明說明（138）

輔助內容網站

輔助內容網站(圖中未示出)存有安全數位內容電子式配送系統100的熱門內容113。這些網站在地理上係分佈在世界各地，且設於接近網路接取點(NAP)處，以便縮短下載時間。當對主要代管內容網站111的需求接近最大容量時，即將這些輔助內容網站加入系統中。

IX.電子數位內容商店

A.概述-對多個電子數位內容商店103之支援

電子數位內容商店103本質上是零售商。這些電子數位內容商店是行銷內容113以便將內容113配送到客戶之實體。對於內容113的配送而言，該系統將包含數位內容零售網站、數位內容零售店、或想要涉入將電子內容113配送到消費者的任何企業。這企業可以只行銷電子內容113，或者可選擇將電子式貨品的銷售加入其目前用來銷售的其他行銷管道中。經由爲電子數位內容商店103開發而爲安全數位內容電子式配送系統100的一部分之一組工具程式，即可完成將可下載的電子式貨品導入電子數位內容商店103的服務提供中。

電子數位內容商店103利用這些工具程式來進行下列事項：

- 取得內容提供者101所包封的中介資料SC(s) 620。
- 自這些SC(s)提取內容113，而用來作爲建立其服務提供之輸入。
- 產生用來描述其提供銷售的可下載內容113之報價SC(s)

五、發明說明（139）

641。

- 藉由交易SC(s) 640的產生並將該交易SC(s) 640傳送到最終使用者裝置109，而處理銷售的確認及下載的啓動。
- 管理可下載內容113的銷售之交易記錄、及每一次下載的狀態。
- 處理狀態通知及交易確證要求。
- 執行帳户一致性確認。

這些工具程式被設計成可容許電子數位內容商店103希望將可下載電子內容113的銷售整合到其服務的方式之彈性。可以下列的方式使用這些工具程式：縱使不是必要的，也要求交換所105處理所購買的可下載內容113之所有金融結算。這些工具程式也可讓電子數位內容商店103完全服務其客户，並自行處理金融交易，其中包括提供促銷及特價供應。這些工具程式可讓電子數位內容商店103迅速地將可下載內容113的銷售整合到其現有的服務中。此外，電子數位內容商店103無須設有可下載內容113的網站，且無須管理內容113的傳送。係由內容提供者101所選擇的代管內容網站111執行上述的功能。

在較佳實施例中，係利用Java來實施用於電子數位內容商店103的各工具程式，但是亦可使用諸如C/C++、組合語言及等效語言等其他的程式語言。我們當了解，可在多種硬體及軟體平台上執行用於電子數位內容商店103而將於下文中說明之該等工具程式。可以一電腦可讀取的媒體中

五、發明說明（140）

的一應用程式之形式配送作爲一完整系統或一完整系統的組成部分之電子數位內容商店103，該電腦可讀取的媒體包括(但不限於)諸如網路的電子式配送、以及軟碟、CD-ROM、及抽取式硬碟機。

在另一實施例中，電子數位內容商店103的各組成部分是一程式設計師的軟體工具程式套件的一部分。該工具程式套件起動將於下文中說明的一般性電子數位內容商店103組成部分及工具程式之預定介面。這些預定介面的形式爲應用程式介面(API)。使用這些API的開發人員可自一高階應用程式執行該等組成部分之任何功能。由於提供這些組成部分的API，所以程式設計師可迅速地開發出一自訂規格的電子數位內容商店103，而無須重新設計任何這些組成部分的這些功能及資源。

電子數位內容商店103並不限於網路型的服務提供。想要銷售可下載電子內容113的所有電子數位內容商店103都可使用所提供的該等工具程式，而不必顧及用來將內容113配送到最終使用者的傳輸基礎設施或傳送模式。經由衛星或纜線基礎設施而提供的廣播服務也利用這些工具程式來取得、包封、及追蹤電子內容113的銷售。供銷售的電子式貨品之展現方式及將這些電子式貨品配送到最終使用者的方法是廣泛型服務提供與點對點互動網路型態服務提供之間主要的不同點。

B.點對點電子數位內容配送服務

點對點主要意指電子數位內容商店103與最終使用者裝

五、發明說明（141）

置109之間的一對一互動式服務。此種方式通常代表一種經由電話或纜線數據機連線而提供的網際網路型服務。在本模型中也支援網際網路以外的網路，只要這些網路符合網路伺服器/用户端瀏覽器的模型即可。圖9是一電子數位內容商店103的主要工具程式、組成部分、及程序之方塊圖。

1.整合要求

安全數位內容電子式配送系統100不只是產生了新的線上業務，而且也提供了一種讓現有企業將可下載電子內容113的銷售整合到其現有銷售管道之方法。提供給電子數位內容商店103的工具程式套件簡化了此種整合的程序。內容取得工具程式171及SC(s)包封工具程式153提供了一種方法給電子數位內容商店103，電子數位內容商店103利用該方法自參與的內容提供者101取得其可用來銷售的資訊，並產生將這些可下載物件對照到其本身庫存中的項目所需之檔案。可以批次方式驅動該程序，並可將該程序的大部分自動化，並且只在將新的內容113整合到網站時才執行該程序。

用於安全數位內容電子式配送的工具程式已被設計成可將可下載電子內容113的銷售整合到網路型電子數位內容商店103的典型實施例(例如 Columbia House Online、Music Boulevard、@Tower)及等效實施例，而且只需對其現行的內容113零售典範作最小的改變。有數種可行的整合方法，而且在較佳實施例中，電子數位內容商店103對全產

五、發明說明（142）

品搜尋、預覽、選擇(購物車)、及購買都提供了支援。每一電子數位內容商店103都要培養其客户的忠誠度，並以目前所作的相同方式持續提供其本身的促銷方案且行銷其產品。在安全數位內容電子式配送系統100中，只需指示其庫存中的哪些產品可供電子式下載，並讓其客户於進行購買選擇時可選擇電子式下載的選項。在另一實施例中，客户的購物車可混合包含電子(內容113)及實體媒體的選擇。在客户結帳之後，電子數位內容商店103已完成了金融結算，並記錄及通知其出貨及裝卸貨功能，以便處理所購買的實體貨品，電子數位內容商店103的商務處理函式然後呼叫交易處理模組175以處理所有的電子式下載。電子數位內容商店103只傳送所需的資訊，且自該時點起，將由安全數位內容電子式配送系統100的工具程式套件處理所有的程序。在另一實施例中，如果電子數位內容商店103只希望銷售可下載的貨品，或希望將實體的及可下載的貨品之金融結算分開，則亦可利用安全數位內容電子式配送系統100的工具程式而執行其他的交易處理方法，以便處理金融結算。

爲了處理貨品的下載，針對自內容提供者101的內容促銷網站156取得的每一種可下載產品，將一產品識別碼(圖中未示出)提供給電子數位內容商店103。該產品識別碼係與客户對一可下載產品的購買選擇相關聯。電子數位內容商店103將該產品識別碼傳送到交易處理模組175，以便識別使用者所購買的產品。爲了描述產品而產生的SC(s)(報

五、發明說明（143）

價SC(s) 641)係與電子數位內容商店103隔離，且係存放在一報價資料庫181中，以便簡化對這些物件的管理，並使這些物件的存在對電子數位內容商店103具有透通性。

提供交易處理模組175及其他額外的函式作爲網路伺服器端的可執行檔(亦即CGI及NSAPI、ISAPI可呼叫函式)，或只將各API整合到一DLL或C物件函式庫中。這些函式處理最終使用者互動及與交換所105間的或有互動之執行時程序。這些函式與網路伺服器的客户服務程式互動，以便產生用來啓動內容113下載程序所需的檔案，並將該等檔案下載到最終使用者裝置109。這些函式也處理或有的互動，以便提供授權及接受活動完成的通知。

也提供一對帳工具程式，以便協助電子數位內容商店103聯繫交換所105，以便根據其本身的交易記錄及交換所105的交易記錄而對帳。

2.內容取得工具程式 171

內容取得工具程式171負責連接到內容促銷網站156，以便預覽及下載中介資料SC(s) 620。因爲內容促銷網站是一標準網站，所以電子數位內容商店103利用一網路瀏覽器來瀏覽該網站。瀏覽的特性將依據內容提供者101的網站設計而有所不同。也些網站可能使許多的促銷資訊畫面具有廣泛的搜尋能力。其他的網站可能只提供簡單的瀏覽器介面，用以自曲名、演出者、或新發行項目的清單中作選擇。所有網站都包含中介資料SC(s) 620的選擇，而中介資料SC(s) 620包含了一首歌曲或一張專輯的所有促銷資訊及

五、發明說明（144）

描述性資訊。

此外，電子數位內容商店103可訂閱內容更新，並經由FTP而自動接收更新。

閱覽中介資料

內容取得工具程式171是一網路瀏覽器協助應用程式，而當在內容促銷網站156上選擇一中介資料SC(s) 620連結時，即啓動該內容取得工具程式171。選擇該SC(s)時，將使內容取得工具程式171下載到電子數位內容商店103，並啓動該協助應用程式。內容取得工具程式171開啓中介資料SC(s) 620，便顯示中介資料SC(s) 620內含的無加密資訊。在一音樂的例子中，所顯示的資訊包括所提取的中介資料173、與歌曲相關聯的圖形影像、及描述該歌曲的資訊，而如果該歌曲的一試聽片段包含在中介資料SC(s) 620中，則亦可收聽該試聽片段。在內容113是音樂的一個例子中，如果內容提供者101有提供，則亦顯示與歌曲或專輯有關的促銷資訊、專輯名稱、及藝人。係顯示該資訊作爲瀏覽器視窗中的一系列連結HTML網頁。無法自零售內容網站180取得諸如歌曲及歌詞等的可購買內容113、以及內容提供者101想要保護的中介資料。

在另一實施例中，內容提供者101提供付費下載的可選用之促銷內容。在該實施例中，係在中介資料SC(s) 620中將該促銷內容加密。當已向電子數位內容商店103的帳户索取指定的費用時，即可經由交換所105而處理因開啓該資料所發生的金融結算。

五、發明說明（145）

提取中介資料

除了預覽的能力之外，該工具程式提供了兩種額外的特殊功能：中介資料提取、及報價SC(s) 641的準備。選擇中介資料提取選項時，提示電子數位內容商店103將路徑及檔案名稱輸入到將要儲存該中介資料的位置。係將諸如圖形及音樂試聽片段等的二進位中介資料儲存成獨立的檔案。將文字中介資料儲存在一ASCII定界文字檔，零售內容網站180然後可將該ASCII定界文字檔輸入到其資料庫中。也在一獨立的TOC檔案中產生用來描述該ASCII定界文字檔之一表。也有額外的選項，可在其他國家語言支援(National Language Support；簡稱NLS)所支援的格式中進行提取。

所提取的資料中提供的一件重要資訊是產品識別碼。該產品識別碼是電子數位內容商店103的商務處理函式用來識別交易處理模組175(若要得知更多的資訊，請參閱交易處理該節)及使用者所購買的內容113之產品識別碼。交易處理模組175利用該產品識別碼來適當地自報價資料庫181擷取適當的報價SC(s) 641，以供隨後下載到最終使用者裝置109。電子數位內容商店103可完全控制其將可下載內容113在其網站上展現的方式。電子數位內容商店103只需要保留一份報價給該產品識別碼的內容113之交互對照，以便適當地連接到安全數位內容電子式配送系統100之工具程式。在此處提供該資訊時，可讓電子數位內容商店103以與報價SC(s) 641程序平行之方式，將該產品或內

五、發明說明（146）

容113整合到其庫存及銷售網頁(資料庫)中，這是因爲這兩個程序使用相同的產品識別碼來對照到該產品。下文中將進一步說明此種情形。

報價SC(s)產生包封工具程式153

電子數位內容商店103需要產生一報價SC(s) 641，用以描述供銷售的可下載內容113。係自中介資料SC(s) 620取得被放入報價SC(s) 641的資料中之大部分。內容取得工具程式171以下列步驟產生該報價SC(s) 641：

- 自中介資料SC(s) 620中移除並不需要被包含在中介資料SC(s) 620中的報價SC(s)樣板所指定的報價SC(s) 641中之各組成部分。
- 加入電子數位內容商店103的該工具程式組的組態設定選項所規定的預設項目指定之額外必須組成部分。
- 提示中介資料SC(s) 620的報價SC(s)樣板指定的額外必須輸入或選擇。
- 呼叫SC(s)包封工具程式153，以便將該資訊包封到SC(s)格式中。

在中介資料SC(s) 620中保留將由播放應用程式195在最終使用者裝置109上顯示的中介資料。自中介資料 SC(s) 620中移除只被電子數位內容商店103用來作爲其網路服務資料庫的輸入之其他促銷中介資料。亦保留諸如浮水印指令、加密的對稱金鑰623、及指定物件的容許使用的使用條件517等內容提供者101所提供之權利管理資訊。

然後在報價SC(s) 641中包含該拆開的中介資料SC(s)

五、發明說明（147）

620。電子數位內容商店103也將稱爲商店使用條件519或購買選項的其本身之使用條件附加到報價SC(s) 641。可以互動方式完成上述步驟，或經由一組預設的指令而自動完成上述步驟。如果被設定爲以互動方式處理，則以內容提供者101規定的一組容許之物件使用條件517來提示電子數位內容商店103。電子數位內容商店103然後選擇其想要提供給其客户的選項。這些選項現在變成新的使用條件或商店使用條件519。爲了自動地處理，電子數位內容商店103設定一組針對所有內容113而提供的預設購買選項。將這些預設選項自動比對內容提供者101規定的容許使用條件517，並於兩者並無不一致時，在報價SC(s) 641中設定這些預設選項。

一旦產生報價SC(s) 641之後，即將該報價SC(s) 641儲存在一報價資料庫181中，並以中介資料SC(s) 620中預先指定的產品識別碼作爲該中介資料SC(s) 620之索引。當一客户稍後連線到報價資料庫181而擷取報價SC(s) 641，以便包封並傳送到該最終使用者客户時，電子數位內容商店103利用該產品識別碼來識別該客户所購買的可下載內容113。若要得知更多的細節，請參閱交易處理模組175的該節。

在另一實施例中，電子數位內容商店103將報價SC(s) 641放在其網站上。該實施例需要改變報價SC(s) 641，例如以電子數位內容商店103的網址取代代管內容網站111的網址。

五、發明說明（148）

3.交易處理模組175

電子數位內容商店103將帳單開立的工作轉送到交換所105。此外，電子數位內容商店103亦可直接向交換所105要求金融清算。有兩種處理最終使用者對可下載內容113的購買要求之基本模式。如果電子數位內容商店103並不希望處理購買的金融結算，且並無將影響到貨品的銷售之特殊促銷及獎勵辦法，而且並未使用將購買要求批次化的一購物車圖像，則電子數位內容商店103可選擇提供將其內容113下載網頁直接連結到報價SC(s) 641。將以中介資料中包含的零售價格資訊建立這些報價SC(s) 641。展現具有銷售條款的購買選項之一特殊HTML報價網頁也是包含在報價SC(s) 641中。係利用建立報價SC(s) 641時所產生的一樣板來建立該網頁。當最終使用者點選到報價SC(s) 641的該直接連結時，即將該報價SC(s) 641下載到最終使用者裝置109之瀏覽器，而啓動一個用來開啓該容器物件並展現該報價SC(s) 641中包含的報價網頁之協助應用程式。該網頁包含一個用來收集客戶資訊之表格，該客戶資訊包括信用卡資訊及購買選項。然後將該表格直接傳送到交換所105，以供金融結算其處理。該表格可選擇包含使用最終使用者的信用資訊或工業標準的區域交易控制常式之欄位。

現在將說明電子數位內容商店103處理帳單開立的一實施例。處理購買要求的較典型模式可讓電子數位內容商店103處理金融結算，然後將下載授權許可傳送到最終使用

五、發明說明（149）

者。該方法可讓電子數位內容商店103將可下載內容113的銷售與所提供其他貨品整合，而在其網站上銷售，並可進行購買要求的批次處理，只須(經由一購物車圖像)向客户作一次的合併收費，而無須向每一次下載要求作個別的收費，並且可讓電子數位內容商店103直接追蹤其客户的購買模式，且提供特殊的促銷及會員優惠選項。在此種環境中，可下載內容113的報價係包含在電子數位內容商店103的購物網頁中，且當最終使用者選擇該內容113時，即將該內容113放到一購物車中，並以如同電子數位內容商店103現有購物模型之方式進行處理及金融結算。一旦完成該金融結算之後，安全數位內容電子式配送系統100的商務處理程序隨即呼叫交易處理模組175，以便完成該交易。

交易處理模組175

交易處理模組175的功能在於整合最終使用者裝置109所需的資訊，以便啓動並處理所購買內容113之下載。將該資訊包封到一交易SC(s) 640，網路伺服器然後回應該購買成交而將該交易SC(s) 640送回到最終使用者裝置109。交易處理模組175向電子數位內容商店103的商務處理程序要求三件資訊：所購買內容113之產品識別碼、交易資料642、及確認該購買結算的一HTML網頁或CGI網址。

該產品識別碼是在與所銷售內容113相關聯的中介資料SC(s) 620中而提供給電子數位內容商店103之值。該產品識別碼係用來自報價資料庫181擷取相關聯的報價SC(s)

五、發明說明（150）

641。

交易資料642是電子數位內容商店103的交易處理函式所提供的一資訊結構，且隨後利用該交易資料642使交換所105的處理與電子數位內容商店103執行的金融結算交易相關聯，並提供將包含在下載到最終使用者裝置109的內容113的浮水印之使用者識別資訊。當交換所105接收一有效的訂單SC(s) 650時，交換所105即記錄一個指示電子數位內容商店103已銷售內容113的交易，並記錄其中包括最終使用者的名稱及一交易識別碼535之交易資料642。交易識別碼535可提供對金融結算交易的一對照。交換所105隨後將該資訊送回到電子數位內容商店103，以便用來核對其帳户與自內容提供者101(或其代理商)接收的帳單開立報表是否一致。內容提供者101可利用交換所交易記錄178來決定其已銷售了哪些內容113，並使其得以向每一電子數位內容商店103開立帳單，以便收取其應得的授權費。亦可替代性地利用帳單開立以外的其他電子方式來結算內容提供者101與電子數位內容商店103之間的帳目。

交易SC(s) 640中提供的資訊以及交易SC(s) 640的安全性及完整性足以使交換所105信賴該購買交易是有效的，且在交換所105記錄該銷售之前，不需要有進一步的確認。然而，電子數位內容商店103可選擇在向其帳户收費之前(交換所105記錄交易而向內容提供者101指示電子數位內容商店103已收到銷售該內容113的帳款之時)，先要求該交易的確證。交易資料642中的一旗標指示對確證/通知的

五、發明說明（151）

該要求。在此種情形中，交換所105聯繫電子數位內容商店103，並在向其帳户收費且釋出加密金鑰623之前，先自電子數位內容商店103取得授權。自交換所105將該交易識別碼535傳送到電子數位內容商店103，作爲該確證要求的一部分，而使電子數位內容商店103得以將該要求與對最終使用者進行的一先前交易相關聯。該交易識別碼535可以是電子數位內容商店103希望使用且只用於此一功效的任何特有值。

交易資料642亦包含一客户名稱。該名稱可來自使用者購買時所填寫的購買表格的使用者名稱欄位，或來自先前電子數位內容商店103的某一使用者登錄程序期間所登錄的資訊，或與用於該交易的信用卡相關聯的信用卡資訊所得到的正式名稱。隨後將該名稱包含在授權許可浮水印527中。

交易資料642亦包含最終使用者所購買的商店使用條件519。該資訊係包含在授權許可浮水印527中，且最終使用者裝置109將該資訊用於拷貝及播放控制。

交易處理模組175所需的最後參數是確認該購買結算之HTML網頁或CGI網址。該參數之目的在於可讓電子數位內容商店103回應最終使用者，且電子數位內容商店103係利用金融結算的一確認訊息及其想要在其回應訊息中包含的任何其他資訊來回應該最終使用者。當接收並處理交易SC(s) 640時，該HTML網頁及CGI網址係包含在交易SC(s) 640中，且係顯示在最終使用者裝置109的瀏覽器視窗上。

五、發明說明（152）

交易SC(s) 640是在處理購買提交之後自電子數位內容商店103到最終使用者的HTTP回應。傳送一SC(s)作爲直接HTTP回應時，將強制在最終使用者裝置109上自動載入一SC(s)處理器協助應用程式，因而可自動完成交易，而無須依賴進一步由最終使用者啓動的動作。將在後文的最終使用者裝置109及播放應用程式195的該節中詳述該程序。

當以必須的參數呼叫交易處理模組175時，交易處理模組175建立一交易SC(s) 640，該交易SC(s) 640包含交易資料642、交易確認HTML網頁或參照網址、及SC(s)的其他必須安全特性，且交易處理模組175擷取及嵌入與該購買相關聯的報價SC(s) 641。交易處理模組175也記錄與該交易相關的資訊，以供爾後爲通知介面模組176及對帳工具程式179所使用。

4.通知介面模組176

通知介面模組176是一網路伺服器端的可執行常式(NSAPI、ISAPI、或等效API可呼叫的CGI或函式)。通知介面模組176處理來自交換所105、最終使用者裝置109、代管內容網站111、及內容提供者101之選項要求及通知。電子數位內容商店103可選擇要求通知的事件有：

- 交換所105對最終使用者裝置109要求一加密金鑰623且對稱金鑰623正針對指定的內容113釋出加密金鑰623之通知。可選擇將該通知設定成再將加密金鑰623傳送到最終使用者裝置109之前先要求來自電子數位內容商店103的確証。

五、發明說明（153）

- 代管內容網站111對已將內容SC(s) 630傳送到最終使用者裝置109之通知。
- 最終使用者裝置109對已接收到內容SC(s) 630及授權許可SC(s) 660並成功地利用該等SC(s)來處理內容113或發現該等SC(s)被篡改之通知。
- 內容提供者101對已將新的內容113置於內容促銷網站156之通知。

這些通知中的任一通知都不是安全數位內容電子式配送系統100中的一必須步驟，但是提供這些通知作爲使電子數位內容商店103有機會可關閉其有關成功完成銷售的記錄。這些通知由於讓電子數位內容商店103得知在交易的金融結算之後已透露了哪些功能，或得知於嘗試完成銷售的期間發生了哪些錯誤，而也提供了處理客户服務要求時可能需要用到的資訊。此外，可視需要而經由客户服務介面184自交換所105得到許多這類狀態。

由內容提供者101決定對在內容促銷網站156上可取得新內容113的通知頻度。可在每當加入新的中介資料SC(s) 620時，提供該通知，或者每天通知當天所加入的所有新中介資料SC(s) 620。

所有這些通知都將資料項加入交易記錄178。電子數位內容商店103想要對這些通知執行本身的處理，則電子數位內容商店103可攔截CGI呼叫，執行其特有的函式，然後可選擇將該要求傳送到通知介面模組176。

5.對帳工具程式179

五、發明說明（154）

對帳工具程式179聯繫交換所105，以便將交易記錄178與交換所105的記錄比較。上述程序是一種可供選用的程序，可用來協助電子數位內容商店103對安全數位內容電子式配送系統100的會計程序有信心。

在另一實施例中，可更新該工具程式，而提供電子式資金移轉，以便自動化對內容提供者101及交換所105的週期性付款。亦可將該工具程式設計成：在與交易記錄178對過帳單之後，於自交換所105接收到一電子式帳單時，可自動處理付款。

C.廣播電子數位內容配送服務

廣播主要意指一種一對多的傳輸方法，其中在最終使用者裝置109與電子數位內容商店103之間沒有可隨客户的需要而選擇閱覽或收聽的個人化介面。通常經由數位衛星或纜線基礎設施而提供廣播，此時係預先設定內容113，因而所有的最終使用者裝置109都接收相同的資訊流。

亦可界定一種混合式模型，使電子數位內容商店103可提供一種數位內容服務，且該數位內容服務的構成方式爲：可經由一網際網路連線而提供一網路配送介面，並可經由一廣播服務而提供寬頻衛星或纜線配送介面，且與網站的設計有相當大的共通性。如果IRD反向頻道串列介面係連接到網路，且該IRD支援網路瀏覽，則最終使用者可經由該反向頻道串列介面而以一般方式瀏覽數位內容服務，並預覽及選擇所要購買的內容113。使用者可選擇高品質的可下載內容113，然後購買這些選擇，並完全經由

五、發明說明（155）

一網際網路連線接收必須的授權許可SC(s) 660，然後要求經由寬頻廣播介面而傳送內容113(內容SC(s) 630)。網路服務可根據廣播時間表而指示可以此種方式下載哪些內容113，或者可完全根據所購買的內容113而建立廣播資訊流。此種方式可讓一網路型數位內容服務公司與一廣播機構簽約，而將高品質的內容113提供給配備有適當設備的使用者，因而每天可以此種高品質方式提供有限數目的特定內容113(例如歌曲或CD)，並將經由網路介面而以低品質方式提供可供下載的完整目錄。

亦可設計出並無通到最終使用者裝置109的網路介面之其他廣播模型。在此種模型中，係將促銷內容包封在特殊格式的數位流，以便用廣播方式傳送到最終使用者裝置109(亦即IRD)，在最終使用者裝置109上執行特殊的處理，以便將該數位流解碼，並向最終使用者顯示可用來作購買選擇的該促銷內容。

仍然係經由自最終使用者裝置109到交換所105的反向頻道通訊而啓動實際的購買選擇，且將利用SC(s)來執行所有的資料交換。提供給電子數位內容商店103的工具程式套件之架構及開發方式爲：大部分的工具程式都同時適用於點對點網際網路服務提供、及廣播衛星或纜線服務提供。衛星型電子數位內容商店103也利用數位內容網站型電子數位內容商店103取得及管理內容113並準備SC(s)所用之工具程式來管理並準備內容113，以便在一廣播基礎設施上配送。經由一網路服務而配送之SC(s)與經由一廣

五、發明說明（156）

播服務而配送之SC(s)相同。

X.最終使用者裝置109

安全數位內容電子式配送系統100的最終使用者裝置109中之應用程式執行兩個主要功能：第一，SC(s)處理及拷貝控制；以及第二，加密的內容113之播放。不論最終使用者裝置109是一個人電腦或一專用的消費電子裝置，該最終使用者裝置109都必須可執行這些基本功能。最終使用者裝置109也提供各種額外的特性及功能，例如產生播放清單、管理數位內容資料庫、於播放內容時顯示資訊及影像、以及錄製到外部媒體裝置。這些功能隨著這些應用程式支援的服務及這些應用程式被設計使用的裝置類型的不同而有所變化。

A.概述

現在請參閱圖10，圖中示出主要組成部分及程序、以及最終使用者裝置109的功能流程。被設計用來支援一個人電腦型網路介面內容113服務的應用程式包含兩個可執行的軟體應用程式：SC(s)處理器192、及播放應用程式195。SC(s)處理器192是一種可執行的應用程式，該應用程式被配置成一個放入最終使用者網路瀏覽器191之協助應用程式，用以處理SC(s)檔案/MIME類型。當自電子數位內容商店103、交換所105、及代管內容網站111接收到SC(s)時，瀏覽器即啓動該應用程式。該應用程式負責對SC(s)執行所有必須的處理，並將內容113加入最終使用者的數位內容資料庫196。

五、發明說明（ 157)

播放應用程式195是一獨立的可執行應用程式，最終使用者載入該播放應用程式195，以便執行其數位內容資料庫196中之內容113，管理其數位內容資料庫196，以及在容許時產生內容113之拷貝。可以Java、C/C++、或任何等效語言撰寫播放應用程式195及SC(s)處理器192應用程式。在較佳實施例中，可自諸如網站等的電腦可讀取的裝置下載該等應用程式。然而，也可利用其他的配送機制，例如在軟碟或CD等的電腦可讀取的媒體上配送該等應用程式。

完全係經由最終使用者網路瀏覽器191處理內容113資訊的搜尋及瀏覽、諸如歌曲片段的試聽、以及選擇所要購買的歌曲。電子數位內容商店103以與目前許多內容113零售網站所提供的相同方式來提供購物的體驗。與最終使用者經由目前的網路型內容113購物之不同處在於：使用者裝置現在可選擇將可下載的內容113物件加入其購物車中。如果電子數位內容商店103除了可下載的物件之外，還有其他可供銷售的貨品，則最終使用者可將實體貨品及電子式可下載貨品合併放到其購物車中。在最終使用者結帳並將其最後的購買授權傳送到電子數位內容商店103之前，安全數位內容電子式配送的最終使用者裝置109並不涉入其間。在該時點之前，係在電子數位內容商店103的網路伺服器與最終使用者裝置109的瀏覽器191之間進行所有的互動。這些互動包括數位內容樣本片段的預覽。數位內容片段並未被包封到SC(s)中，而是被整合到電子數位內容

五、發明說明（ 158）

商店103的網路服務中作爲可下載的檔案，或是自一串流伺服器傳送該數位內容片段。本系統架構並未規定內容113片段的格式。在另一實施例中，播放應用程式195可與電子數位內容商店103或交換所105直接互動，或利用促銷CD而進行離線互動。

B.應用程式安裝

將播放應用程式195及協助應用程式198被包封到可自許多網站下載的一自行安裝之可執行程式。交換所105係作爲在一公眾網站上存有主下載網頁的一中央網站。交換所105包含可下載安裝套裝軟體的各網站之連結。可在所有的代管內容網站111取得該安裝套裝軟體，以便在地理上分散下載的要求。每一參與的電子數位內容商店103亦可使該套裝軟體可自其網站下載，或者可只提供到交換所105的公眾網站上的主下載網頁之連結。

想要購買可下載內容113的任何最終使用者下載及安裝該套裝軟體。該安裝係自行包含在該可下載套裝軟體。該套裝軟體打開及安裝協助應用程式198及播放應用程式195，且亦將協助應用程式198的組態設定到所安裝的網路瀏覽器。

作爲該安裝的一部分，爲最終使用者裝置109產生一公用/祕密金鑰661對，以便用於處理訂單及授權許可SC(s)660。也產生一隨機對稱金鑰(祕密使用者金鑰)，以便用來保護授權許可資料庫197中之歌曲加密金鑰。將祕密使用者金鑰(圖中未示出)分散成多個部分，並將該金鑰的各

五、發明說明（ 160）

第一，該防篡改軟體包含可使駭客使用的除錯程式及反組合程式等標準軟體工具程式失效或至少降低其有效性之技術。第二，該防篡改軟體包含自我完整性檢查，因而將偵測到單一修改、甚至小量的修改，並造成不正確的作業。最後，該防篡改軟體包含可誤導駭客有關其確實作業的模糊點。最後一種技術大都是特別的技術，但是前兩種技術係根據加密及數位簽名等密碼學中習知的工具程式而建立。

C.安全容器物件處理器192

當最終使用者將其收集在其購物車中的貨品之最後購買授權傳送到電子數位內容商店103時，該最終使用者的網路瀏覽器即保持在連線狀態，等候來自網路伺服器的一回應。電子數位內容商店103上的網路伺服器處理該購買，並執行金融結算，然後將一交易SC(s) 640送回到最終使用者裝置109。網路瀏覽器啓動SC(s)處理器192(協助應用程式198)，以便處理與交易SC(s) 640相關聯的SC(s)多媒體網際網路郵件延伸(MIME)類型。圖14是播放應用程式195根據本發明而將內容下載到圖10所示的一本機資料庫的一使用者介面畫面實例。

SC(s)處理器192開啓交易SC(s) 640，並提取該SC(s)內含的回應HTML網頁及報價SC(s) 641。係在瀏覽器視窗中顯示回應HTML網頁，用以確認最終使用者的購買。然後在步驟1401中開啓報價SC(s) 641，並自這些報價SC(s) 641提取內容113(例如歌曲或專輯)名稱、及預計下載時間。然

五、發明說明（ 161）

後在步驟1402中利用該資訊顯示一個新的視窗，且將內容113(例如對於音樂而言，爲歌曲或整張專輯)下載的排定時程選項提供給最終使用者。最終使用者可選擇立即下載，或將下載安排在一稍後的時間。如果選擇了一稍後的時間，則將下載排程資訊儲存在一記錄中，而且在最終使用者裝置109於所安排的時間開機的情形下於該安排的時間開始下載。如果電腦在在所安排的下載時間並未開機，或通訊鏈路斷線，則在該電腦下一次開機時提示最終使用者重新安排下載的時間。

當到了所安排的下載時間，或要求立即下載時，則SC(s)處理器192利用交易SC(s) 640、報價SC(s) 641中的資訊、以及安裝時所產生的最終使用者公共金鑰661來產生訂單SC(s) 650。係經由HTTP要求將該訂單SC(s) 650傳送到交換所105。當交換所105送回授權許可SC(s) 660時，重新呼叫協助應用程式198來處理授權許可 SC(s) 660。然後開啓授權許可SC(s) 660，且自所參照的訂單SC(s) 650提取代管內容網站111之網址。然後經由瀏覽器的 HTTP 要求將授權許可SC(s) 660傳送到指定的代管內容網站111，而要求內容SC(s) 630的下載。當內容SC(s) 630傳送回瀏覽器時，再度重新呼叫協助應用程式198。SC(s)處理器192顯示所下載內容113的名稱、一下載進度指示器、及一預估完成時間。

當SC(s)處理器192正在接收內容113時，SC(s)處理器192將資料下載到記憶體緩衝區，以供解密。該緩衝區的容量

五、發明說明（ 162）

取決於加密演算法及浮水印技術193的需求，且該容量是可能作到的最小容量，以便減少未加密內容113洩漏給駭客程式碼的量。當一緩衝區填滿時，即利用自授權許可SC(s) 660提取的最終使用者金鑰623(對應於公共金鑰661)，將該緩衝區之內容解密，且係先利用祕密金鑰將金鑰623本身解密。然後將解密後的緩衝區內容傳送到加浮水印函式。

加浮水印程序193自授權許可SC(s) 660提取浮水印指令，並利用最終使用者的祕密金鑰將該等指令解密。然後自授權許可SC(s) 660提取浮水印資料，該浮水印資料包括諸如購買者名稱等的交易資訊，而該購買者名稱可以是登錄到購買內容113的電子數位內容商店103之購買者名稱，或者在電子數位內容商店103並未提供一登錄功能時可以是自信用卡登錄資訊得到的名稱。購買日期及交易識別碼535也係包含在浮水印中，其中係由電子數位內容商店103指定該交易識別碼535，以便對照到爲該交易記錄的特定記錄。也包含將爲播放應用程式519的拷貝控制功能所使用的商店使用條件195。

利用防篡改程式碼技術保護加浮水印程序193，以便不會洩漏浮水印指令，因而避免駭客發現浮水印的位置及技術。此種方式可防止駭客移除或修改浮水印。

在將任何必須的浮水印加到該內容緩衝區之後，將該緩衝區的內容傳送到亂序加密函式，以便進行重新加密程序194。利用諸如IBM的SEAL加密技術等的一有處理效率之

五、發明說明（ 164）

之方式。

解密與重新加密程序194的程序有兩個用途。儲存利用類似一演算法的SEAL加密的內容113時，可執行更快速的即時解密，且只需比諸如DES等更爲工業標準類型的演算法所需更少的處理器利用率，即可執行解密。此種方式可讓播放應用程式195對內容113執行一即時且並行的解密-解碼-播放，而無須在解碼及播放之前先將內容113的整個檔案解密。該SEAL演算法及一高效率解碼演算法的效率不只可進行並行的作業(自加密檔案的串流式播放)，而且也可在一效能低許多的系統處理器上執行該程序。因此，可在一諸如效能低至60百萬赫Pentium系統或效能更低的系統等的一最終使用者裝置109上支援該應用程式。使最後儲存內容113所用的加密格式與原始的加密格式分離時，可在選擇原始內容的加密演算法時有較大的彈性。因此，可使用被廣泛接受且經過考驗的工業標準演算法，因而進一步強化了數位內容業界對安全數位內容電子式配送系統100的接受度。

該解密與重新加密程序194之第二個目的在於：不再需要將內容提供者101用來將內容113加密的原始主加密金鑰623儲存在取得該內容113授權許可的每一個最終使用者裝置109。只在一段很短的時間中將作爲授權許可 SC(s) 660一部分的該主加密金鑰623緩衝儲存在最終使用者裝置109的硬碟上，而且該主加密金鑰623只在一段很短的時間中儲在記憶體上。在該執行階段期間，係經由防篡改程式碼

五、發明說明（ 165）

技術保護該金鑰623。一旦完成了該解密與重新加密194階段之後，就不再需要以任何形式將該金鑰623保留在最終使用者裝置109上，因而大幅降低了駭客進行破解的機率。

一旦將歌曲重新加密之後，即將該歌曲儲存在數位內容資料庫196中。在步驟1403中，自相關聯的報價SC(s) 641提取播放應用程式195所需的所有中介資料，並也將該等中介資料儲存在數位內容資料庫196。以前文中針對其他內容所述的相同方式，將諸如歌詞等的中介資料中之任何加密部分解密並重新加密。用來將內容113加密的同一SEAL金鑰係用於需要加密的任何相關聯之中介資料。

D.播放應用程式195

1.概述

安全數位內容電子式配送的播放應用程式195(在本文中稱爲播放應用程式195)類似於CD、DVD、或其他的數位內容播放機，並類似於CD、DVD、或其他的數位內容儲存管理系統。在該應用程式最簡單的功能中，係執行內容113，例如播放歌曲或視訊。在另一層級的功能中，該應用程式提供最終使用者一種管理該最終使用者的數位內容資料庫196之工具程式。在另一種同樣重要的功能中，該應用程式提供了對諸如歌曲等的內容資料庫(在此例中稱爲播放清單)之編輯及播放。

利用一組可以是經過個別選擇且針對內容提供者101及電子數位內容商店103的需求而訂製的組成部分組合成該

五、發明說明（166）

播放應用程式195。現在將說明該播放應用程式之一般性版本，但是使用者自訂的版本也是可行的。

現在請參閱圖15，圖中示出在圖10所示最終使用者裝置109上執行的播放應用程式195的主要組成部分及程序之方塊圖。

有數組構成播放物件管理程式1501的各子系統之元件：

1. 最終使用者介面元件1509
2. 拷貝/播放管理元件1504
3. 解密1505、解壓縮1506、播放元件1507、及可能包括的記錄元件。
4. 資料管理1502及資料庫存取元件1503
5. 應用程式間通訊元件1508
6. 其他雜項(例如安裝等)元件

可根據下列的需求而選擇每一個這類組內之各元件：

- 平台(Windows、Unix、或同等的作業系統)
- 通訊協定(網路、纜線等)
- 內容提供者101或電子數位內容商店103
- 硬體(CD、DVD等)
- 交換所105技術及其他技術。

下列各節將詳述各種元件組。最後一節將詳述如何將這些元件整合到該一般性播放應用程式，並說明如何依使用者的需求而自訂這些元件。

在另一實施例中，播放應用程式195及SC(s)處理器192的各元件可用來作爲程式設計師的軟體工具程式套件之一部

五、發明說明（167）

分。該工具程式套件起動前文所述一般性播放應用程式的各元件之預定介面。這些預定介面的形式爲應用程式介面(API)。利用這些API的開發人員可自一高階應用程式執行該等元件之任何功能。由於提供了這些元件的API，所以程式設計師可迅速開發一客户自訂規格的播放應用程式195，而無須重新產生任何這些元件的函式及資源。

2.最終使用者介面元件1509

該組的各元件合而提供播放應用程式195的螢幕上顯示。請注意，該設計並未建立這些元件的任何限定性配置。該一般性播放應用程式中提供了一個此種配置。可根據內容提供者101及(或)電子數位內容商店的需求以及其他需求，而提供替代性的配置。

該組被分成若干次組，第一個次組具有若干元件，用以展現最終使用者顯示幕1510，並處理用於音樂播放低階功能的稱爲最終使用者控制裝置1511之控制裝置，以及展現中介資料。然後再將最終使用者顯示幕元件1510分成若干特殊的功能組(播放清單、數位內容資料庫等)，然後利用物件容器元件將這些低階元件分類及放置。

在下文所述的元件清單內，任何提到產生CD或將內容113拷貝到一CD或其他可記錄媒體之處時，只適用於播放應用程式195已起動該功能的情形。亦請注意，在前後文中提及術語CD時意指總稱的CD，亦可代表諸如MD或DVD等各種其他的記錄裝置。

圖16是根據本發明的圖15所示播放應用程式195的一例

五、發明說明（ 168)

示使用者介面畫面。最終使用者控制裝置1511的功能包括(一最終使用者介面的對應畫面係示爲1601–1605)：

執行內容113之控制：

- 播放/停止按鈕
- 播放按鈕
- 停止按鈕
- 暫停按鈕
- 快速前轉按鈕
- 快速後轉按鈕
- 音量控制
- 音軌位置控制/顯示
- 聲道音量位準顯示及其他功能。

顯示與內容113相關聯的中介資料之控制裝置：

- 封面圖片按鈕
- 封面圖片物件
- 藝人照片按鈕
- 藝人照片物件
- 音軌表按鈕
- 音軌表資訊物件
- 音軌表選擇器物件(點選播放)
- 音軌名稱物件
- 音軌資訊物件
- 音軌歌詞按鈕
- 音軌歌詞物件

五、發明說明 (169)

- 音軌藝人名稱物件
- 音軌貸項按鈕
- 音軌貸項物件
- CD名稱物件
- CD貸項按鈕
- CD貸項物件
- 一般性(可設定組態之)中介資料按鈕
- 一般性中介資料物件及其他。

最終使用者顯示幕1510的功能包括(一最終使用者介面的對應畫面係示爲1601–1605):

顯示容器物件之播放清單

- 播放清單管理按鈕
- 播放清單管理視窗
- 數位內容搜尋按鈕
- 數位內容搜尋定義物件
- 數位內容搜尋送出按鈕
- 數位內容搜尋結果物件
- 播放清單按鈕之拷貝選擇搜尋結果
- 播放清單物件(可編輯的)
- 播放清單儲存按鈕
- 播放清單播放按鈕
- 播放清單暫停按鈕
- 播放清單重新開始按鈕
- 自播放清單按鈕產生CD及其他。

五、發明說明（ 170)

數位內容資料庫196之顯示

- 數位內容資料庫按鈕
- 數位內容資料庫管理視窗
- 數位內容種類按鈕
- 數位內容種類物件
- 按照藝人選擇按鈕
- 按照類型選擇按鈕
- 按照品牌選擇按鈕
- 按照種類選擇按鈕
- 刪除按鈕
- 增加到播放清單按鈕
- 拷貝到CD按鈕
- 歌曲清單物件
- 歌曲清單顯示容器物件及其他

容器物件及雜項

- 播放機視窗容器物件
- 音樂控制裝置容器物件
- 中介資料控制裝置容器物件
- 中介資料顯示容器物件
- 工具列容器物件
- 樣本按鈕
- 下載按鈕
- 購買按鈕
- 記錄按鈕

五、發明說明（ 171）

- 播放機名稱物件
- 品牌/提供者/商店廣告物件
- 品牌/提供者/商店網址按鈕
- 藝人網址按鈕及其他

3.拷貝/播放管理元件1504

這些元件處理加密金鑰、加入浮水印程序、拷貝管理、及其他程序之建立。也有與交換所105通訊的介面、傳輸購買要求的介面、以及諸如計次付費等特殊服務的介面、或按照每次對內容113的存取收費的情形之介面。目前係由SC(s)處理器192處理與交換所105各功能之通訊。

係將最終使用者裝置109上的播放應用程式195對內容113之使用記錄在一個諸如授權許可資料庫197等的資料庫。可將播放應用程式195對內容113的每一次使用之追蹤傳送到諸如交換所105、內容提供者101、電子數位內容商店103、或耦合到傳輸基礎建設107的任何指定網站等的一個或多個記錄網站。可將該傳輸安排在一預定時間，以便將使用資訊上傳到一記錄網站。可考慮的一個時間是傳輸基礎建設107上並無網路塞車現象的清晨之時。利用習知的技術在一預定時間將播放應用程式195喚醒，並將該資訊自本機的記錄資料庫傳送到該記錄網站。內容提供者101檢查記錄網站的資訊，即可衡量其內容113受歡迎的程度。

在另一實施例中，並不記錄內容113的使用，以供爾後上傳到一記錄網站，而是在每一次使用內容113時將內容

五、發明說明 (172)

113的使用狀況上傳到該記錄網站。例如，當將最終使用者裝置109中儲存的內容113複製或拷貝到諸如DVD、數位式磁帶、快閃記憶體、MD、或等效的可讀取/寫入之抽換式媒體等的一外部裝置時，即在該記錄網站上更新其使用狀況。上述情形可能是購買內容113時所傳送的使用條件206中對拷貝內容113規定的一先決條件。此種方式確保內容提供者101可在其內容113的播放、複製、或對內容113的進行的其他動作時，能夠精確地追蹤到其內容113的使用狀況。

此外，可將與內容113有關的其他資訊上傳到該記錄網站。例如，上一次執行內容113的時間(日期及小時)；已執行了內容113多少次；是否曾將內容113複製到或拷貝到一諸如DVD、數位式磁帶、或MD等的經授權之外部裝置。在最終使用者裝置109上的一單一播放應用程式195有多個不同的使用者之情形中，例如在一個家庭中的不同成員之情形中，係將內容113使用者的識別碼連同使用資訊傳送到該記錄網站。內容提供者101檢查上傳到該記錄網站的使用資訊，即可根據實際的使用狀況、使用者的身分、及內容113被執行的次數，而衡量內容113受歡迎的程度。此種實際使用的量度方式使本系統接近事實的程度優於諸如Nielsen對電視收視率的收視記錄器調查或電話抽樣調查等使用抽樣方法的系統，在此類抽樣方法的系統中，係在任何一個時間中只對數目有限的使用者進行抽樣調查，並以外差法推論出結果。在本實施例中，可針對記錄

五、發明說明（ 173）

到諸如電子數位內容商店103或內容提供者101等的一指定網站之使用者，而量度實際的使用狀況。

4.解密1505、解壓縮1506、及播放元件1506

這些元件使用拷貝/播放管理元件取得的金鑰將自資料管理及資料庫存取元件取得的音訊資料解密，然後進行適當的解壓縮，以便將該資料準備好以供播放，並利用系統音訊服務程式來播放該資料。在一替代實施例中，可將自該等資料管理及資料庫存取元件取得的音訊資料拷貝到諸如CD、軟碟、磁帶、或MD等的抽換式媒體。

5.資料管理1502及資料庫存取元件1503

這些元件係用來儲存及擷取最終使用者的系統上各種儲存裝置上之歌曲資料，並用來處理對所儲存歌曲有關的資訊之要求。

6.應用程式間通訊元件1508

這些元件係用於安全數位內容電子式配送的播放應用程式與其他應用程式(例如瀏覽器、協助應用程式、及(或)外掛應用程式等)間之協調，其中該等其他應用程式可能呼叫該播放應用程式195，或者該播放應用程式195與執行其功能時需要用到該等其他應用程式。例如，當起動一網址的控制元件時，該網址的控制元件呼叫適當的瀏覽器，並指示該瀏覽器載入適當的網頁。

7.其他雜項元件

無法歸類到上述各種類的一些個別元件(例如安裝)被歸類到此種類。

五、發明說明（ 174)

8.一般性播放應用程式

在本節中，將說明如何將上述各元件組合到一個版本的播放應用程式195。這只是多種不同的可能實例中之一實例，這是因爲播放應用程式195被設計成可根據軟體物件而自訂規格。

播放物件管理程式1501是一種整合所有其他元件之軟體架構。如同上述各節所說明的，在本圖示中在播放物件管理程式1501之下的各元件是任何播放應用程式中必須的元件，但是可根據所用的加密或亂序加密形式、音訊壓縮類型、以及對內容113資料庫的存取方法等的各種因素，而以特殊的版本取代該等元件。

在播放物件管理程式1501之上的是若干可變物件1512，且大部分係自與所播放或所搜尋的內容113相關聯的中介資料中衍生出該等可變物件1512。最終使用者裝置109利用最終使用者顯示幕1510及自最終使用者控制裝置1511接收的輸入，即可取得這些可變物件。所有物件的組態都是可設定的，且所有容器物件的配置都是可自訂的。可利用Java或任何等效的程式語言來實施這些物件。

使用播放應用程式195

下列實施例是最終使用者裝置109上執行的播放應用程式195是一音訊播放應用程式且內容113是音樂的一個例子。熟悉本門技術者當可了解，播放應用程式195亦可支援其他類型的內容113。典型的音樂愛好者都有歌曲CD的收集。在安全數位內容電子式配送系統100內可取得所有

五、發明說明（ 175）

這些歌曲CD。係將自電子數位內容商店103購買的一組歌曲儲存在這些音樂愛好者系統上的數位內容資料庫196內。係以播放清單之方式儲存類似於實體CD的各組歌曲。在某些情形中，播放清單係完全模擬CD的形式(例如，可自市場上購得的一CD之所有音軌都可以線上版CD之方式自一電子數位內容商店103購買，並以等同於CD方式之一播放清單界定該等所有音軌)。但是，多半係由最終使用者整合出播放清單，以便將其儲存在其系統的數位內容資料庫中的歌曲分類。然而，爲了便於後續的討論，在提及播放清單的術語時，係意指一使用者自行製作的音樂CD之例子。

當最終使用者明確地啓動播放應用程式195，而不是經由SC(s)處理器192應用程式的呼叫而啓動播放應用程式195時，播放應用程式195預先載入被存取的上一個播放清單。如果數位內容資料庫196中並無任何播放清單，則自動啓動播放清單編輯器(除非使用者已經由偏好設定而關閉了該功能)。若要得知更多的細節，請參閱下文中之播放清單該節。

亦可利用作爲一引數的一首特定的歌曲來呼叫播放應用程式195，在此種情形中，該播放應用程式195立即進入歌曲播放模式。亦可選擇使歌曲進入已準備好可播放的狀態，但是在播放之前須等候最終使用者的動作。若要得知此種情形的更多資訊，請參閱下文的歌曲播放一節。

播放清單(一最終使用者介面1603之對應畫面):

五、發明說明（ 176)

當最終使用者已呼叫播放清單功能時，有下列可使用的功能：

- 開啓播放清單
- 呼叫數位內容資料庫管理程式顯示所儲存播放清單之一清單，以供選擇。若要得知更多的資訊，亦請參閱下文的數位內容資料庫管理程式一節。
- 編輯播放清單
- 呼叫播放清單編輯器(請參閱下文)，如果已載入了播放清單，則亦可使用現行的播放清單。否則，該編輯器將產生一個空的播放清單作爲開始。
- 執行播放清單
- 自所選擇的歌曲開始(如果並未選擇歌曲，則自該播放清單的第一首開始)，以一次一首之方式播放歌曲。播放清單編輯器中設定的選項將影響到播放的順序。然而，可利用控制功能來越過播放清單的這些播放選項。
- 播放歌曲
- 只播放自播放清單選出的歌曲。若要得知更多的資訊，請參閱下文的歌曲播放一節。
- 播放清單資訊
- 與播放清單有關的顯示資訊。
- 歌曲資訊
- 與播放清單內所選擇歌曲有關的顯示資訊。
- 連線到網站

五、發明說明（ 177）

- 將與該播放清單相關聯的網站載入瀏覽器中。
- 資料庫管理程式
- 開啓數位內容資料庫管理程式視窗。若要得知更多的資訊，亦請參閱下文的數位內容資料庫管理程式一節。

播放清單編輯器(一最終使用者介面1603之對應畫面)：

當呼叫播放清單編輯器時，有下列的最終使用者選項：

- 閱覽/載入/刪除播放清單
- 呼叫數位內容資料庫管理程式顯示所儲存播放清單的一清單，以便選擇一個要載入或刪除的播放清單。若要得知更多的資訊，亦請參閱下文的數位內容資料庫管理程式一節。
- 儲存播放清單
- 將現行版本的播放清單儲存在數位內容資料庫196中。
- 刪除歌曲
- 自播放清單中刪除目前選擇的歌曲。
- 加入歌曲
- 在歌曲搜尋模式中呼叫數位內容資料庫管理程式，以便選擇要加入播放清單之歌曲。若要得知更多的資訊，亦請參閱下文的數位內容資料庫管理程式一節。
- 設定歌曲資訊
- 顯示與播放清單內所選擇歌曲有關之資訊，且容許對該資訊的改變。該資訊係儲存在播放清單內，且並不

五、發明說明（ 178）

改變與數位內容資料庫196內儲存的歌曲有關之資訊。

- 顯示歌曲名稱
- 最終使用者加上與歌曲有關的註釋
- 播放歌曲時的引入延遲
- 在播放歌曲之後的跟隨延遲
- 播放時歌曲內的起點
- 播放時歌曲內的終點
- 隨機模式的加權
- 該歌曲的音量調整及其他。

設定播放清單屬性：顯示內容庫的屬性，並容許對該屬性的改變。可設定的這些屬性有：

- 播放清單名稱
- 播放清單模式(隨機、循序等)
- 重播模式(播放一次、播放完畢後重新開始等)
- 最終使用者對該播放清單所加上的註釋。

資料庫管理程式(一最終使用者介面1601之對應畫面)：

- 開啓數位內容資料庫管理程式視窗。若要得知更多的資訊，亦請參閱下文的數位內容資料庫管理程式一節。

歌曲播放

當利用該歌曲作爲引數呼叫播放應用程式195，或自一播放清單或在數位內容資料庫管理程式內選擇一歌曲以供播放，而準備該歌曲以供播放時，有下列的最終使用者選項(一最終使用者介面1601的對應畫面)：

五、發明說明（ 179）

- 播放
- 暫停
- 停止
- 快速後轉
- 快速前轉
- 調整音量
- 調整音軌位置
- 預覽歌詞
- 預覽貸項
- 閱覽CD封面
- 閱覽藝人照片
- 閱覽音軌資訊
- 預覽其他中介資料
- 連線到網站
- 播放清單
- 資料庫管理程式。

數位內容資料庫管理程式

可於選擇歌曲或播放清單時自動呼叫數位內容資料庫管理程式(請參閱前文)，或可在其本身的視窗中開啓數位內容資料庫管理程式，以便管理最終使用者系統上的歌曲資料庫。在此種情形中，有下列的最終使用者選項：

對歌曲的操作：

根據藝人、種類、品牌、及其他因素而分類所有的歌曲

五、發明說明（ 180）

根據藝人、種類、品牌、及其他因素而選擇歌曲

將所選擇的歌曲加入現行播放清單

將歌曲拷貝到CD(如果被起動)

刪除歌曲

將歌曲加入種類，及其他。

對播放清單的操作：

根據名稱而分類

根據種類而分類

根據關鍵字而搜尋

根據所包含歌曲的名稱而搜尋

載入所選擇的播放清單

重新命名播放清單

刪除播放清單

自所選擇的播放清單(如果被起動)產生CD，及其他。

雖然已揭示了本發明的一特定實施例，但是熟悉本門技術者當可了解，在不脫離本發明的精神及範圍下，尚可對該特定實施例作出改變。因此，本發明之範圍並不限於該特定實施例，且最後的申請專利範圍將涵蓋本發明範圍內的任何及所有此類申請案、修改、及實施例。

A5
B5

四、中文發明摘要（發明之名稱：　電子內容傳送系統之多媒體播放機　）

本發明揭示一種播放已在一系統上壓縮過且利用一第一加密金鑰加密過的數位內容資料之方法。根據該方法，係利用一對應於該第一加密金鑰的一第一解密金鑰將至少部分的該內容資料解密。將該解密的內容資料解壓縮，以便產生解壓縮的內容資料，並播放該解壓縮的內容資料。在一較佳方法中，擷取分別儲存在該系統上的一第二解密金鑰之多個區段，且利用該第二解密金鑰將該第一解密金鑰解密。此外，本發明供了一種用來播放已壓縮過且利用一第一加密金鑰加密過的數位內容之數位內容播放機。該數位內容播放機包含：一解密器，用以利用一對應於該第一加密金鑰的第一解密金鑰將至少部分的該內容資料解密；一解壓縮器，用以將該解密的內容資料解壓縮；以及一播

英文發明摘要（發明之名稱：　"MULTIMEDIA PLAYER FOR AN ELECTRONIC CONTENT DELIVERY SYSTEM"　）

A method of playing digital content data that has been compressed and encrypted with a first encrypting key on a system. According to the method, at least part of the content data is decrypted with a first decrypting key that corresponds to the first encrypting key. The decrypted content data is decompressed to produce decompressed content data, and the decompressed content data is played. In one preferred method, multiple segments of a second decrypting key that are stored separately on the system are retrieved, and the first decrypting key is decrypted using the second decrypting key. Additionally, a digital content player for playing digital content that has been compressed and encrypted with a first encrypting key is provided. The digital content player includes a decrypter for decrypting at least part of the content data using a first decrypting key that corresponds to the first encrypting key, a decompressor for decompressing the decrypted content data, and a player for playing the decompressed content data. In one preferred player, the decrypter retrieves multiple segments of a second decrypting key that are stored separately on the computer system, and decrypts the first decrypting key using the second decrypting key.

Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system, the method comprising the steps of: transferring the encrypted data decrypting key to a clearing

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

A5
B5

四、中文發明摘要（發明之名稱：　　）

放機，用以播放該解壓縮的內容資料。在一較佳的播放機中，該解密器擷取分別儲存在該電腦系統上的一第二解密金鑰之多個區段，且利用該第二解密金鑰將該第一解密金鑰解密。

本發明揭示了一種安全地將資料提供給一使用者的系統之方法及裝置。將資料加密，以便只能夠利用一資料解密金鑰將該資料解密，其中係利用一第一公開金鑰將該資料解密金鑰加密，且該使用者的系統可存取該加密的資料，該方法包含下列步驟：將該加密的資料解密金鑰傳送到一擁有對應於該第一公開金鑰的一第一私人金鑰之交換所；利用該第一私人金鑰將該資料解密金鑰解密；利用一第二公開金鑰將該資料解密金鑰重新加密；將該重新加密的資料解密金鑰傳送到該使用者的系統，而該使用者的系統擁有一對應於該第二公開金鑰之第二私人金鑰；以及利用該第二私人金鑰將該重新加密的資料解密金鑰解密。

英文發明摘要（發明之名稱：　　）

house that possesses a first private key, which corresponds to the first public key; decrypting the data decrypting key using the first private key; re-encrypting the data decrypting key using a second public key; transferring the re-encrypted data decrypting key to the user's system, the user's system possessing a second private key, which corresponds to the second public key; and decrypting the re-encrypted data decrypting key using the second private key.

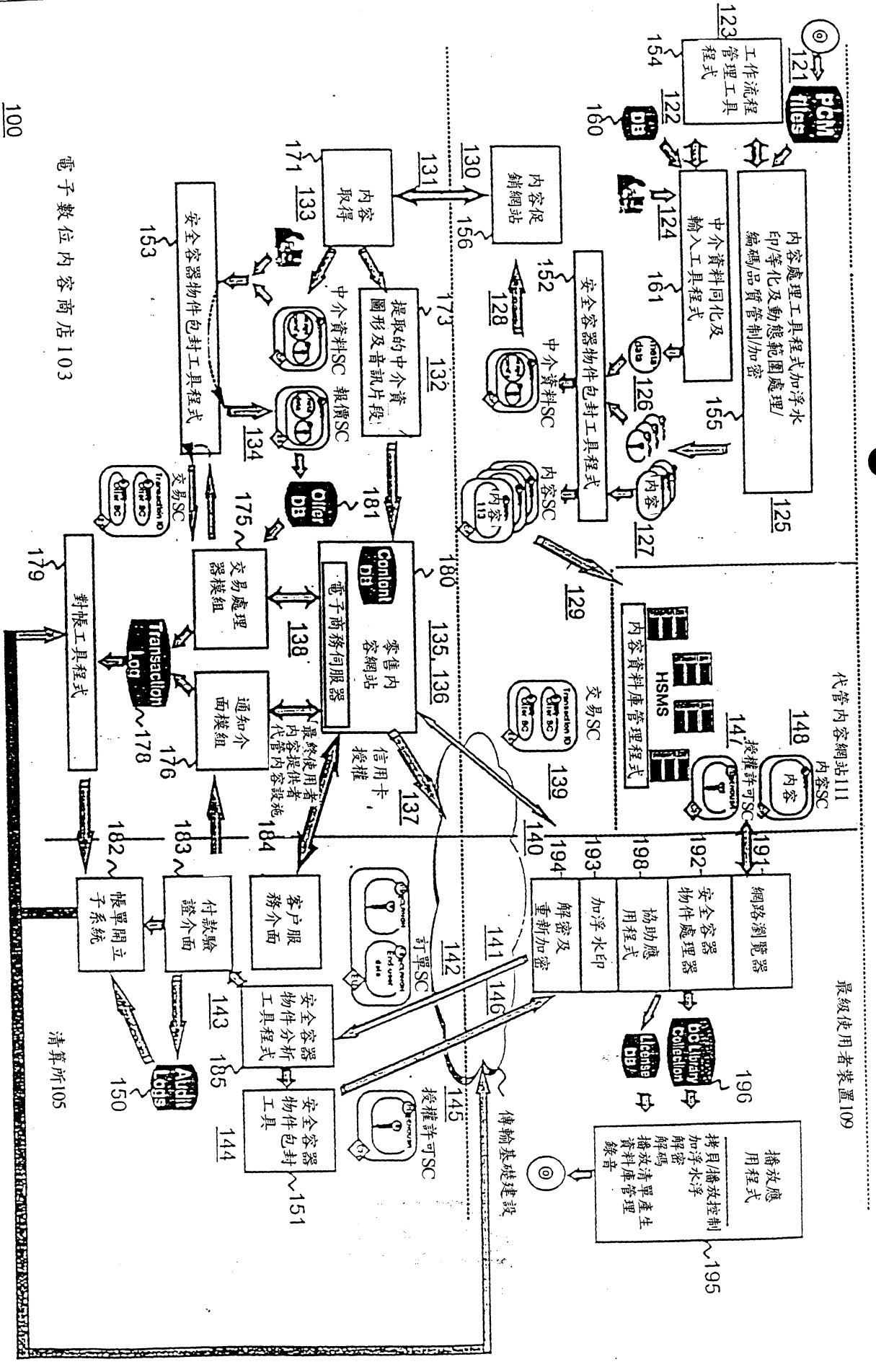

圖1. 安全數位內容電子式配送系統

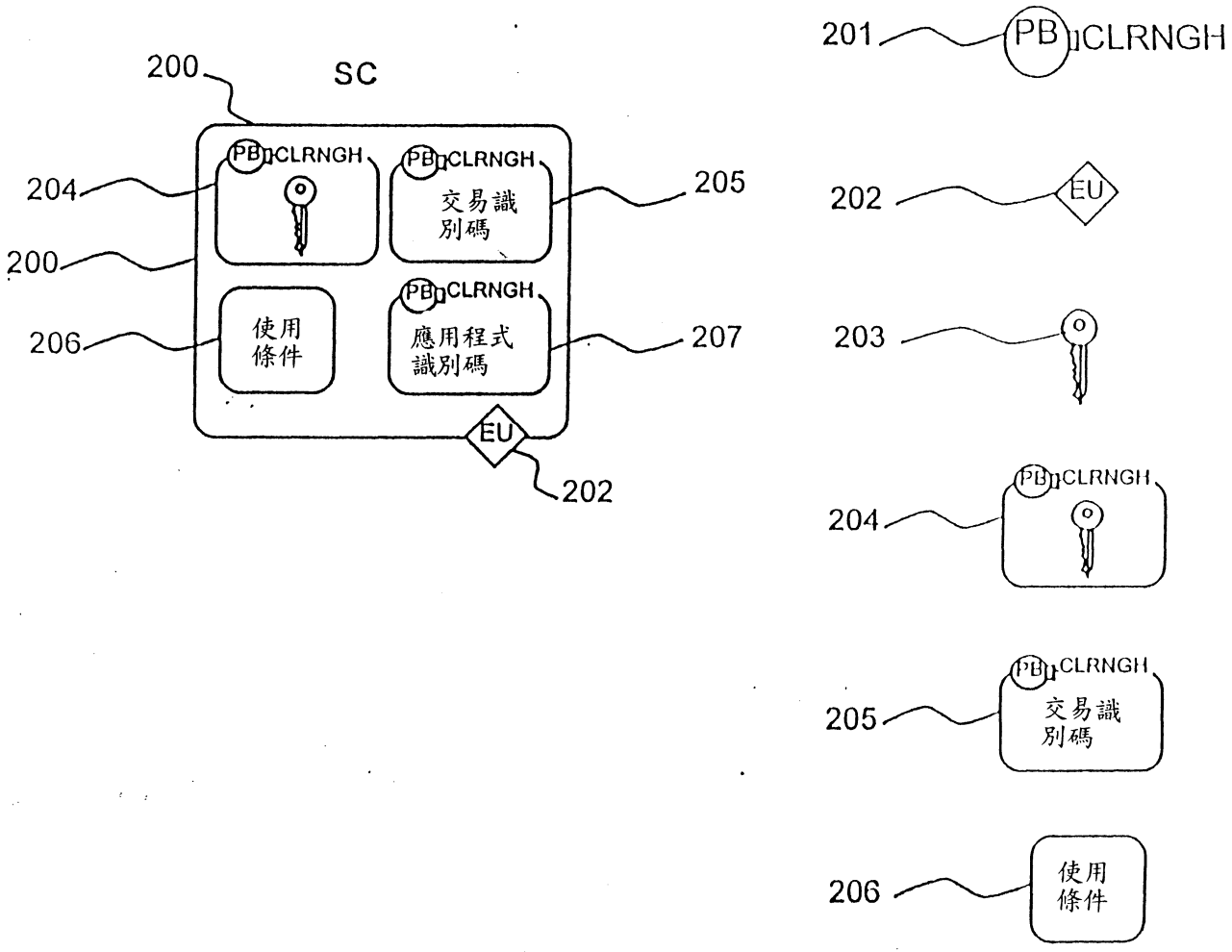

圖 2. 對本發明的一實施例說明中所用的圖形符號

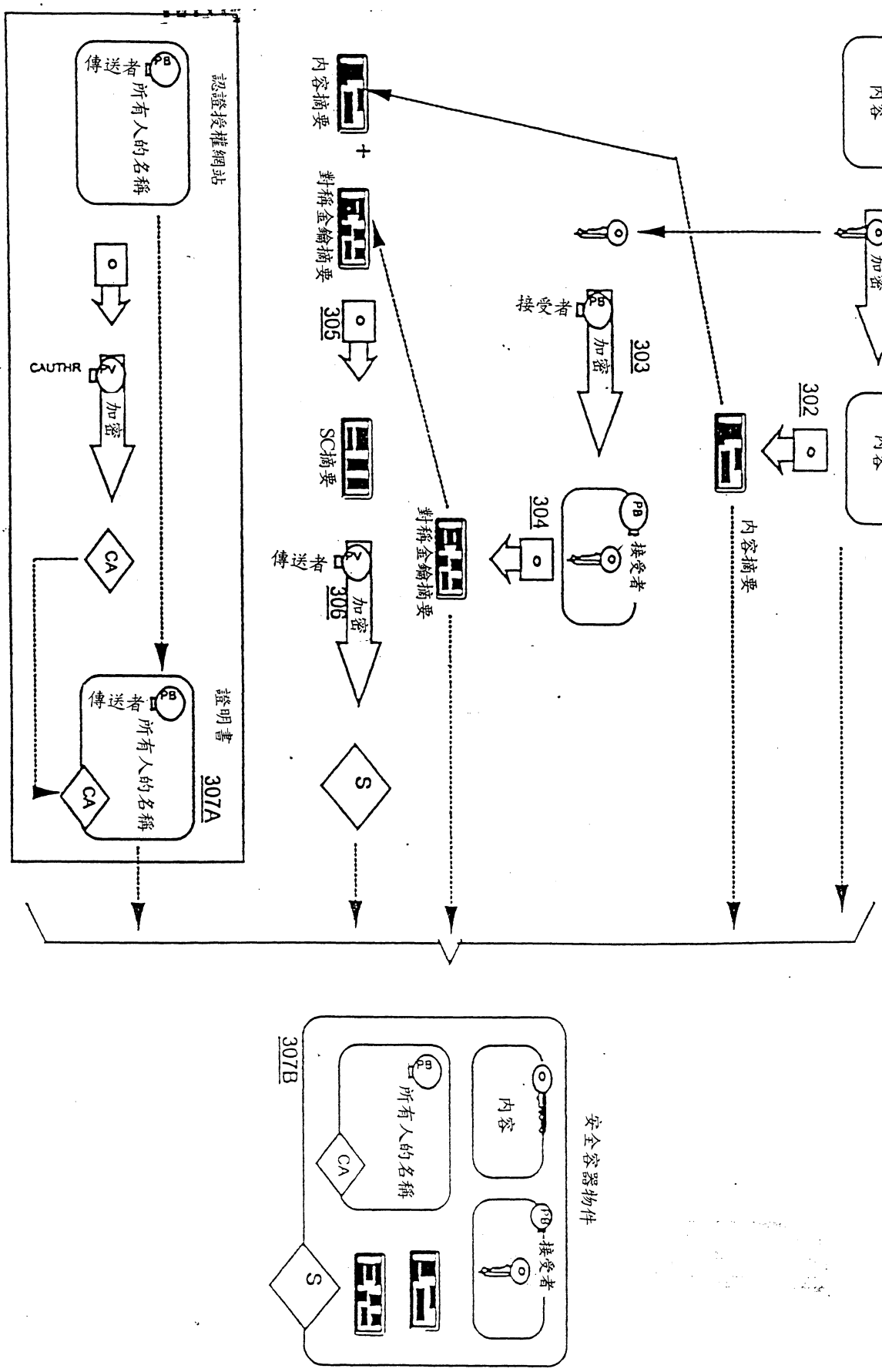
內容
301
加密
內容
302
內容摘要
303
加密
接受者
304
接受者
對稱金鑰摘要
內容摘要
+
對稱金鑰摘要
305
SC摘要
加密
306
S
認證授權網站
所有人的名稱
加密
CA
證明書
307A
所有人的名稱
CA
安全容器物件
內容
接受者
所有人的名稱
CA
S
307B

圖 3. 加密程序

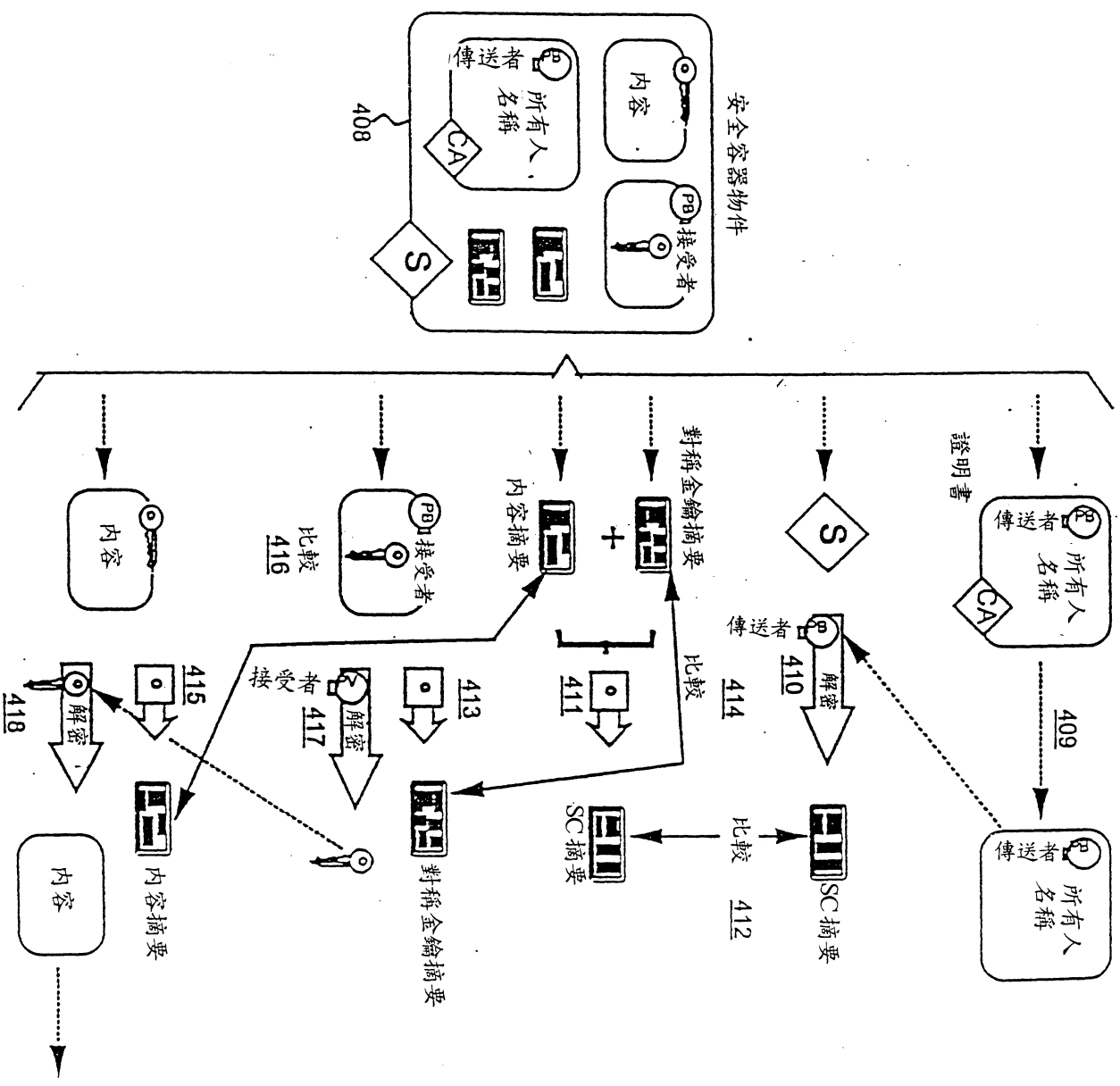
安全容器物件
408
內容
PB 接受者
所有人名稱
者送傳
CA
S
證明書
所有人名稱
者送傳
CA
409
S
解密
者送傳
410
SC摘要
比較
412
414
對稱金鑰摘要
+
內容摘要
411
比較
SC摘要
對稱金鑰摘要
413
內容摘要
415
解密
者受接
417
解密
418
內容
比較
416
PB 接受者
內容

圖4. 解密程序

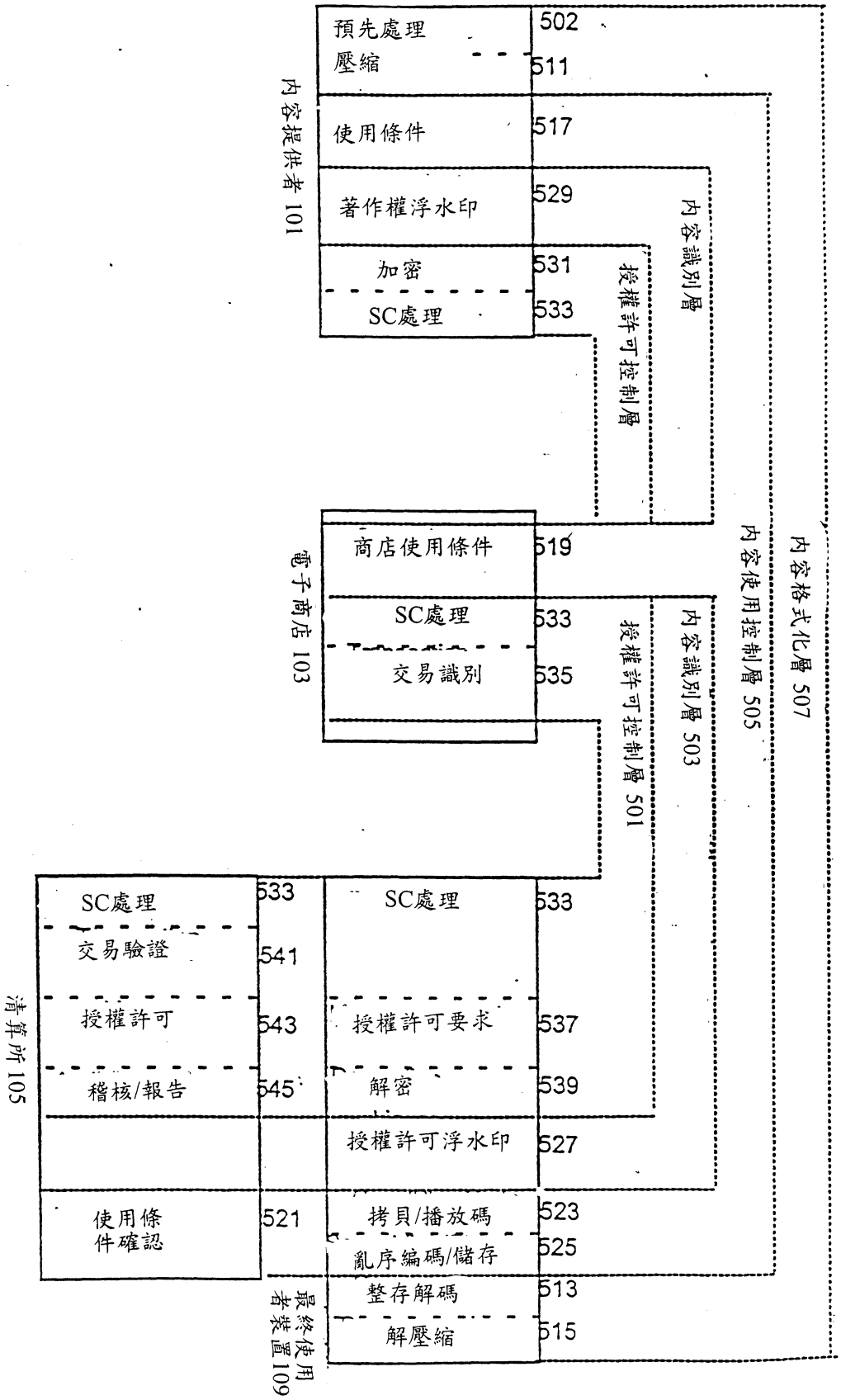
內容格式化層 507
內容使用控制層 505
內容識別層 503
授權許可控制層 501
內容提供者 101
預先處理
壓縮
502
511
使用條件
517
著作權浮水印
529
加密
531
SC處理
533
電子商店 103
商店使用條件
519
SC處理
533
交易識別
535
清算所 105
SC處理
533
交易驗證
541
授權許可
543
稽核/報告
545
使用條件確認
521
SC處理
533
授權許可要求
537
解密
539
授權許可浮水印
527
拷貝/播放碼
523
亂序編碼/儲存
525
整存解碼
513
解壓縮
515
最終使用者裝置 109

圖 5. 權利管理架構

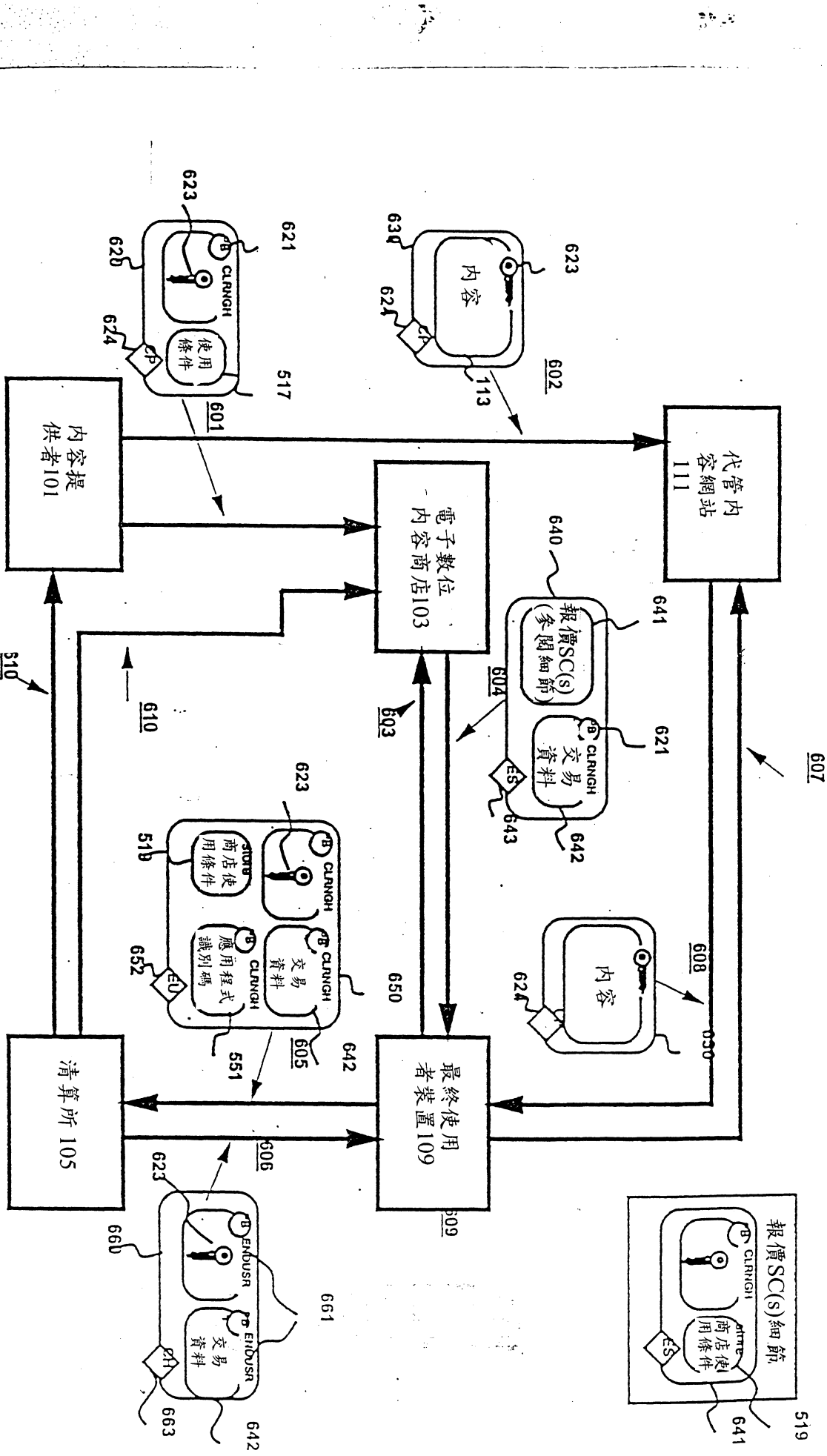

圖 6. 內容配送及授權許可控制

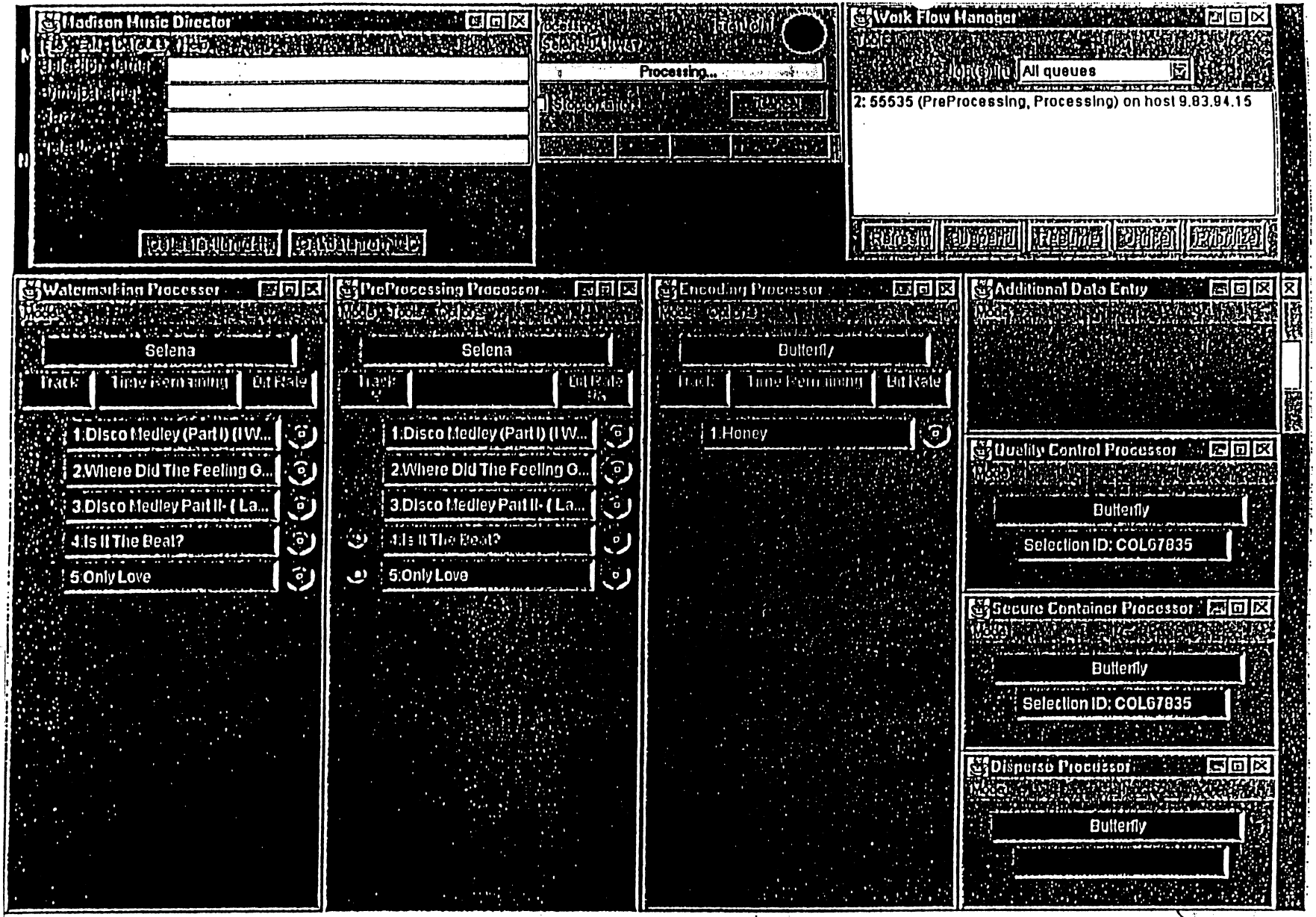

圖 7. 工作流程管理工具程式之使用者介面

700

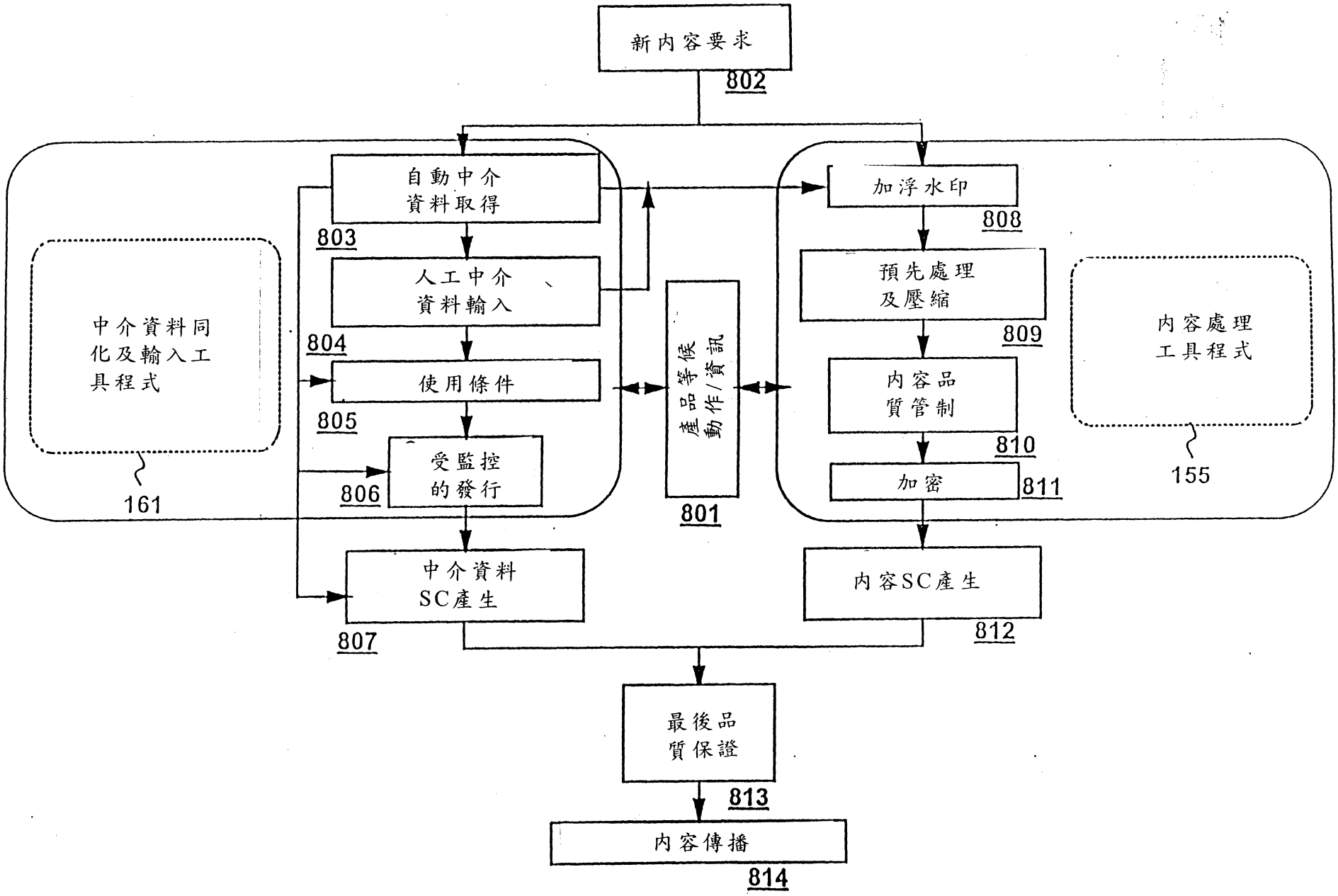

圖8. 工作流程管理工具程式

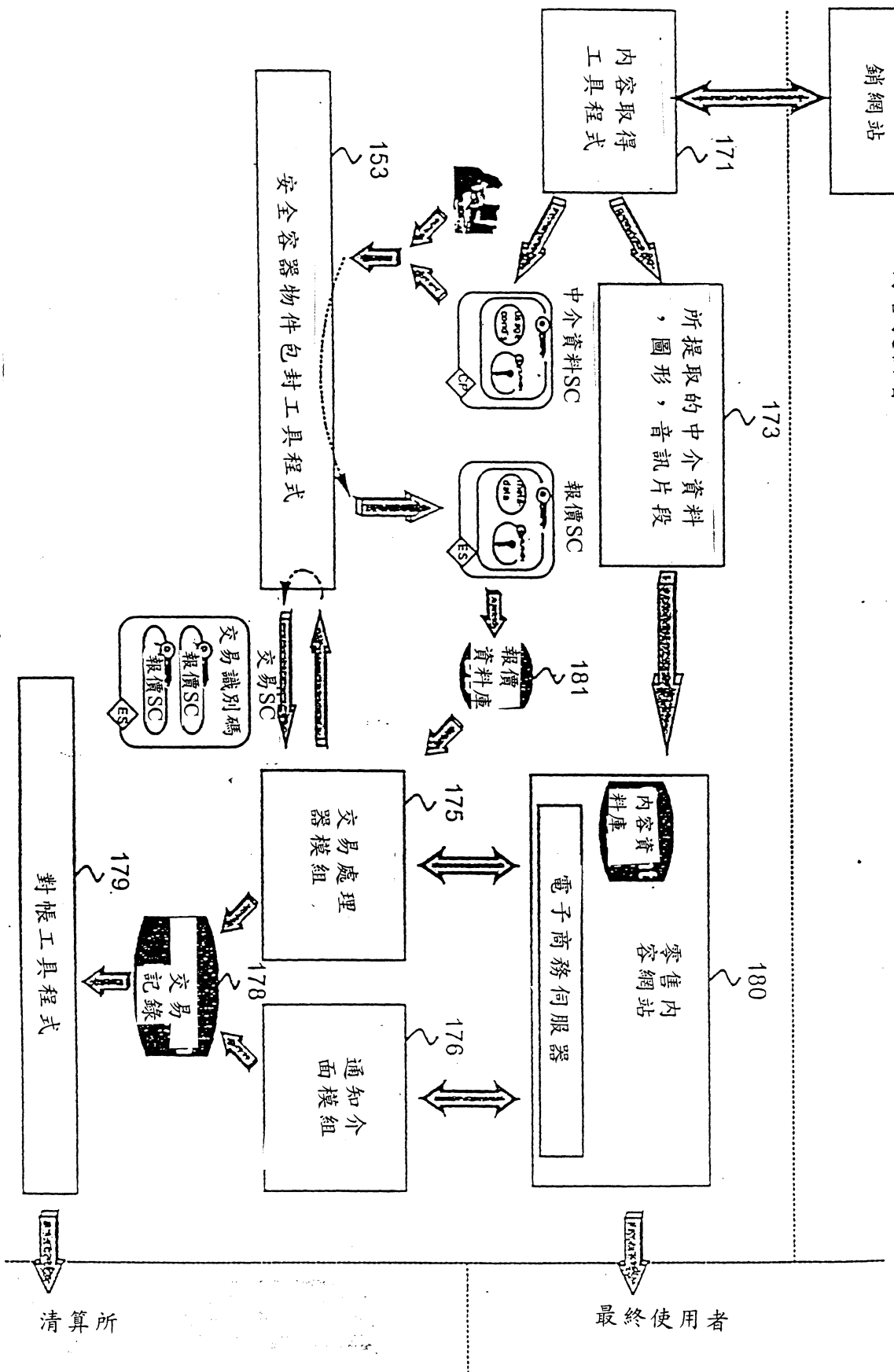
156
內容促銷網站
內容提供者
171
內容取得工具程式
173
所提取的中介資料，圖形，音訊片段
中介資料SC
報價SC
153
安全容器物件包封工具程式
181
報價資料庫
交易識別碼
報價SC
交易SC
175
交易處理器模組
176
通知介面模組
178
交易記錄
179
對帳工具程式
180
零售內容網站
內容資料庫
電子商務伺服器
最終使用者
清算所

圖 9. 電子數位內容商店

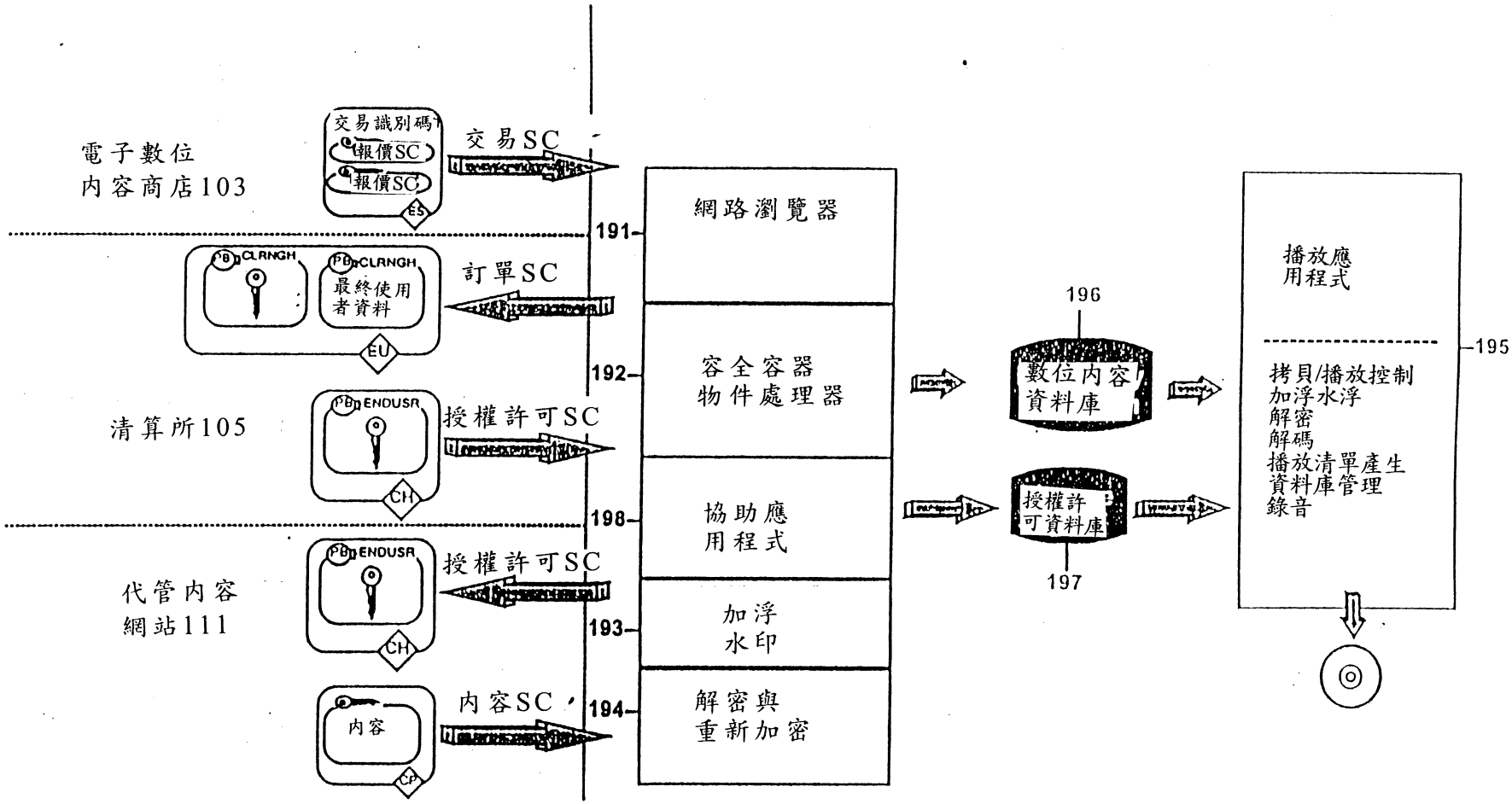

圖10.最終使用者裝置109

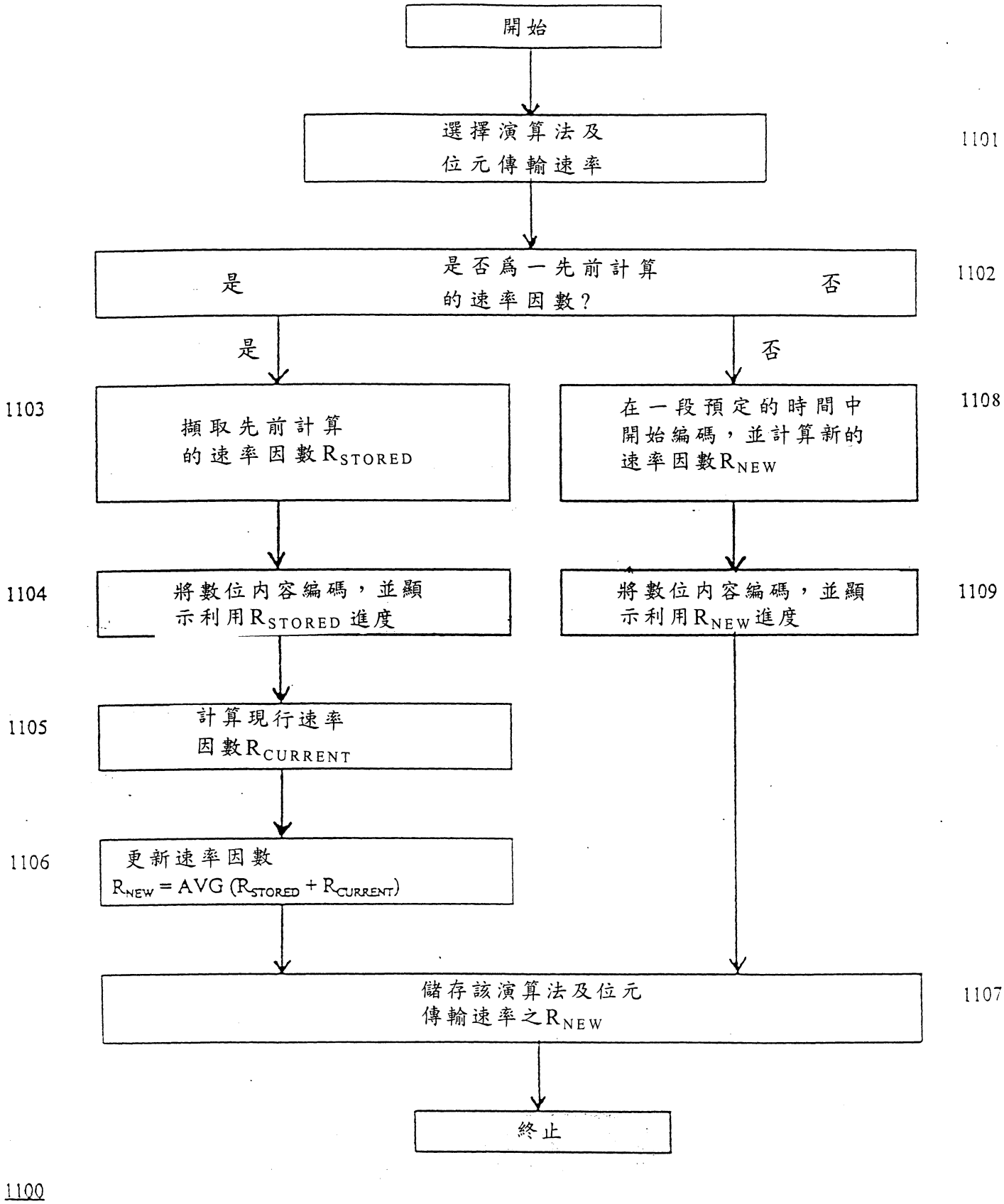
開始
選擇演算法及
位元傳輸速率
1101
是否爲一先前計算
的速率因數？
是
否
1102
是
否
1103
擷取先前計算
的速率因數 R_{STORED}
在一段預定的時間中
開始編碼，並計算新的
速率因數 R_{NEW}
1108
1104
將數位內容編碼，並顯
示利用 R_{STORED} 進度
將數位內容編碼，並顯
示利用 R_{NEW} 進度
1109
1105
計算現行速率
因數 $R_{CURRENT}$
1106
更新速率因數
$R_{NEW} = AVG\ (R_{STORED} + R_{CURRENT})$
儲存該演算法及位元
傳輸速率之 R_{NEW}
1107
終止
1100

圖 11. 速率因數計算

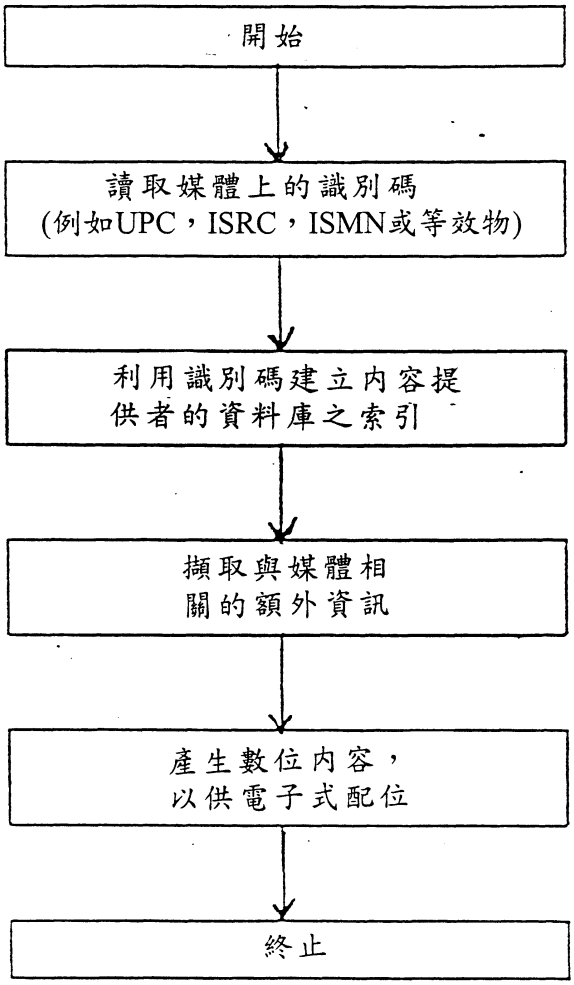
開始
讀取媒體上的識別碼
(例如UPC，ISRC，ISMN或等效物)
1201
利用識別碼建立內容提
供者的資料庫之索引
1202
擷取與媒體相
關的額外資訊
1203
產生數位內容，
以供電子式配位
1204
終止

圖 12. 自動資料擷取

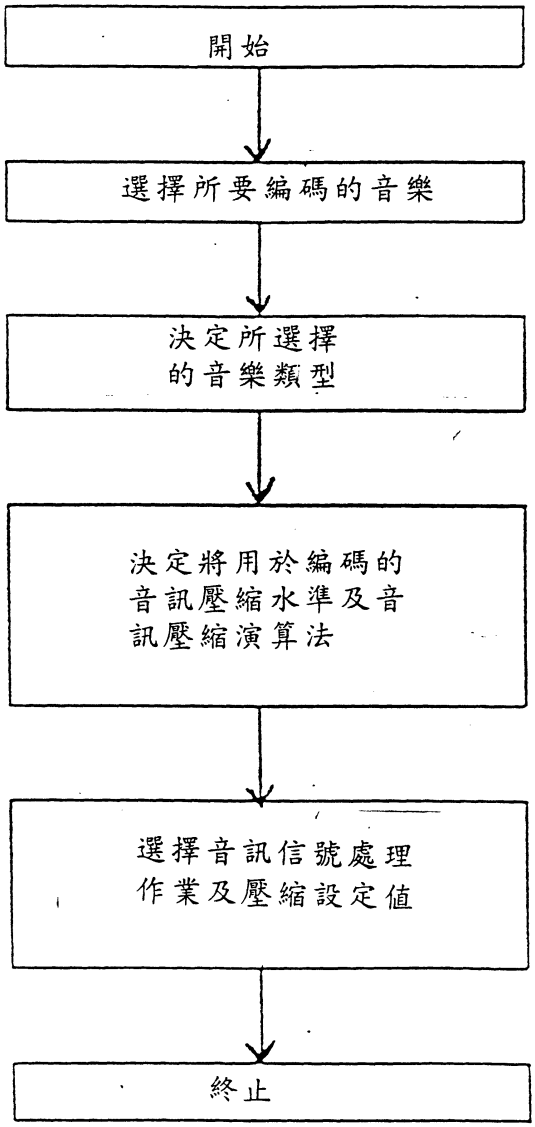

圖 13. 自動決定處理參數

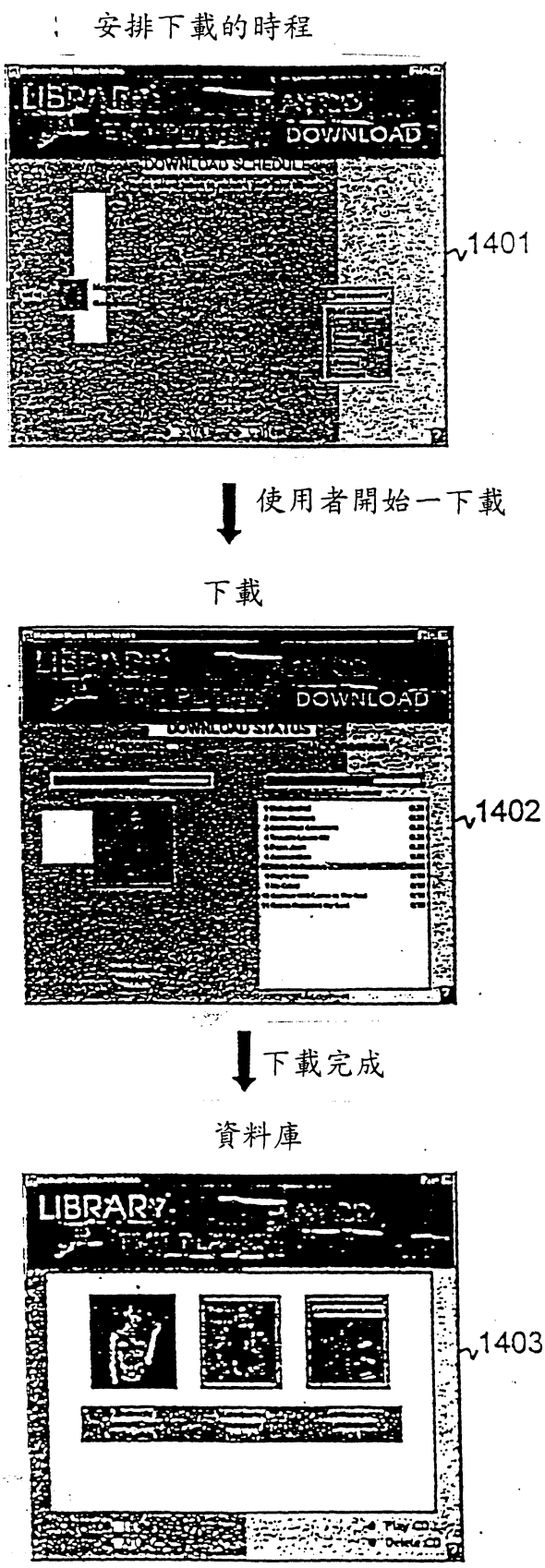

圖14.下載到播放應用程式之例示使用者介面畫面

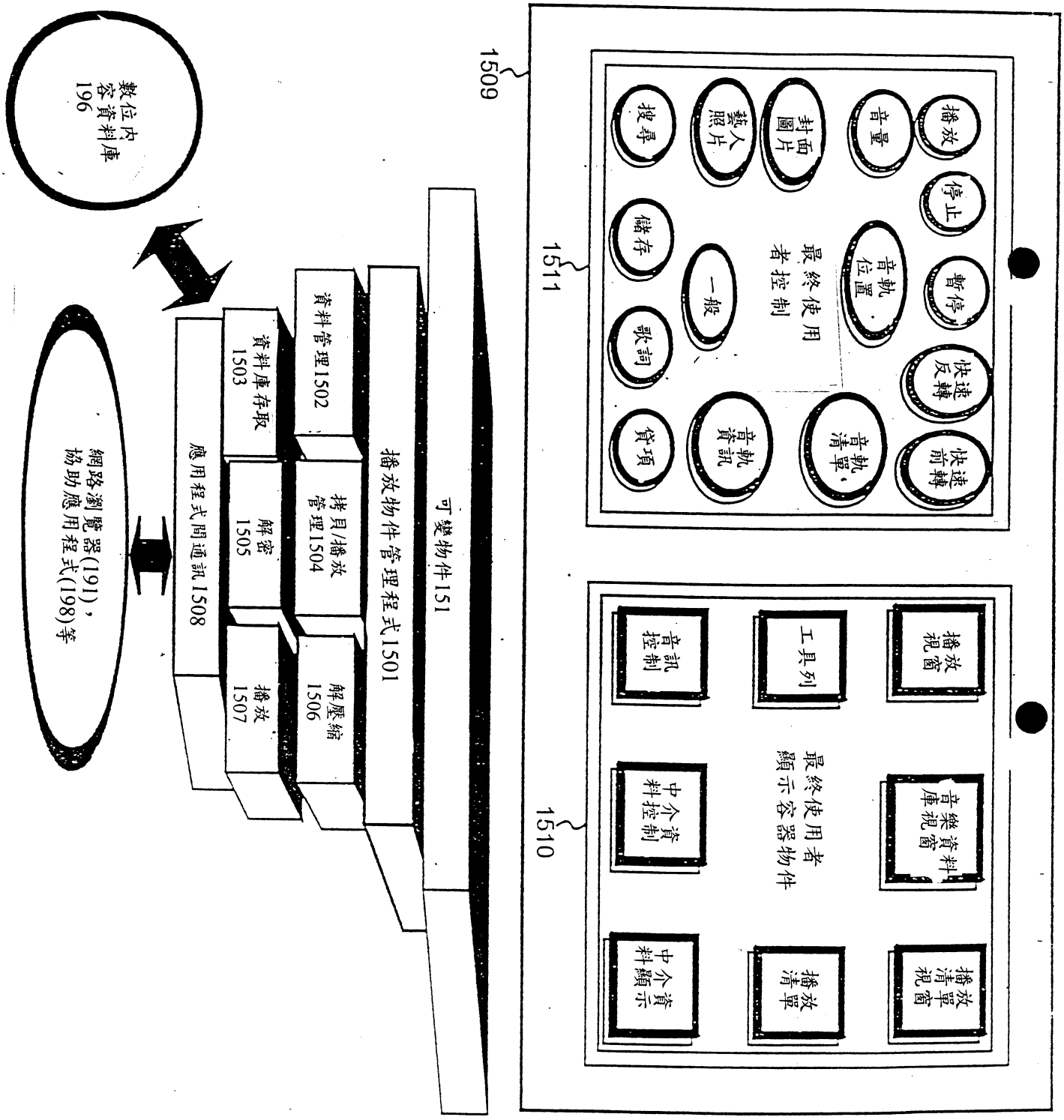
播放
停止
暫停
快速轉反
快速轉前
音量
音軌位置
音軌清單
封面圖片
藝人照片
音軌資訊
搜尋
儲存
歌詞
資頂
最終使用者控制
一般
1509
1511
播放視窗
音樂資料庫視窗
播放清單視窗
工具列
播放清單
音訊控制
介資料控制
介資料顯示
最終使用者顯示容器物件
1510
可變物件151
播放物件管理程式1501
資料管理1502
拷貝/播放管理1504
解壓縮1506
資料庫存取1503
解密1505
播放1507
應用程式間通訊1508
數位內容資料庫196
網路瀏覽器(191)，協助應用程式(198)等

圖15．播放應用程式

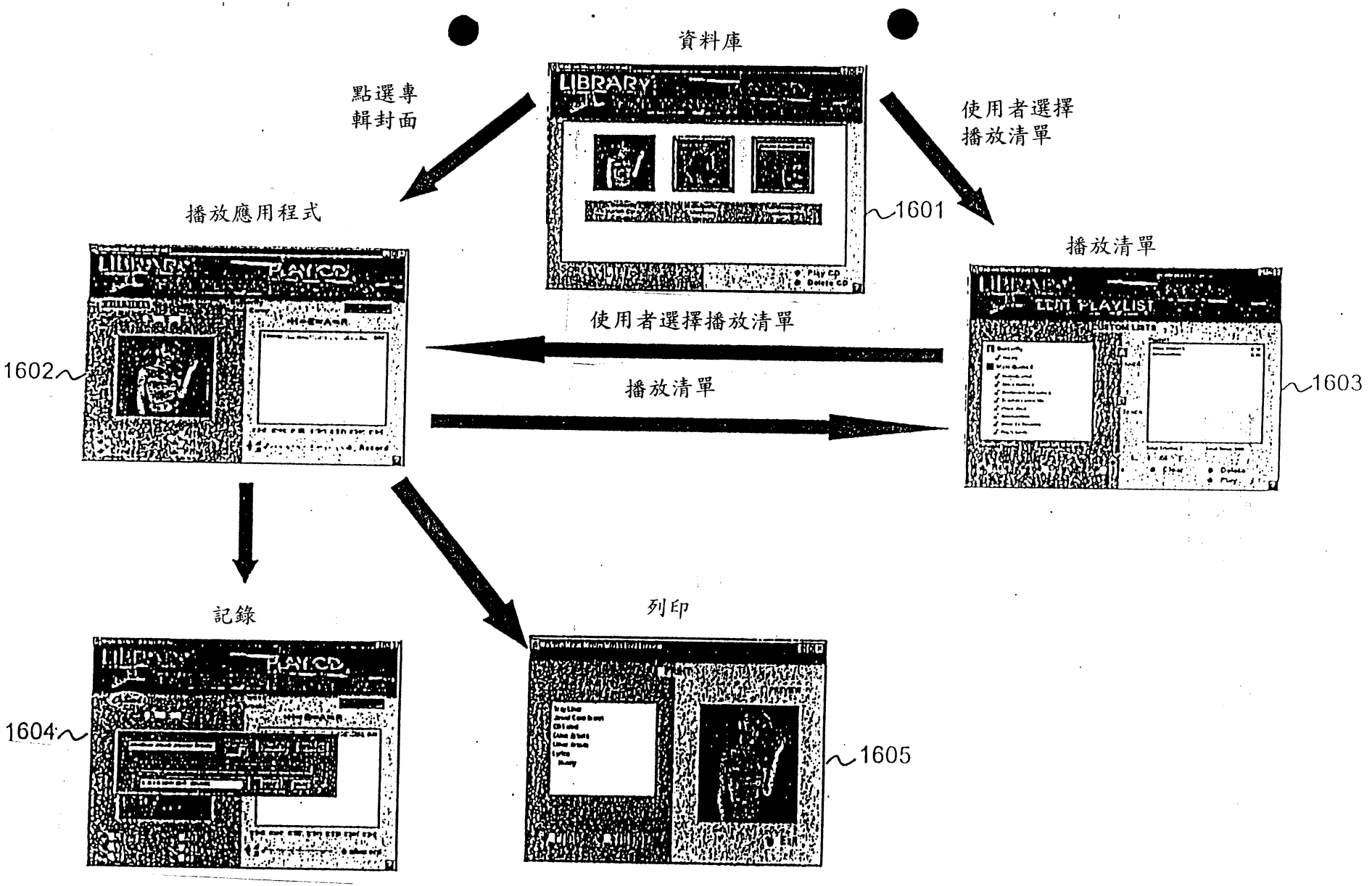

圖 16. 播放應用程式之例示使用者介面畫面

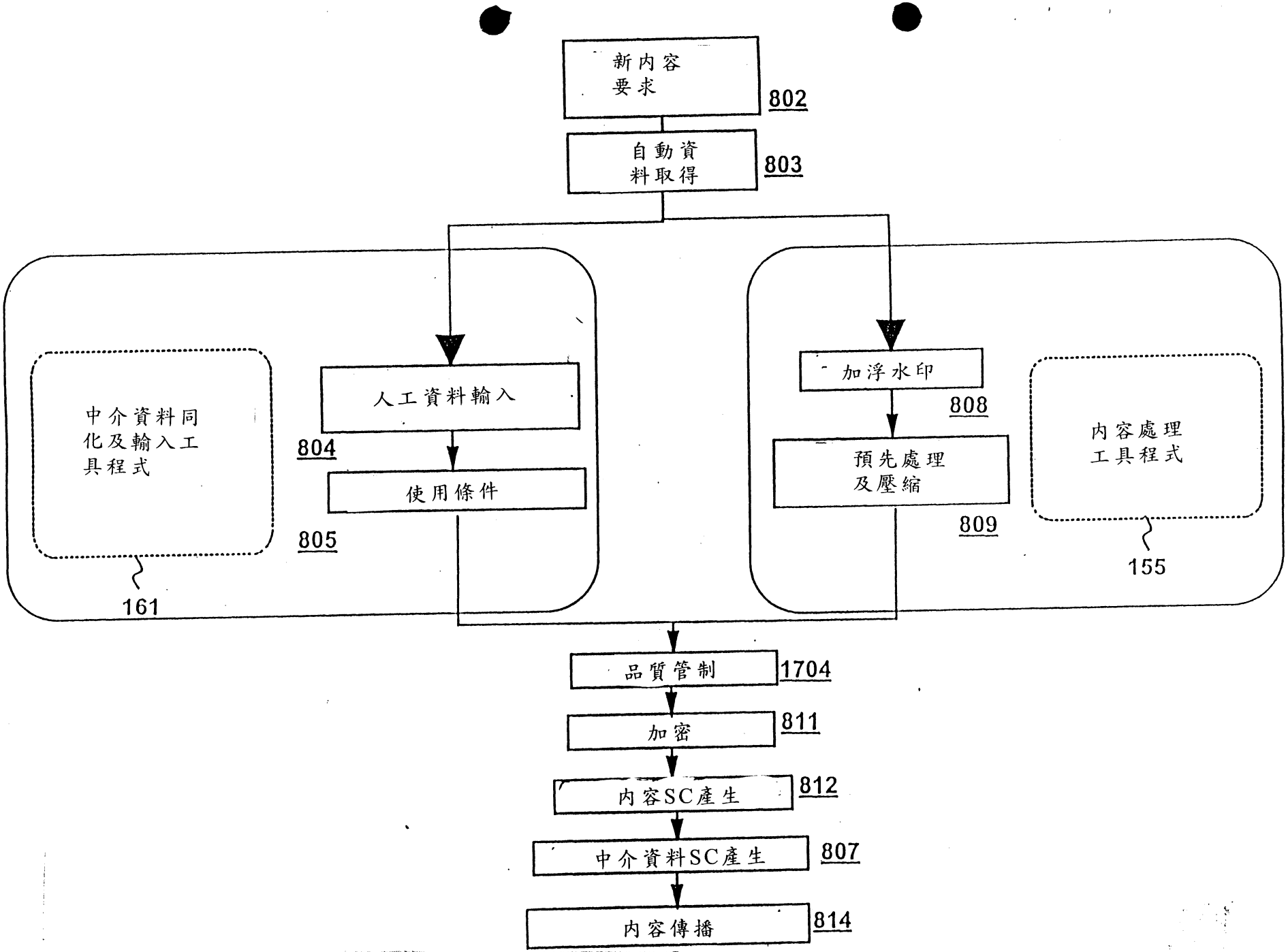

圖 17. 工作流程管理程式之替代實施例

五、發明說明(30)

有很大的彈性。在此同時，安全數位內容電子式配送系統100將某一程度的保證提供給內容提供者101，使內容提供者101的數位資產得到保護及量度，因而內容提供者101可因內容113的授權而收到適當的報酬。

II. 密碼觀念及其在安全數位內容電子式配送系統上的應用

安全數位內容電子式配送系統100中之授權許可控制係基於密碼的使用。本節介紹本發明的基本密碼技術。公共金鑰(public key)加密、對稱金鑰(symmetric key)加密、數位簽名、數位浮水印、及數位證明書都是習知的。

A.對稱演算法

在安全數位內容電子式配送系統100中，內容提供者101利用對稱演算法將內容加密。因為此種演算法利用同一金鑰將資料加密及解密，所以被稱為對稱演算法。資料傳送者及訊息接收者必須共用該金鑰。本文中將共用的金鑰稱為對稱金鑰。安全數位內容電子式配送系統100與針對一特定實施例而選擇的特定對稱演算法無關。

常見的對稱演算法有DES、RC2、及RC4。DES及RC2都是區段密碼(block cipher)。區段密碼一次利用一區段的資料位元將資料加密。DES是一種美國政府官方的加密標準，具有64位元的區段長度，並使用56位元的金鑰。通常利用三重DES(Triple-DES)來增加簡單DES所能達到的安全性。RSA資料安全(RSA Data Security)設計出RC2。RC2使用一可變金鑰長度的密碼，且具有64位元的區段長度。也是由RSA資料安全設計出的RC4是一種可變金鑰長度的

五、發明說明（　　）

159

部分儲存在最終使用者電腦的多個儲存位置，即可保護該金鑰。係利用防篡改軟體技術來保護該區域的程式碼，以便不會洩漏該金鑰的分割方式及儲存位置。防止包括最終使用者在內的人存取該金鑰有助於避免內容113被其他的電腦盜用或共用。若要得知與如何使用這些金鑰的更多細節，請參閱SC(s)處理器192的該節。

防篡改軟體技術是一種防止駭客在未經授權的情形下入侵一電腦軟體應用程式。駭客通常想要知道及(或)修改軟體，以便移除對使用的限制。事實上，並沒有無法破解的電腦程式，這就是不將防篡改的軟稱為"保證無法篡改的軟體"的原因。但是破解一以防篡改技術保護的應用程式所需的工作量通常將嚇阻大部分的駭客，這是因為所耗用的工作量超過了可能的收穫。此處的工作將是破解內容113的一部分之金鑰，或許是一張CD上的一首歌之金鑰。

其中一類的防篡改軟體技術是來自IBM。導入該程式碼的一種產品是IBM ThinkPad 770膝上型電腦。在該產品中，防篡改軟體係用來保護電腦中的DVD電影播放機。諸如好萊塢電影廠商等的數位內容提供者關心數位電影的到來、以及製作完美拷貝的容易程度，因而該等數位內容提供者堅持放在DVD上的電影必須包含著作權保護的機制。IBM的防篡改軟體使其難以規避這些著作權保護機制。這是防篡改軟體非常典型的應用；該軟體係用來強制執行內容113的某些受保護類型的使用。

IBM的防篡改軟體在入侵者的路徑中設置了數種障礙。

五、發明說明（ 163 ）

安全加密演算法，而使用一隨機對稱金鑰將內容113重新加密。一旦完成了下載及解密與重新加密程序194之後，現在即毀掉內容提供者101原先將內容113加密的加密金鑰623，並利用在安裝時所產生及隱藏的祕密使用者金鑰將新的SEAL金鑰本身加密。現在將該新的加密後SEAL金鑰儲存在授權許可資料庫107。

與在內容提供者101處執行的來源不同，在最終使用者裝置109上執行的使用者浮水印程序可能不需要變成一個有效的工業標準。這些標準仍然在進展中。該技術可讓控制資訊嵌入音樂中，並可將控制資訊更新若干次。在拷貝控制標準更穩定之前，在安全數位內容電子式配送系統100中已提供了拷貝控制的替代方法，因而無須依賴拷貝控制浮水印，即可在消費電子裝置中提供權利管理。利用連接到最終使用者裝置109的加密之數位內容資料庫196實施儲存及播放/記錄使用條件的安全性，且係經由防篡改環境而保護該儲存及播放/記錄使用條件的安全性。當採用標準時，係利用軟體追蹤點(hook)來支援拷貝控制浮水印。目前已可支援在各種壓縮等級下的加浮水印AAC及其他編碼的音訊流，但是此時該技術仍不太成熟，而無法用來作為拷貝控制的唯一方法。

解密與重新加密程序194是另一程式碼領域，其中係利用防篡改程式碼技術保護該程式碼，以便不會洩漏了原始內容113的加密金鑰、新的SEAL金鑰、及祕密使用者金鑰，且其中儲存了各祕密使用者金鑰區段及將該金鑰分段

六、申請專利範圍

1. 一種在一使用者系統上播放數位內容之方法，該內容資料以一第一加密金鑰來壓縮及加密，該方法包括下列步驟：

產生該第一加密金鑰及相對應之第一解密金鑰於該使用者系統上；

加密該第一解密金鑰，以產生一儲存於該使用者系統上之已加密第一解密金鑰；

使用一第二解密金鑰來解密該已加密第一解密金鑰;

以該第一解密金鑰來解密至少該該內容資料之部分，以產生已解密內容資料；

解壓縮該已解密內容資料，以產生已解壓縮內容資料;以及

播放或記錄該已解壓縮內容資料，

其中該第二解密金鑰係一秘密使用者金鑰，其隱藏於該使用者系統上。

2. 如申請專利範圍第1項之方法，進一步包含下列步驟：擷取分別儲存在該系統上的該第二解密金鑰之多個區段。

3. 如申請專利範圍第1項之方法，其中該第一加密金鑰及該第一解密金鑰是對稱金鑰，且該第二解密金鑰是一對稱金鑰。

4. 如申請專利範圍第3項之方法，其中係在一防竄改的環境中執行該等擷取及解密步驟，以便阻止對該第一解密金鑰及該第二解密金鑰作未經授權的存取。

六、申請專利範圍

5. 如申請專利範圍第1項之方法，其中係在一防竄改的環境中執行該解密步驟，以便阻止對該第一解密金鑰作未經授權的存取。

6. 如申請專利範圍第1項之方法，進一步包含下列步驟：在一抽換式媒體上記錄至少部分的該解壓縮的內容資料。

7. 如申請專利範圍第6項之方法，進一步包含下列步驟：在該記錄步驟之前，先在該解壓縮的內容資料中加上浮水印。

8. 如申請專利範圍第6項之方法，進一步包含下列步驟：在該抽換式媒體上記錄之前，先檢查該內容資料中包含的使用權資訊，以便決定在該抽換式媒體上的記錄是否已被授權。

9. 如申請專利範圍第6項之方法，進一步包含下列步驟：在該抽換式媒體上記錄之前，先聯絡一交換所，以便決定在該抽換式媒體上的記錄是否已被授權。

10. 如申請專利範圍第1項之方法，進一步包含檢查該內容資料中包含的使用權資訊之步驟，以便在播放該解壓縮的內容資料之前，先決定該內容資料之播放是否已被授權。

11. 如申請專利範圍第10項之方法，其中該使用權資訊限制了該內容資料可被播放的次數。

12. 如申請專利範圍第10項之方法，其中該使用權資訊限制了該內容資料可被播放的時間。

六、申請專利範圍

13. 如申請專利範圍第1項之方法，其中該內容資料包含音樂資料，且該播放步驟包含下列子步驟：

播放該音樂資料；以及

顯示與所播放的該音樂資料相關聯之資訊。

14. 如申請專利範圍第13項之方法，其中所顯示的該資訊包含與該音樂資料相關聯的影像及文字。

15. 如申請專利範圍第13項之方法，進一步包含下列步驟：列印與該音樂資料相關聯的至少部分之該資訊。

16. 如申請專利範圍第1項之方法，進一步包含下列步驟：

在該系統上儲存該數位內容資料，作為複數個檔案；以及

在該系統上儲存複數個播放清單，每一播放清單識別該等檔案中的一組所選擇之檔案、及播放該等所選擇檔案之順序，

其中該播放步驟進一步包含下列步驟：按照一播放清單所指定的順序而播放該播放清單中之各檔案。

17. 如申請專利範圍第16項之方法，進一步包含下列步驟：產生及(或)編輯各播放清單。

18. 如申請專利範圍第16項之方法，進一步包含下列步驟：在一抽換式媒體上記錄至少一個播放清單。

19. 如申請專利範圍第1項之方法，進一步包含下列步驟：

安排自一網路下載至少部分的該內容資料之時程；以及

當到達所安排的時程時，下載該內容資料。

六、申請專利範圍

20. 一種用以播放一電腦系統上之數位內容資料之數位內容播放機，該內容資料是以一第一加密金鑰來壓縮及加密，該數位內容播放機包括：

一金鑰產生器，其用以產生該第一加密金鑰及相對應之第一解密金鑰於該電腦系統上；

一加密器，其用以加密該第一解密金鑰，以產生一已加密第一解密金鑰；

儲存器，其用以儲存該已加密第一解密金鑰；

一解密器，其使用一第二解密金鑰，以解密該已加密第一解密金鑰，及使用該第一解密金鑰，以解密至少該內容資料之部分，以產生已解密內容資料；

一解壓縮器，其用以解壓縮該已解密內容資料，以產生已壓縮內容資料；以及

一播放器，其用以播放該已解壓縮內容資料，

其中該第二解密金鑰係一秘密使用者金鑰，其隱藏於該電腦系統上。

21. 如申請專利範圍第20項之數位內容播放機，其中該解密器包含一個擷取分別儲存在該電腦系統上的該第二解密金鑰的多個區段之機制。

22. 如申請專利範圍第20項之數位內容播放機，其中該第一加密金鑰及該第一解密金鑰是對稱金鑰，且該第二解密金鑰是一對稱金鑰。

23. 如申請專利範圍第22項之數位內容播放機，其中該解密器係在一防竄改的環境中操作，以便阻止對該第一

六、申請專利範圍

解密金鑰及該第二解密金鑰作未經授權的存取。

24. 如申請專利範圍第20項之數位內容播放機，其中該解密器係在一防竄改的環境中操作，以便阻止對該第一解密金鑰作未經授權的存取。

25. 如申請專利範圍第20項之數位內容播放機，其中該播放機亦包含一個在至少部分的該解壓縮的內容資料中加上浮水印之機制，用以產生加上浮水印的內容資料，且該播放機在一抽換式媒體上記錄該加上浮水印的內容資料。

26. 如申請專利範圍第25項之數位內容播放機，其中該播放機包含一檢查機制，用以在該抽換式媒體上記錄之前，先檢查該內容資料中包含的使用權資訊，以便決定在該抽換式媒體上的記錄是否已被授權。

27. 如申請專利範圍第25項之數位內容播放機，其中該播放機包含一聯絡機制，用以在該抽換式媒體上記錄之前，先聯絡一交換所，以便決定在該抽換式媒體上的記錄是否已被授權。

28. 如申請專利範圍第20項之數位內容播放機，其中該播放機亦包含一在該壓縮的內容資料中嵌入一浮水印之機制。

29. 如申請專利範圍第20項之數位內容播放機，其中該播放機檢查該內容資料中包含的使用權資訊之步驟，以便在播放該解壓縮的內容資料之前，先決定該內容資料之播放是否已被授權。

六、申請專利範圍

30. 如申請專利範圍第20項之數位內容播放機，其中該內容資料包含音樂資料，且該播放機播放該音樂資料，並顯示與所播放的該音樂資料相關聯之資訊。

31. 如申請專利範圍第20項之數位內容播放機，其中該內容資料包含音樂資料，且係將該音樂資料儲存成複數個檔案，而且該內容資料包含複數個播放清單，

每一播放清單識別該等檔案中的一組所選擇之檔案、及播放該等所選擇檔案之順序，以及

該播放機按照一播放清單所指定的順序而播放該播放清單中之各檔案。

32. 如申請專利範圍第20項之數位內容播放機，進一步包含一下載器，用以安排自一網路下載至少部分的該內容資料之時程，並當到達所安排的時程時，下載該內容資料。

33. 一種以一程式來編碼用以播放一電腦系統上之數位內容資料之電腦可讀取媒體，該內容資料以一第一加密金鑰來壓縮及加密，該程式包含用以執行下列步驟之指令：

產生該第一加密金鑰及相對應之第一解密金鑰於該電腦系統上；

加密該第一解密金鑰，以產生一儲存於該電腦系統上之已加密第一解密金鑰；

使用一第二解密金鑰來解密該已加密第一解密金鑰；

使用該第一解密金鑰來解密至少該內容資料之部分，

六、申請專利範圍

以產生已解密內容資料；

解壓縮該已解密內容資料，以產生已解壓縮內容資料；以及

播放該已解壓縮內容資料，

其中該第二解密金鑰係一秘密使用者金鑰，其隱藏於該電腦系統上。

34. 如申請專利範圍第33項的以一用來播放數位內容資料的程式編碼的電腦可讀取之媒體，其中該程式進一步包含用來執行下列步驟之指令：擷取分別儲存在該系統上的該第二解密金鑰之多個區段。

35. 如申請專利範圍第33項的以一用來播放數位內容資料的程式編碼的電腦可讀取之媒體，

其中該第一加密金鑰及該第一解密金鑰是對稱金鑰，且該第二解密金鑰是一對稱金鑰。

36. 如申請專利範圍第35項的以一用來播放數位內容資料的程式編碼的電腦可讀取之媒體，其中係在一防竄改的環境中執行該等用於擷取及解密之程式指令，以便阻止對該第一解密金鑰及該第二解密金鑰作未經授權的存取。

37. 如申請專利範圍第33項的以一用來播放數位內容資料的程式編碼的電腦可讀取之媒體，其中係在一防竄改的環境中執行該等用於解密之程式指令，以便阻止對該第一解密金鑰作未經授權的存取。

38. 如申請專利範圍第33項的以一用來播放數位內容資料

六、申請專利範圍

的程式編碼的電腦可讀取之媒體，其中該程式進一步包含用來執行下列步驟之指令：在一抽換式媒體上記錄至少部分的該解壓縮的內容資料。

39. 如申請專利範圍第38項的以一用來播放數位內容資料的程式編碼的電腦可讀取之媒體，其中該程式進一步包含用來執行下列步驟之指令：在該抽換式媒體上記錄之前，先在該解壓縮的內容資料中加上浮水印。

40. 如申請專利範圍第38項的以一用來播放數位內容資料的程式編碼的電腦可讀取之媒體，其中該程式進一步包含用來執行下列步驟之指令：在該抽換式媒體上記錄之前，先檢查該內容資料中包含的使用權資訊，以便決定在該抽換式媒體上的記錄是否已被授權。

41. 如申請專利範圍第33項的以一用來播放數位內容資料的程式編碼的電腦可讀取之媒體，其中該程式進一步包含用來執行下列步驟之指令：在播放該解壓縮的內容資料之前，先檢查該內容資料中包含的使用權資訊，以便決定該內容資料之播放是否已被授權。

42. 如申請專利範圍第33項的以一用來播放數位內容資料的程式編碼的電腦可讀取之媒體，其中該內容資料包含音樂資料，且該等用於播放的程式指令包含用來執行下列步驟之指令：

播放該音樂資料；以及

顯示與所播放的該音樂資料相關聯之資訊。

43. 如申請專利範圍第33項的以一用來播放數位內容資料

六、申請專利範圍

的程式編碼的電腦可讀取之媒體，其中該程式進一步包含用來執行下列步驟之指令：

在該系統上儲存該數位內容資料，作為複數個檔案；以及

在該系統上儲存複數個播放清單，每一播放清單識別該等檔案中的一組所選擇之檔案、及播放該等所選擇檔案之順序，

其中該等用於播放的程式指令包含用來執行下列步驟之指令：按照一播放清單所指定的順序而播放該播放清單中之各檔案。

44. 如申請專利範圍第33項的以一用來播放數位內容資料的程式編碼的電腦可讀取之媒體，其中該程式進一步包含用來執行下列步驟之指令：

安排自一網路下載至少部分的該內容資料之時程；以及

當到達所安排的時程時，下載該內容資料。

45. 一種將資料安全地提供給一使用者的系統之方法，該方法包含下列步驟：

利用一第一加密金鑰將該資料加密；

利用一第二加密金鑰將一第一解密金鑰加密；

將已利用該第一加密金鑰加密的該加密之資料傳送到該使用者的系統；

將已利用該第二加密金鑰加密的該加密之第一解密金鑰傳送到該使用者的系統；

六、申請專利範圍

將已利用該第二加密金鑰加密的該加密之第一解密金鑰傳送到一擁有一第二解密金鑰之交換所；

利用該第二解密金鑰將該第一解密金鑰解密；以及

將解密的該第一解密金鑰傳送到該使用者的系統。

46. 如申請專利範圍第45項之方法，其中傳送該解密的第一解密金鑰之該步驟包含下列子步驟：

利用一第三加密金鑰將該第一解密金鑰重新加密；

將該解密後再重新加密的第一解密金鑰傳送到該使用者的系統；以及

利用一第三解密金鑰將該重新加密的第一解密金鑰解密。

47. 如申請專利範圍第45項之方法，其中該第一加密金鑰及該第一解密金鑰是對稱金鑰。

48. 如申請專利範圍第47項之方法，其中該第二加密金鑰是該交換所的一公開金鑰，且該第二解密金鑰是該交換所的一對應之私人金鑰。

49. 如申請專利範圍第48項之方法，其中傳送該解密的第一解密金鑰之該步驟包含下列子步驟：

利用一第三加密金鑰將該第一解密金鑰重新加密，該第三加密金鑰是該使用者的一公開金鑰；

將該解密後再重新加密的第一解密金鑰傳送到該使用者的系統；以及

利用一第三解密金鑰將該重新加密的第一解密金鑰解密，該第三解密金鑰是該使用者的一對應之私人金

六、申請專利範圍

鑰。

50. 如申請專利範圍第45項之方法，其中係由一線上零售商執行將該加密的第一解密金鑰傳送到該使用者的系統之該步驟，且該步驟包含下列子步驟：

自該線上零售商發動對該資料的一購買、或該資料的一授權許可；以及

將該加密的第一解密金鑰及購買交易資料傳送到該使用者的系統。

51. 如申請專利範圍第50項之方法，其中將該加密的第一解密金鑰傳送到該使用者的系統之該步驟進一步包含下列子步驟：針對該資料或該授權許可向該使用者收費，以及

由該交換所執行將該第一解密金鑰解密之該步驟，且該步驟包含下列子步驟：

驗證該使用者是否已支付該資料或該授權許可之費用；以及

利用該第二解密金鑰將該第一解密金鑰解密。

52. 如申請專利範圍第50項之方法，其中係由該交換所執行將該第一解密金鑰解密之該步驟，且該步驟包含下列子步驟：

針對該資料或該授權許可向該使用者收費；以及

利用該第二解密金鑰將該第一解密金鑰解密。

53. 如申請專利範圍第45項之方法，進一步包含下列步驟：利用該第一解密金鑰將該資料解密。

六、申請專利範圍

54. 如申請專利範圍第45項之方法，其中該資料包含音樂資料。

55. 一種安全地將資料提供給一使用者的系統之方法，該資料係經過加密，以便只能夠利用一資料解密金鑰將該資料解密，其中係利用一第一公開金鑰將該資料解密金鑰加密，且該使用者的系統可存取該加密的資料，該方法包含下列步驟：

將該加密的資料解密金鑰傳送到一擁有對應於第一公開金鑰的一第一私人金鑰之交換所；

利用該第一私人金鑰將該資料解密金鑰解密；

利用一第二公開金鑰將該資料解密金鑰重新加密；

將該重新加密的資料解密金鑰傳送到該使用者的系統，而該使用者的系統擁有一對應於第二公開金鑰之第二私人金鑰；以及

利用該第二私人金鑰將該重新加密的資料解密金鑰解密。

56. 如申請專利範圍第55項之方法，其中將該加密的資料解密金鑰傳送到一交換所之該步驟包含下列子步驟：

將該加密的資料解密金鑰傳送到該使用者的系統；以及

隨即將該加密的資料解密金鑰自該使用者的系統傳送到該交換所。

57. 如申請專利範圍第56項之方法，其中係由一線上零售商執行將該加密的資料解密金鑰傳送到該使用者的系

六、申請專利範圍

統之該子步驟，且該子步驟包含下列子步驟：

自該線上零售商發動對該資料的一購買、或該資料的一授權許可；以及

將該加密的資料解密金鑰及購買交易資料傳送到該使用者的系統。

58. 如申請專利範圍第57項之方法，其中將該加密的資料解密金鑰傳送到該使用者的系統之該子步驟進一步包含下列子步驟：針對該資料或該授權許可向該使用者收費，以及

由該交換所執行將該資料解密金鑰解密之該步驟，且該步驟包含下列子步驟：

驗證該使用者是否已支付該資料或該授權許可之費用；以及

利用該第一私人金鑰將該資料解密金鑰解密。

59. 如申請專利範圍第57項之方法，其中係由該交換所執行將該資料解密金鑰解密之該步驟，且該步驟包含下列子步驟：

針對該資料或該授權許可向該使用者收費；以及

利用該第一私人金鑰將該資料解密金鑰解密。

60. 如申請專利範圍第55項之方法，進一步包含下列步驟：用該資料解密金鑰將該加密的資料解密。

61. 一種操作一交換所而使一商務通路具有完整性之方法，該商務通路包含一供應商、一配銷商、及一購買者，該供應商產生資料，並將該資料加密，以便只能

六、申請專利範圍

利用一資料解密金鑰將該資料解密，該購買者可存取該加密的資料，該方法包含下列步驟：

利用該交換所的一公開金鑰將該資料解密金鑰加密；

將該加密的資料解密金鑰自該供應商傳送到該配銷商；

當該購買者想要購買該資料、或資料使用的一授權許可時，將該加密的資料解密金鑰自該配銷商傳送到該購買者；

將該加密的資料解密金鑰自該購買者傳送到該交換所；

利用該交換所的一私人金鑰將該資料解密金鑰解密，並利用該購買者的一公開金鑰將該資料解密金鑰重新加密；以及

將該重新加密的資料解密金鑰自該交換所傳送到該購買者。

62. 如申請專利範圍第61項之方法，其中在該配銷商將該加密的資料解密金鑰傳送到該購買者之前，該配銷商先向該使用者收費，以及

在該交換所將重新加密的資料解密金鑰傳送到該購買者之前，該交換所先驗證該使用者是否已付費。

63. 如申請專利範圍第61項之方法，其中該交換所在將該重新加密的資料解密金鑰傳送到該購買者之前，該交換所先向該使用者收費。

64. 如申請專利範圍第61項之方法，進一步包含下列步驟：

六、申請專利範圍

利用該購買者的該私人金鑰將該重新加密的資料解密金鑰解密；以及

利用該資料解密金鑰將該加密的資料解密。

65. 一種將資料安全地提供給一使用者的系統之系統，該系統包含：

一內容系統；

一第一公開金鑰；

一個對應於該第一公開金鑰之第一私人金鑰；

一資料加密金鑰；

一資料解密金鑰，用以將利用該資料加密金鑰加密的資料解密；

第一資料加密裝置，用以將資料加密，以便只能由資料解密金鑰將該資料解密；

第二資料加密裝置，用以利用該第一公開金鑰將該解密金鑰加密；

一交換所；

第一傳送裝置，用以將已被加密的該資料解密金鑰傳送到該交換所，其中該交換所擁有該第一私人金鑰；

第一解密裝置，用以利用該第一私人金鑰將該資料解密金鑰解密；

一第二公開金鑰；

一個對應於該第二公開金鑰之第二私人金鑰；

重新加密裝置，用以利用該第二公開金鑰將該資料解密金鑰重新加密；

六、申請專利範圍

第二傳送裝置，用以將該重新加密的資料解密金鑰傳送到該使用者的系統，其中該使用者的系統擁有該第二私人金鑰；以及

第二解密裝置，用以利用該第二私人金鑰將該重新加密的資料解密金鑰解密。

66. 如申請專利範圍第65項之系統，其中該第一傳送裝置進一步包含：

一第三傳送裝置，用以將該加密的資料解密金鑰傳送到該使用者的系統；以及

一第四傳送裝置，用以隨即將該加密的資料解密金鑰自該使用者的系統傳送到該交換所。

67. 如申請專利範圍第66項之系統，其中係由一線上零售商執行該第三傳送裝置，且該第三傳送裝置進一步包含：

發動裝置，用以自該線上零售商發動對該資料的一購買、或該資料的一授權許可；以及

傳送裝置，用以將該加密的資料解密金鑰及購買交易資料傳送到該使用者的系統。

68. 如申請專利範圍第67項之系統，其中該傳送裝置進一步包含：

收費裝置，用以針對該資料或該授權許可向該使用者收費；以及其中係由該交換所執行該第一解密裝置，且該第一解密裝置進一步包含：

驗證裝置，用以驗證該使用者是否已支付該資料或該

六、申請專利範圍

授權許可之費用；以及

第三解密裝置，用以利用該第一私人金鑰將該資料解密金鑰解密。

69. 如申請專利範圍第67項之系統，其中係由該交換所執行該第一解密裝置，且該第一解密裝置進一步包含：

收費裝置，用以針對該資料或該授權許可向該使用者收費；以及

第四解密裝置，用以利用該第一私人金鑰將該資料解密金鑰解密。

70. 如申請專利範圍第65項之系統，進一步包含：

資料解密金鑰解密裝置，用以利用該資料解密金鑰將該加密的資料解密。

71. 如申請專利範圍第1項之方法，更包括下列步驟：

產生該第二解密金鑰於該使用者系統上，如此該第二解密金鑰係一只有該使用者系統知道之秘密金鑰，

其中產生於該使用者系統之該第一解密金鑰亦為一只有該使用者系統知道之秘密金鑰。

72. 如申請專利範圍第20項之數位內容播放機，

其中該金鑰產生器亦產生該第二解密金鑰於該電腦系統上，該二解密金鑰係一只有該電腦系統知道之秘密金鑰，及產生於該使用者系統上之該第一解密金鑰亦為一只有該電腦系統知道之秘密金鑰。