

國立交通大學

資訊學院 資訊學程

碩士論文

可權限轉移之數位版權管理系統
的研究與實現



A Study and Implementation of Transferable Rights
for Digital Rights Management Systems

研究生：陳俊廷

指導教授：陳登吉 博士

葉義雄 博士

中華民國九十八年三月

可權限轉移之數位版權管理系統的研究與實現

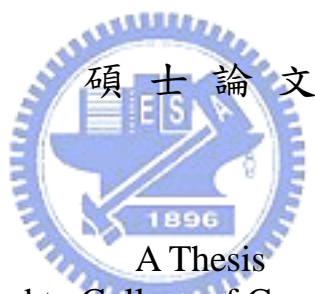
A Study and Implementation of Transferable Rights for Digital Rights Management Systems

研究生：陳俊廷
指導教授：陳登吉 博士
葉義雄 博士

Student : Chun-Ting Chen
Advisors : Dr. Deng-Jyi Chen
Dr. Yi-Shiung Yeh

國立交通大學

資訊學院 資訊學程



Submitted to College of Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Master of Science
in
Computer Science
March 2009

Hsinchu, Taiwan, Republic of China

中華民國九十八年三月

可權限轉移之數位版權管理系統 的研究與實現

學生：陳俊廷

指導教授：陳登吉 博士

葉義雄 博士

國立交通大學資訊學院 資訊學程碩士班

摘要

隨著網際網路與數位科技的發展，使用者可以利用各種傳輸方式取得未經授權的數位內容。數位內容的非法複製與大量散佈，不但嚴重危害到數位內容提供業者的利益，而且也違反了智慧財產法與著作權法，同時更遏阻了數位內容產業的發展。所以如何防止數位內容被不當的大量散佈給其他沒有經過合法授權的使用者，遂成為大家關心的話題。因此，數位版權管理(Digital Rights Management, DRM)系統被提出來解決這個問題。亦即我們可以經由DRM系統控制並設定存取權限，使得只有經過適當授權的使用者，才能夠使用這些受保護的內容，避免數位內容被不當的散佈與使用。

DRM系統雖然提供了數位內容的權限管控及保護，但目前的DRM系統卻不存在「權限轉移」的功能，以致一些消費者傳統的使用行為，例如：租借、轉售等交易行為，到目前為止都還沒有辦法實現。而這些使用行為會嚴重影響消費者購買受DRM保護的數位內容的意願，同時也遏阻了DRM系統的發展。在本論文中，我們提出一個具有Transferable Rights機制的DRM系統，可以讓我們解決有關「權限轉移」的問題，亦即讓購買的數位內容可以合法轉售或借給他人。基於Transferable Rights的實現，我們也可以展示兩個新的商業應用情境：一個是數位學習教材出租中心—消費者可以在線上租用數位學習教材的數位內容；另一個是數位學習教材二手商店—消費者可以轉賣他們已購買的數位學習教材的使用權利。透過這兩個應用情境，讓我們的DRM系統顯得更有彈性而且合理。

A Study and Implementation of Transferable Rights for Digital Rights Management Systems

Student: *Chun-Ting Chen*

Advisors: *Dr. Deng-Jyi Chen*

Dr. Yi-Shiung Yeh

Degree Program of Computer Science

National Chiao Tung University

Abstract

While the digital technologies have become highly utilized in the Internet, the on-line users are able to acquire the digital contents very easily in variant ways. However these emerging trends did not benefit the content providers because of their copyrights had been violated. This drawback restrained the development of the digital content market. The content providers would need some mechanisms to enforce access policies and to enable the consumers for better utilizing the licensed contents with extended allowances. The approach, DRM (Digital Rights Management) system was proposed to resolve these related problems. The DRM system is a system to protect and manage digital contents, and to control the usage and distribution of digital contents. It is intended to only allow proper authorized user to access the protected digital information.

Although DRM systems have already prevented digital contents from unauthorized access, it is still insufficient to provide the adequate functions to address the “Transfer Rights”. For example, the possible transactions of digital contents might occur at rental store, secondhand market, etc. These traditional business behaviors were not well considered and put into design of current DRM systems. This ignorance definitely lowered the consumer’s desire for purchasing the DRM protected contents. Furthermore, consumer still cannot resell copyrighted contents arbitrarily within the existing DRM systems. This limit violated the common use of property in a real world. In this thesis, we proposed an enhanced mechanism in which the “Transfer Rights” should be allowed in a DRM system. Based on implementation of transferable rights in DRM systems, we proposed two new business scenarios. One is an “e-Learning Content Rental Store” in which consumer is able to rent the e-Learning content media via on-line. The other is “e-Learning Content Secondhand Store” in which consumers can resell the e-Learning content media, specifically for those they purchased from others. These two proposed scenarios would enable the transferable rights with more reasonable and legal use in the DRM systems.

誌謝

首先要感謝兩位指導教授，陳登吉老師與葉義雄老師；葉老師是帶領我進入研究領域的恩師，但在前年七月葉老師不幸逝世。在此藉由本論文感謝並悼念葉老師的指導；同時感謝陳老師繼續指導我論文的方向與研究的方法，當我遇到問題時，總是適時給予我實質上的建議及指導，使本研究能夠順利完成。

此外，感謝撥空擔任口試委員的曾健超老師、黃世昆老師以及黃中見博士，提出許多寶貴的意見，使我受益良多。最後，特別感謝李鎮宇學長，在研究的過程中提供許多的想法，並給予我適時的協助，在此由衷感謝。



目錄

摘要.....	i
Abstract.....	ii
誌謝.....	iii
目錄.....	iv
表目錄.....	vi
圖目錄.....	vii
一、 緒論.....	1
1.1 研究背景、動機與目標.....	1
1.2 論文架構.....	1
二、 相關文獻探討.....	3
2.1 DRM系統簡介.....	3
2.1.1 典型的DRM商業模型.....	3
2.1.2 DRM系統的參考架構及運作流程.....	4
2.1.3 數位內容的發行管道及商業模式.....	5
2.2 DRM系統的安全機制.....	6
2.2.1 密碼學機制.....	6
2.2.2 獨特化機制.....	8
2.2.3 數位浮水印機制.....	8
2.3 數位版權描述語言.....	9
三、 可權限轉移的DRM機制.....	14
3.1 具有Transferable Rights的DRM商業模型.....	14
3.2 Transferable Rights的定義.....	15
3.3 Transferable Rights的運作模型.....	16
3.4 Transferable Rights的運作流程.....	18
3.5 Transferable Rights的License作法.....	20
四、 系統架構.....	23
4.1 系統模組.....	23
4.2 系統架構.....	24
4.2.1 Packager架構.....	25
4.2.2 DRM Server架構.....	26
4.2.3 DRM Client架構.....	27
4.2.4 Clearing House架構.....	27
4.3 系統機制.....	27
4.4 系統基本運作的流程設計.....	29
五、 系統實作.....	32
5.1 系統發展的背景環境.....	32
5.2 實作方法.....	33
5.3 使用情境與系統實作展示.....	36
六、 新的商業應用情境及展示.....	48
6.1 數位學習教材出租中心.....	48
6.1.1 出租交易情境.....	48
6.1.2 出租之Rights Grant流程及系統展示.....	49

6.2 數位學習教材轉售中心.....	52
6.2.1 轉售交易情境.....	52
6.2.2 轉售之Rights Transfer流程及系統展示.....	53
七、 結論及未來建議.....	57
7.1 結論.....	57
7.2 未來建議.....	57
參考文獻或資料.....	58



表目錄

表 3-1 使用期限的驗證 18



圖目錄

圖 2-1 典型的DRM商業模型	4
圖 2-2 典型的DRM系統架構	4
圖 2-3 傳統式加密的過程	7
圖 2-4 公開鑰匙式加密的過程	8
圖 2-5 ODRL 語法架構	10
圖 2-6 ODRL的License範例	10
圖 2-7 XrML語法架構	11
圖 2-8 MPEG-21 REL 語法架構	12
圖 2-9 MPEG-21 REL語法的基本資料結構	12
圖 2-10 MPEG-21 REL的License範例	13
圖 3-1 具有權限轉移的DRM商業交易模型	15
圖 3-2 具有使用權限及Transferable Rights的License	15
圖 3-3 Transferable Rights的示意圖	16
圖 3-4 Rights Grant的運作模型	17
圖 3-5 Rights Transfer的運作模型	17
圖 3-6 Rights Grant的運作循序圖	19
圖 3-7 Rights Transfer的運作循序圖	20
圖 3-8 Transferable Rights模型的REL語法	20
圖 3-9 License Traceability of Transferable Rights	21
圖 3-10 具有Transferable Rights之License範例	22
圖 4-1 系統功能模組	23
圖 4-2 本研究的DRM系統架構	25
圖 4-3 本研究的Packager架構	25
圖 4-4 本研究的DRM Server架構	26
圖 4-5 本研究的DRM Client架構	27
圖 4-6 本研究的Clearing House架構	27
圖 4-7 SSL數位憑證運作流程	28
圖 4-8 內容提供者上傳數位內容至DRM系統流程	29
圖 4-9 消費者至DRM系統購買數位內容流程	30
圖 4-10 消費者轉售數位內容的流程	31
圖 4-11 消費者取得數位內容的License流程	31
圖 5-1 本研究之DRM系統實現方式	33
圖 5-2 Transferring Rights Flowchart for Authorization Module	34
圖 5-3 XML-based License Generating Procedure for Transferable Rights	34
圖 5-4 License的Usage Rights解譯和驗證作法	35
圖 5-5 Player Functioning Flowchart	36
圖 5-6 註冊階段流程圖	37
圖 5-7 使用者登入畫面	37
圖 5-8 新使用者的註冊畫面	38
圖 5-9 使用者註冊畫面	38
圖 5-10 使用者憑證儲存詢問畫面	39
圖 5-11 使用者憑證儲存畫面	39

圖 5-12 發行階段流程圖	40
圖 5-13 Demo DRM UI 登入畫面	40
圖 5-14 Packager 之 UI 畫面	41
圖 5-15 Packager 之登入 DRM 管理平臺畫面	41
圖 5-16 DRM 管理平臺的 License 清單畫面	42
圖 5-17 DRM 管理平臺之授權清單畫面	42
圖 5-18 轉移階段流程圖	43
圖 5-19 使用者登入畫面	43
圖 5-20 Rights 轉移前之被授權者 License 清單畫面	43
圖 5-21 Rights 轉移產生之畫面	44
圖 5-22 Rights 轉移後之被授權者 License 清單畫面	44
圖 5-23 被授權者的 XML-Base 之 License 內容畫面	45
圖 5-24 被授權者的 License 清單畫面	45
圖 5-25 播放階段流程圖	46
圖 5-26 Demo DRM UI 登入畫面	46
圖 5-27 使用者選擇受保護的數位內容的清單畫面	47
圖 5-28 開始播放數位內容的畫面	47
圖 6-1 出租交易情境	49
圖 6-2 數位學習教材出租之 Rights Grant 流程	49
圖 6-3 使用者未取得出租授權的錯誤提示畫面	50
圖 6-4 DRM 管理平臺之授權清單畫面	50
圖 6-5 Rights Grant 之 License 產生畫面	51
圖 6-6 消費者的 License 清單畫面	51
圖 6-7 觀賞數位學習教材的畫面	52
圖 6-8 轉售交易情境	53
圖 6-9 數位學習教材轉售之 Rights Transfer 流程	53
圖 6-10 Rights Transfer 前之授權者 License 清單畫面	54
圖 6-11 Rights Transfer 時之 License 產生畫面	54
圖 6-12 Rights Transfer 後之授權者 License 清單畫面	55
圖 6-13 使用者未取得出租授權的錯誤提示畫面	55
圖 6-14 消費者的 License 清單畫面	55
圖 6-15 Demo DRM UI 之消費者 License 內容資訊畫面	56
圖 6-16 消費者的 License Transfer 資訊畫面	56
圖 6-17 播放器播放數位學習教材的畫面	56

一、緒論

1.1 研究背景、動機與目標

隨著資訊科技的日新月異，人們的生活也跟著漸漸地改變。例如，以前的學生上學時，背包裡總是裝滿著一本本厚厚的書，現在可經由數位化的技術，將這些書籍變成數位化的檔案，再透過能閱讀數位化檔案的設備，像平板電腦、PDA 等便可以閱讀書本上的知識，也因此學生就不用再背著厚厚的書包到學校去。然而以數位化表現的資訊，卻很容易地被複製及傳遞，造成創作者的版權受到損害，這無疑將對數位內容產業造成極大的衝擊，但也因此突顯出數位版權管理 (Digital rights management, DRM)[1] 系統的重要，因為數位內容可以透過 DRM 系統的保護，避免被不當的散佈與使用。

DRM 系統的發展對版權擁有者固然是好事，但從另外一個角度來看，現今大多數的 DRM 系統在設計時，對於一些傳統市場上的使用習慣都沒有考慮到，因此過於限制使用者應有的權利。舉例來說，如果使用蘋果電腦的 iTunes[2] 來下載音樂檔案的話，最多只允許在五部 PC 播放，但使用一般的音樂 CD 卻是沒有這種限制，我們只要帶在身邊，任何地方都可以播放，當然我們也可以把購買的音樂 CD 借給朋友播放。當然隨著科技的進步，消費者的行為也有所改變，如今許多消費者可隨時透過「消費者對消費者」(customer-to-customer or C2C) 的電子商務模式來轉售物品，這種可由消費者同時扮演買家與賣家所形成的網路市場，已經成為最受歡迎的電子商務模式之一，當越來越多消費者參與網路拍賣銷售物品時，消費者的網路轉售行為就成為消費者行為中不可忽視的領域。在 C2C 市場中，由消費者同時擔任供應商(賣家)與購買者(買家)的雙重角色，不一定需要傳統零售廠商加入才可構成網路市場，單由消費者本身，就可自行形成具有特色的活絡市場，舉例來說，eBay 就是最好的例子。諸如以上這些消費者傳統的使用習慣，都可能影響到使用受 DRM 系統所保護的數位內容的意願。

從古至今在現實生活中，都存在著把所購買的物品或資產轉移給其他人的行為或權利，就好像中古車或房子的買賣。但在現有的 DRM 系統中，都沒有提供類似的權限轉移機制給消費者去使用。在本論文中，我們提出及實現一個具有 Transferable Rights 機制的 DRM 系統，用以解決「權限轉移」的問題。藉著我們的 DRM 系統更可以提出兩個新的商業應用情境，讓 DRM 系統擴充到更有彈性的商業模式：一個是「租賃」，讓消費者可以用較低的價格在期限內自由使用所租賃的數位內容檔案，期限一過，授權自動失效，也不必將數位內容檔案歸還，不像傳統出租方式，逾期歸還還會被罰款。另一個是「二手市場」，提供消費者方便轉移版權的機制，開創廠商另一種收益途徑，消費者也可以將購買金額作最大的利用。

1.2 論文架構

本論文共分為七章，各章的主要內容及架構安排如下：

第一章：緒論，介紹了本論文研究的相關背景，針對 DRM 系統目前使用上出現

的問題，提出研究重點與要達成之目的。

第二章：在實現具有權限轉移功能的 DRM 系統之前，必須對 DRM 系統的架構有所瞭解並熟悉其各項技術與相關應用知識。

第三章：主要提出轉讓者與被轉讓者之間所需的 Transferable Rights 機制並探討其結合 DRM 系統之影響及效果。

第四章：提出具有 Transferable Rights 的 DRM 系統的模型，並設計其應具有之架構與功能模組，同時指出其應具有的系統運作流程。

第五章：則是系統的實作方法，並展示實作完成的功能畫面。

第六章：提出兩個商業應用情境，且以實作之具有 Transferable Rights 之 DRM 系統作為展示及驗證。

第七章：總結本論文的主要研究成果，並提出未來的建議。



二、 相關文獻探討

在對權限轉移機制做深入的探討之前，勢必要對DRM及其相關技術有所認識。因此本章首先介紹典型的DRM系統架構及商業模式，而後是DRM的安全機制，最後再對數位版權描述語言(Rights Expression Language, REL)作一相關文獻的探討與研究。

2.1 DRM 系統簡介

國際數據資訊中心(Internet Data Center, IDC)對DRM的定義如下：「整合軟硬體之存取與控管機制，將數位資訊賦予存取權限，於數位資訊之生命週期內(從產生到廢止)，不論其使用與複製之途徑，仍可持續追蹤與管理數位資訊之使用狀況，以提供完善保護數位資訊與權限之管理技術，稱為數位版權管理」[3]。從這個定義可以知道，能在數位資訊生命週期內運用軟、硬體服務的結合，進行有效地保護數位內容與版權管理之系統，即可稱為DRM系統。

早期的DRM系統只專注於數位內容的保護，避免未經授權的使用者使用，我們稱之為「第一代的DRM系統」，例如Adobe公司所出的Acrobat。另外符合IDC所定義的DRM系統，我們稱其為「第二代的DRM系統」。兩者之間最大的差別在於第二代DRM系統並不單單只有保護數位內容而已，也包含了數位內容的描述、識別、交易及其使用的監控與追蹤。

2.1.1 典型的 DRM 商業模型

典型的DRM商業模型，如圖2-1[4]所示，而其主要四個角色說明如下：

- 數位內容提供者(Content provider)：
主要負責將自己出版的數位內容進行加密與封裝動作，再將封裝後的數位內容交付數位內容散佈者(Distributor)。並與License Server進行該數位內容的版權規範以及數位內容保護金鑰(Content Key)的交付。
- 數位內容散佈者(Distributor)：
主要的工作在於將封裝後的數位內容經由合法管道，以方便讓消費者進行購買或下載的動作。
- 使用許可證伺服器(License Server)：
數位內容提供者針對數位內容進行版權規範後，產生與數位內容對應的使用許可證並將數位內容保護金鑰放入使用許可證之中。
- 消費者(End User)：
在購買或下載數位內容之後，當消費者要使用數位內容的時候，DRM應用程式會自動連線到License Server，在雙方身分驗證合法後，消費者便

會收到該數位內容對應的使用許可證，並在版權規範下進行播放或使用數位內容。

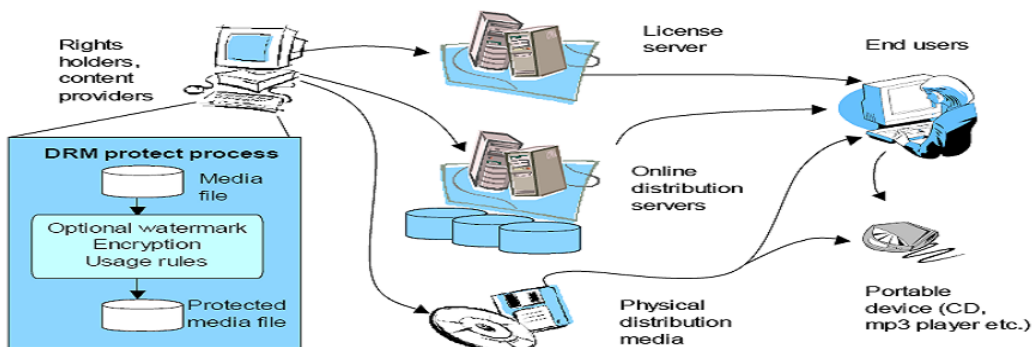


圖2-1 典型的DRM商業模型

2.1.2 DRM 系統的參考架構及運作流程

DRM 系統的架構，會根據不同需求與技術而有所差異，但其參考架構則大同小異。如圖 2-2 所示，此架構為 InterTrust[5]公司所提出。目前許多 DRM 系統除了數位內容的加密與認證技術不同外，其他皆以此圖作為參考架構來發展。

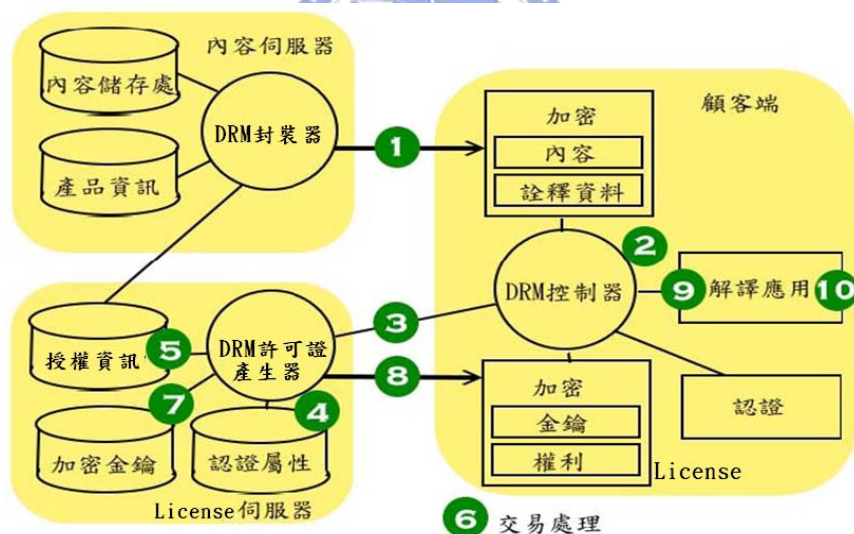


圖2-2 典型的DRM系統架構

我們由圖2-2可知使用權限的管理主要運作在三個核心元件間，這些元件分別是DRM的封裝器(DRM Packager)、DRM的許可證產生器(DRM License Generator)以及DRM的控制器(DRM Controller)。說明如下：

- DRM封裝器：

主要是處理封裝來自內容儲存處與產品資訊資料庫的資訊，同時有關加密等保護動作也會在此處完成。產品資訊資料庫裡儲存了關於數位內容的描述資料(metadata)，例如作者、內容標題等資訊。另外，為了保護這些資料不被竄改，亦會使用特殊的保護機制，例如數位簽章，作為證明

該資訊的完整性。

- **DRM License 產生器:**
主要的工作在於管理許可證的資訊、解密金鑰以及認證屬性資料庫。其中License資訊會對應到DRM封裝器所管理的內容，解密金鑰則對應其加密的動作。
- **DRM控制器:**
異於前兩者屬於伺服器端的元件，它必須安裝於客戶端。DRM控制器負責解譯並接收受保護的數位內容，然後向License伺服器申請License並同時進行身份認證，接著還要解譯取得之License及為受保護的數位內容解密，最後再根據License上所載的允許權利來呈現數位內容。

我們如果以使用者的觀點來解釋圖2-2，其運作流程可說明如下：

- (1) 使用者取得數位內容。
- (2) 客戶端的DRM控制器要求執行使用權限。
- (3) 客戶端的DRM控制器傳送使用者身份與內容資訊至license伺服器。
- (4) License伺服器根據在資料庫的註冊資訊辨識使用者身份。
- (5) License伺服器根據使用者的需求收集使用權限資訊。
- (6) License伺服器檢查使用者的付費狀況，若條件符合則準備產生License檔案。
- (7) License伺服器製作符合使用者需求的License檔案，其中包括使用權限與數位內容的解密金鑰等。
- (8) License檔案可利用伺服器端與客戶端協調好的資訊做加密，例如：使用者密碼或其他可透過客戶端的DRM系統得知的軟硬體序號，並透過安全的網路連線傳送給使用者。
- (9) DRM控制器解開License檔案，並利用金鑰將受保護的數位內容解密並交由應用程式處理。
- (10) 應用程式將數位內容顯示或播放。

此架構的DRM系統，由於License與數位內容分開發行，因此消費者需要重新購買使用權限時，並不需要重新下載數位內容。且值得注意的是，消費者雖然可以任意的散佈從內容伺服器所下載的受保護的數位內容，但是其它使用者將因沒有DRM伺服器所核發的License，而無法使用取得的數位內容。由於數位內容的使用完全取決於License的有無與其條件限制，所以為了避免License被破壞或竄改，一定要做到非常嚴謹的保護與管理。

2.1.3 數位內容的發行管道及商業模式

目前受到DRM系統保護的數位內容，其發行的模式(Distribution Models)，大致有下列幾種方式[21]：

- **直接發行(Direct Distribution)：**數位內容供應商必須為消費者封裝唯一

的數位內容，以方便做到數位內容的追蹤。

- 超級發行(Super Distribution)：在DRM的機制下，可允許消費者將自己所購買的數位內容，以不同散佈方式(如E-mail、FTP Server)傳送給自己的朋友或家人，但接受方依然必須支付版權費用後，以取得對應之License方可使用數位內容。
- 可攜式的裝置(Portable Device Support)：允許將受保護的數位內容轉移到可攜性裝置內，例如：蘋果電腦的iTune音樂平台就可以將受保護的音樂，在自己開發的隨身聽iPod上進行播放。

而受到DRM系統保護的數位內容的商業模式(Business Models)，大致上也可分為下列幾種：

- 直接販售模式(Direct Sales Model)：消費者直接上網購買數位內容，在經由付費之後可以直接下載該數位內容，適用於可以重複使用的數位內容。
- 單次計費(Pay Per View/Listen/Read)：每次使用數位內容前便需付費一次，主要使用於汰換率較高的數位內容，例如：每日的股票分析或者線上電影。
- 預付模式(Subscription Models)：消費者預先付費，來獲取一段期間的數位內容使用權，例如：有線電視的節目收費。
- 租賃模式(Lending Plan)：數位內容性質上屬於租借狀態，所以數位內容將會限制在使用期間才能使用，需要有時間規範的版權管理。例如：百事達的影片租借。
- 預覽模式(Preview and Purchase)：消費者可以先進行數位內容試用再決定購買與否，此模式顧及了消費者的權益，相當符合消費者需求。

2.2 DRM 系統的安全機制

對於DRM系統用以確保數位內容的安全機制，例如；密碼學(Cryptographic)、獨特化(Individualization)以及數位浮水印(Digital Watermarking) [6]等安全機制，以下章節將逐一介紹。

2.2.1 密碼學機制

保護數位內容的能力，是所有對DRM系統感興趣的數位內容提供商，最注重的一點。因為它是數位出版品不會被盜版與濫用的最基本要素，而加密技術是目前最常使用的方法之一。目前加密的方式主要有兩種，一為傳統式加密，另一為公開鑰匙式加密，說明如下：

- 傳統式加密 :在加解密時所使用的鑰匙是相同的，也就是說當訊息傳送方用某把鑰匙將資料區段加密之後，接收方也必須使用此一相同的鑰匙才能解開並獲得其中的內容，所以又稱作對稱式加密(Symmetric Encryption)。使用最廣的對稱式加密方法為AES(Advanced Encryption Standard)[7]，AES在1977年被美國國家標準與技術協會(National Institute of Standards and Technology, NIST)所採用。AES使用一把128位元的鑰匙來對128位元的資料區段進行加密，這個演算法會透過一連串的步骤，將明文輸入資料轉變為密文輸出資料，過程如圖2-3所示。

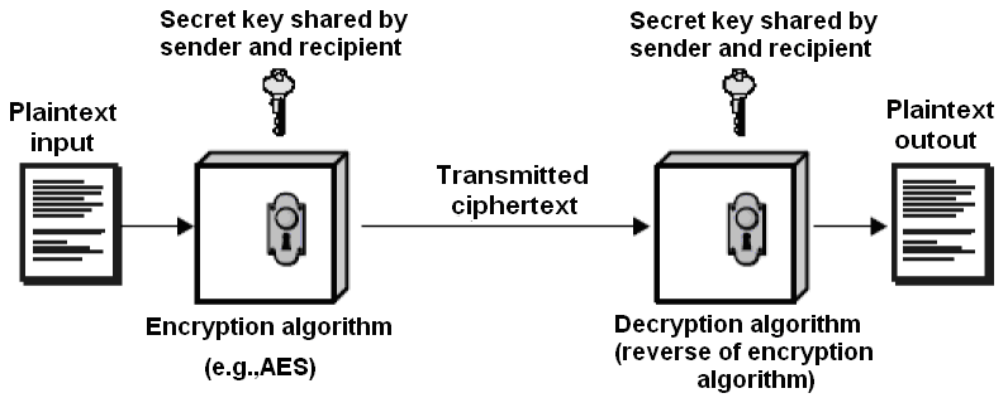


圖2-3 傳統式加密的過程

- 公開鑰匙式加密:在加密與解密時使用了兩把不同的鑰匙，一把稱之為公鑰(Public Key)，另一把稱之為私鑰(Private Key)，兩把鑰匙可互為加解密的鑰匙。所以又稱為非對稱式加密(Asymmetric Encryption)。如圖2-4所示，Alice可公開其公鑰並保管好私鑰，當Bob需要傳送訊息給Alice時便可用Alice的公鑰將訊息加密起來傳送給Alice，於是Alice在收到加密的資料後則可用自己的私鑰解開以獲得訊息，這個訊息也只有持有私鑰的Alice可以獲得。同樣的，若Alice要傳送訊息給Bob的話便可用Bob的公鑰來加密資料傳給Bob。公開鑰匙加密最著名的演算法為RSA[8]，RSA中使用的鑰匙並不限於一固定長度，通常所用的長度為512位元的倍數。公開鑰匙式加密法也不僅僅應用於資料的加密上，同時也可以用在數位簽章和鑰匙交換上。數位簽章代表了如何證明某一段加密過的資料或訊息確實是某一個人加密所發出的，也就是加密資料傳送後的不可否認性。RSA是目前最受好評的加密方法，能承受現今的密碼攻擊技術。當然在DRM系統的應用上，我們也可把這兩種加密演算法結合在一起使用，例如：利用AES來加密數位內容，而使用RSA來傳遞AES的金鑰。

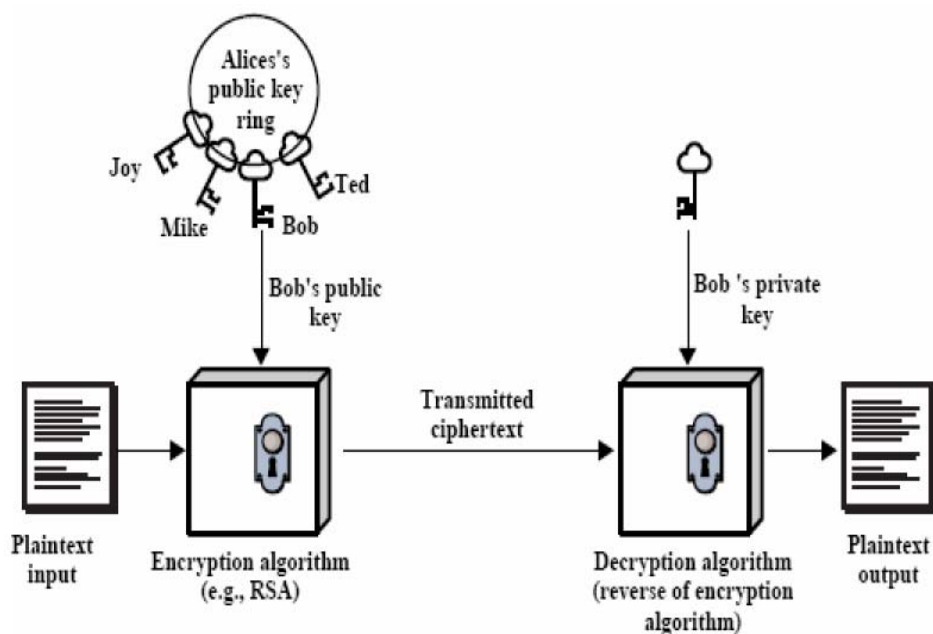


圖2-4 公開鑰匙式加密的過程

2.2.2 獨特化機制

目前許多DRM系統會使用不同的獨特化機制，確保使用者端的Rights執行軟體(或硬體)是可唯一辨識的。通常是在初始階段先利用使用者端的硬體資訊或個人身份產生唯一的註冊碼，以此產生一組非對稱金鑰或憑證，保存在使用者端的Rights執行軟體(或硬體)之安全空間。要使用數位內容時，只有使用者端Rights執行軟體(或硬體)的私密金鑰才能解開License，得出數位內容的解密金鑰與Rights，在權限規範下解密使用數位內容。因為每個註冊的裝置或使用者都有不同的認證授權金鑰以及一組License。因此只能由單一裝置或使用者解開，所以其數位內容也就限定為單一裝置或使用者所使用。

2.2.3 數位浮水印機制

對DRM系統而言，單純使用加解密技術來對數位內容作保護是不夠的。因為數位內容被合法使用者的金鑰解密後，在輸出到外部硬體設備時，就很有可能從中被擷取完整的明文資料，所有的努力都白費，所以我們需要另一種的保護機制—數位浮水印。數位浮水印技術可應用在資訊隱藏(Information Hiding)方面，將秘密資訊嵌入數位內容之中，待日後發現可疑數位內容(經由非法複製)時，可將隱藏的數位浮水印取出作為其原版數位內容的驗證與非法複製和非法傳播的證明。對於DRM技術的應用，數位浮水

印可將一些智慧財產權的訊息，例如原作者、版權擁有者、使用次數等等資訊隱藏在數位內容上，以控制數位內容的複製控制與版權執行。

而數位浮水印技術與密碼學系統不同的是，並不是去限制或控制存取數位內容，而是可將一些控制訊息加入，以保護數位內容的版權使用。相對於密碼學系統，將密文解密後所得的明文將毫無保障，而數位浮水印技術可藉由加入一些隱藏資訊，正好彌補密碼學系統對解開後的明文無法保障的缺點。大部份數位浮水印技術至少必須符合以下二項基本的要求：

- 數位內容若具有可見數位浮水印，除非經過版權擁有者許可後才可將數位浮水印移除，若自行將數位浮水印去除，將會嚴重破壞數位內容的播放效果。對於不可見的數位浮水印則必須達到無法任意移除和任意修改等特性。
- 一個數位浮水印必須能承受任何外部攻擊和額外的內容處理。這些處理包括在類比訊號與數位訊號之間的轉換，影像濾波處理(Filtering)和壓縮(Compression)等等。

數位浮水印在DRM技術上的應用，並不注重在數位內容的存取控制上，而是當數位浮水印遭到非合法移除時，會嚴重影響播放品質，除此之外，更可做到Rights的嚴格執行(隱藏播放次數...等)。

2.3 數位版權描述語言

為了傳送 Rights 的使用權限，包括：合法使用者的個人資訊、使用規則與相關限制、被使用的數位內容資訊與付費條件等，必須有一個資料結構來記錄這些訊息。此時就需要數位版權描述語言(Rights Expression Language, REL)來定義 Rights 的相關內容，其中包括 Rights 的擁有者以及使用的相關權限，並由 REL 中的規範來限制 Rights 的使用。目前常見的 REL 標準有 W3C 的 ODRL[9]、ContentGuard 的 XrML[10]以及 MPEG 的 MPEG-21 REL[11]等等，針對這些 REL，分述如下：

- ODRL 的結構與語法較為簡單，其基本元件包括權利 (Rights)、資產 (Asset) 和當事人 (Party)，並提供三種擴充元件為 Offer 與 Agreement 等元件 (見圖 2-5)。ODRL 還定義了一些基本模組，描述在使用資產前所必須具有的條件，和對當事人的一些認證與安全功能。在架構及語法的比較上，ODRL 較簡單且容易明瞭，而其功能上較著重於數位內容的使用，有關付費的機制相對較少，只提供簡單的付費資訊交換而已，適用於學術與研究單位的研究，或應用於圖書館的 DRM 系統。

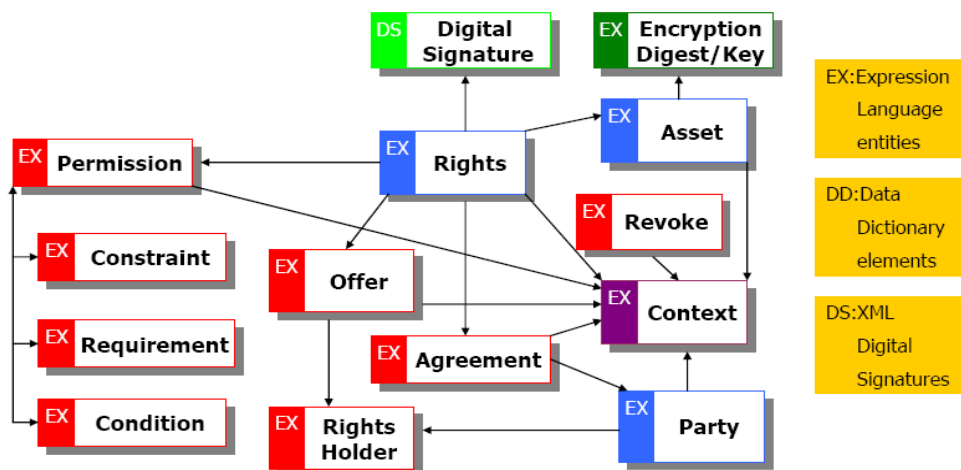


圖 2-5 ODRL 語法架構

如圖2-6所示，為ODRL的License範例，在這個範例中說明Alice可以列印電子書的內容三次並在資源部份指出此電子書的網路位置。

```

<?xml version="1.0" encoding="UTF-8" ?>
<o-ex:rights xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
  xsi:schemaLocation="http://odrl.net/1.1/ODRL-EX ../schemas/ODRL-EX-11.xsd
  http://odrl.net/1.1/ODRL-DD ../schemas/ODRL-DD-11.xsd">

  <o-ex:asset>
    <o-ex:context>
      <o-dd:uid>urn:ebook.world/999999/ebook/rossi-000001</o-dd:uid>
      <o-dd:name>Why Cats Sleep and We don't</o-dd:name>
    </o-ex:context>
  </o-ex:asset>

  <o-ex:permission>
    <o-dd:print>
      <o-ex:constraint>
        <o-dd:count>3</o-dd:count>
      </o-ex:constraint>
    </o-dd:print>
  </o-ex:permission>

  <o-ex:party>
    <o-ex:context>
      <o-dd:name>Alice</o-dd:name>
    </o-ex:context>
  </o-ex:party>
</o-ex:rights>

```

Asset

Permission

Constraint

Party

圖 2-6 ODRL 的 License 範例

- XrML 最初是由 Xerox 所發展的 REL，當時主要用途在於提供可以辨識與管理所有的數位內容與服務的安全方法，直到 XML 發表之後，XrML 才改成目前的格式。XrML 同樣具有擴充性，可根據 DRM 系統製造商設計目的自行加上所需的模組（見圖 2-7），如若需要額外對數位內容作描述，則可加入其他的 metadata 描述語法。XrML 的主體架構可分為三大模組：

- (1) Core Schema：包含所有核心部分模組的定義。
- (2) Standard Extension Schema：包含一般在使用 XrML 定義數位版權時所需的模組定義。
- (3) Content Specific Extension Schema：定義數位內容或服務的 DRM 模組。

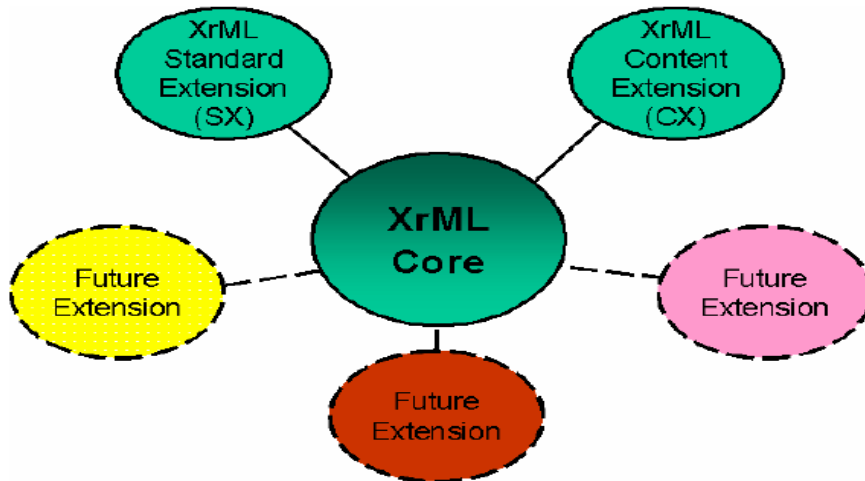


圖 2-7 XrML 語法架構

XrML 與 ODRL 的不同處，在於描述方式的不同與商業模式支援的多寡，ODRL 屬於純文字的描述方法，所有的權限、條件與責任都以文字直接表述，而 XrML 除了純文字的描述外，還可透過其他服務識別標準，如：通用描述、探索與整合（Universal Description, Discovery, and Integration, UDDI），可讓使用者透過識別碼至伺服器端的服務檢查使用權限與條件是否符合，因此常被發展 DRM 系統的廠商視為首選。

- MPEG-21 REL (MPEG 21 Part 5 Rights Expression Language) 是在 XrML 2.0 正式發行且發展的期間，而 MPEG (Motion Picture Experts Group) 正好在發展一連串數位影音多媒體的標準規格時所提出。MPEG-21 REL 是以 XrML 為基礎發展，並於 2003 年成為 ISO 標準。MPEG-21 REL 可以說是整個 MPEG-21 多媒體框架中的一個部分，就像 MPEG 所制訂的其他標準一樣，每個標準都是由很多次部分所組成的，並且可以單獨地被拿來使用並提供有彈性且具互通性的機制[12]。它同樣也希望能夠在尊重隱私權以及個人資料的處理之下，達到使用者表達自己 Rights 與興趣的需求。MPEG-21 REL 大致上可以分為三個部分，第一部份是主要(Core)部分，第二個部分是標準延伸(Standard Extension)部分，第三個部分是多媒體延伸(Multimedia Extension)部分。如圖 2-8 所示，三個部分共同組成 MPEG-21 REL，並保留了未來可延伸的部分。

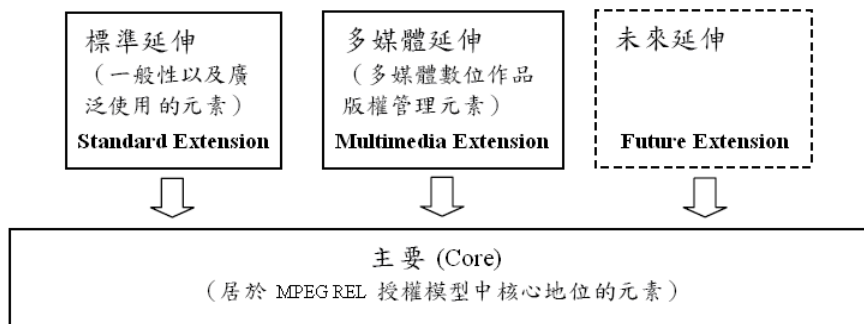


圖 2-8 MPEG-21 REL 語法架構

接著我們簡單介紹如何由REL來形成License，以下用MPEG-21 REL來作一說明。首先如圖2-9所示為MPEG-21 REL語法的基本資料結構，而其基本概念為主體(Principal)可在某種條件(Condition)下，對於特定資源(Resource)享有某種版權(Rights)。接著對於MPEG-21 REL的四種基本元素分述如下：

- (1) 主體(Principal)：一般由資源的提供者(provider)、使用者、傳播者或管理者對於每種不同的物件來描述其屬性。MPEG-21 REL對於非對稱的密鑰體系中可定義密鑰的持有者<keyHolder>的內容，通常用來表示主體的身份與其相關連的驗證機制所需要的資訊。
- (2) 條件(Condition)：版權約束的描述。一般常用的屬性包括了時間的存取期限<validityInterval>、執行次數<exerciseLimit>等標籤。
- (3) 版權(Rights)：根據主體可執行的一種或一類行為，例如文件管理的標籤中有寫入<mx:write>、讀取< mx:read>、列印 < mx:print>等多種實用的標籤。
- (4) 資源(Resource)：指主體所要執行之數位內容物件，在描述一件數位內容時使用<digitalResource >。

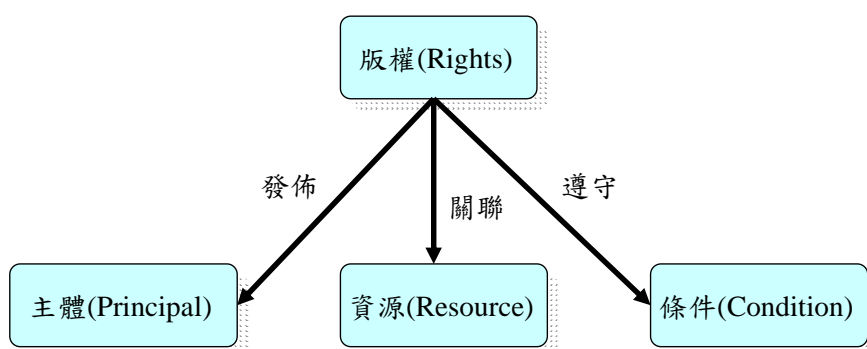


圖 2-9 MPEG-21 REL 語法的基本資料結構

如圖2-10所示，為MPEG-21 REL的License範例，在這個範例中說明Alice可以列印電子書的內容三次並在資源部份指出此電子書的網路位置。

```

<?xml version="1.0" encoding="UTF-8" ?>
<r:license xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
  xmlns:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS"
  xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS"
  xmlns:sx="urn:mpeg:mpeg21:2003:01-REL-SX-NS"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:mpeg:mpeg21:2003:01-REL-R-NS ../schemas/rel-r.xsd
  urn:mpeg:mpeg21:2003:01-REL-SX-NS ../schemas/rel-sx.xsd
  urn:mpeg:mpeg21:2003:01-REL-MX-NS ../schemas/rel-mx.xsd">
  <r:grant>
    <r:keyHolder>
      <r:info>
        <dsig:KeyName>Alice</dsig:KeyName>
      </r:info>
    </r:keyHolder>
    <mx:print />
    <r:digitalResource>
      <r:nonSecureIndirect URI="urn:ebook.world/999999/ebook/rossi-000001" />
    </r:digitalResource>
    <r:allConditions>
      <sx:exerciseLimit>
        <sx:count>3</sx:count>
      </sx:exerciseLimit>
    </r:allConditions>
  </r:grant>
</r:license>

```

圖 2-10 MPEG-21 REL 的 License 範例

至於ODRL、XrML與MPEG-21 REL在權限轉移方面的描述能力，探討如下：

- ODRL: 在 ODRL 當中，「give」有將Rights整個轉讓的意味。give的定義是，允許資產作所有權的轉移，而且是永久性的所有權轉移，不必有付費的動作。亦即，「give」這個權利元素，其意義不帶價值交換。相對的另一個權利元素「sell」是要金錢交易的。還有一個權利元素「transfer」，似乎也有將Rights作轉讓的意味。但實質上，以上幾個權利元素描述的轉讓行為，其實是指資產在裝置設備之間的轉讓，並不是Rights在用戶之間的轉讓。
- XrML: 在 XrML 中，並沒有類似Rights轉讓的權利元素，但可以改用另一種方式，衍生一個新資源(Resource)，並擁有其版權。例如在XrML裡，屬於衍生新資源的權利有「edit」、「embed」、「extract」三個，這些元素的應用，意味著假使要取得完全的版權，就必須對原來舊的資源作加工，使之改變，然後新資源便屬於被授權人的創作，被授權人也擁有新資源的版權。換句話說，XrML並無現有Rights完全轉讓的權利元素。
- MPEG-21 REL: 在 MPEG-21 REL 中，「adapt」、「diminish」、「enhance」三者也都是可以衍生新資源的，但並不能達成整個轉讓資源的狀況。亦即，MPEG-21 REL也無現有Rights完全轉讓的權利元素存在。

三、可權限轉移的 DRM 機制

本章首先提出一具有 Transferable Rights 的 DRM 商業交易模型，並定義 Transferable Rights 及其相關作法，同時介紹必須的運作流程，其次說明 License 的格式及其相關機制，最後再看一實際之 XML-Based License 範例。

3.1 具有 Transferable Rights 的 DRM 商業模型

目前 DRM 系統的數位內容，在使用上缺乏可轉移性，而且對於消費者使用數位內容的限制甚多，最重要的是，並無法提供一般傳統的消費使用習慣給使用者，例如：租借、轉售等交易行為，而這種現象只會讓一般消費者對 DRM 系統望而卻步。況且在 Wang 等人[13]的研究中，認為 C2C 的數位內容 reselling model 有助於數位內容銷售的提升。而數位內容的租借、轉售等交易行為，其實就是「權限轉移」的實際應用。

針對數位內容的「權限轉移」這個研究議題，Chong 等人[14]在 2006 年提出 Transfer Rights 的概念，認為消費者可在任何一個可執行使用權限(Usage Rights)的軟硬體上播放自己合法購買的數位內容。不過，在目前的 DRM 系統上，還沒有看到相關的實現或應用。先前也有人提出在不影響數位內容的安全性下，以智慧卡(Smart card)來解決有關「權限轉移」的問題。其方法為將原本數位內容指定的授權對象，由消費者的電腦換成消費者隨身攜帶的智慧卡，然後便可在不同的電腦上使用數位內容。亦即消費者可以在個人擁有的多台裝置上合法使用其購買的數位內容。因為智慧卡不可能被仿製，可保證數位內容在同一時間只在一個裝置使用，達成數位內容的 Usage Rights 可轉移性與合理使用之目的。不過，在一般的 PC 上，智慧卡並不够普及，其原因如下：

- 需要額外的裝置，如讀卡機
- 增資額外的成本
- 智慧卡的容量與運算能力有限
- 在一般 PC 上，以智慧卡做為身份辨識有時比軟體方式的「Software Token」效率還差

不過，目前有關「權限轉移」的 DRM 研究及作法，都局限在個人使用上，並未提到轉移給他人的情形，所以並無法達到我們想要的「權限轉移」。但數位內容的租借、轉售等交易行為，其實就是把使用權限轉移給他人的作法。因此如圖 3-1 所示，我們將提出一具有 Transferable Rights 的 DRM 商業交易模型來解決數位內容的「權限轉移」問題。

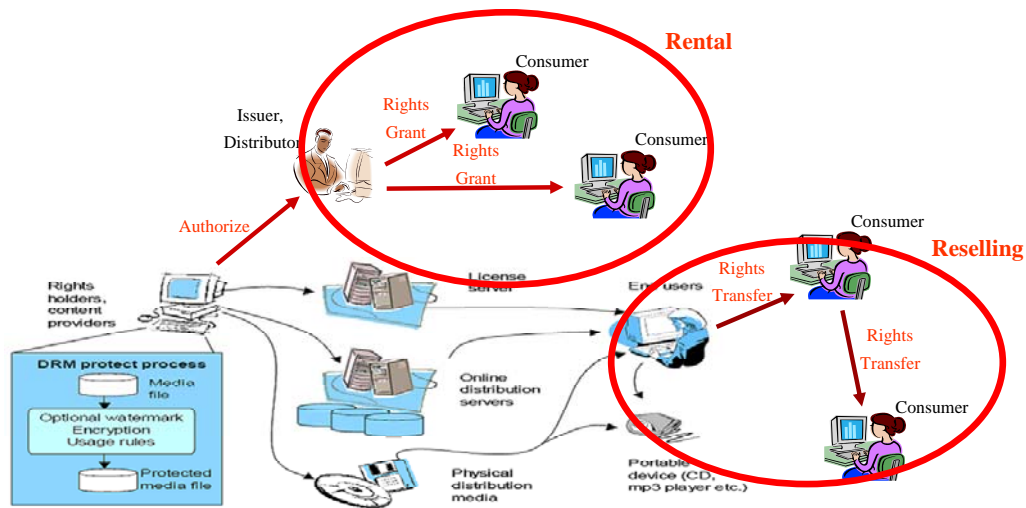


圖3-1 具有權限轉移的DRM商業交易模型

3.2 Transferable Rights 的定義

如前圖3-1所示之具有權限轉移的DRM商業交易模型，其使用的License架構應如圖3-2所示。

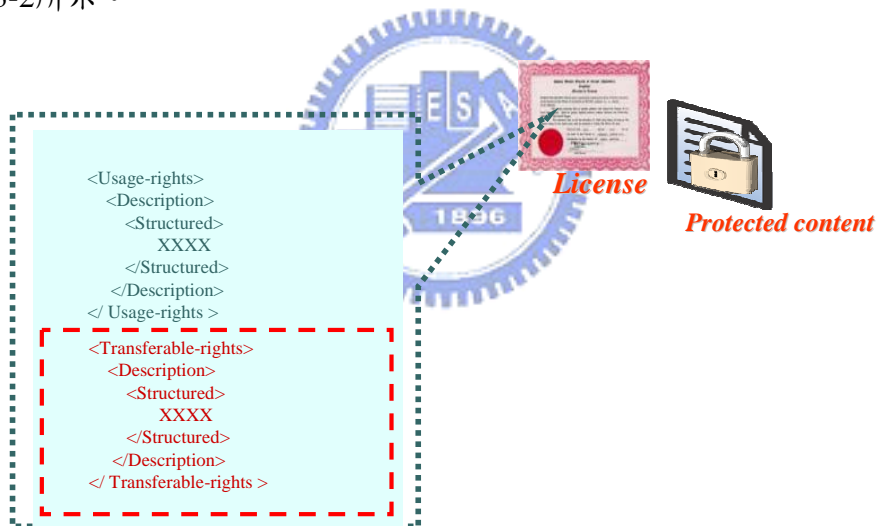


圖3-2 具有使用權限及Transferable Rights的License

此License架構除了有一般的使用權限(Usage Rights)外，另外我們增加了Transferable Rights，而有關於其定義說明如下，並參考圖3-3：

- Rights Grant：可對使用權限做多次性轉移。亦即版權擁有者可授予Rights Grant給被授權者，此時被授權者具有可將來自版權擁有者的Usage Rights授予他人的權利，且在Grant之後本身權利不受影響。
- Rights Transfer：只能對使用權限做一次性轉移。亦即版權擁有者可授予Rights Transfer給被授權者，但被授權者在Transfer Rights給他人後，就完全失去被授予的權利。

Transferable Rights

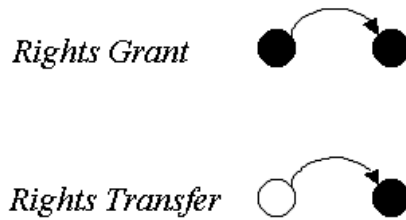


圖3-3 Transferable Rights的示意圖

3.3 Transferable Rights 的運作模型

在說明Transferable Rights的運作模型之前，我們先介紹各個不同角色在「內容提供者-零售出租者-消費者」此種數位內容發行模式中所擔任的工作：

- (1) 內容提供者 (Content Provider)：內容提供者經過DRM系統的認證後，開始上傳數位內容檔案至DRM系統，接著利用DRM系統提供的加密技術將上傳之數位內容做安全保護處理，並將metadata輸入資料庫，再將相關權限條件與付費資訊輸入，建立與零售出租者交易之版權提議。另外，內容提供者必須提供網頁介面給零售出租者選擇數位內容檔案與提議，待產生協議後，製作版權協議檔案與受保護之數位內容檔案給零售出租者。
- (2) 零售出租者 (Renter)：首先必須先經過DRM系統認證後，再利用DRM系統提供的網頁介面尋找數位內容資訊，確定要取得授權之數位內容與選擇提議後，進而取得版權協議檔案，並依協議建立與消費者交易之版權提議，進而授予消費者適當之Rights。另外，零售出租者必須提供網頁介面給消費者選擇數位內容檔案與提議，待產生協議後，建立消費者使用的資訊至資料庫，並提供已受保護的數位內容檔案供消費者下載。
- (3) 消費者 (Consumer)：經過DRM系統的認證後，消費者可透過網頁介面提供的數位內容清單挑選欲購買的數位內容檔案後，再選擇交易模式與提議，雙方交易完成後，零售出租者必須提供消費者數位內容檔案的下載服務，消費者取得後利用客戶端的DRM系統開啟數位內容檔案。

在內容提供者-零售出租者-消費者此種數位內容發行模式中，內容提供者對數位內容的發行數量不能超過授權協議的設定，而零售出租者能取得的發行數量也決不可能大於內容提供者可發行的數量。由此Rights的授權雙方在同樣的使用權利下，許多權限條件會重複出現，而被授權者的權限條件，會受限於授權者擁有的權限條件範圍內，因此在Rights的轉移過程中，權限條件會產生繼承的效應，而且不會影響授權者的使用權限，但也不是所有的權限條件都有繼承性。

在商業模式中，內容提供者對發行權限提供的訂購方式不一定與零售出租者相同，因此在Rights權限規則中並不需要考慮類似的條件，而條件是否具繼承性

則需要系統實作者自行判斷。然而數位內容的Rights，雖然部分具有包容性，例如：Rights擁有者對數位內容具有覆寫權利，必定能夠讀取內容，但這些權利在Rights轉移過程中不一定會繼承給被授權者，是任由提議制訂者規範，因此不需要考慮Rights是否具有繼承性。如圖3-4所示，即為一Rights Grant的運作模型，透過此模型我們可以實現諸如租借等交易行為。

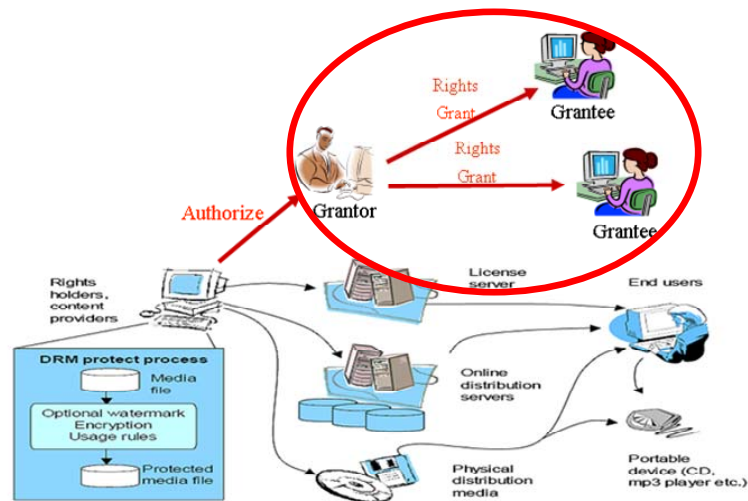


圖 3-4 Rights Grant 的運作模型

另外，在實際的應用中，取得數位內容授權的角色應可透過授權者的DRM系統伺服器，將Rights轉移給對等的另一角色，這樣才合理。例如：在內容提供者-零售出租者-消費者此種數位內容發行模式中，倘若授權協議允許Rights的轉移，此時消費者便可透過DRM系統將Rights轉移給好友或其他的消費者，亦即消費者之間的Rights Transfer，而其權限條件比較單純，就只有繼承的效應。但與Rights Grant不同的是，轉移者的Usage Rights需在轉移完後被系統自動撤銷，可參考如圖3-5所示之Rights Transfer的運作模型，透過此模型我們可以實現諸如轉售等交易行為。但是有關零售出租者之間的Rights Transfer尚涉及各零售出租者與其消費者之間的數位版權管理問題，因此在特性上比較難做到彼此的Rights Transfer。

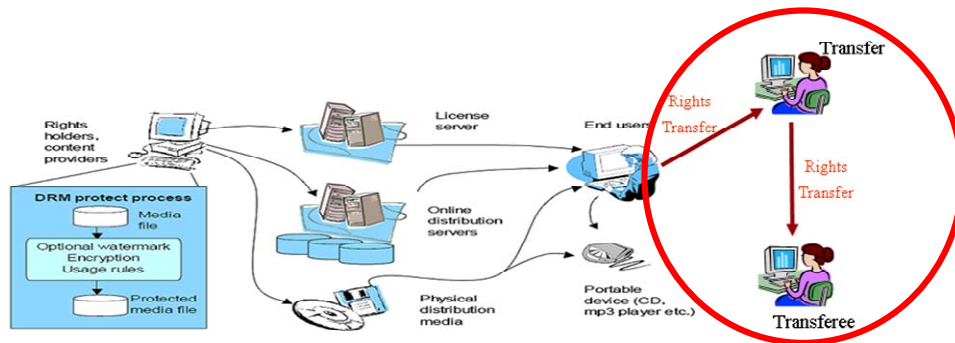


圖 3-5 Rights Transfer 的運作模型

3.4 Transferable Rights 的運作流程

我們可以藉著轉讓者(Grantor)與被轉讓者(Grantee)於DRM系統，透過以下程序進行Rights Grant。其轉移過程作法如圖3-6所示，主要步驟說明如下：

- Content Registration：輸入Grantor的Content以及相關資料到DRM系統。
- Purchase Request：Grantee如欲購買Grantor的數位內容時，Grantee須傳送Purchase Request給DRM系統。
- 雙方的權限轉移之協議及付款處理。
- License issue Request：在進行LicenseCreate()時，對於權限條件上的轉移，預設上都是以Grantor的License可用權限條件為主。例如，Grantor的權限結束時間為Grantee的權限結束時間以及轉讓時的系統時間為Grantee的權限開始時間。但為了合理及正確起見，必須在License產生時驗證其權限條件，而此必要的驗證規則如下：

(1) 使用期限驗證：

使用期限可分為一般日期表示與週期表示，其驗證如表3-1。週期限制的第二點表示新的檢查週期可比舊的檢查週期更頻繁，而第一點與第三點用以保證新的執行檢查的期間與原來的設定相同。

(2) 使用次數的驗證：

若原使用次數為N，則 $0 \leq \text{新使用次數} \leq N$ 。

若只有部分的使用次數要轉移給被轉讓者，則可轉移的使用次數必須介於0與目前轉讓者真正擁有的使用次數之間。

(3) 使用區域限制驗證：

新的使用區域限制必須在使用原區域限制的子範圍內。

(4) 其他文字性驗證：

若條件限制描述不具分割性，如：版權聲明等，則直接引用。

- Output License：發放新的License給Grantee。

日期限制	$Old_BeginDate$ 、 $Old_EndDate$ 、 $New_BeginDate$ 、 $New_EndDate$ 均表示日期，且 $Old_BeginDate \leq \text{原日期限制} \leq Old_EndDate$ $New_BeginDate \leq \text{新日期限制} \leq New_EndDate$ 則 $Old_BeginDate \leq New_BeginDate$ $Old_EndDate \geq New_EndDate$
週期限制	1. 開始日期不變 2. $T_{new} \leq T_{old}$ 3. $T_{new} * \text{新週期循環次數} = T_{old} * \text{原週期循環次數}$

表 3-1 使用期限的驗證

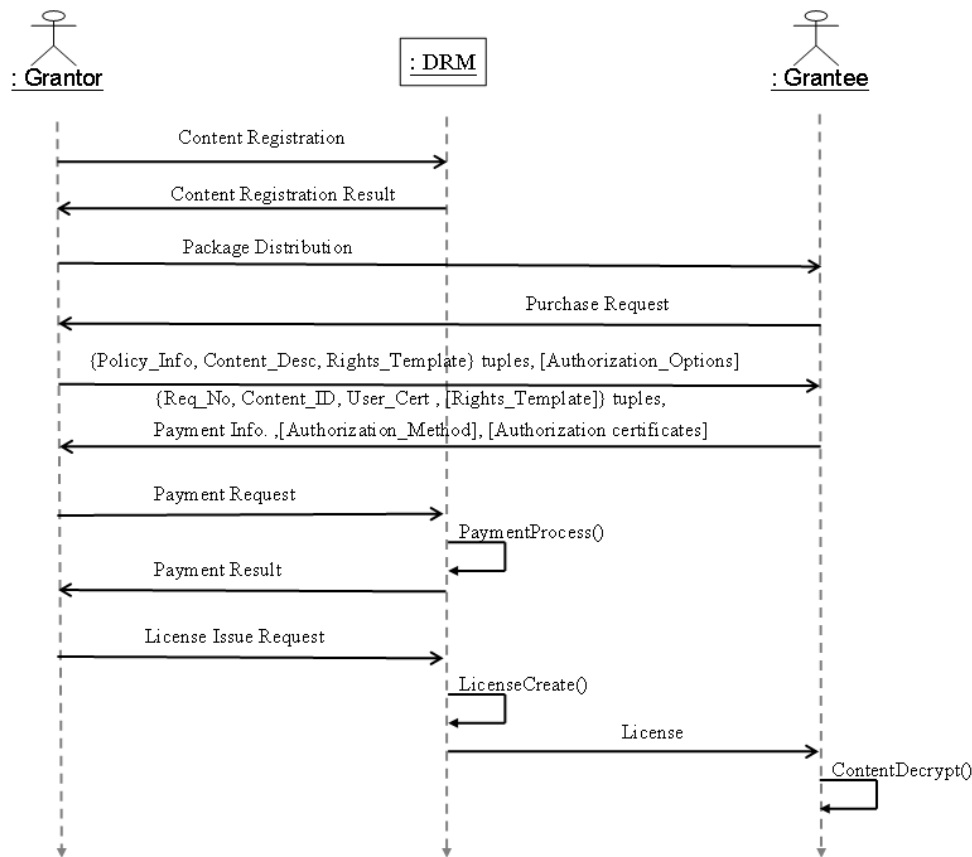


圖 3-6 Rights Grant 的運作循序圖

而Rights Transfer的轉移過程作法如圖3-7所示，主要步驟說明如下：

- Transfer Registration：輸入Transfer的License以及相關資料到DRM系統。
- Transfer Request：Transferee如欲購買Transfer的數位內容時，Transferee須傳送Transfer Request給DRM系統。
- 雙方的權限轉移之協議及付款處理。
- License transfer Request：在進行LicenseCreate()時，同樣必須驗證權限條件。
- Output License：發放新的License給Transferee。
- Revoke transfer's license：在轉移License給Transferee之後，將Transfer的License註銷。

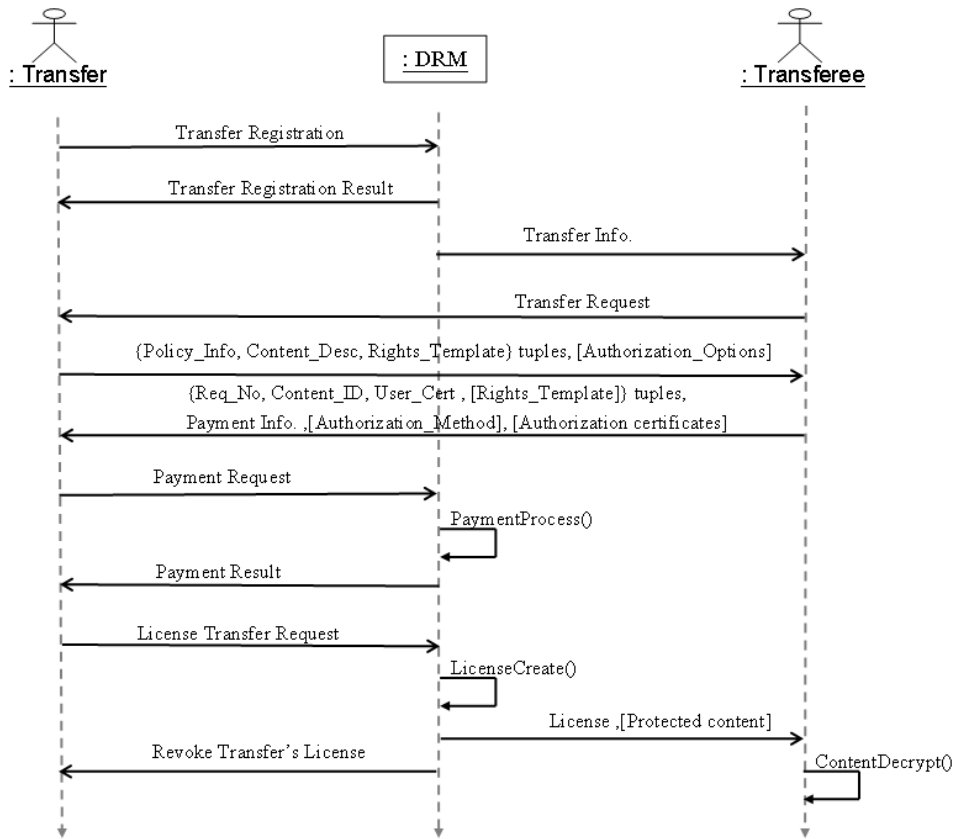


圖 3-7 Rights Transfer 的運作循序圖

3.5 Transferable Rights 的 License 作法

如圖3-8所示，我們需要新增一具有Transferable Rights的REL模型給License使用。具有Transferable Rights的Transfer實體是由兩個實體聚集組成，說明如下：

- Rights-Type實體：此實體是用來表達對特定的Usage Rights可以作什麼樣的動作。在Rights-Type實體裡，可以指定授與的權利，比如說用rights-grant元素來表示Rights Grant動作或者用rights-transfer元素來表示Rights Transfer動作。
- Constraint實體：此實體是用來限制Transferable Rights的權利，也就是針對Rights-Type實體所載被授與的權利去作限制，用法與REL中之Constraint相同。限制有許多不同的面向，例如限制使用者、裝置、範圍、時間等。

```

<transfer>
  <rights-type>... </ rights-type >
  <constraint>... </constraint>
</transfer>
  
```

圖3-8 Transferable Rights模型的REL語法

接著，我們探討具有Transferable Rights的License Traceability機制，如圖3-9範例所示。這裡的Rights Transfer是，Jim的權限條件轉移給Bob後而Bob再把權限條件轉移給Mark，不過這種權限條件轉移的動作越到轉移末端權利條件會越被限制，因為通常被授權者的權限條件會被限制在不大於授權者的權限條件，也就是說Jim所擁有的權限條件(例如，播放次數)，那麼Bob跟Mark就絕對不會有大於Jim的權限條件的情形發生，但是有可能等於Jim的權限條件的情形發生。而系統一旦要確定Mark的權限條件是否具有合法及有效性，它必須先去找到Mark授權的源頭Bob，然後再往上回溯到Jim，如此才能確定Mark的License是否具備合法及有效性。

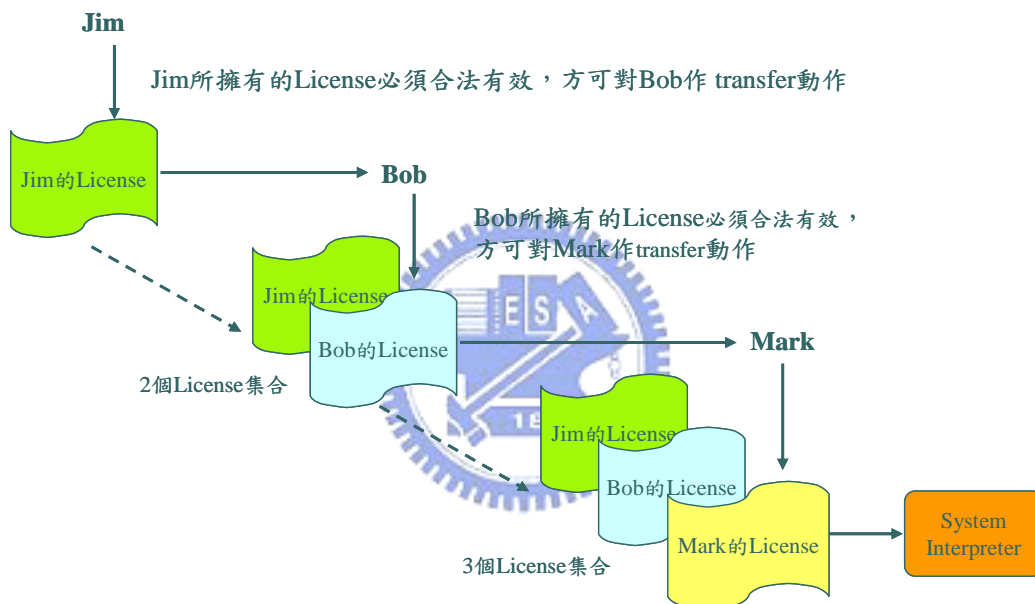


圖3-9 License Traceability of Transferable Rights

最後我們再以一個實際的XML-Base License範例，來展示具有Transferable Rights之License內容，如圖3-10所示。

SELAB DRM SYSTEM
Digital-Content Rights Management

> Manage Rights

XML-Based License

```

<mx:play />
- <mx:diReference>
  <mx:identifier>DRM-Report</mx:identifier>
</mx:diReference>
- <r:validityInterval>
  <r:notBefore>2008-11-01T00:00:00</r:notBefore>
  <r:notAfter>2009-10-31T00:00:00</r:notAfter>
</r:validityInterval>
</r:grant>
- <r:transfer>
  <r:rights-type>
    <mx:rights-transfer />
  </r:rights-type>
  <r:constraint>
    <r:notBefore>2008-11-01T00:00:00</r:notBefore>
    <r:notAfter>2009-10-31T00:00:00</r:notAfter>
  </r:constraint>
</r:transfer>
- <r:issuer>
- <r:keyHolder>

```

Transferable Rights Entity

another is "rights-grant"

Go back

CONTENT CRYPT

圖3-10 具有Transferable Rights之License範例



四、系統架構

在OM-AM (Objective, Model, Architecture, and Mechanism) [15]的概念中，目標、模型、架構和機制是設計一個完整系統的基本流程，首先設計者必須決定系統的設計目標並提出基本的系統模組，再透過架構與機制設計出符合需求的系統。許多資訊安全系統，例如：DRM系統，都是依循此概念設計出符合要求的系統。因此本章將以OM-AM的方法，目標為設計具有如前述所提的Transferable Rights機制的系統，以符合實際上的應用。

4.1 系統模組

系統模組設計上，除了參考前面探討的DRM系統之架構及安全技術，並以內容提供者-零售出租者-消費者的數位內容發佈方式作為系統運作的模式，且採用ODRL以及MPEG-21 REL等作為REL語言，並結合Transferable Rights機制及方法，提出如圖4-1所示之系統模組作為我們系統架構設計的基礎。

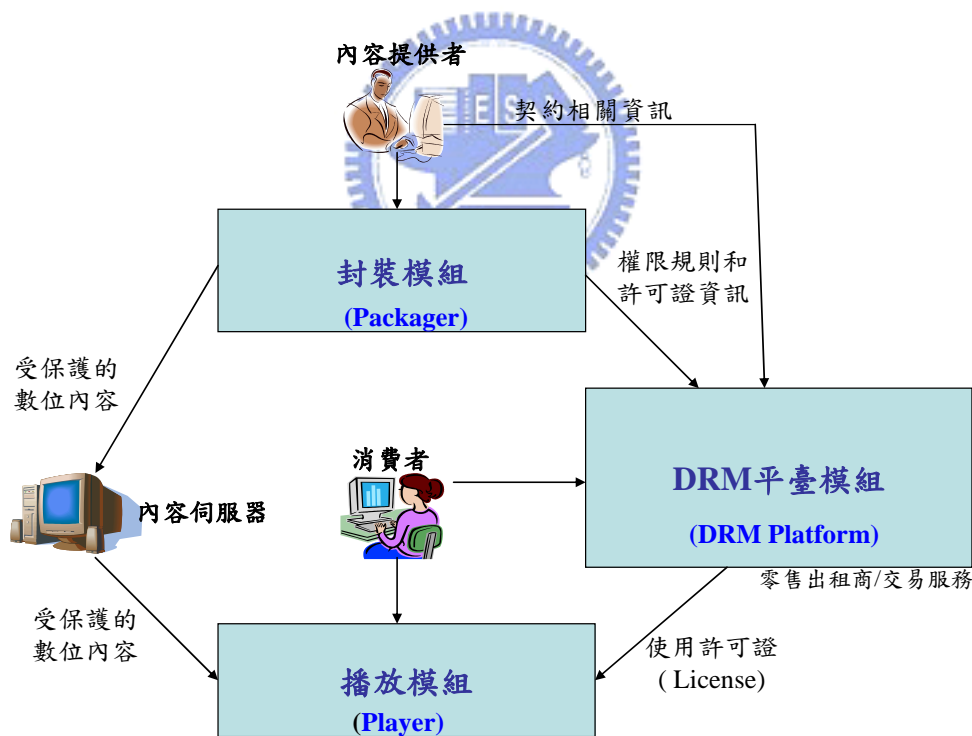


圖 4-1 系統功能模組

以下針對此三大系統模組之主要功能作一說明：

- 封裝模組(Packager)：主要是用來保護數位產品，並將其註冊到 DRM 系統中。通常是使用加密的手段來保護數位產品。
- 播放模組(Player)：主要是用來播放受保護的數位內容檔案。通常需要與 DRM 管理模組連線通信，獲取 License 並根據使用許可權來進行播

放的服務。

- DRM 平臺模組(DRM platform): 主要是提供以下五項服務。
 - (1) 使用者註冊服務:是一個伺服器端提供的服務,允許用戶在 DRM 系統中註冊,在註冊的過程中,為用戶分發 ID 以及 License 等,用戶可以使用它們與伺服器通信,獲取伺服器中的數位內容資源。與伺服器的通信都是透過加密的安全通道進行的。
 - (2) 內容管理服務:是一個伺服器端提供的服務,允許內容提供商發佈新的數位內容資源,並且對已經發佈的資源進行管理。一旦完成數位內容資源在 DRM 系統中的註冊,該資源即受到 DRM 系統保護。用戶端與內容管理服務的通信也是透過加密安全通道進行的。
 - (3) 權限授權服務:是一個伺服器端提供的服務,允許內容提供商或者代理人對註冊的數位內容等資源的使用許可權進行管理,透過加密安全通道通信。
 - (4) License 管理服務:是一個伺服器端提供的服務,處理用戶端發出的獲取 License 的請求,透過加密安全通道通信。
 - (5) 權限轉移服務:是一個伺服器端提供的服務,允許消費者或者代理人對註冊的數位內容等資源的權限進行轉移,透過加密安全通道通信。

在我們的系統模組設計上,須將權限轉移的機制以及相關方法導入,以期改善目前的DRM系統在設計上不具有權限轉移功能的問題;而在安全機制上,同樣將DRM系統所應具有的安全機制加以整合實現,確保數位內容的安全及完整。

4.2 系統架構

我們的系統架構如圖 4-2 所示,此架構是利用目前最常見的 DRM 安全技術,例如:加密、認證...等,並參考數位內容發行模式中各角色需執行之動作,且根據使用目的與商業模式,同時加入付費機制及憑證授權中心認證的功能,以期建立一具有認證及收費的 DRM 系統。後面將針對此系統架構之 DRM server 等架構逐一作說明。

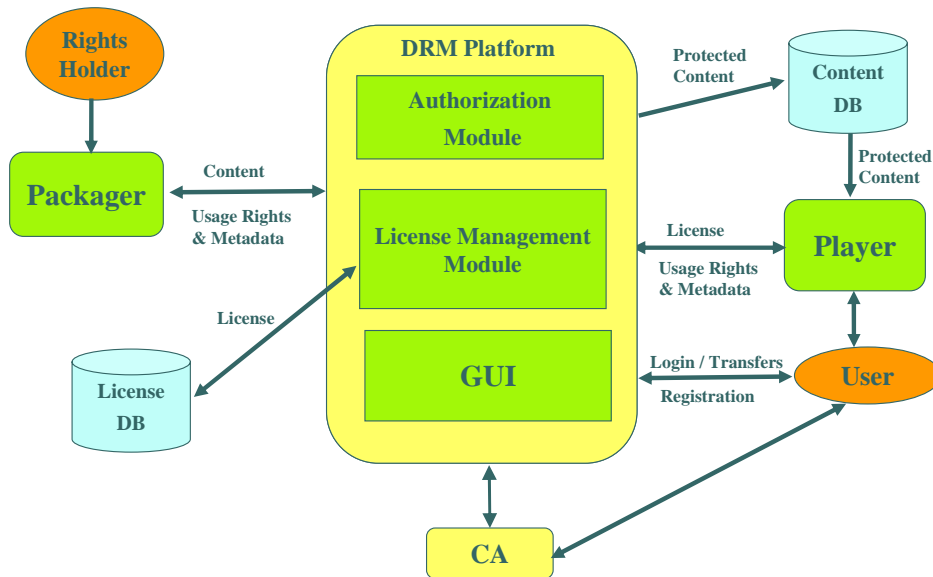


圖 4-2 本研究的 DRM 系統架構

4.2.1 Packager 架構

如下圖 4-3 所示，在 Packager 架構中，上傳模組（Upload Module）主要負責接收內容提供者上傳的數位內容，並利用網頁介面，讓內容提供者填寫數位內容的 metadata，並制訂零售出租者與消費者的權限條件。當內容提供者完成上述動作後，上傳模組先檢查所有的資料型態是否正確與合理，檢查完畢後利用使用許可證產生器（License Creator）產生 Rights 檔案，其他的 metadata 則儲存至對應的資料庫中，然後利用 License 管理模組產生的加密金鑰與內容包裝器（Content Encoder）對數位內容做保護，最後再將受保護的數位內容上傳到內容資料儲存器（Content Repository）。

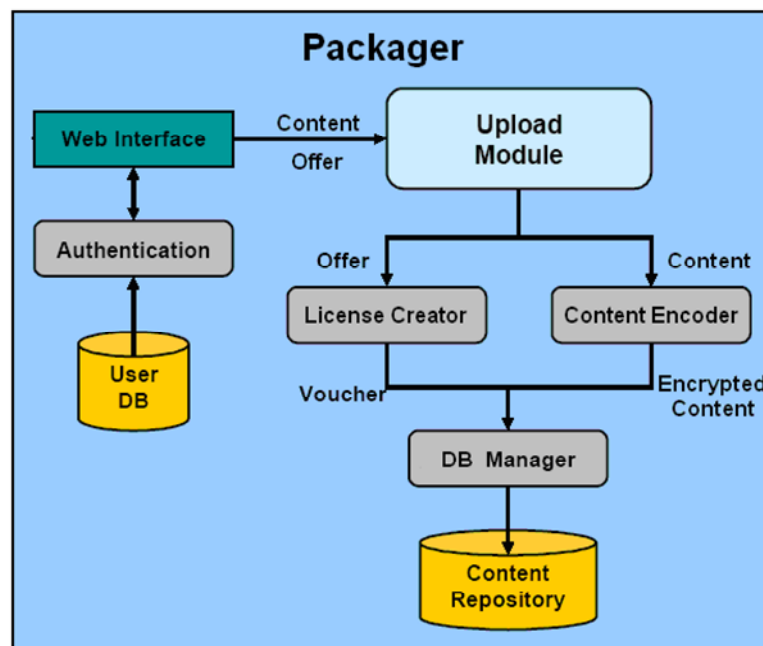


圖 4-3 本研究的 Packager 架構

4.2.2 DRM Server 架構

如下圖 4-4 所示，在 DRM Server 架構中，主要包含了使用許可證管理模組（License Management Module）與授權模組（Authorization Module）。以下將針對這些模組功能作一詳細說明：

- License 管理模組：

此模組主要負責加解密金鑰的產生與管理，其主功能有三：首先，當上傳模組需要保護數位內容檔案時，必須向本模組要求加密金鑰，本模組必須依加密演算法的特性產生對稱或非對稱的加解密金鑰，並將加密金鑰傳送給上傳模組作為保護數位內容之用。其次，當使用者利用授權模組取得授權時，授權模組會將授權資訊傳送給本模組管理，而使用者透過 License 要求模組要求 License 時，就必須檢查使用者的授權資訊決定是否給予適當的權限與控制條件。最後，當消費者要求數位內容的 License 時，用戶端媒體播放器中的 License 控制器會對本模組進行要求，而本模組必須檢查此消費者是否有權限使用該數位內容，若條件允許則可進一步轉而發放 License 給 License 控制器。

- 授權模組：

此模組主要負責提供被授權者授權協議及條件。當被授權者經過驗證登入系統，被授權者先行挑選欲取得之數位內容，再利用本模組取出所有已制訂之授權提議及條件，被授權者與系統以交互溝通方式產生授權協議，完成後系統產生一組授權編號用以識別授權，而被授權者取得之授權資訊與條件必須傳送給 License 管理模組，並利用使用許可證產生器（License Creator）產生出專屬於被授權者的 License 檔案，讓被授權者下載數位內容與 License 檔案。

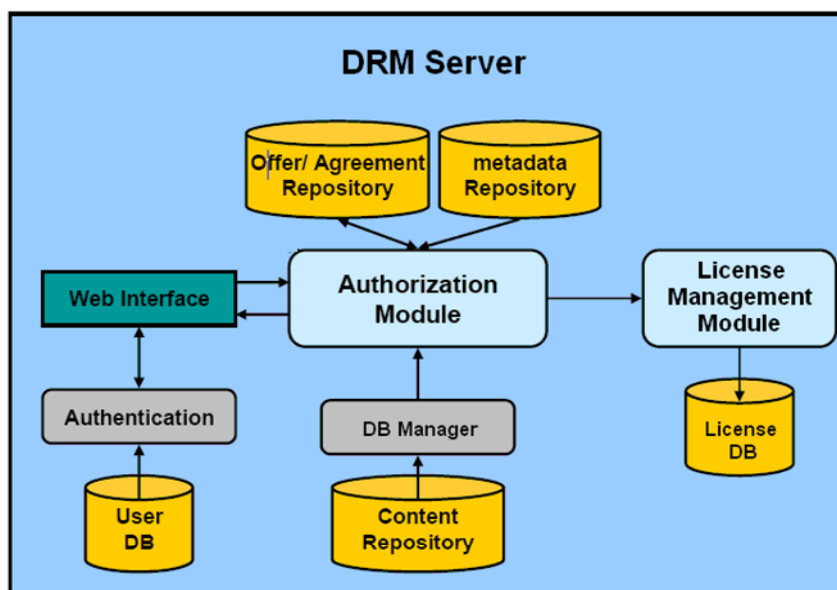


圖 4-4 本研究的 DRM Server 架構

4.2.3 DRM Client 架構

如下圖 4-5 所示，在 DRM Client 架構中，播放器(Player) 主要負責解密與分析數位內容裡封裝的資訊。當消費者要求 License 時，播放器會先從數位內容檔案中分析出 metadata 與檔案加密部分，此 metadata 中會存有 License 的要求方法，播放器再把這些資訊交由 License 控制器，而 License 控制器便可依據 License 的資訊，檢查客戶端是否有此 Rights 可以使用，若無 License 資訊與解密金鑰，則分析 metadata 中要求 License 的位址，進而向 DRM Server 的 License 管理模組取得 License，等待 DRM Server 的存取控制模組均允許後，並回傳數位內容的 License，License Controller 再從 License 中取出解密金鑰並交由播放器，進行檔案的解密與使用。

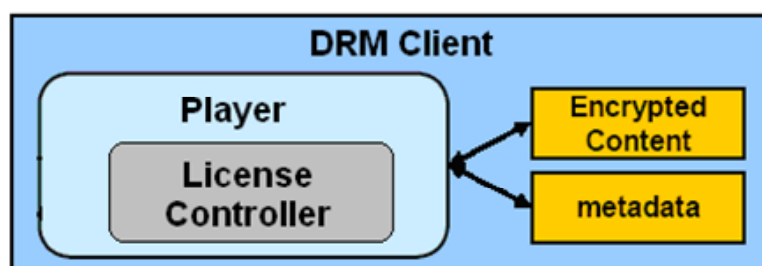


圖 4-5 本研究的 DRM Client 架構

4.2.4 Clearing House 架構

如下圖 4-6 所示，在 Clearing House 架構中，付款模組(Payment Module) 主要負責消費者付款的部份。收到消費者購買數位內容的付款指示產生 Receipt 後儲存至付款 Database 中，以及通知 DRM Server 產生 License。

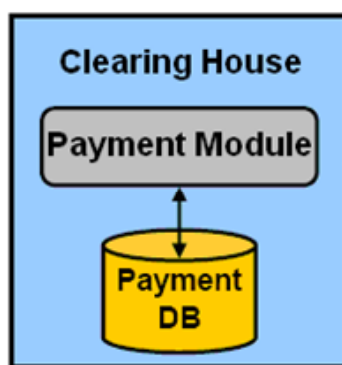


圖 4-6 本研究的 Clearing House 架構

4.3 系統機制

符合Transferable Rights機制的DRM系統，除了融入Rights的轉移方法外，還必須加入許多常用的DRM技術，諸如 SSL (Secure Socket Layer) 數位憑證、存

取控制與授權溝通等系統機制，以提升系統的價值與實用性，以下將說明這幾種系統機制如何應用在本系統架構與其功能中：

- **SSL數位憑證：**

在使用網路服務時，一般都會採用帳號密碼驗證使用者，而驗證過程前後所傳遞的資訊通常具有隱私性與機密性，若在不安全的網路環境下，傳輸資料可能會遭受網路攻擊者的監聽與竊取，因此為了保護使用者的權益與資訊的安全性，必須為網路連線建立安全通道。目前應用於網頁伺服器的網路連線保護方法最常見的是SSL。此協定是由NetScape公司提出的資料保密協定，它採用了RC4[16]、MD5[17]與RSA等加密演算法，主要目的在於保證網路資料傳輸的安全性、完整性與驗證性，其流程如圖4-7所示，伺服器端必須先取得憑證授權中心發給的非對稱演算法的憑證，當客戶端要求連線時，伺服器將公開金鑰的憑證傳送給客戶端，客戶端再利用此公開金鑰加密並回傳對稱加密演算法的金鑰，雙方有此對稱演算法之金鑰後，便可透過此對稱加密演算法保護之後要傳遞的訊息。

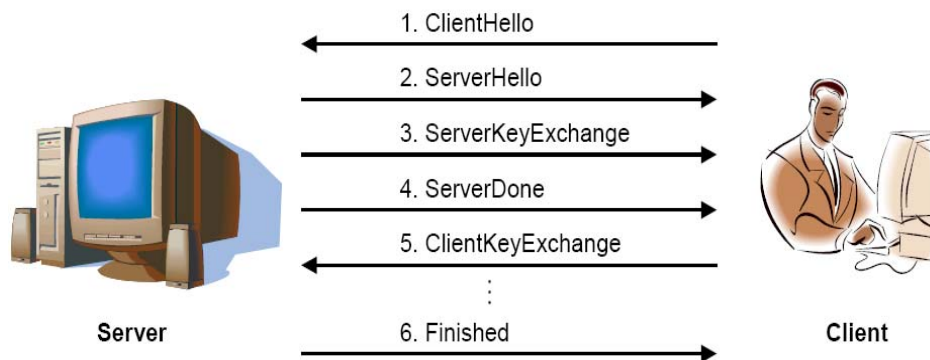


圖 4-7 SSL 數位憑證運作流程

- **存取控制機制：**

存取控制的主要目的在於控制使用者權限，最簡單的控制方法便是利用帳號密碼驗證使用者身份，並根據記錄在資料庫的使用資料給予使用者數位內容的使用權限，而一般存取控制技術除了上述方法外，還可將所有使用者分類至不同角色，當使用者通過系統的身份驗證後，系統主要以相對應的角色看待使用者，而使用者可取得的授權提議也因角色的不同而有所差異。在本系統的設計上，基本角色有內容提供者、零售出租者與消費者，因此系統必須有此三種角色供使用者存取。

- **授權溝通機制：**

在本系統架構，被授權者可選擇的提議中，所有權限條件的限制範圍可根據 Rights 轉移機制變化。例如：內容提供者提供最多一萬份的數位內容發行量，零售出租者可只要求一千份的零售出租權。之後再經由授權模組進行範圍的檢查與審核，確保不違背原先的 Usage Rights。

4.4 系統基本運作的流程設計

在規劃好系統的權限種類與商業模式後，以下將依數位內容發行模式中遭遇的角色說明整個系統基本流程如何運作：

- 內容提供者上傳數位內容至DRM系統流程：

在我們設計的DRM系統中，內容提供者經過DRM系統驗證後便可將數位內容檔案上傳，其流程如圖4-8所示，過程如下：

- (1) 上傳檔案並制訂metadata：內容提供者上傳數位內容檔案後，透過網頁表格填寫檔案描述與授權提議，而提議上必須確定零售出租者與消費者的數位權利，並規範可發行次數、Rights期限與利益分配比率。
- (2) 數位內容檔案保護處理：系統利用內容包裝器保護上傳之數位內容檔案，產生出的解密資訊則交由DRM伺服器的License管理模組儲存至資料庫上。
- (3) 產生License檔案：系統利用License產生器與內容提供者輸入的Rights資訊產生License檔案。
- (4) 檔案管理：系統將已保護的數位內容檔案與License檔案交由檔案管理器儲存至內容資料儲存器（Content Repository），並新增一筆上傳記錄。

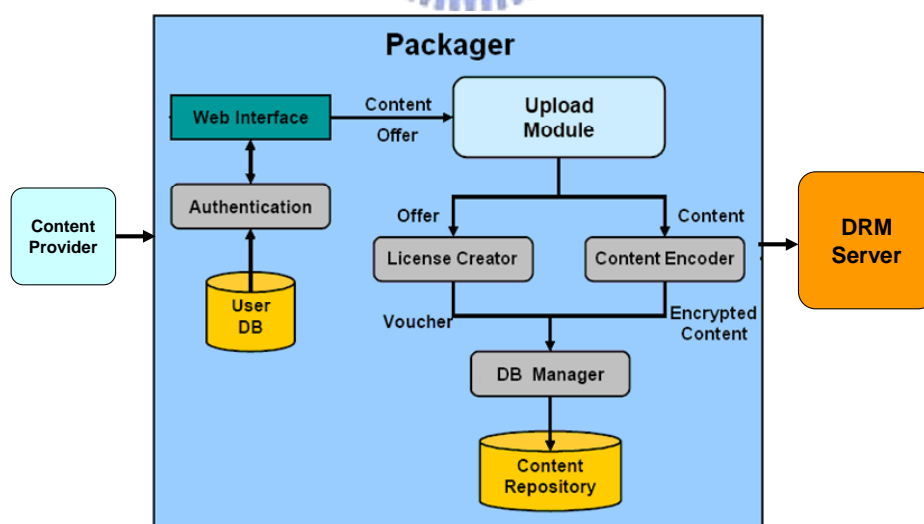


圖 4-8 內容提供者上傳數位內容至 DRM 系統流程

- 消費者至DRM系統購買數位內容流程：

消費者經過 DRM 系統驗證後，便可進行訂購程序，過程如圖 4-9 所示，說明如下：

- (1) 消費者選擇數位內容：授權模組從提議/協議資料儲存器與 metadata 儲存器取出所有可發行的數位內容與 Rights 資訊，以網頁方式供消費者選擇。
- (2) 消費者取得授權協議：消費者確定欲取得的數位內容後，DRM 系統將數位內容的 Rights 資訊以網頁方式呈現，除了基本的 Rights 與權限條件外，系統會根據設定提供零售與出租二種 Rights 的授權方式，前者可讓每一位消費者可購買一份數位內容，而出租授權方面，消費者可選擇以使用次數或期間訂購。
- (3) 消費者付費：所有的購買資訊呈現給消費者後，只有以出租方式取得之授權，必須馬上根據發行期間計算權利金轉帳給零售出租者，付費模組檢查消費者回傳的交易序號並將其與 License 編號存放至 Payment DB 中；而在檔案下載方面，由於消費者使用的 Rights 資訊由 DRM 伺服器發行，因此消費者不需取得 License 檔案。

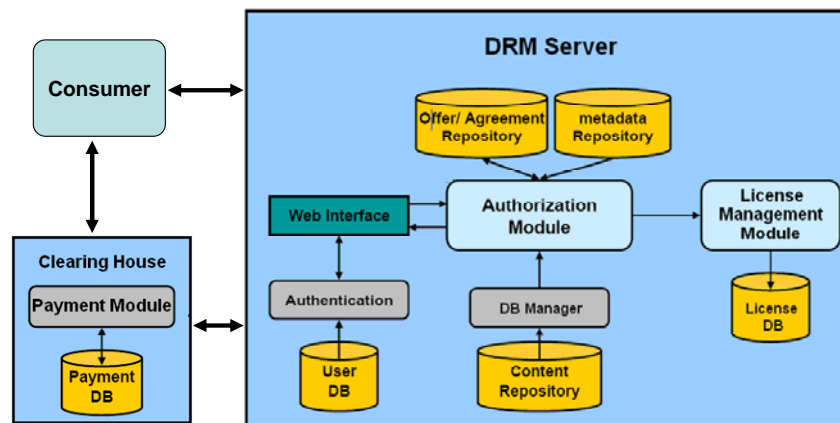


圖 4-9 消費者至 DRM 系統購買數位內容流程

● 消費者轉售數位內容的流程：

消費者經過DRM系統驗證後，便可進行轉售數位內容的程序，過程如圖4-10所示，說明如下：

- (1) 消費者A連線到DRM系統的網頁介面，並且通過身分驗證。消費者A登入DRM系統除了將License傳送給DRM系統驗證之外，也把轉讓數位內容的價格一起傳送給 DRM系統。當DRM系統收到License時，會先比對資料庫中消費者的相關資訊以及License 是否一致。在DRM系統驗證License無誤後，DRM系統會以網頁方式公告消費者A要移轉的數位內容、剩餘的播放次數(或期限)以及轉售價格等訊息。
- (2) 消費者B如欲購買消費者A的數位內容時，消費者B須傳送Transfer Request給DRM系統。在DRM系統收到消費者B的Transfer Request後，須將消費者A的License資訊和付費方式回傳給消費者B。
- (3) 當消費者B透過DRM系統付款給消費者A後，DRM系統會將網路銀行核發的付款證明回傳給消費者A及B，同時系統開始進行數位內容的Rights移轉。

- (4) 在數位內容的Rights移轉成功後，DRM系統會核發新的License以及未來用來取得數位內容的解密金鑰給消費者B。
- (5) 最後，DRM系統會傳送數位內容移轉成功訊息給消費者A，並且註銷消費者A的License。同時DRM系統將移 除公告在網頁上有關消費者A轉售數位內容的訊息。

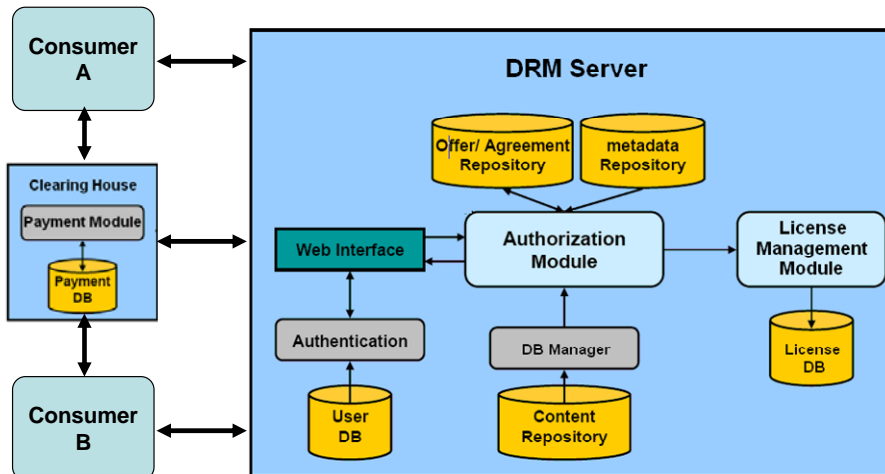


圖4-10 消費者轉售數位內容的流程

● 消費者取得數位內容License的流程：

取得數位內容的消費者，利用客戶端的播放器開啟數位內容檔案，播放器分析檔案中記錄之License資訊，向License控制器要求播放權利，流程如圖4-11所示，以下為求取License之過程說明：

- (1) DRM系統的存取控制檢查：消費者透過License Controller向License管理模組要求License，而License管理模組會根據消費者身份與License Controller上傳之數位內容的metadata，確認與消費者是否有此交易並檢查權限是否符合，若檢查通過的話，則根據客戶端的metadata中的數位內容編號製作出解密金鑰，並包裝成License後回傳給消費者。
- (2) 數位內容使用：客戶端播放器中的License Controller取得License後，取出解密金鑰後交由播放器解密播放。

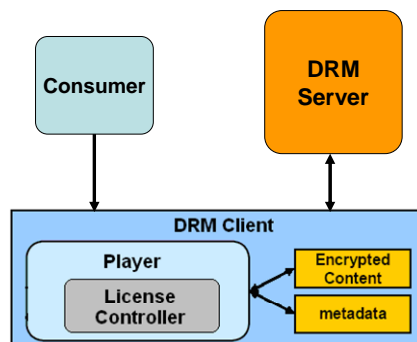


圖 4-11 消費者取得數位內容的 License 流程

五、系統實作

在這個章節中，我們將經由一些Open-source的移植與修改，加上Transferable Rights機制的導入，並透過使用者介面的整合來實現一具有Transferable Rights的DRM系統，作為驗證本論文所提出的研究架構及理論之可行性。

5.1 系統發展的背景環境

從1990年至今，DRM系統的研發已有許多的成果，尤其是提供保護文件或多媒體相關產品的DRM系統。所以目前有不少的DRM系統有發展套件供研究單位下載進行其他方面的開發與應用，例如：IBM的EMMS與微軟的RMS均提供套件供研究發展單位申請下載，但EMMS套件只供應客戶端的發展套件，無法發展伺服器端的DRM系統，顯然不符合我們的需要。另外，微軟的RMS也只注重於企業內部文件的保護，對於多媒體的數位內容的保護支援較少，而且與我們提出的系統架構差異較大，所以也不符合我們的要求。

而Open-source的OpenIPMP是一個可以提供典型Client-Server架構的DRM開發平臺Solution，因其具有基本的數位內容保護機制以及DRM機制，而且所有程式碼都可免費下載取得，加上系統並未實作任何的商業模式，可讓研究開發單位自由規劃，正符合本論文自行設計整體架構與流程的要求。還有OpenIPMP是以JSP及JAVA程式語言開發設計的，因此其具有能跨平台執行，良好的可攜性及擴充性等優點，而且JAVA有關網路部份的API相當完整且容易使用，這些都可以縮短我們的開發時間。所以本論文的DRM平臺採用Open-source的OpenIPMP作為我們的DRM開發平臺的基礎，並藉此基礎發展其餘功能模組及相關介面，以期完成上述所提具有Rights轉移的DRM平臺。而在數位內容封裝及播放等功能實現方面，我們採用Open-source中的MPEG4IP專案[18]來實現數位內容封裝及播放的大部份功能。MPEG4IP為Cisco使用C++所開發的一套多媒體播放及串流的應用程式，它可以解碼並播放MPEG4壓縮的影音檔案。

另外，本系統使用對JSP (Java Servlet Page) [19]程式語言最佳化的Apache Server所提供的功能來建構網頁伺服器，所有連往網頁伺服器的連線則以SSL做保護，並搭配MySQL[20]及一些相關的函式庫作為資料庫來儲存相關資訊及資料，而有關檔案保護與數位版權存取控制以及播放控制等程式，均以VC++ 6.0撰寫或修改。此外，本系統也使用ODRL及MPEG-21 REL作為傳遞Rights資訊及設定的REL。最後再利用JSP網頁程式將各個模組結合起來形成一具有Transferable Rights的DRM系統。

5.2 實作方法

對於實現前面所提的系統架構，我們可以參考如圖 5-1 所示，只要對 OpenPMP 與 MPEG4IP 進行部分修改以及開發使用者介面作整合的工作，再加上一些 Transferable Rights 機制所需的模組，這樣就可以實現一個具有 Transferable Rights 的 DRM 系統。後面將說明重要的修改及需要之功能模組的實現方法。

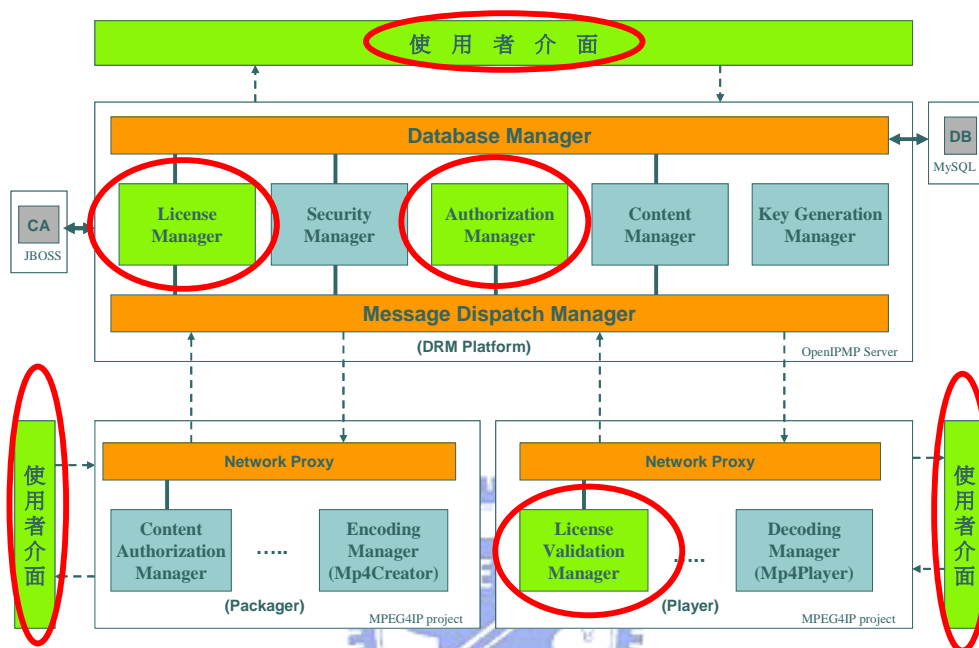


圖 5-1 本研究之 DRM 系統實現方式

在系統實作上，我們只專注於 Transferable Rights 的實現，並未規劃實際之付費機制及實作相關模組。但在實際的商業應用上，DRM 系統應有付費機制要求使用者付費。因此本系統如果加上一個簡單的網路銀行，而其具備註冊、轉帳與查詢功能，讓每一位註冊的使用者會有一組銀行行號與帳號資訊，且使用者可以轉帳至同一銀行下的其他帳戶，而轉帳資訊也可透過查詢功能得知。在新增網路銀行功能與付費機制後，本系統就能以各種商業模式發行數位內容，再加上各個角色之間也有利益之分配機制，就更可以顯現出各種角色在商業模式上的應用及改變，也更可驗證 DRM 系統之彈性與合理性。

至於 DRM Platform 的建立與實現中，其中最重要的工作即為授權管理 (Authorization Manager) 模組功能的建立。如圖 5-2 所示的 Transferring Rights Flowchart，即為授權管理模組的主要決策流程。本流程主要在處理，根據 License 的 Transferable Rights 的 REL 元素來進行相對應的權限轉移。

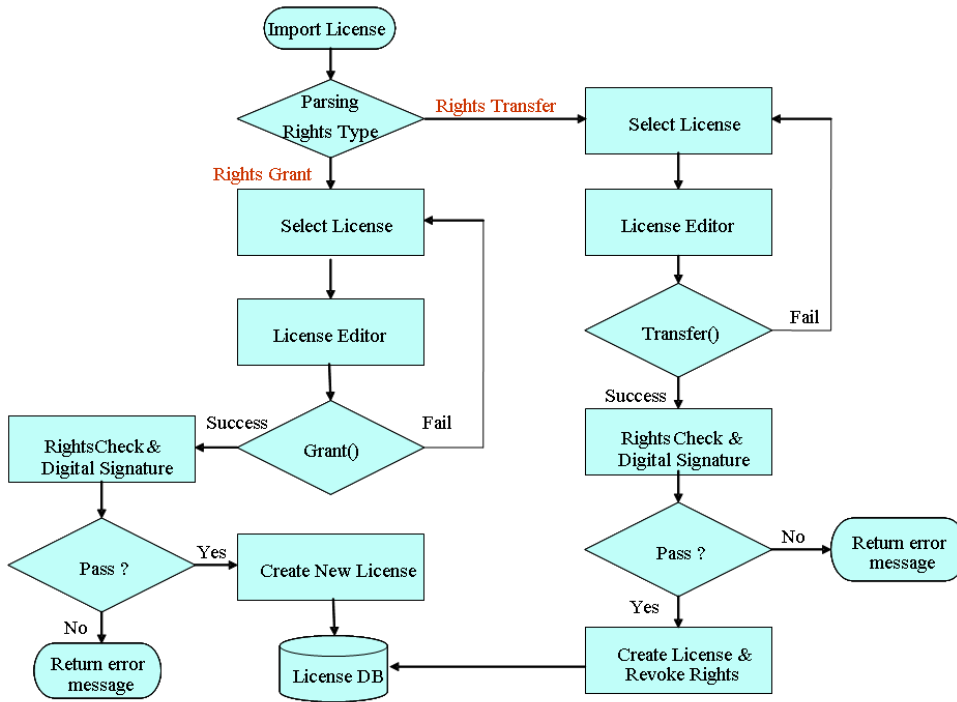


圖 5-2 Transferring Rights Flowchart for Authorization Module

在 Transfer Rights 的過程中，常常會需要產生各種權限的 License 來滿足我們的需求。因此我們實現了一個名為使用許可證產生器(License Creator)的功能模組，而其實現方式及運作過程，請參考圖 5-3 所示。我們可透過網頁表單的方式，輸入授權相關資訊，在經過 Java Servlet 的處理及運作之後，我們就可以產生出具有 XML-Base 的 License，最後再儲存到資料庫裡。

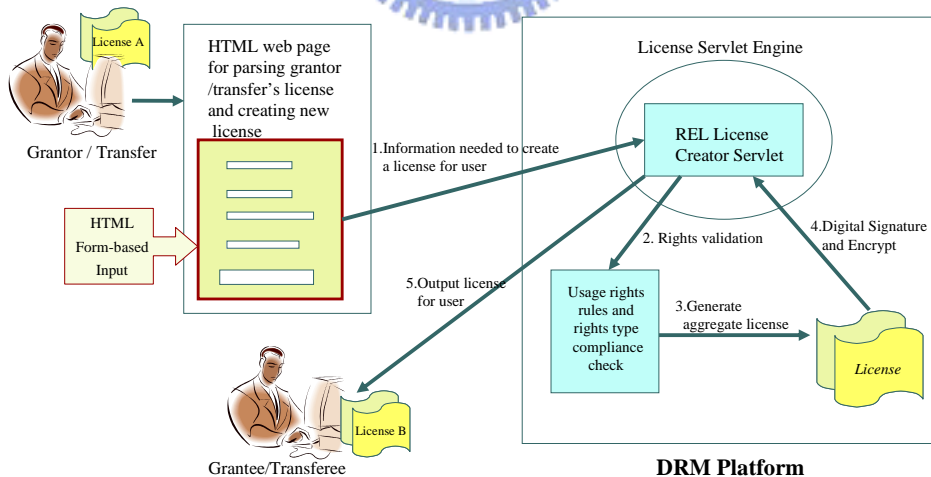


圖 5-3 XML-based License Generating Procedure for Transferable Rights

接著我們說明一下License的Usage Rights解譯和驗證作法，如圖5-4所示。其運作流程說明如下：

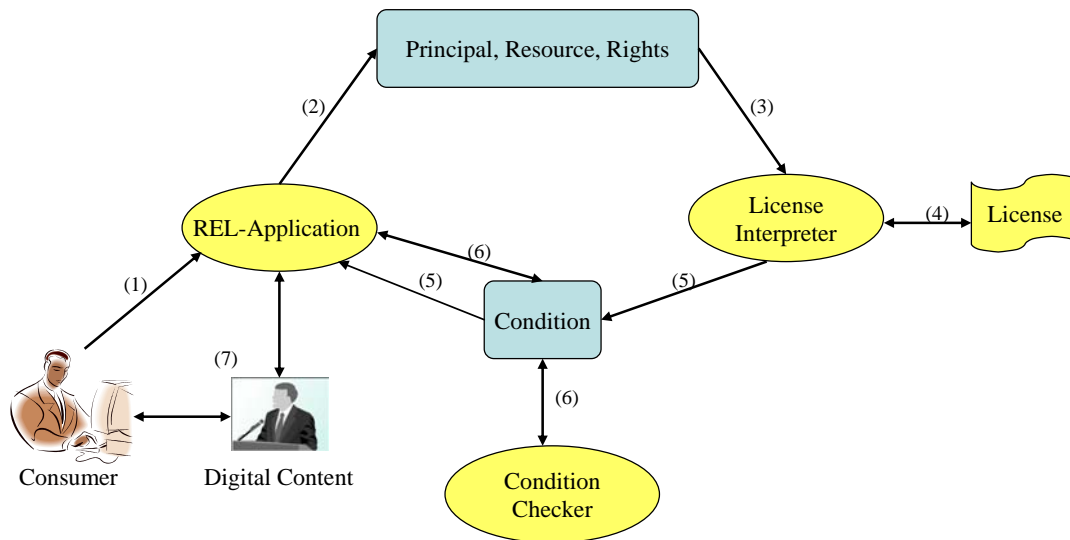


圖5-4 License的Usage Rights解譯和驗證作法

- (1) 消費者要求播放一個受保護的數位內容。
- (2) 收到消費者的播放請求後，播放控制程式(REL-Application)開始收集消費者以及數位內容等相關資訊。
- (3) 對License Interpreter發出請求。
- (4) License Interpreter獲取相對應的License並驗證其有效性，確認該License未被篡改，然後解譯License，檢查是否包含播放許可權，並驗證該許可權是否確實為當前消費者所擁有。
- (5) 如果檢驗通過，則返回相對應的限制條件和前提條件給播放控制程式。
- (6) 播放控制程式要求系統的條件檢查器(Condition Checker)驗證是否滿足相關條件，例如播放次數是否在許可範圍內。
- (7) 如果驗證無誤，消費者可以播放該數位內容。

而播放器是使用者觀看數位內容的工具，同時也是 DRM 系統達成數位內容保護的關鍵所在。因此我們必須在播放器裡實現一個具有許可版權控管的功能模組，來決定是否播放數位內容。所以我們實現了一個名為使用許可證驗證管理(License Validation Manager)的功能模組，而其主要運作流程，請參考圖 5-5 所示。當播放器收到加密的 License 時，播放器的使用許可證驗證管理模組會將加密的 License 利用私鑰進行解密，解密完後接著分析驗證 License 中的數位簽章、Rights 權限條件等資訊是否符合播放許可，若是則從 License 中取出可以為受保護的數位內容解密的 RSA 公鑰。

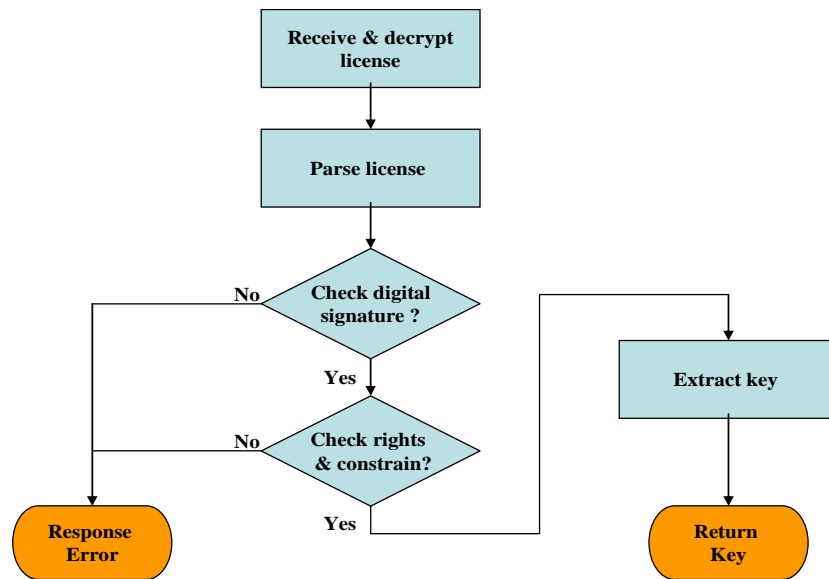


圖 5-5 Player Functioning Flowchart

5.3 使用情境與系統實作展示

針對我們實現的 DRM 系統，我們可用註冊、發行、轉移及播放等四階段來作一使用情境的介紹與系統功能展示，說明如下：

- 註冊階段

- (1) 如下圖 5-6 所示，使用者可透過 DRM 管理平臺註冊，輸入使用者資訊，包括 name、password、Email 位址等等資料。
- (2) DRM 管理平臺將使用者註冊資訊增加到 DRM 平臺資料庫中。
- (3) DRM 管理平臺將使用者資訊註冊到 CA 伺服器資料庫中，同時 CA 伺服器產生一個 X.509 簽名證書。
- (4) CA 伺服器將使用者名字、密碼以及 RSA 公鑰生成的 X.509 簽名證書返回給 DRM 管理平臺。
- (5) DRM 管理平臺將 RSA 密鑰對、簽名證書以及由用戶名稱、RSA 私鑰和簽名證書構成的 PKCS12 格式的憑證返回給使用者，此時使用者可將 PKCS12 憑證儲存起來。

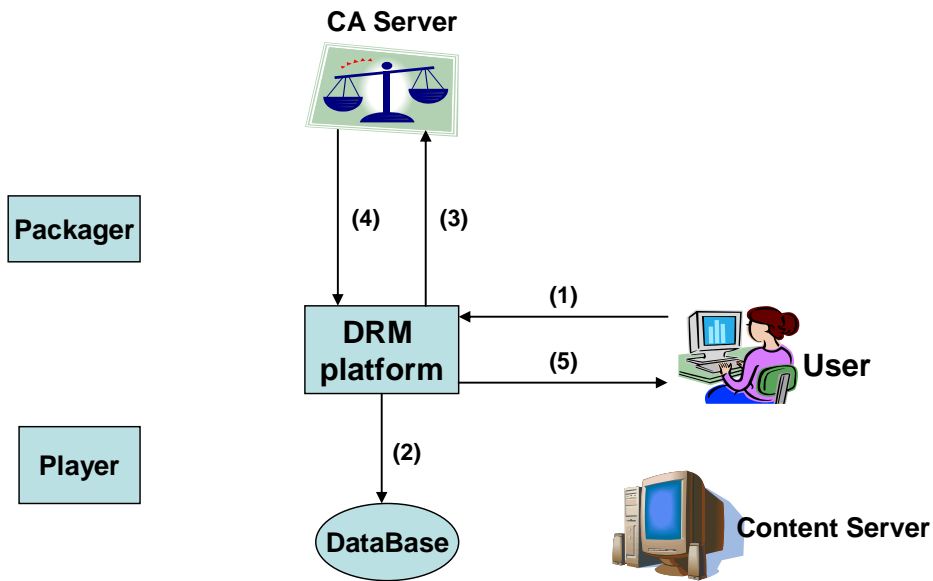


圖 5-6 註冊階段流程圖

● 註冊階段功能畫面展示如下：

- (1) 在連線到我們實現的 DRM 管理平臺時，會出現如圖 5-7 所示之使用者登入畫面。

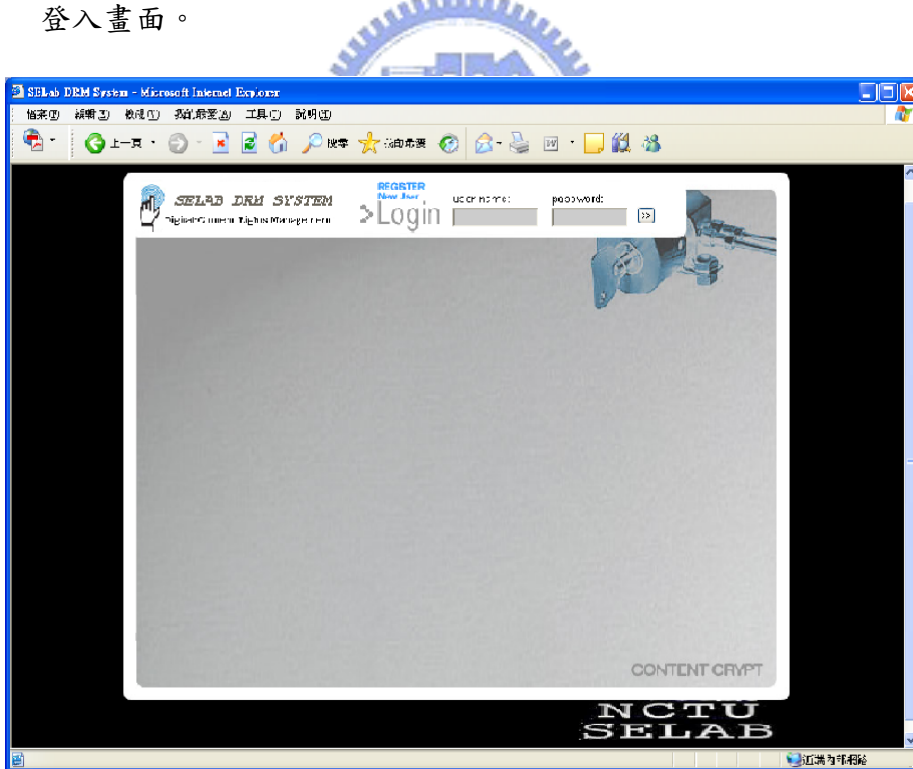


圖 5-7 使用者登入畫面

- (2) 使用者如需註冊時，須點選如圖 5-8 所示之「REGISTER New User」所在區域。



圖 5-8 新使用者的註冊畫面

- (3) 進入如圖 5-9 所示之使用者註冊畫面，輸入使用者資訊，包括 name、password、Email 位址等等資料，最後再按下「Submit」按鈕送出表單。



圖 5-9 使用者註冊畫面

- (4) 註冊成功後，會自動登入系統且看到如圖 5-10 所示之使用者 PKCS12 格式的憑證儲存詢問畫面。

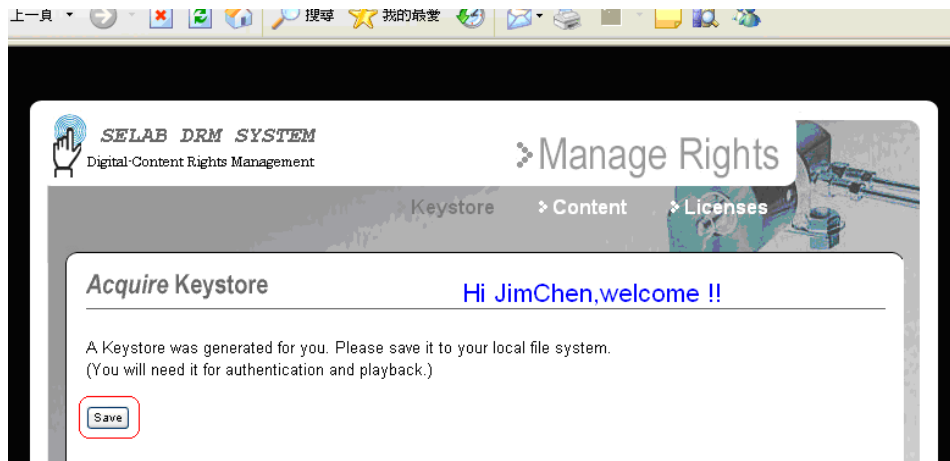


圖 5-10 使用者憑證儲存詢問畫面

- (5) 在按下上圖之「Save」按鈕後，會出現如圖 5-11 所示之畫面，這時可下載個人的 PKCS12 憑證並儲存起來，作為日後登錄系統或播放器使用。

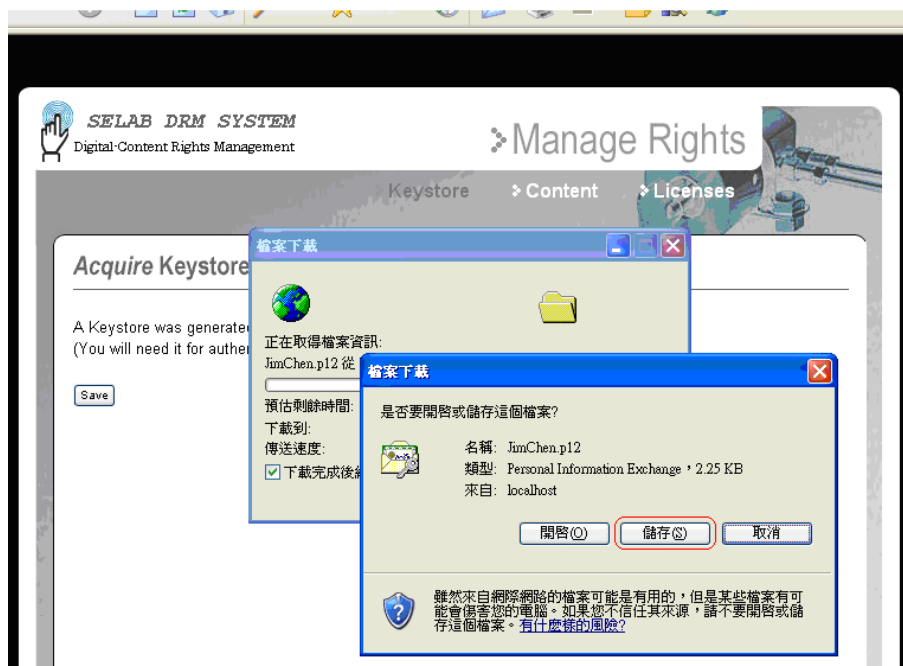


圖 5-11 使用者憑證儲存畫面

● 發行階段

- (1) 如下圖 5-12 所示，使用者可使用 Packager，輸入自己的憑證名稱以及欲授權的資料和數位內容等資訊做為登入及授權之用。
- (2) 使用者使用 Packager 提供的非對稱加密演算法對數位內容進行加密處理，得到 MP4 格式的保護檔後，再放到內容伺服器。
- (3) 同時 Packager 會自動發送登入 DRM 管理平臺的請求。
- (4) DRM 管理平臺將使用者的 PKCS12 憑證送到 CA 伺服器做驗證。
- (5) CA 伺服器返回驗證結果給 DRM 管理平臺。如果認證通過，管理平臺

開始處理用戶的 License 請求，如果認證沒有通過，則繼續提示用戶名和密碼。

- (6) DRM 管理平臺會將 Packager 送交的資訊，如內容註冊資訊、數位內容授權協定及保護檔加密的密鑰等資訊添加到資料庫中，以便之後發放 License 時使用。

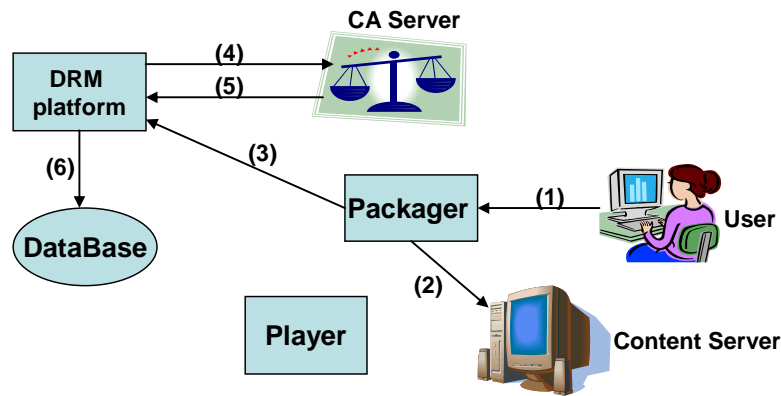


圖 5-12 發行階段流程圖

- 發行階段功能畫面展示如下：

- (1) 當使用者執行 DRM_UI.exe 時，會出現如圖 5-13 所示之 Demo DRM UI 登入畫面。此時使用者須要輸入憑證名稱、密碼以及 DRM 管理平臺的位址等等資料作為登入 DRM 系統之用。

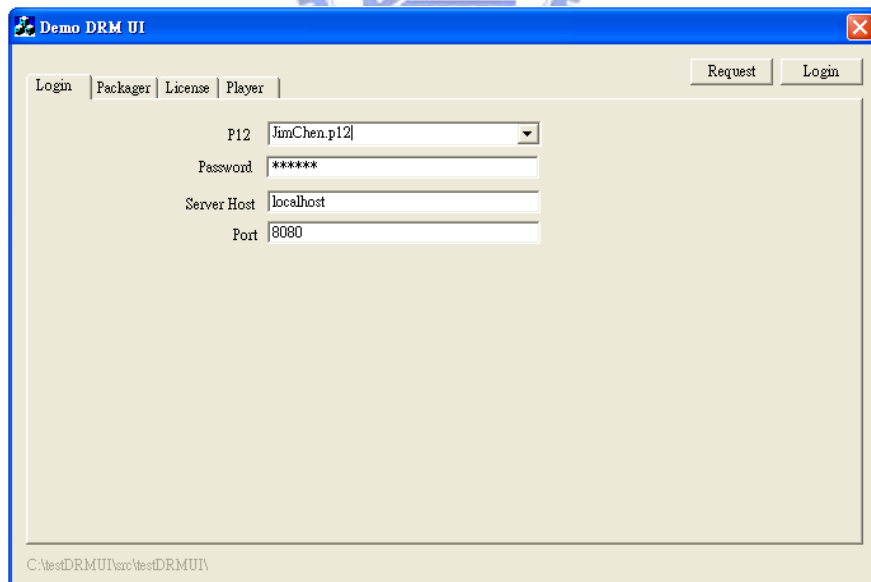


圖 5-13 Demo DRM UI 登入畫面

- (2) 如下圖 5-14 所示，使用者可使用 Packager 選項，輸入欲授權的數位內容和 Rights 權限等資料作為發行之用。在按下圖中之「Package」按鈕後，會產生一加密之數位內容，同時也完成內容授權註冊相關資訊到 DRM 管理平臺的動作。

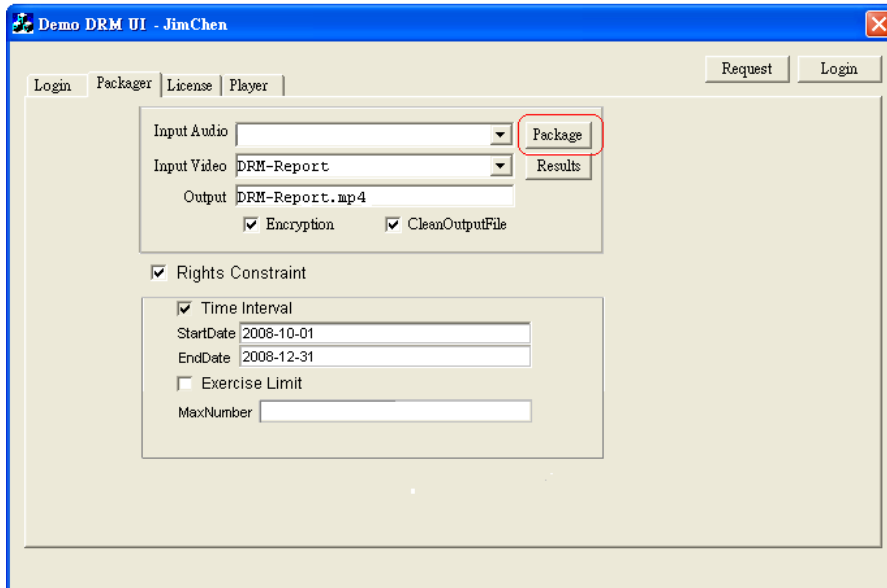


圖 5-14 Packager 之 UI 畫面

- (3) 如下圖 5-15 所示，使用者在按下「Login」按鈕後，可以登入 DRM 管理平臺的網頁。

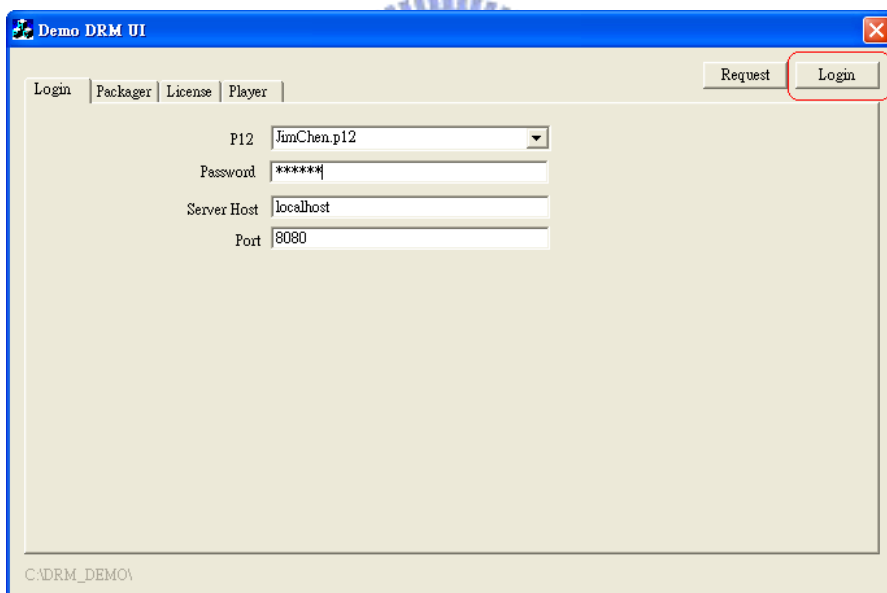


圖 5-15 Packager 之登入 DRM 管理平臺畫面

- (4) 如下圖 5-16 及 5-17 所示，使用者可以從 DRM 管理平臺的 License 清單以及授權清單畫面，發現已完成的内容授權註冊及 License 清單等相關資訊。

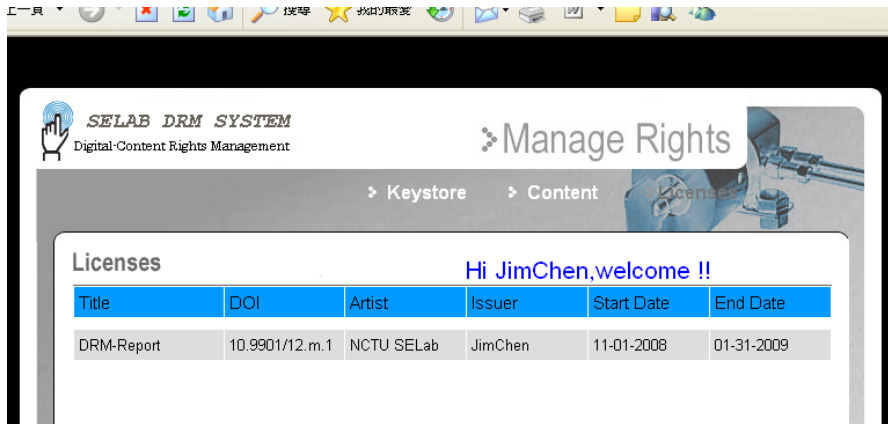


圖 5-16 DRM 管理平臺的 License 清單畫面

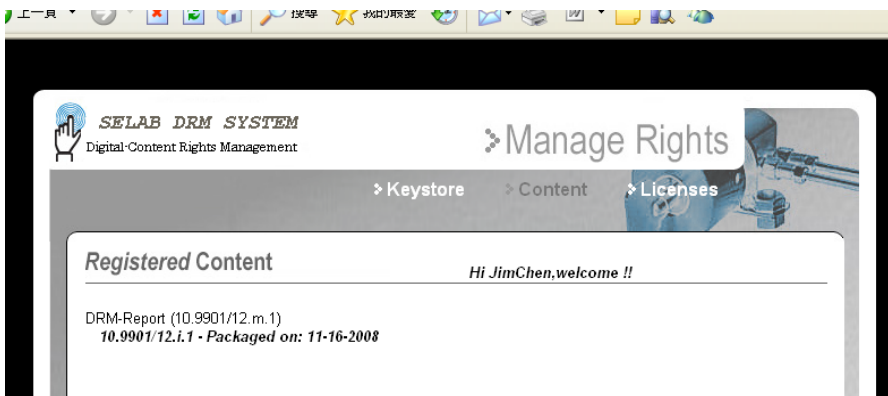


圖 5-17 DRM 管理平臺之授權清單畫面

● 轉移階段

- (1) 如下圖 5-18 所示，為了將 Rights 轉移給使用者 B，使用者 A 進行登入 DRM 管理平臺的請求。
- (2) DRM 管理平臺將使用者 A 的 PKCS12 憑證送到 CA 伺服器做驗證。
- (3) CA 伺服器返回驗證結果給 DRM 管理平臺。如果認證通過，DRM 管理平臺開始處理用戶的 Rights 轉移請求，如果認證沒有通過，則繼續提示用戶名稱和密碼。
- (4) DRM 管理平臺會將 Rights 轉移的相關資訊，如授權者、被授權者、使用權利及限制、數位內容相關資訊以及保護檔加密的密鑰等等資訊添加到資料庫中，以便 License 發放使用。
- (5) DRM 管理平臺返回 Rights 轉移結果給使用者 A。
- (6) 使用者 B 為了觀看受保護的數位內容，向 DRM 管理平臺要求 License。
- (7) DRM 管理平臺發放新的 License 給使用者 B。

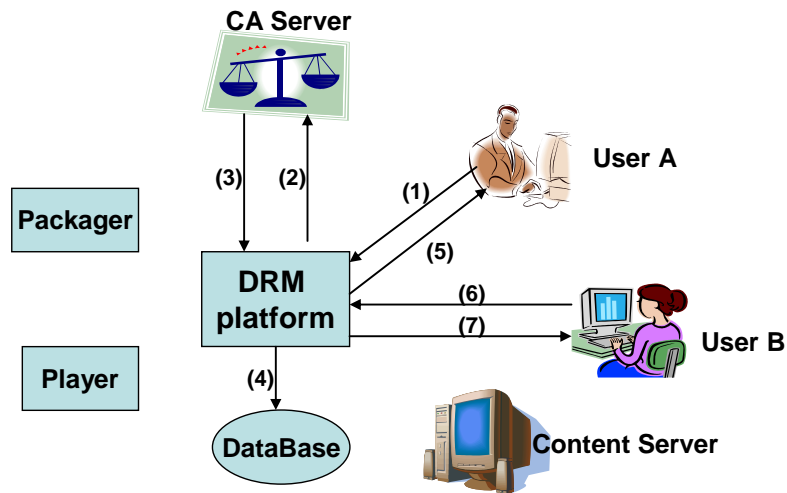


圖 5-18 轉移階段流程圖

- 轉移階段功能畫面展示如下：

(1) 為了作 Rights 轉移給使用者 B，使用者 A 須要登入 DRM 管理平臺。如下圖 5-19 所示，使用者 A 須要輸入自己的憑證名稱及密碼。

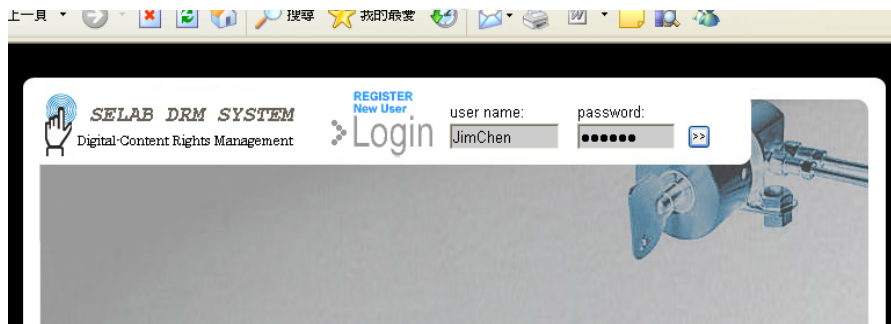


圖 5-19 使用者登入畫面

(2) 如下圖 5-20 所示，使用者 A 進入 DRM 管理平臺後，可以看到自己的 Rights 轉移前之被授權者清單畫面。

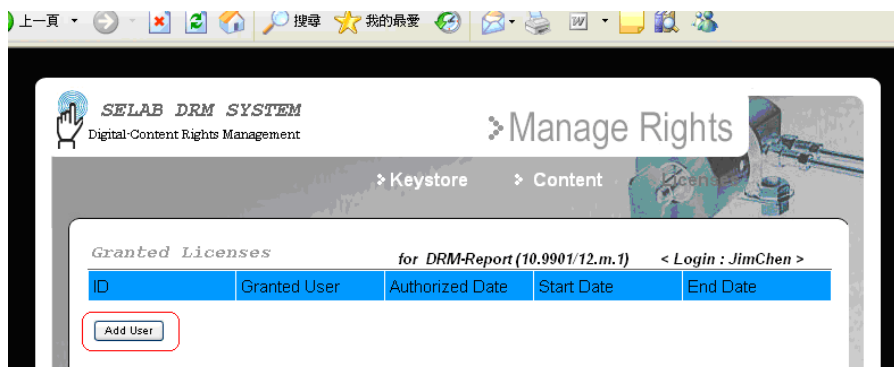


圖 5-20 Rights 轉移前之被授權者 License 清單畫面

(3) 在上圖中，當使用者 A 按下「Add User」按鈕後，會出現如下圖 5-21 所示之 Rights 轉移產生畫面。輸入 Rights 轉移的相關資訊，如接受 Rights

轉移者、Rights 限制以及數位內容名稱等資訊，最後按下「Grant」按鈕送出表單。

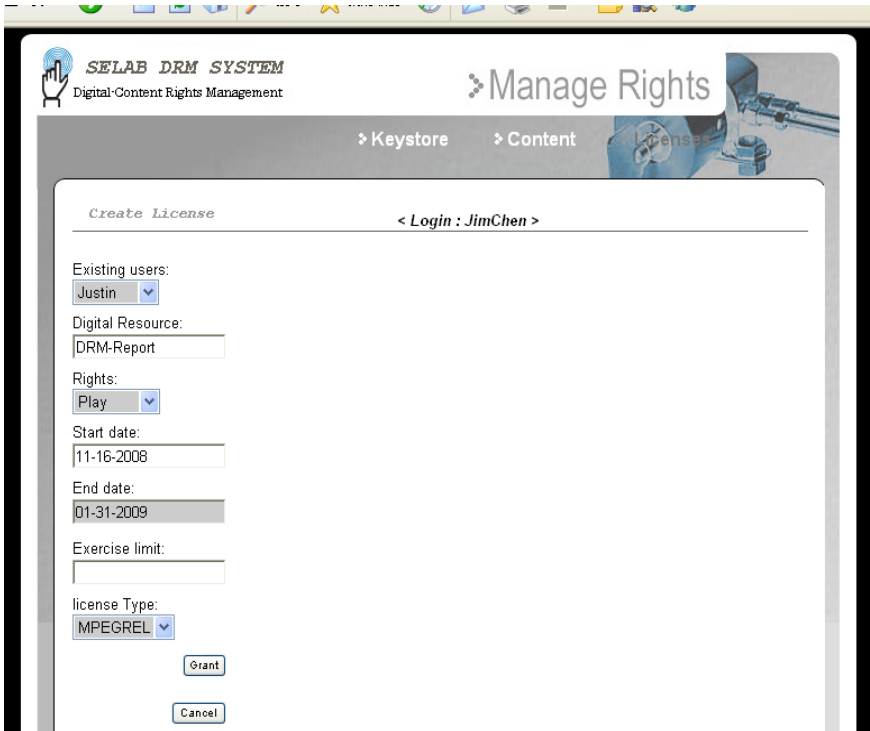
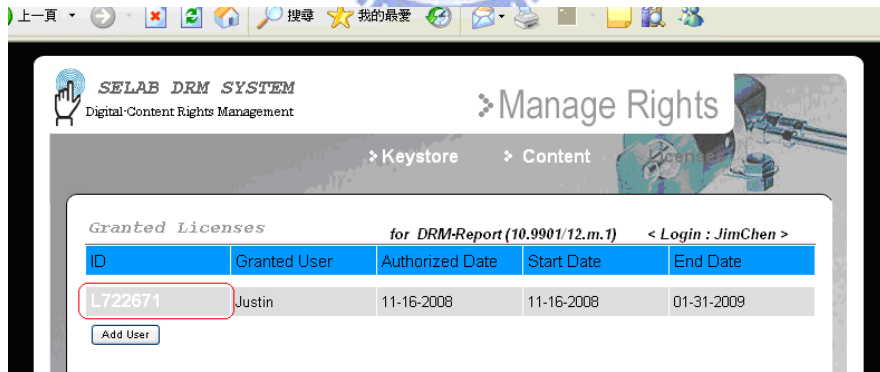


圖 5-21 Rights 轉移產生之畫面

- (4) 如下圖 5-22 所示，使用者 A 在送出表單後，可以看到自己的 Rights 轉移後之被授權者 License 清單畫面。



ID	Granted User	Authorized Date	Start Date	End Date
L722671	Justin	11-16-2008	11-16-2008	01-31-2009

圖 5-22 Rights 轉移後之被授權者 License 清單畫面

- (5) 在上圖中，當使用者 A 按下 License ID 後，會出現如下圖 5-23 所示之被授權者 XML-Base 的 License 內容畫面。

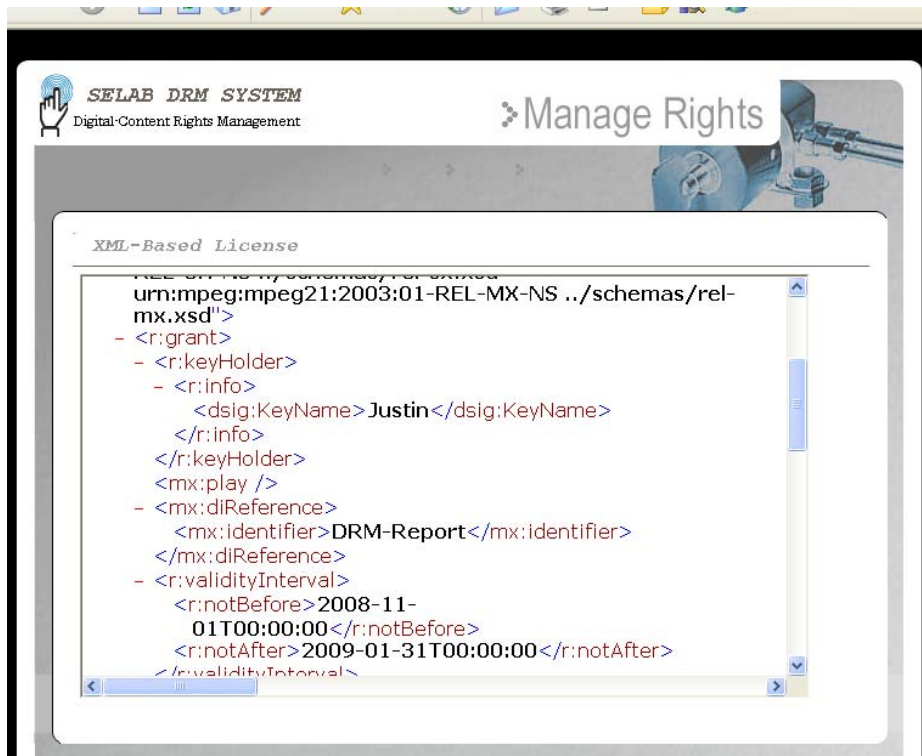


圖 5-23 被授權者的 XML-Base 之 License 內容畫面

- (6) 如下圖 5-24 所示，在使用者 A 的 Rights 轉移之後，使用者 B 登入 DRM 管理平臺，可以發現使用者 A 轉移給自己的 Rights。

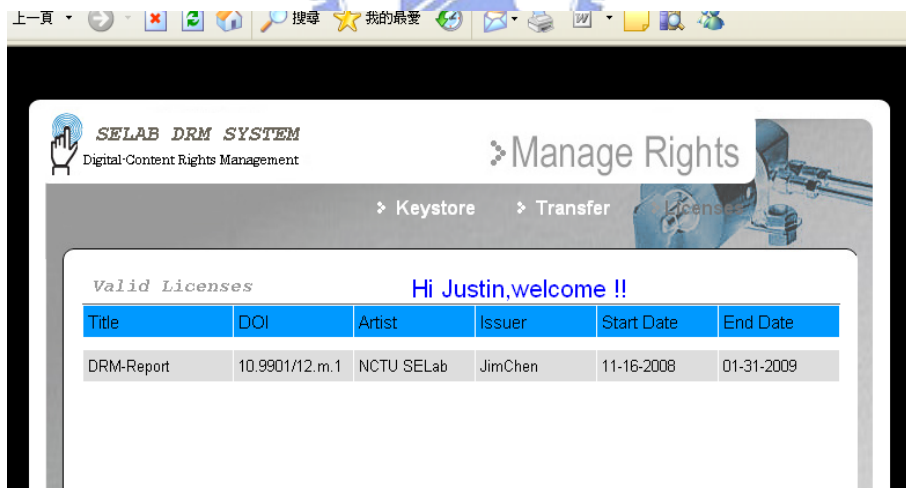


圖 5-24 被授權者的 License 清單畫面

● 播放階段

- (1) 如下圖 5-25 所示，用戶可先從內容伺服器下載受保護的數位內容。
- (2) 使用我們提供的播放器輸入憑證名稱及密碼後，再選擇想要播放的數位內容。
- (3) 接著播放器會發送登入 DRM 管理平臺的請求。
- (4) DRM 管理平臺將使用者的 PKCS12 憑證送到 CA 伺服器做驗證。
- (5) CA 伺服器返回驗證結果給 DRM 管理平臺。如果認證通過，管理平臺

開始處理用戶的 License 請求，如果認證沒有通過，則繼續提示用戶名和密碼。

- (6) DRM 管理平臺根據用戶的憑證名稱和要播放的內容資訊在資料庫中搜索此內容對此用戶的授權協定，如果有授權協定，並且授權合法，則驗證用戶的使用權利及條件是否有效，如果有效則發放加密過的 License 給播放器。當播放器收到加密的 License 時，播放器會將加密的 License 利用 PKCS12 憑證中的私鑰進行解密，再檢查 License 中的授權相關資訊，決定是否允許播放。同時也將收到的 License 存到用戶的 PKCS12 憑證中。
- (7) 用戶開始使用受保護的數位內容。

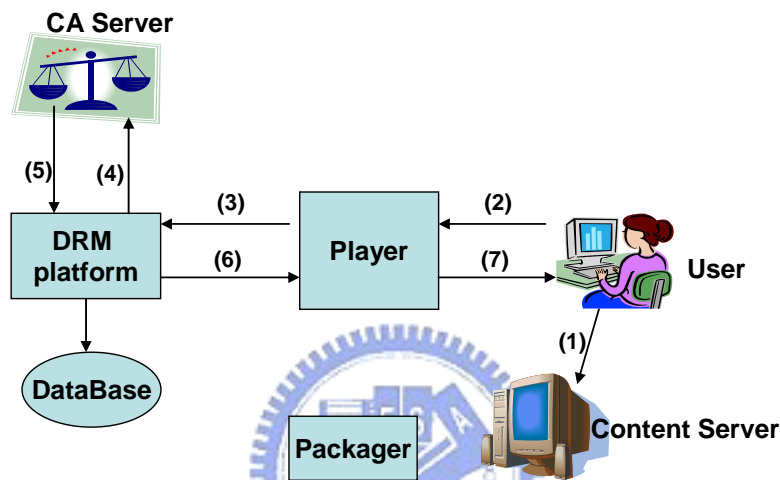


圖 5-25 播放階段流程圖

- 播放階段功能畫面展示如下：

- (1) 當使用者執行 DRM_UI.exe 時，會出現如圖 5-26 所示之 Demo DRM UI 登入畫面。此時使用者須要輸入自己的憑證名稱、密碼以及 DRM 管理平臺的位址等等資料作為登入 DRM 系統之用。

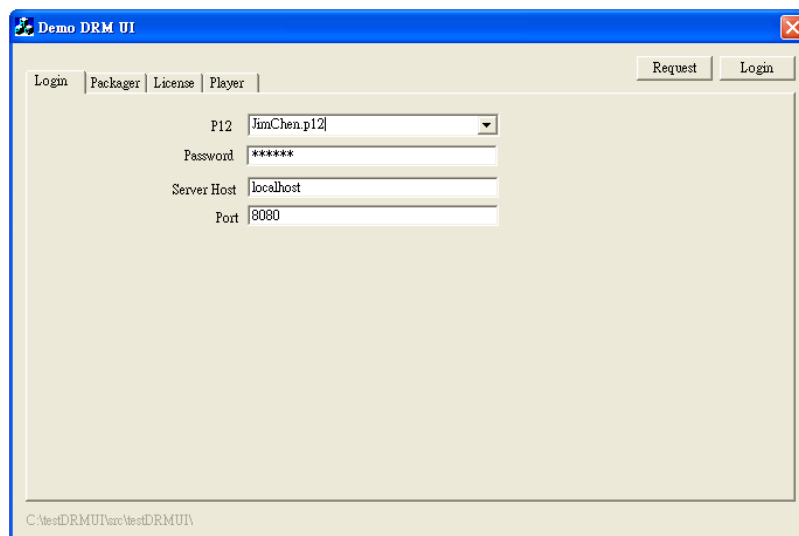


圖 5-26 Demo DRM UI 登入畫面

- (2) 如下圖 5-27 所示,使用者可透過 Demo DRM UI 之受保護的數位內容的清單畫面,選擇受保護的數位內容。

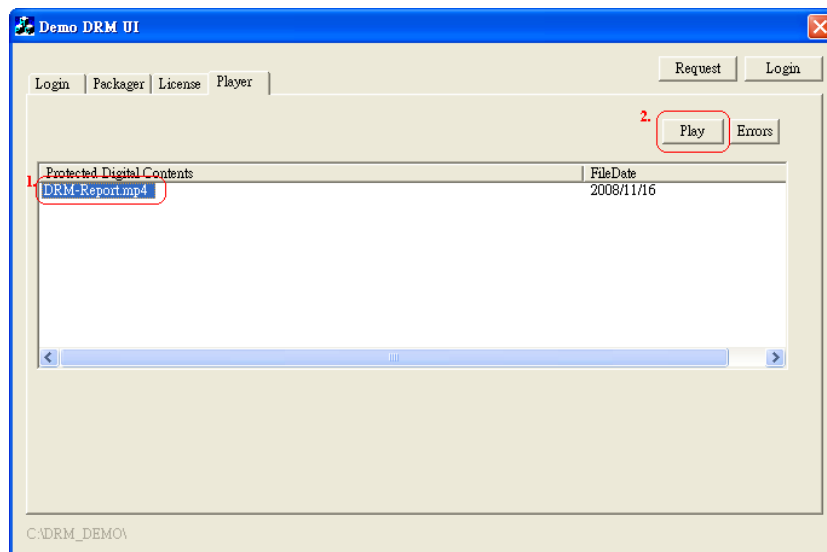


圖 5-27 使用者選擇受保護的數位內容的清單畫面

- (3) 在上圖中,當使用者按下「Play」按鈕後,當播放器驗證使用者的使用權利及條件通過時,會出現如下圖 5-28 所示之數位內容的播放畫面。

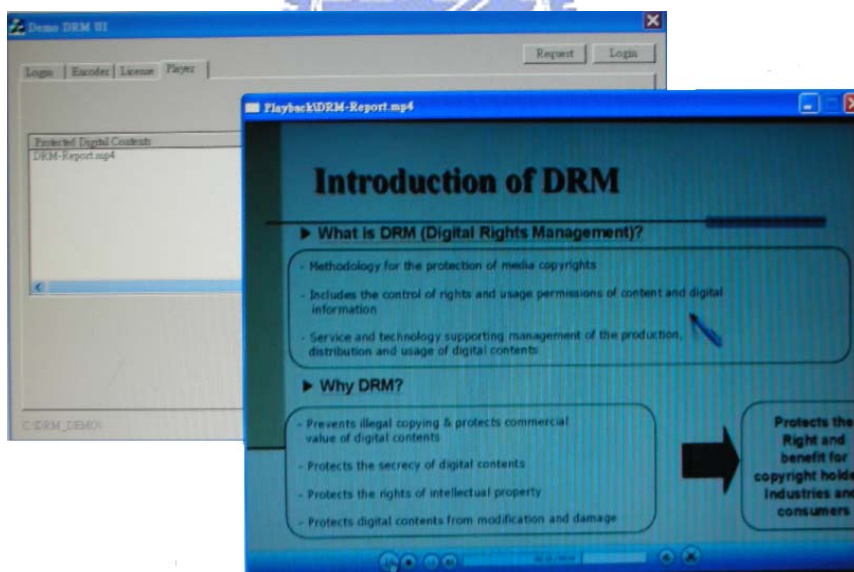


圖 5-28 開始播放數位內容的畫面

六、新的商業應用情境及展示

在本論文中，我們提出 Transferable Rights，讓購買的數位內容的使用權利，可以合法轉移給其他消費者。基於這個新功能的實現，我們可以提出兩個新的商業應用情境：一個是數位學習教材出租中心—消費者可以在線上租用數位學習教材的數位內容；另一個是數位學習教材轉售中心—消費者可以轉賣他們已購買的數位學習教材的使用權利。

6.1 數位學習教材出租中心

基於提供 Rights Grant 的服務，我們可以提出一種新的商業模式—數位學習教材出租中心。在現實生活中，我們會想去影片出租店租影片來看，而不會想去買影片來看，就是因為租會讓我們覺得比買來得划算。同理，昂貴的學習教材也會讓我們覺得租比買來得划算。所以在數位世界中，我們應該也要提供相同的租借服務。如此一來，消費者就可以用較低的價格在期限內自由使用所租借的數位內容，期限一過，Rights 自動失效，也不必將數位內容檔案歸還，不像傳統出租方式，逾期歸還還會被罰款。相對於傳統的出租方式，數位內容出租的是 Rights 而不是實體物品。還有，出租店通常會複製幾份有版權的影片拿來出租，或者消費者也會複製起來做為其他用途。而對於這種非法的行為，我們就可以利用 DRM 的機制來管制。

相對於傳統的出租商店，數位化的出租商店有更靈活的租借規章。它可以指定消費者使用數位內容的次數，或者使用數位內容時間長短，使用時間一到，就無法再利用原先合法取得的內容，除非再取得合法授權。更重要的是，數位內容的複製、散播是可以被嚴格禁止，這是一件還無法在傳統的出租商店被實現的事。還有，不同的限制將有不同的價格，這也滿足各種使用者的不同需要。

6.1.1 出租交易情境

消費者經過系統註冊及認證登入後，便可進行租借程序，過程如圖 6-1，情境說明如下：

- (1) Consumer -> Rental Store：出租中心將所有可發行的數位學習教材之相關資訊，以網頁方式供消費者選擇。
- (2) Rental Store -> Consumer：消費者確定欲取得的數位學習教材後，出租中心將數位學習教材的版權資訊以網頁方式呈現，除了基本的 Rights 與權限條件外，消費者可選擇以使用次數或期間租借，此外出租中心還會提供付費方式及交易模式。
- (3) Consumer -> License Server：所有的租借資訊呈現給消費者後，同時消費者在取得授權協議之後，必須馬上根據發行期間計算權利金轉帳給出租中心，再進行檔案下載程序。
- (4) License Server -> Rental Store：出租中心收到權利金之後，馬上通知授權伺服器，進行授權相關程序。
- (5) Rental Store -> License Server：授權伺服器提供 License 給出租中心，出租中心交給消費者。
- (6) License Server -> Consumer：系統必須提供消費者受保護的數位學習教材下載服務，讓消費者在收到 License 之後，可以經由內容伺服器下載租借的數位學習教材來使用。

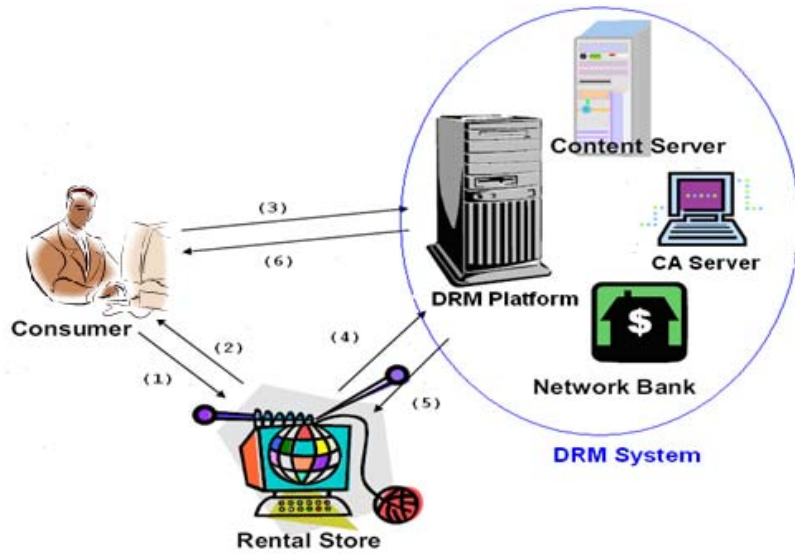


圖 6-1 出租交易情境

6.1.2 出租之 Rights Grant 流程及系統展示

由於本論文著重於 Transferable Rights 的研究與實現，因此對於商業交易模式及付費機制等相關情境及描述，就不多做介紹及展示。有關數位內容出租之 Rights Grant 流程，如圖 6-2 所示。我們將以範例說明並搭配我們的 DRM 系統作出租之 Rights Grant 展示。

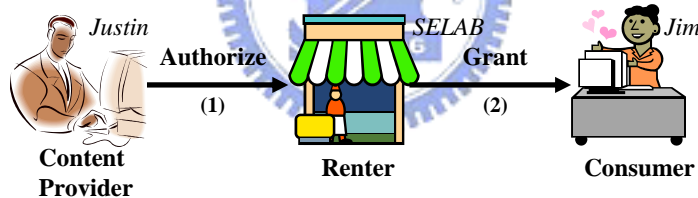


圖 6-2 數位學習教材出租之 Rights Grant 流程

當內容提供者(Justin)將其數位內容作品的使用權，授權給出租店 SELAB 發行，如圖 6-2 所示之步驟(1)，且指定一年發行期間以及無限量等條件限制。此時，出租店 SELAB 因其享有一年內無限量發行的權利，所以可如圖 6-2 所示之步驟(2)，授權給想要租借此數位內容的消費者，例如 Jim。當然以上的 Rights Grant 結果，皆需符合規定的權限條件以及雙方的授權協議。

而有關出租的 Rights Grant，其過程展示如下：

- 當消費者 Jim 使用播放器觀看沒有出租授權的數位內容時，會出現如圖 6-3 所示之錯誤畫面。

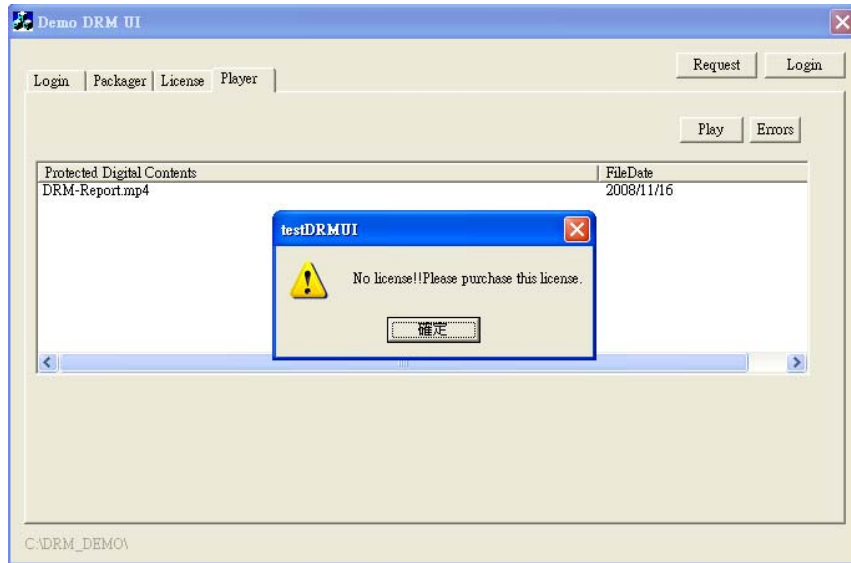


圖 6-3 使用者未取得出租授權的錯誤提示畫面

- 消費者 Jim 向出租店 SELAB 租借此數位內容，而 SELAB 可透過 DRM 管理平台作 Rights Grant 之動作。如圖 6-4 及 6-5 所示。



圖 6-4 DRM 管理平臺之授權清單畫面

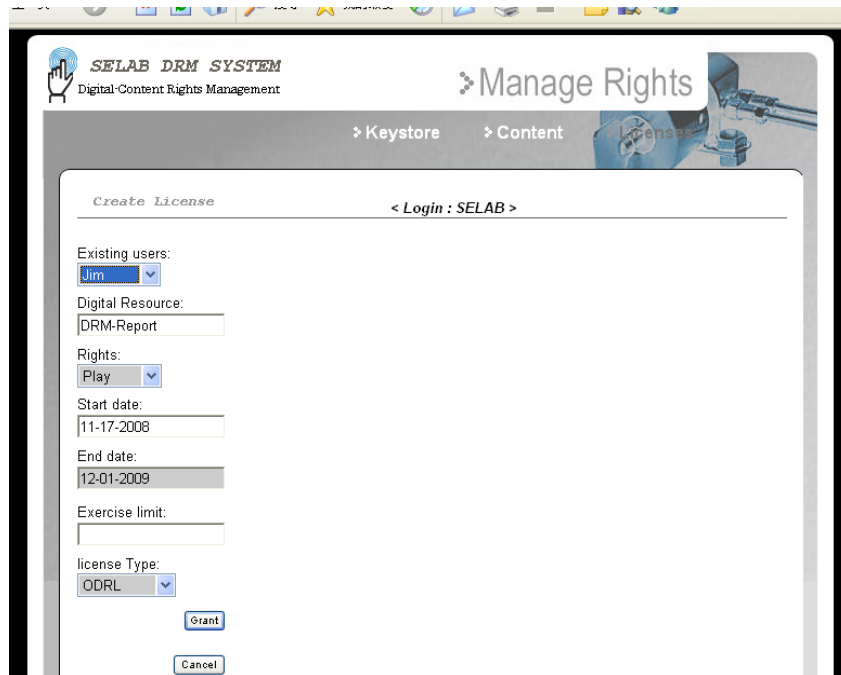


圖 6-5 Rights Grant 之 License 產生畫面

- 在出租店 SELAB 完成 Rights Grant 給消費者 Jim 之後，消費者 Jim 可從 DRM 管理平臺發現 SELAB 授權的 License 資訊，如圖 6-6 所示。

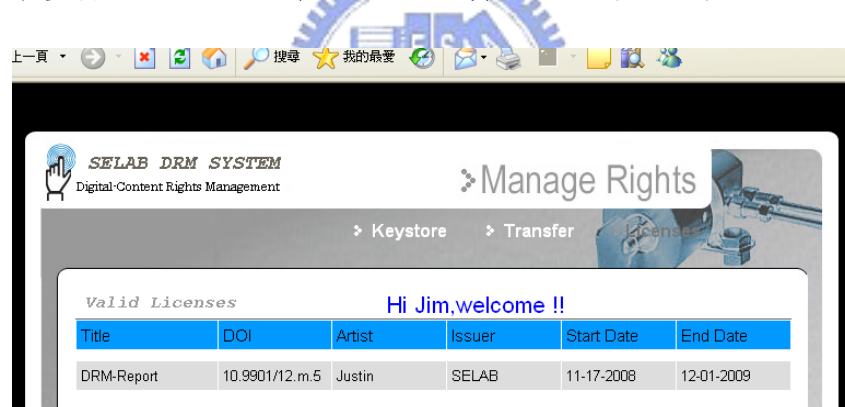


圖 6-6 消費者的 License 清單畫面

- 如圖 6-7 所示，消費者 Jim 可以使用播放器來觀看租借的數位學習教材。

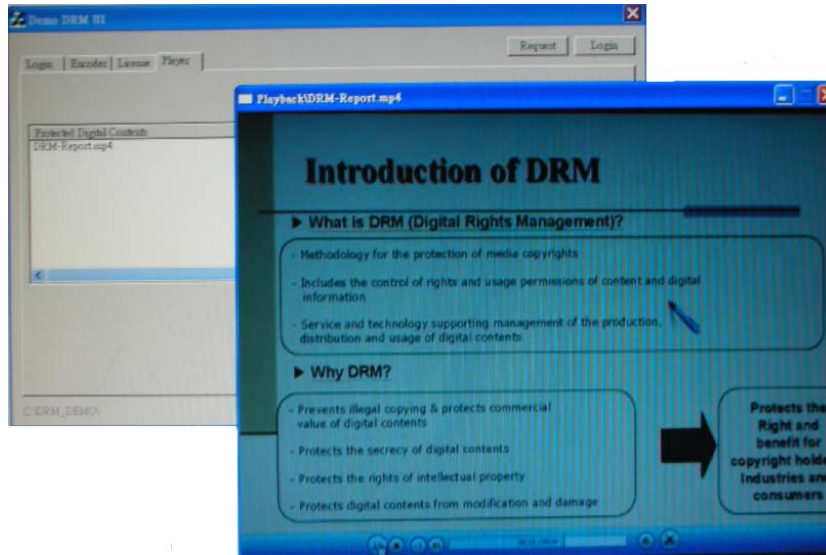


圖 6-7 觀賞數位學習教材的畫面

6.2 數位學習教材轉售中心

eBay 以及 Yahoo 拍賣網站的成功，不僅是開創了網路的二手交易市場，更讓我們意識到數位內容的二手市場也有著龐大的商機。例如，某位消費者 A 想要賣掉他使用過，但仍然可以使用且合法授權的數位內容時，剛好也有消費者 B 想要用較低的價格來購買相同的數位內容。此時，就需要數位內容的二手市場來滿足消費者的需求。

經過我們的調查，目前現有的 DRM 系統都沒有支援轉售這種服務。而我們的 DRM 系統因具有 Rights Transfer 的功能，所以我們可以提供轉售這種服務，讓數位內容的二手市場發展起來。以下舉出一轉售交易之情境及其 Rights Transfer 展示。

6.2.1 轉售交易情境

消費者可以透過二手商店，進行轉售之交易，過程如圖 6-8，情境說明如下：

- (1) Client A -> Secondhand Store：二手商店以網頁的方式提供消費者做轉售的選擇。消費者 A 可將想要轉售的數位學習教材的 Rights 權限及其相關訊息，透過網頁提出申請。
- (2) Secondhand Store -> License Server：二手商店將消費者提供的所有相關資訊交給授權伺服器做權限驗證。
- (3) License Server -> Secondhand Store：授權伺服器回覆二手商店驗證的結果，若無問題，二手商店透過網頁之方式發佈消費者 A 的轉售訊息。
- (4) Client B -> Secondhand Store：消費者 B 看到這項轉售訊息，且也有意願購買時，可按照網頁提供的購買程序進行交易。
- (5) Secondhand Store -> License Server：交易成功後，二手商店提供雙方消費者的資訊給授權伺服器，且通知做轉售的 Rights 轉移工作。
- (6) License Server -> Secondhand Store：授權伺服器完成雙方消費者的 Rights 轉移之後，將結果及新的 License 交給二手商店。
- (7) Secondhand Store -> Client A & B：二手商店將結果通知消費者 A 及將新的 License 交給消費者 B。

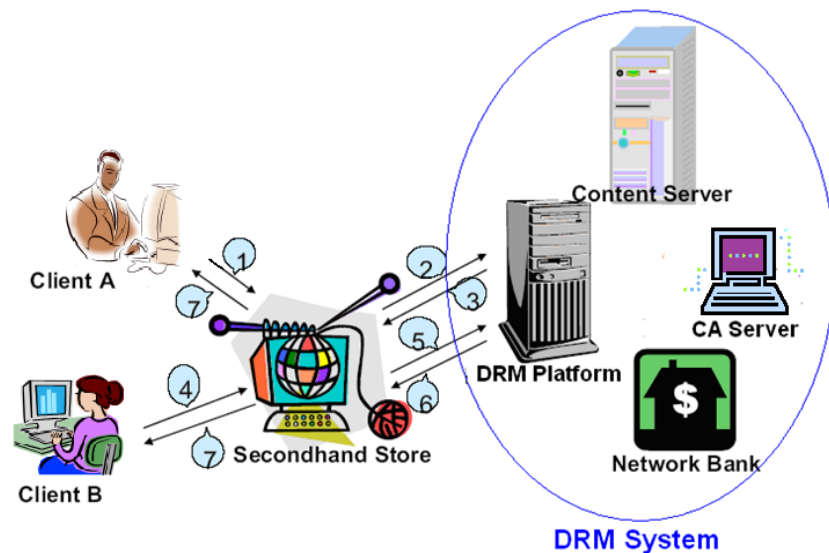


圖 6-8 轉售交易情境

6.2.2 轉售之 Rights Transfer 流程及系統展示

如圖 6-9 所示，即為轉售之 Rights Transfer 流程。為了進一步解說 Rights Transfer 流程，以下我們將以範例說明並搭配我們的 DRM 系統作轉售之 Rights Transfer 展示。

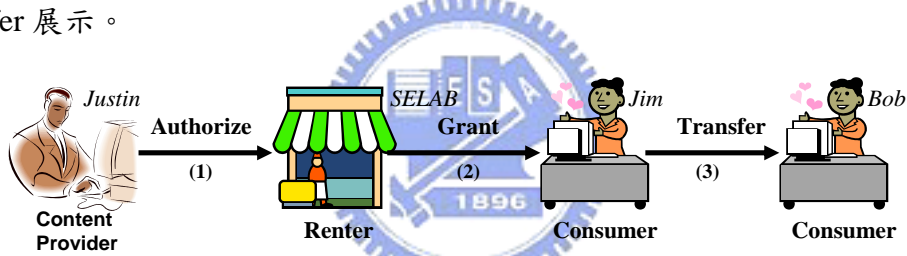


圖 6-9 數位學習教材轉售之 Rights Transfer 流程

我們拿消費者之間的 Rights Transfer (如圖 6-9 所示之步驟 3)，跟出租店與消費者之間的 Rights Grant 作比較(如圖 6-9 所示之步驟 2)，可以發現最大的不同點，在於消費者的 Rights 會因 Transfer 而消失。例如：當消費者 Jim 透過 DRM 系統申請將數位內容的 Rights 轉讓給 Bob 時，DRM 系統只需簽發新的 License 給 Bob(內含 Jim 的權限條件)，這樣就能將 Jim 的 Rights 成功轉移給 Bob，而且 Jim 所擁有的 License 會自動失效(因為 DRM 系統會廢止之前核發的 License)，此時 Bob 就可以合法的使用該數位內容，同時原先使用者 Jim 再也無法使用該數位內容。至於轉售的 Rights Transfer 展示如下：

- 如下圖 6-10 所示，消費者 Jim 進入 DRM 管理平臺後，可以看到自己的 Rights Transfer 前之授權者清單畫面。



圖 6-10 Rights Transfer 前之授權者 License 清單畫面

- 在上圖中，當消費者 Jim 按下「L722673」之 License ID 區域後，會出現如下圖 6-11 所示之 Rights Transfer 的 License 產生畫面。輸入 Rights Transfer 的相關資訊，如接受 Rights Transfer 者以及 License 型態等資訊，最後按下「Transfer」按鈕送出表單。

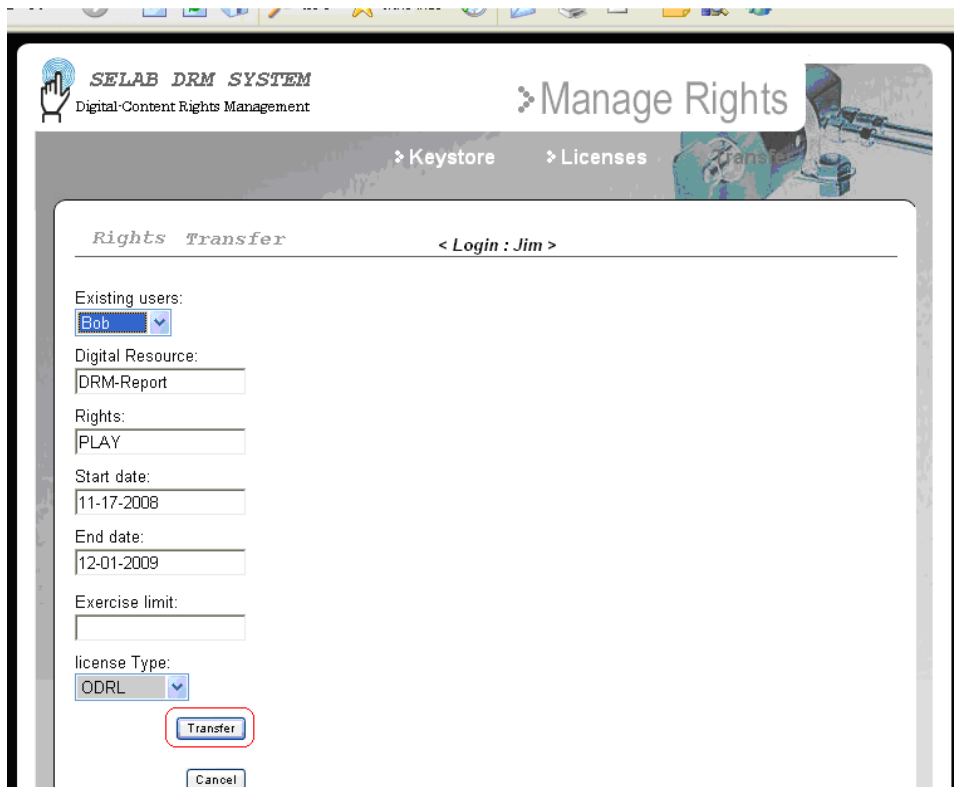


圖 6-11 Rights Transfer 時之 License 產生畫面

- 如下圖 6-12 所示，消費者 Jim 在系統完成 Rights Transfer 後，可以發現自己的 License 的使用期限已經無效。

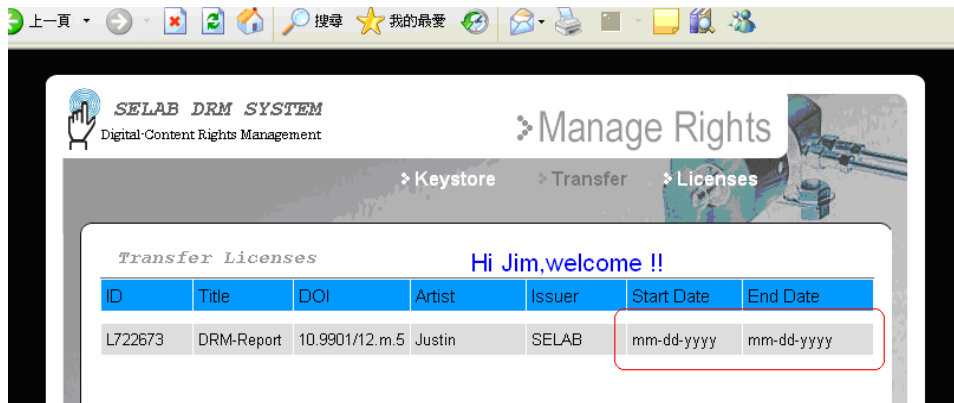


圖 6-12 Rights Transfer 後之授權者 License 清單畫面

- 同時消費者 Jim 也沒有權利再使用原數位內容，如下圖 5-13 所示。

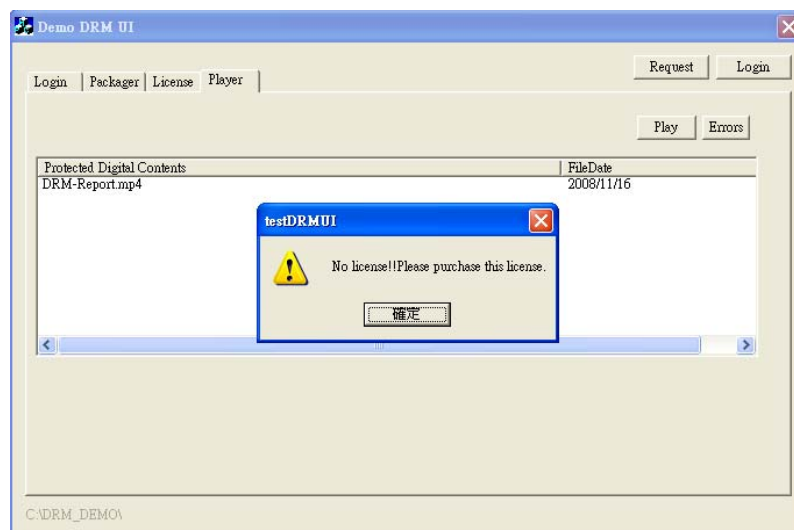


圖 6-13 使用者未取得出租授權的錯誤提示畫面

- 消費者 Bob 在系統完成 Rights Transfer 後，在 DRM 管理平臺可以看到自己新的 License 資訊，如下圖 6-14 所示。



圖 6-14 消費者的 License 清單畫面

- 如下圖 6-15 所示，消費者 Bob 也可以透過 Demo DRM UI 的 License 選項，來選擇 License list 裡想知道的 License 項目，再按下「View」按鈕送出表單，就能看到自己新的 License 資料以及 Rights Transfer 的相關資訊，如圖 6-16 所示。

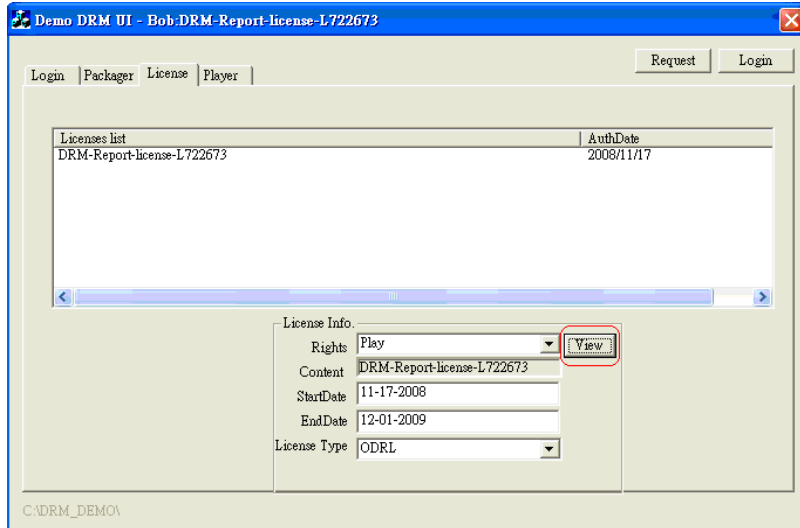


圖 6-15 Demo DRM UI 之消費者 License 內容資訊畫面



圖 6-16 消費者的 License Transfer 資訊畫面

- 如圖 6-17 所示，消費者 Bob 可以使用播放器來觀看購買的二手數位學習教材。

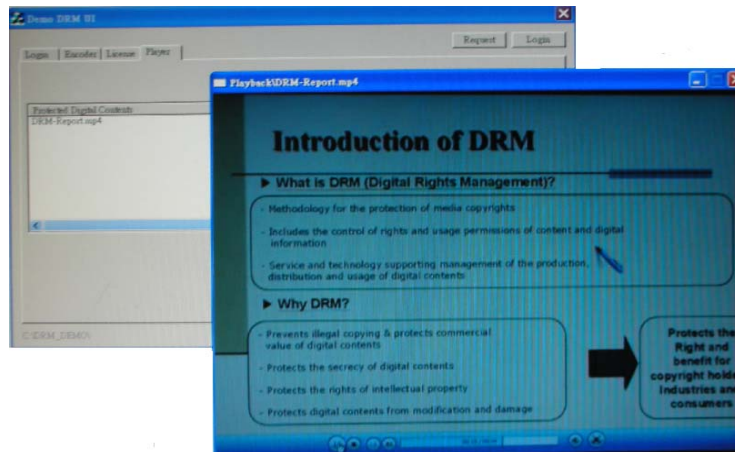


圖 6-17 播放器播放數位學習教材的畫面

七、 結論及未來建議

7.1 結論

在本論文的開始，我們指出目前的 DRM 系統所欠缺的功能，同時也解釋對於一個發展中的 DRM 系統，這些功能的重要性，也因此知道權限轉移機制對 DRM 系統的迫切需要性。接著，我們在第二章之中簡單的介紹現行 DRM 系統的基本架構、安全保護機制以及運作方式。藉由這些資料的收集與研究，可幫助我們建構出一個實作 DRM 系統的方法。

在第三章，我們研究與探討 Rights 的可轉移性與實現方法，並說明設計一個可權限轉移的 DRM 系統所應具有的相關機制。在系統設計與實作方面，首先提出具有權限轉移的 DRM 系統的模型，並設計其架構與功能模組，同時指出其應具有的系統運作流程。接著我們導入權限轉移機制，以及利用 Open-source 與 DRM REL 語言來實現我們的 DRM 系統。

觀看 ebay、Pchome 及 Yahoo 等拍賣網站的成功，每天都在創造不少的商機，本論文設計及實現一個可權限轉移的 DRM 系統，希望能夠替數位內容產業帶來更大的商機。藉著權限轉移的作法，我們能讓購買的數位內容可以合法借給朋友，也不會造成發行者的損失，更可轉賣給他人。最後我們提出兩個新的商業應用情境，且以我們的系統作為展示及驗證。總之，我們的 DRM 系統讓消費者更願意使用線上交易的行為且減少其對產品的顧慮以及使用風險，而且比以往對數位內容使用限制甚多的 DRM 系統更具彈性與合理性，並且更能被大眾接受。

7.2 未來建議

在未來的工作中，建議將各種商業交易模式導入我們的 DRM 系統並實現各項付費機制所需具備之功能，以及建立對於非法使用者的追蹤機制，這樣一來就能顯現出各種角色在商業模式上的應用及改變，也可驗證我們的 DRM 系統之彈性與合理性。除此之外，如能提供消費者一個合法且便利又收費低廉的交易管道，將使整個數位內容之發展環境更臻完整也更加完備。

參考文獻或資料

- [1] Q. Liu, R. Safavi-Naini, and N. P. Sheppard, "Digital Rights Management for Content Distribution," Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003, vol. 21, 2003.
- [2] iTunes, Available HTTP: <http://www.apple.com/itunes/>
- [3] InterTrust Technologies – About DRM, Available HTTP: <http://www.intertrust.com/main/overview/drm.html>
- [4] "Digital Rights Management White Paper," Sonera Plaza Ltd. MediaLab, February 2002.
- [5] Microsoft, "Microsoft Window Right Management Services System", Available HTTP:<http://www.microsoft.com/taiwan/windowsserver2003/technologies/rights/mgmt/default.aspx>
- [6] RSA Security, Available HTTP: <http://www.rsasecurity.com/rsalabs/node.asp?id=2009>
- [7] Hsiao Jen-Hao, "2004 Digital Watermark Competition: The Technical Report", Technical Report, IIS Academia Sinica, April 2004
- [8] Schaefer Edward, "A Simplified Data Encryption Standard Algorithm", Cryptologia, pp.77-84, 1996
- [9] X. Wang, "Extensible rights Markup Language (XrML) Specification 2.0, " ContentGuard Inc. White Paper, Available HTTP: <http://www.xrml.org>, 2001
- [10] X. Wang, T. DeMartini, B. Wragg, M. Paramasivam, and C. Barlas, "The MPEG-21 Rights Expression Language and Rights Data Dictionary, " *IEEE Multimedia*, vol. 7, no. 3, pp. 408-417, June 2005
- [11] Bok-Nyong Park; Jae-Won Kim; Wonjun Lee, " a privacy-enhancing license management protocol for digital rights management, " Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on Volume 1, Issue , 2004 Page(s): 574 - 579 Vol.1, Available HTTP: <https://ieeexplore.ieee.org/iel5/9028/28652/01283971.pdf>
- [12] Microsoft, "Windows Media Digital Rights Management", Available HTTP: <http://www.microsoft.com/windows/windowsmedia/>
- [13] Rivest R., "The MD5 Message-digest Algorithm", IETF IEEE RFC1392, April 1992
- [14] JSP,Java Servlet Page, Available HTTP: <https://java.sun.com/products/jsp>
- [15] OpenIPMP, open-source DRM solution, Available HTTP: <http://objectlab.com/clients/openipmp/index.htm>
- [16] Kwok S.H., "Digital Rights Management for the Online Music Business", ACM SIGecom Exchanges, Vol. 3, No. 3, August 2002, Pages 17-24
- [17] Chong, Cheun Ngen , Iacob, Sorin, Koster, Paul, Montaner, Javier, Van Buuren, Rene, " License transfer in OMA-DRM", Proc. of 11th European Symposium on Research in Computer Security, LNCS 4189, pp. 1611-3349, 2006.

- [18] MySQL, Available HTTP: <http://www.mysql.com/>
- [19] D.K. Mulligan, J. Han, and A.J. Burstein, "How DRM-Based Content Delivery Systems Disrupt Expectations of Personal Use", ACM DRM 2003, Washington D.C., USA, October 27, 2003, pp.77-89
- [20] Rivest R., Shamir A., Adleman L, "A Method for Obtaining Digital Signatures and Public Key cryptosystems, " Communications of the ACM, February 1978
- [21] 陳煜文,"以數位權利為基礎的商品交易機制",世新大學資訊管理學系碩士論文, 2002 年 6 月

