數位視訊平臺傳輸發展方案-94年度委託研究案

數位視訊服務平臺系統及其數位智慧財產管理之研究

期末報告

委託機關：交通部電信總局

受委託機關：成功大學 電腦與通信研究所

計畫主持人：楊家輝 教授
子計畫協同主持人：謝錫堃、賴溪松、蘇文鈺、郭文光 教授
研究生：陳明陽、吳昌隆、蘇育禕、李文豪、江昀諭、郭建邦、
連紹宇、黃圳柏、郭禹鴻、莊景翔、吳明達、劉明松

電腦與通信工程研究所
財團法人成大研究發展基金會

目錄

摘　要

新一代的數位多媒體服務隨著數位電視的開播將有劃時代的演進，經無線或有線的方式大量傳送至所需的個人或家庭。本計畫的目的在於探討國際數位電視廣播發展趨勢與以及我國目前廣播數位電視系統的現況，並提出整合無線、有線、衛星廣播電視系統共通平台(Multimedia Home Platform，簡稱 MHP)建置之整合具體方案。由於網際網路的盛行，數位娛樂在此間已經風行的同時，網際網路勢必不能在數位電視廣播的進展中缺席的因素。因此，我們亦規劃整合目前已經在國外啟動的網路電視(Internet Protocol Television，簡稱 IPTV)及數據廣播(Internet Protocol Datacasting，簡稱 IPDC)服務系統共通平台。同時，為保障著作權人和消費者，以及避免因數位內容的容易複製而產生侵權的動作，進而研究兼具數位智財管理(Digital Right Management，簡稱 DRM)以及條件式接取(Conditional Access，簡稱 CA)之視訊服務共同平台，研擬管理規範及註冊機制，以協助國內廠商對國內外數位電視、相關機上盒以及未來可能的相關產品技術及功能之認識，掌握時效以研製適當規格之產品，並期待對數位內容產業有所助益。本期末報告已完成下列研究內容：

- 完成條件式接取及數位智財管理(DRM)技術發展標準架構。
- 完成數位智財管理(DRM)的核心技術分析報告，提出整合無線數位電視多媒體共通平台技術規範草案的可行性建議，對於無線、有線、衛星廣播電視系統的整合可行性建議。
- 完成蒐集我國無線數位廣播電視頭端系統之差異性與相似性及其他有關整合特性之完整分析研究。
- 完成蒐集互動式數位電視廣播(IPTV)平台以及其數位視訊服務系統之間的差異性與共通性之研究報告，並提出可能的整合規劃報告。
- 完成蒐集互動式無線數據廣播(IPDC)系統，及初步規劃與其他數位視訊系統之平台整合，並提出可能的整合規劃報告。
- 完成數位智財管理(DRM)之無線廣播電視數位系統共通平台建置整合之方案研究報告。
- 完成修正 MHP 技術規範草案中適度加入近端互動與遠端互動之回傳通道(Return Channel)之部署。
- 完成修正 MHP 網路擷取技術導入及整合 IP 網路與數位電視之相關應用，藉以增訂技術規範草案之相關部署時程及技術內容。
- 完成整合電信網路之整合互動無線數位電視(IPTV)廣播之統合機制與共通平台之模擬模式(Simulation Model)。
- 完成整合電信網路之整合互動數據廣播(IPDC)系統之統合機制與共通平台之模擬模式(Simulation Model)。
- 完成利用數位視訊廣播建立我國全民危機警報系統之可行性建議。

第一章 介 紹

數位廣播視訊匯流的發展已然成為不可抵擋的趨勢。在期初報告中，我們已探討了歐洲數位視訊廣播技術（Digital Video Broadcasting，簡稱 DVB），更述及在 2004 年中邁入驗證與標準化程序的手持式數位視訊廣播（DVB-Handheld，簡稱 DVB-H）技術規格[2]。所以，DVB-T 標準為基礎加上 DVB-H 技術之增加，使用者將可以滿足互動式手持式裝置所需之功能。因此，透過既有之通訊系統(如行動電話、有線電話)之具回傳機制之廣義個人互動式裝置，來接收數位視訊/音訊等多媒體節目，將為將來之一項應用的趨勢及研究的課題。而隨著網際網路的發達以及 3G 的日漸成熟，數位廣播系統與通訊網路系統合流是勢在必行的。

依據行政院 NICI 小組九十二年三月三十一日第八次委員會議暨行政院視訊整合指導小組九十二年八月十五日第二次會議結論，平台傳輸分組由交通部執行「研究評估與規劃廣播電視系統數位共通營運平台之建置」並「推動引進廣播電視系統條件式接取系統同步加密共通國際標準（Simulcrypt）」。為確定標準及整合之環境，鼓勵產官學研積極投入國內數位視訊平台，去年電信總局依行政院國家資訊通信發展推動小組視訊整合指導小組九十三年元月二日第三次會議主席裁示有關數位電視多媒體共通平台（Multimedia Home Platform，簡稱 MHP）標準，電信總局乃邀集經濟部相關部會研商一致的標準，配合電信國家型計畫之執行，規劃「數位視訊整合–數位廣播電視系統整合之研究」以落實推動整合。

雖然在期初報告中已經就數位電視多媒體共通平台（DVB-MHP）的基本面加以闡述，不過在期中報告中我們還是再次的概述其基本要件如下:

1. 加強廣播版(Enhanced Broadcast Profile)

加強廣播版之電視多媒體共通平台適用於數位電視接收機沒有回傳路徑(Return Channel) 的情況，使用者只能透過遙控器等人機界面，與數位電視接收機上之 MHP 應用程式互動，但 MHP 應用程式無法回傳資料給電視台。此規格對電視台來說，是最容易採行的，因只需透過廣播網路播送 MHP 應用程式，不須考慮數位電視接收機回傳資料的問題，與電視台原本播送非互動節目的方式完全相符。因此近端互動建置即可採用規格實作。

2. 互動廣播版(Interactive Broadcast Profile)

互動廣播版電視多媒體共通平台適用於數位電視接收機有回傳路徑的情況。其回傳路徑之實體媒介可為 PSTN Modem、Cable Modem、ADSL、Ethernet 等等。由於目前台灣 ADSL 之普及化，家庭用戶之回傳路徑之實體媒介建議使用有線 ADSL，無線行動用戶則可採 GSM/GPRS/3G 之回傳路徑。然而，不管開發者使用那一類回傳路徑媒介，MHP 在回傳路徑上都是使用 TCP/IP 協定。如採用此規格，便可開發更複雜而多樣化的 MHP 互動式應用程式，如線上購物、線上卡拉 OK 點唱系統、互動式遊戲、網路相簿[2]等等。因此遠端互動回

傳通道即可採用此規格實作。目前已有相關產品都提供回傳通道功能的數位電視接收機，如 NDS 公司所開發的 MediaHighWay 中介軟體[7]，其中 MediaHighway Advanced 符合電視與 Web 開放標準，包含 DVB-MHP、HTML 4.0 和 JavaScript，MediaHighway Advanced 中的回傳路徑管理(Return Path Management)功能可用來作為用戶回應 回答民調 採購訂單與其他使用者互動等等，而這些資訊都會經由回傳路徑傳到頭端。除此之外，MediaHighway Advanced 更能提供 TCP/IP 協定的傳輸。

3. 網路接取廣播版(Internet Access Profile)

網路接取廣播版之主要的目的是定義 MHP 的應用程式，如何跟數位電視接收機上的 Internet Client，彼此雙向互動的能力。例如，如何從 MHP 的 Xlet 程式裡，透過瀏覽器開啟某個網頁，或是加入某些 URL 的書籤，也可能發送 email 等。因此 IP 網路與數位電視整合即可採用此規格實作。DVB-J 為一 Java Virtual Machine，其目的用來提供 MHP 功能。其中在 java.net 套件裡，提供了 IP over Return Channel 之功能以負責管理回傳通道連線、斷線等等。不過由於此套程式僅提供簡陋的程式介面以及驗證功用，多項 DVB-MHP 所必需要的功能也暫時付之闕如，更因為其平台並不支援多個 Xlet 城市同時運作的機制，因此無法真正地應用在複雜且多功能的網路接取數位廣播的系統上，這是大家必須小心的。未來如果要為開發網路接取數位廣播的相關產品時，一套能實現於電腦與嵌入式系統的功能強大的軟體平台是必要的。我們除了期待 DVB 聯盟將原有的軟體更新外，可能必須考慮由國人自行開發，以免有受制於人的可能。

由於互動式裝置之應用以及網際網路之數位娛樂的風行，其中對於數位資訊或數位廣播媒體之接取、條件式接取、使用權限及付費之相關問題將隨之而來。這些議題密切地關係著數位內容產業的成功與否。而數位智財管理(Digital Right Management，簡稱 DRM) 為結合硬體與軟體的存取機制，將數位內容設定存取權限，並與儲存媒體結合，使得數位內容不管使用過程中，是否被複製到別處仍可以持續追蹤與管理數位內容的使用情況，能提供完善的保護和管理的技術。數位智財管理(DRM)的技術是能夠做到事前防護的安全管理，將數位內容加密、簽章，並設定使用者存取控制，以及追蹤行為等。在數位內容生命週期，不會被隨意複製、竄改、散佈，保障數位內容的完整性以及機密資訊的保密性。目前在 DRM 這部份的發展是較為紛歧的，其原因在於數位內容的保護機制一旦標準化，各家廠商對於其內容的機密性也就可能相對降低。因此，雖然有國際間較為風行的 DMP[24]，我國是否也要直接採用仍須謹慎思考，在此次的報告中我們將對數位智財管理(DRM)技術發展標準架構，包括技術發展和管理技術層面進行分析，並針對歐盟和美國的標準、現況加以探討，期待提供決策單位最完整的參考資料。

網路電視(IPTV)，寬頻電視，利用有限與無線寬頻網路甚至手機上網等產品為使用者提供互動式多媒體服務，為網際網路與電視相互融合的結果。視訊流

經過高效的壓縮編碼後被廣播到 IP 網路上，透過位於寬頻網路邊緣的 IP 電視設備把直播電視、隨選視訊和個人錄影等 IPTV 服務傳送給用戶。它也能根據用戶的選擇配置多種多媒體服務功能，包括數位電視節目、視訊 IP 電話、DVD/VCD 播放、網際網路瀏覽、電子郵件以及多種線上諮詢、娛樂、教育及商務功能。末端使用者可以透過使用電腦或是數位機上盒 Set-Top-Box 甚至行動裝置來使用上述的服務。但是網際網路的頻寬限制以及使用的狀況是隨時在變化的，一般的數位廣播方式是不適合在此一方面應用的，可是 IPTV 是一股抵擋不住的趨勢，數位廣播與 IPTV 結合是必然的，所以在資料格式以及傳輸方式勢必要有所不同，根據歐美的數家 IPTV 解決方案的提供者如微軟者，採用的已經不是數位廣播的 MPEG-2，而是資料量更小的 WMV9、MPEG-4、甚至是更先進的 H.264，傳輸方式也因此各有不同，在此次的期中報告內，我們就較為著名的方案進行探討，期待未來可以就國內的整合方案提出一套具體可行的作法。

IPDC 之系統架構分為以下幾個層次(Layer): 內容層(Content Layer)、服務傳送層(Service Delivery Layer)、播種層(Corn Layer)、廣播回傳網路層(Broadcast and Return Channel Network Layers)、使用者平台層(Client Platform Layer)與使用者應用層(Client Application Layer)，雖然 IPDC 系統架構如同 OSI Model 一樣具有階層式的架構，但 OSI Model 在 Client 端與 Server 端皆具有對等的 7 Layers，但 IPDC 則 Client 與 Server 端共享以上所敘述的 6 Layers。此次我們對 IPDC 的架構以及其未來發展性將做更進一步的討論，此外對於將數位視訊整合進 IPDC 的可能性進行探討，並且以實例講述 IPDC 的應用。

最後是關於回傳通道的技術之分析。在今後的數位娛樂趨勢與技術的開發中，舉凡互動式的機制必然牽涉到回傳通道的建立問題，惟有回傳通道的建立與運作，點播、認證、收費、傳輸、互動、隨選、...等議題方能得到解決，此次我們將分析歐盟及美國 MHP 近端與遠端回傳通道之發展現況，可想而知的是根據各國的電信基礎建設的不同，回傳通道方式的差異性是相當大的，期待在期末報告中針對我國的現況提出可能的解決方案。

本期初報告共分下列十章敘述：第二章 針對數位電視多媒體平台(MHP)相關標準及現況分析；第三章 調查歐盟及美國有關 MHP 網路擷取標準部署現況與技術導入；第四章 為對於數位智財管理(DRM)現況分析；第五章 提出條件式接取及數位智財管理技術標準的可能架構；第六章 針對歐盟及美國 MHP 近端與遠端回傳通道之發展現況進行技術分析報告；第七章 為調查我國無線數位廣播電視頭端系統並分析之；第八章 對於互動式數位電視廣播(IP-TV)現況進行資料收集與並對於其與數位視訊服務系統(DVB)的結合提出研究報告；第九章敘述互動式無線數據廣播(IP-DC)的基本技術以及與其他數位視訊系統的可能的整合規劃；第十章 是對於數位智財管理(DRM)之無線廣播電視數位系統的整合性研究；最後第十一章為本期中報告之結論以及對期末報告的規劃。

第二章 數位電視多媒體平台MHP技術

數位電視多媒體共通平台（Multimedia Home Platform，簡稱 MHP）技術為本計畫之核心，亦為互動式數位電視廣播(Internet Protocal Television，簡稱 IP-TV)平台以及互動式無線數據廣播(Internet Protocal Datacasting，簡稱 IP-DC)系統之基礎，更是數位智財管理(Digital Right Management，簡稱 DRM)與無線廣播電視數位系統共通平台建置整合之主要根據。

2.1 MHP介紹

在本章當中，我們首先對 MHP 作一個簡要的介紹，並闡述 Openmhp 的整體程式庫架構和開發環境的需求，接著對整個 MHP 平台的架設及安裝環境的相關步驟作詳細的說明，只要使用者按照說明的步驟進行，即能進一步的開發及應用 Openmhp，應用程式的開發者可以利用外掛函式庫(Third Party Libraries)來開發應用程式，最後舉一個簡單的應用程式範例，說明應用程式在 Openmhp 的環境下所呈現的面貌。

2.1.1. 簡介

- 由歐洲數位電視廣播協會(DVB consortium)所定義，為一個開放性(open)的標準
- 目標是推動共通平台，讓用戶不論透過何種傳輸管道或平台，都能享受到最多的多媒體服務內容，讓生產者和消費者，獲得最大的利益。 MHP 是一個中介軟體。MHP 是一個平臺的定義, 是一系列的 Java APIs, MHP 是一系列的 HTML 文件格式的定義。一系列的相容性測試。

2.1.2. DVB-MHP 的應用領域與版本 MHP 主要根據應用領域的不同而分為三個項目(Profiles)

- 加強型廣播(Enhanced Broadcast)
  提供結合影像，語音，及提供近端互動的應用程式，但不提供互動的管道(channel) 。規格定義於 ES 201 812 (MHP 1.0) 。
- 互動式服務 (Interactive Service)
  提供更強的互動性，且提供互動的管道(channel) 。規格定義於 ES 201 812 (MHP 1.0) 。
- 網際網路 (Internet Access)

提供網際網路的存取，及網際網路服務與廣播服務的連結。規格定義於 TS 102 812 (MHP 1.1) 。

2.2 OpenMHP

2.2.1何謂OpenMHP?

OpenMHP 是一個可以在PC上開發,並且可以達到數位電視多媒體平臺MHP標準的開放性應用軟體, 其作用在於提供執行於機上盒(Set Top Box，簡稱STB)的互動應用程式，而程式設計者不用考量底層的作業系統與硬體驅動程式,可以讓互動應用程式設計者更方便開發應用程式。OpenMHP的範疇相當廣泛,因此目前仍在開發當中

2.2.2 OpenMHP系統需求及作業系統

使用者PC至少需要1G的CPU和256MB的記憶體，目前OpenMHP可以在以下的作業系統環境下執行: Windows 2000, WindowsXP, Linux and MacOS/X。

2.2.3 OpenMHP所提供的功能

OpenMHP所提供的功能如下：

- 提供互動式應用程式的模型(Model)
- 提供繪圖的顯示(Graphics Display)提供存取多個視訊平面(Video Planes)
- 提供[繪圖平面與視訊平面整合]的功能的存取
  影像建議以JPEG格式為主
- 服務資訊(SI)的存取提供使用者輸入介面(經RCU或鍵盤)
  使用者經由遙控器選擇應用程式,OpenMHP會"聆聽"使用者輸入的指令並執行應用程式
- 提供回傳通道的存取(TCP/IP Return Channel)提供記憶體的管理

2.2.4 OpenMHP 程式庫(Library)

OpenMHP 程式庫(library) 主要包含MHP程式庫及MHP適應層模組兩大部分:

- MHP 程式庫 :程式設計者不用考量底層的作業系統與硬體驅動程式, 是一個跨平台的應用程式開發環境，如圖2.1所示。

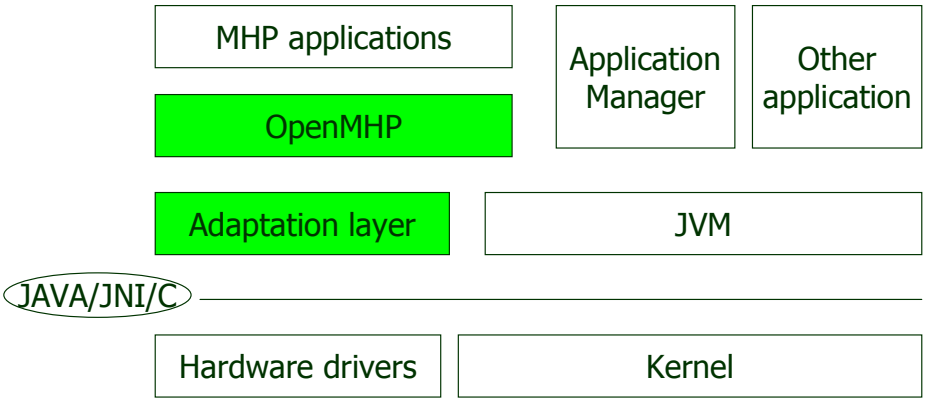

圖2.1. MHP跨平台的應用程式開發環境

- 適應層(The Adaptation Layer)：在特定的平台上開發的平台系統(i.e., 嵌入式平台系統, etc.)，如圖2.2所示。

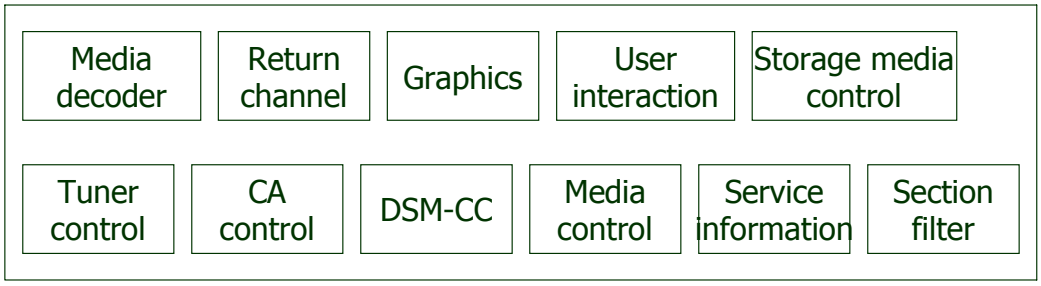

圖2.2. MHP適應層模組

2.3系統安裝(Environment Installation)

2.3.1 安裝必備套件

執行OpenMHP, 必須要先有幫助開發環境的外掛函式庫(Third Party Libraries):

- Java APIs

  此標準由Sun Microsystems所提供(現為J2ME)Java TV

  此標準由Sun Microsystems所提供。在數位電視環境所使用的一些功能

- Java Media Framework (JMF)

  是一個Java函式庫,用來控制或播放Java應用程式的影音環境

2.3.2 系統安裝步驟

- 步驟一

先確定作業系統中是否安裝 Java 1.4. JRE ,如果沒有請至下列的網頁

(Sun Microsystems)下載.

Download page:

http://java.sun.com/j2se/1.4.2/download.html

下載必須的套件:

OpenMHP1.0.4_src.zip　　http://www.openmhp.org

Java TV Version 1.0　　http://wwws.sun.com/software

■　步驟二

解壓縮OpenMHP1.0.4_src.zip至您硬碟裡的任一資料夾中

■　步驟三

解開 JavaTV 套件至OpenMHP's 的安裝資料夾裏.

注意: JavaTV套件裡的 'javatv.jar' 必須在 OpenMHP'的路徑底下. JavaTV中只有名為 'javatv.jar' 的檔案是必要的。

2.3.3 編譯器安裝步驟

■步驟一

您可以用任何適合的編譯器去編譯OpenMHP，但建議可以使用Apache Ant 來做編譯

Download page :http://ant.apache.org/

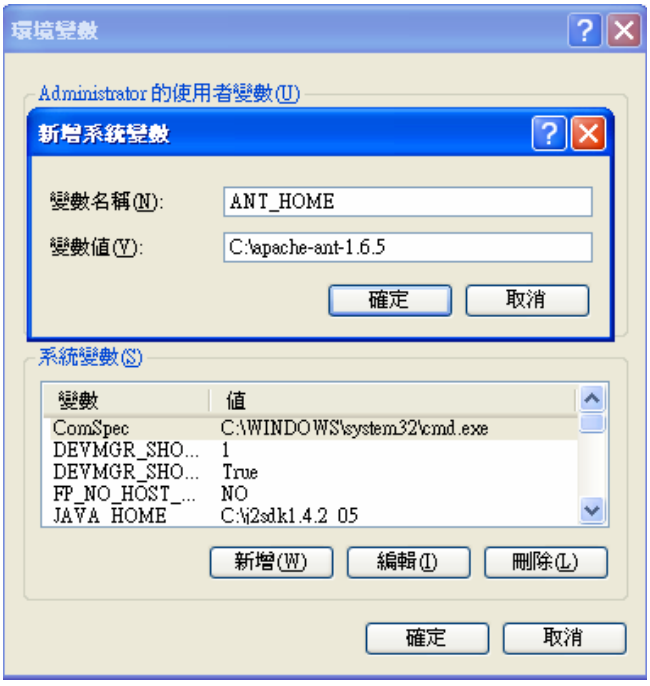

圖2.3 系統環境變數(設定ANT-HOME)

■步驟二

新增系統變數流程:

1.點選"控制台"的"系統"→選擇"進階"→點選"環境變數"→點選"新增"

會出現如下圖2.3畫面，接著輸入"變數名稱"和"變數值"

2.仿照上述步驟1. 設定JAVA_HOME路徑，如下圖2.4所示。

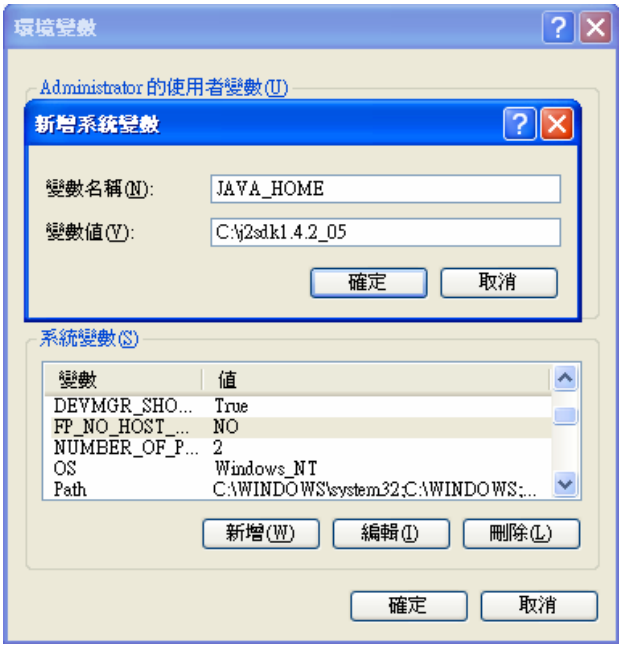

圖2.4 系統環境變數(設定JAVA-HOME)

3.編輯系統變數"path"：在變數值後面新增

" %JAVA_HOME%\bin;%ANT_HOME%\bin" 如下圖2.5所示

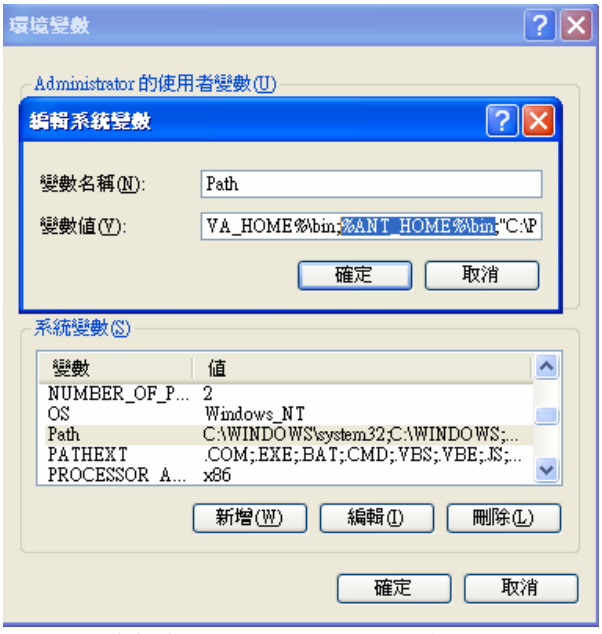

圖2.5 系統環境變數(新增ANT-HOME與JAVA-HOME路徑)

2.4 編譯及執行 OpenMHP1.0.4_src

- 步驟一

打開命令提示字元至openmhp_src104路徑底下

輸入ant conf，然後填入javatv.jar及jmf.jar的路徑並”save”

如下圖2.6所示

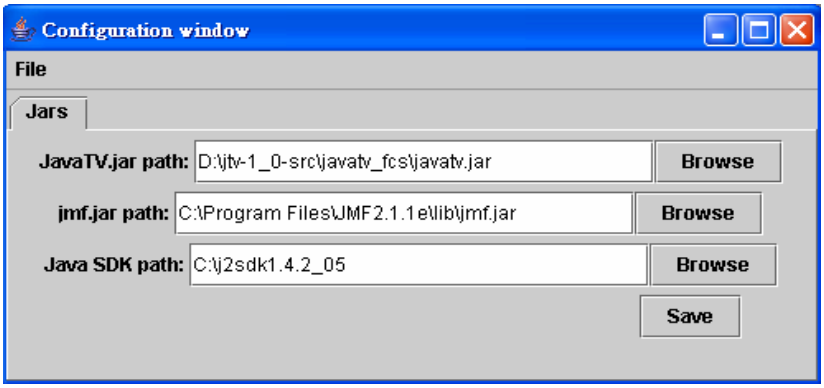

圖2.6 設定Configuration Window

- 步驟二:

  輸入: ant compile ,如果編譯沒有成功,請將openmhp下build.xml中的第91及122行: “bootclasspath=“${java.class.path}“刪除

- 步驟三:

  編譯成功後，則啟動openmhp,輸入: ant run

2.4.1 應用程式管理員(Application Manager)

啟動openmhp後進入的第一個畫面為應用程式管理員，如下圖2.7所示。(經由我們Trace Code後，我們已將應用程式管理員的英文介面改為中文介面)

圖2.7 應用程式管理員

點選遊戲特性,接著設定應用程式相關參數,如下圖2.8所示:

圖2.8 應用程式參數設定

點選“儲存”後, 按右鍵選”開始”,即開始執行應用程式

2.4.2 應用程式範例

以下列舉一個簡單的應用程式範例:

(註: 經由我們Trace Source Code之後,我們已經此應用程式介面大部分中文化)此範例為一個猜謎遊戲,當遊戲啟動以後,會出現如圖2.9的畫面,右側的模擬遙控器可以下達指令

圖2.9 猜謎遊戲首頁

若我們用遙控器選擇”啟動遊戲”,點選”ok”,則遊戲會畫面進入圖2.10。使用者可

以根據右邊的模擬遙控器的"上","下"及"ok鍵"來選擇答案，答題正確與否會顯示在螢幕上

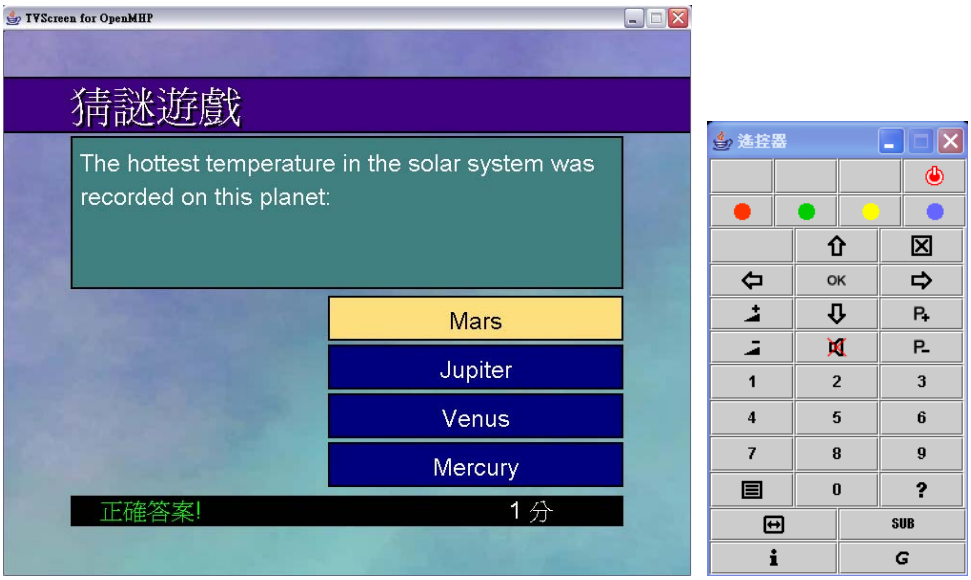

圖2.10 開始猜謎畫面

遊戲結束後,此遊戲會顯示使用者總共獲得的分數!

圖2.11 猜謎遊戲結果

第三章 條件式接取及數位智財管理(DRM)技術發展標準架構

3.1 前言

在類比的時代，要盜拷產品，如黑膠唱片、錄音帶以及參考書籍等，需要花費較長的時間與較大的金錢來達到目的。而盜拷出來的品質只會越來越差，所以，對於版權擁有者和產品製造商而言，盜拷保護技術在類比的產品中並無急迫性。近年來，由於數位技術發展的進步改變了目前的情況。由於數位內容被拿來進行非法的操作、修改、儲存、散佈...等都非常的容易，而且盜拷出來的內容跟原版的品質一樣，相對地使得版權擁有者、製造商、賣方和從數位產品中有從中獲利的中介廠商，也開始受到威脅且逐漸重視盜拷保護的問題。在1970年代，個人電腦慢慢普及化，軟體盜拷的問題也開始重視。在網路盛行的1990年代，促使數位內容可以更快速的散佈，若是非法的散佈數位內容對於從數位產品中有獲利的人更是很大的傷害。所以，對於執行數位內容的權利進行有效的管理和保護是一個很重要的議題。此議題統稱為數位智慧財產權管理。再者無線電視廣播的領域很早就應用在日常生活上，所以針對廣播訊號的安全性同時也提出相對應的技術，為條件式接取技術。主要運用在擾亂無線廣播串流訊號，使得天線接收到訊號時，在接放端若沒有相對應的解擾亂器，就無法看到接收下來的訊號。

在資策會「我國資訊領域規劃報告」[1]中有定義數位內容依其流通型態可分為四種類型：

- 實體數位內容：是數位內容與載體結合而以實體數位商品形式銷售，如影片DVD、音樂CD、遊戲軟體及教育、娛樂用出版品之CD-ROM等商品。
- 網路流通內容：透過網路流通的數位內容，如線上音樂、影片、圖片、付費電子報...等。
- 手機內容：透過手機接收與傳送之數位內容，如待機圖案、鈴聲、手機遊戲...等。
- 數位播放內容：透過衛星、有線或地面電視廣播，以數位形式直接播放以予消費者觀看的內容，如電視節目...等。

而帶動數位智財管理(DRM)重要的原因有：

- 智慧財產權的保護：保護數位內容不會被任意複製、竄改、散佈，讓智慧財產權可以得到一個完善的管理與保護機制。
- 產權利益的衝突：之前曾經被任意複製、散佈，而使收益損少的部份，如燒錄機的普及，使得一些創作人無法獲得應有的利益。在DRM技術建立後，將重新獲利，並且可以進一步對數位內容設定使用次數、時間等，控制使用者一些侵權的行為來保障數位內容的財產權。
- 機密的保護：並不是所有的數位內容都是要做為商業用途，例如台積電的重

要商業機密等，就可取消離職員工的權限，或設定使用的地點、時間，藉由 DRM 技術的控管，受到更完整的管理與保護。

3.2 條件式接取技術研究

在廣播的環境中，條件式接取技術(Conditional Access，簡稱 CA)是非常重要的技術。可以限制有權利的使用者才能收看內容，並防止沒有付費沒有權利的使用者無法順利播放。在 1993 年，最早由 ITU (International Telecommunication Union)組織制定了一套安全條件存取的標準，之後再由 DVB (Digital Video Broadcasting)組織制定了相關的 CA 標準，如 DVB-CSA、DVB-Sim 等等。在本章，我們將介紹這些 CAS 技術並在最後提出我們的建議。

3.2.1 ITU Rec.810 條件式接取技術簡介

ITU 將條件式接取技術(Conditional Access System, 簡稱 CAS)規定在 ITU Recommendation 810 [1]中。這個標準一開始主要的目地是在單向的數位廣播環境中提供一套標準的流程管控來保護所要廣播的資料，使得付費電視等服務能夠安全的運作。舉例來說，電視台等頭端系統所廣播出來的電視節目(收費節目)或是一些互動性的節目如果直接以廣播方式播放，那麼有心人士(沒付費的使用者)必定能很輕鬆地截獲電視台所廣播出來的節目如圖 3.1 所示，如此一來將會對電視台造成莫大的損失。而透過條件接取技術來進行一個安全即時的保護的話，就能達到使用者付費功能並防止沒有權限的使用者觀看付費的節目。因此，CAs 在廣播電視這個領域是非常重要的核心技術。而 CAS 包含了許多重要的元件，如：加解密元件(encrypt/decrypt)、scrambler/descrambler 元件、智慧卡元件等等。以下章節將針對這些元件進行介紹。

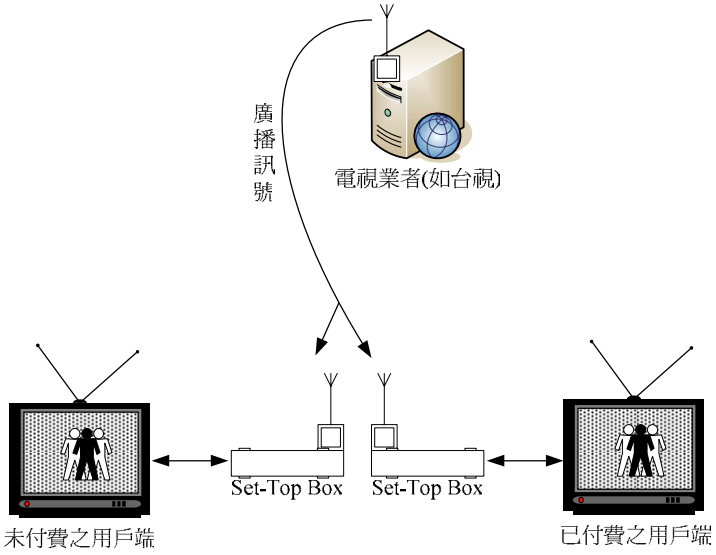

圖 3.1 系統未加入 CAS 示意圖

3.2.1.1 條件式接取技術之需求及建議

在國際標準 ITU 所規定下的條件接取技術制定時，已經考慮到條件式接取系統必須達到幾個需求。如表 3.1 條件式接取系統需求

表 3.1　條件式接取系統需求

要求項目	建議項目
要能保護廣播出去的資料，防止無授權的使用者獲取	此技術一定要很安全
最好能將一些共用的元件建置在接收端以達到一般性	將大部分共用的元件也一併建置在接收端
要能夠有效率的來實作這套條件接取廣播的技術	照著在 ITU Rec.810 中的附錄 Annex 1 所提到的基本原財來設計此套系統
要能適用於有線電視、衛星廣播以及一些電視文字等資料服務	
希望能夠將不同廣播系統服務所以達到的各種需求納入考慮	
能讓內容版權擁有者、節目提供者以及服務提供者能相信在廣播的環境中，條件接取技術能為他們把關	

3.2.1.2 條件式接取技術之基本原理

前面介紹的是條件式接取技術的需求及應用環境，接下將介紹條件式接取系統(CAS)的基本元件及其運作的基本原理，有了這些機制後，CAS 才能夠為數位廣播系統的內容進行保護，使得只有被授權的使用者才能夠有權力來進行播放的動作。一般而言，條件接取技術的安全機制分成二個部份，一部份是節目播出時的擾亂系統(Scrambler)，目的在於為即將送出的節目進行擾亂的動作，使得未經授權的的用戶無法正常的反擾亂(Descrambler)還原節目並播放。另一個部份則是金鑰加密機制，在擾亂節目訊號時，會有一個控制擾亂系統的控制字元(Control Word, 簡稱 CW)如圖 3.2 所示，而 CW 是隨著電視節目一起廣播出去，如果沒有針對 CW 來進行加密保護的話，未經授權的用戶也可以將 CW 一併截取出來，並進行反擾亂的動作，進而播放節目。而除了用來保護 CW 的金鑰以外，系統中通常也會有另外的幾把金鑰，形成一層保護一層的架構，每把金鑰並有其特殊的使用場景，並會針對使用情況，由發送端定期更換金鑰，如 CW 幾乎是每幾秒鐘(5s~20s)即會定期更新一次，保持其隨機性獲得較高的安全性，並降低被駭客破解的機率，而保護 CW 的金鑰(Authorization key, 簡稱 AK)也是定期的進行更新的動作。

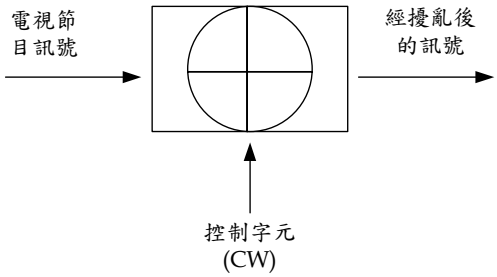

圖 3.2. 擾亂系統(Scrambler)示意圖

3.2.1.3 條件接取技術元件介紹

圖 3.3 為標準的 CAS 的架構，其中包括了幾個核心元件及參數，包括有：CW、AK、ECM 以及 EMM。我們在本節將會逐一介紹。

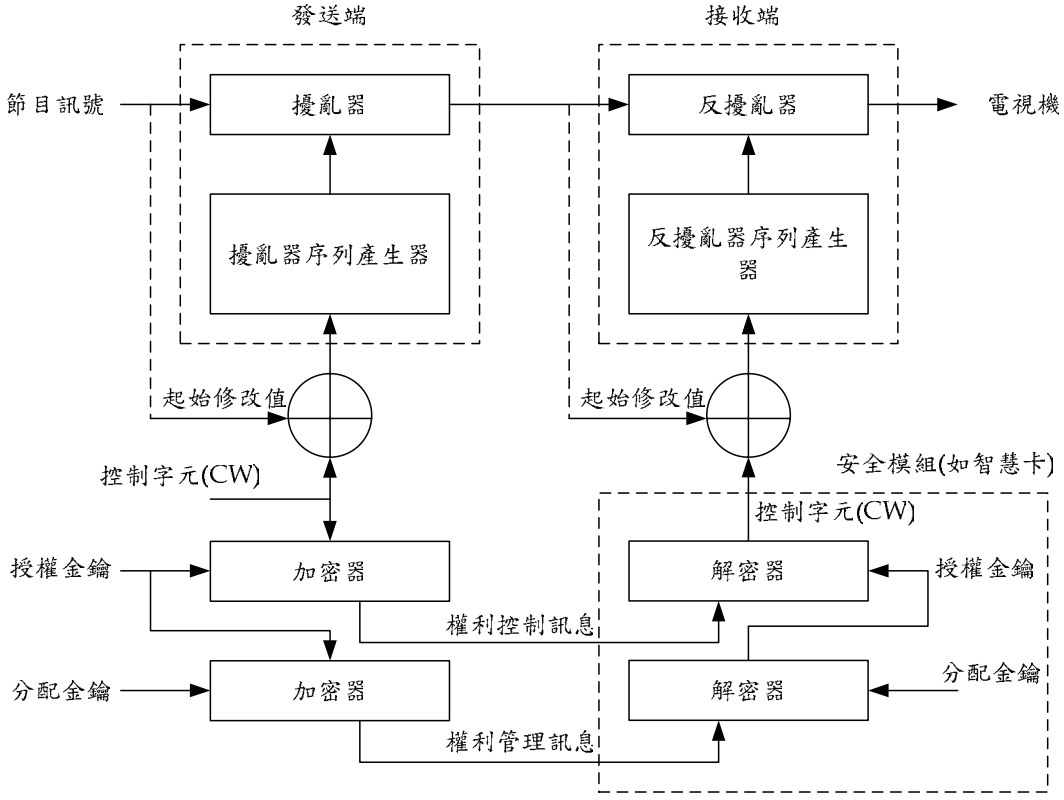

圖 3.3 條件式接取技術架構圖

1. Control Word (CW)：控制字元為此系統中最基本的安全元件，而為了增加整個系統的安全性，控制字元的值將會定期的透過權利控制訊息(ECM)來進行更新。而控制字元可分為兩個部份：

   (a) 發送端(sending end)：在發送端，控制字元會先與起始修改值(Initialization modifier)進行互斥或(XOR)的運算，再成為擾亂序列產生

器的輸入，之後再和節目訊號互斥或成為已擾亂的訊號再發送出去。而需注意的是，起始修改值也一併以明文方式和節目訊號廣播至接收端。同時，控制字元將經由授權金鑰(Authorization key, 簡稱 AK)加密後，透過權利控制訊息方式(ECM)送至接收端。

(b) 接收端(receiving end)：在接收端，用戶這邊進行的運行就等於是發送端的反運算。接收到權利控制訊息方式(ECM)後，用戶端的安全模組(如智慧卡, smart card)會利用之前解出(詳見 EMM)的授權金鑰來解開此次此時的控制字元(CW)，再配合由訊號夾帶的起始修改值，即可將已擾亂的節目訊號反擾亂回來，成為可以播放的多媒體節目。

2. 權利控制訊息 (Entitlement Control Message, 簡稱 ECM)：在 ECM 中，夾帶了許多控制訊號以及最重要的控制字元(已加密過)。包括了有：

(a)控制字元的索引(control word index)：指出目前使用那一個控制字元
(b)控制字元更新的標示(control word change flag)：標示目前控制字元更換的訊息
(c)授權金鑰之指針(authorization pointer)：用於指出目前使用那一把授權金鑰
(d)控制參數：提供節目來源、時間、內容分類和節目價格等節目資訊
(e)加密過的控制字元

此外，安全模組內將會產生一張控制字元的表，用來記錄由 ECM 所定期更新的控制字元資訊。反擾亂器將會透過控制字元索引來指出目前的控制字元為何，才能夠解出正確的節目訊號。

3. 權利管理訊息 (Entitlement Management Message, 簡稱 EMM)：這個訊息中有一把重要的分配金鑰(distribution key, 簡稱 DK)，而這把金鑰通常都是存在於安全模組中(在我們的例子是存在於智慧卡上)。分配金鑰的作用很明顯的是用來加解密授權金鑰(AK)，使用有付費取得授權的用戶可以解出 AK 並進一步解出當時所使用的 CW，之後再與擾亂訊號互斥或成為正常的節目訊號。此外，電視台也可以利用此金鑰 DK 來區分用戶的等級。舉例來說，如果某用戶繳的錢比較多，理應可以收看更多的付費節目，那該用戶的 DK 就必須與其它付費較少的用戶的 DK 不同，以區分用戶之間的等級。除此之外，其它資訊如位址、用戶授權資訊也會藉由 EMM 來傳送，最重要的是，DK 的更新將由 EMM 所負責。最後，整個 EMM 是經由廣播(Broadcast)或以群播(Multicast)等方式送出。

圖 3.4 所示為一階層式金鑰的架構圖，我們假設 DK 存於智慧卡中。由圖中可以看出在時間 T_1 時，該用戶是使用 AK_1 來解開所需要的控制字元 CW_i。之前

有提過，CW 更換的速度相當快，所以在該時間內會有很多 CW。同理，當時間從 T_1 到 T_2 後，原本的 AK_1 被 ECM 更改成 AK_2，而此時的 CW 就要使用 AK_2 來解開，以便進行訊號還原的運作。

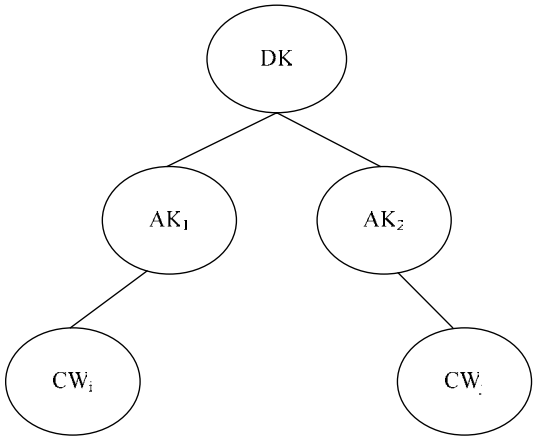

圖 3.4 階層式金鑰架構

3.2.1.4 付費討論

本小節主要是介紹國際標準 ITU 810 條件式接取技術的基本元件、原理及流程。在數位廣播電視中，CAS 是一個很重要的元件，除了可以使得未經授權的用戶無法正確地解出電視節目來以外，在付費電視的環境下，更可以將用戶的等級進行區分。另外，我們的架構不只是簡單的付費系統而已，在結合回傳通道(Return Channel)後，用戶可以透過回傳通道(可能是 Cable 或 PSTN)來點閱自己想看的節目。因此，付費節目又可以分為 Pay-Per-View (PPV) 及 Pay-Per-Channel (PPC)。分別介紹如下：

(a) Pay-Per-View (PPV)：此種付費方式是採取每次點閱一個節目，即收取一個節目的費用。好處是用戶可以決定自己想要觀看的節目或影片，而不用等待想看的節目播放而浪費時間。但缺點就是要額外再多收此次收看的費用。

(b) Pay-Per-Channel (PPC)：由字面即可看出，此種付費電視機制是依頻道來收費，而一般來說，電視台都會有有幾種套餐的型式。例如，可能有一項是基本型的，包括了一些基本的頻道；而用戶可以依需求再追加他所想要的頻道，如 HBO 等。不過用戶必須耐心等待他所想看的節目播出，會比較浪費時間。

上述兩種的付費電視系統，所用到的金鑰問題比我們之前提到的還複雜，如：需要每月或每個星期更換金鑰，或是針對不同群組的用戶提供的金鑰及其階層式金鑰架構的管理問題。場景也比較多變，可以是純 PPC 或 PPV，也可以是混合的型式。更多付費討論請參考第三章。

3.2.2 DVB-CA

在數位電視的環境中，業界通常使用條件式接取系統(Conditional-Access System, CAS)來保護電視台業者頭端至用戶端(Set-top-box)之間的通道安全。而目前主要的 CAS 標準主要是遵循由歐盟 DVB (Digital Video Broadcasting, DVB)組織所制定的 DVB-CSA (Common Scrambling Alogrithm)標準。由於 DVB 只定出擾碼(Scrambling)的標準，並未針對 CAS 其它重要部份如：SMS (Subscriber Management System)、SAS (Subscriber Authorization System)等進行相關規範，所以各家頭端業者此部份都是根據本身公司需求來進行設計自己適用的擾碼系統，而使用 DVB-CSA 只要簽署一份同意書(Agreement)即可。只定義 DVB-CSA 還不夠，為了要使所有業者的擾碼系統都能夠整合在同一個平台，DVB 後來亦定出 SimulCyrpt (DVB-Sim)、MultiCrypt (DVB-CI)等整合技術使得目前各家 CAS 能夠達到相容之目的。另外，美國方面也有其它的 CAS 的選擇—POD (Point of Depolyment)。POD 技術是由北美的 Opencable 公司所制定的。我國已經決定廣播標準要遵循歐盟標準(DVB)，所以 POD 不在我們的討論範圍。

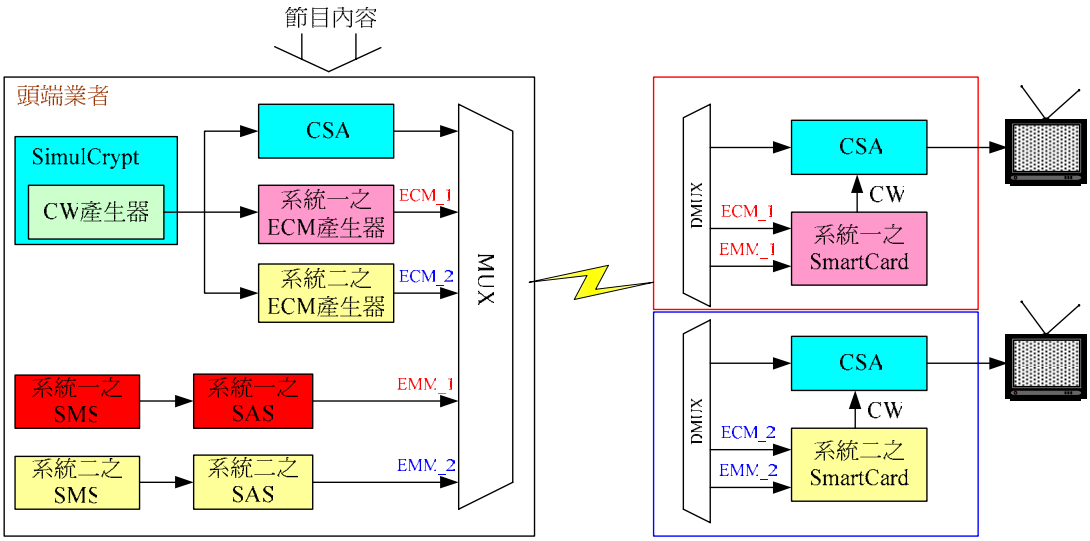

圖 3.5 同密技術示意圖

3.2.2.1 同步加密

DVB 提出了兩種整合的方法，一種是從頭端來進行整合，也就是 SimulCrypt(同密)；另一種就是從使用者端的機上盒進行整合，稱為 MultiCrypt(多密)。同密技術最主要的精神在於以系統頭端來進行整合，每家業者所提供的 CAS 都必須要使用之前提過的 DVD-CSA 並配合同一個控制字元(CW)以便進行共同擾碼。各家 CAS 廠商必須使用同樣的控制字元以及共同的擾碼技術，但是之後的 ECM、EMM 等有關於使用者的重要訊息都由自己產生，每家廠商根據所提供的服務及方式等不同而自行產生對應之 ECM 與 EMM。如

圖 3.5 所示。

由圖 3.5 中可以清楚看出，藉由同一組的控制字元可以產生兩組不同的 ECM 與 EMM 訊息。而使用者只要把自己機上盒之 CAS 對應到的 ECM 及 EMM 解多工後即可以解出一樣的控制字元，進而解擾碼並在電視螢幕播放。但是這也意味著一個風險，當電視台業者的 CAS 廠商更換時，使用者的機上盒的 CAS 也就不能再使用，勢必得更換另一台機上盒才能繼續收看該電視台的節目。換句話說，如果使用者的機上盒只有單一的 CAS 的話，則此技術無法達到跨區的服務，不同的廣播端所使用的控制字元不同將會造成機上盒(只有一種 CAS)無法順利運作。同密技術的作法是將成本幾乎都加在電視台業者這一端，使得使用者的機上盒可以越簡單越好。

3.2.2.2 多重加密

不同於同密技術，多密技術則是在接收端來進行整合的工作，目的在使接收端可以處理不同的 CAS 的訊息(ECM、EMM)。DVB 在 DVB-CI(Common Interface)有相關規定。藉由在機上盒的智慧卡模組的抽換來達到不同的 CAS 的相容，而這樣可抽換的模組以及機上盒的通訊就是由 DVB-CI 來規範，以達到機卡分離(機上盒和智慧卡不用綁在一起，不同於之前的同密技術)。顯而易見的，可抽換的模組可以解決不同的 CAS 的跨區問題，也可以收視不同業者的節目，但其操作卻不方便。除此之外，可抽換的 CI-Module 價格昂貴，使用者如果要收看三家電視台業者(使用不同的 CAS)的節目，則必須要購買三家不同 CAS 的 CI-Module 才可以。此種技術目前只有歐洲某些地區的用戶為了跨區才會採用的解決方式，一般的應用都會因為價格的原因而選擇其它的整合方法。

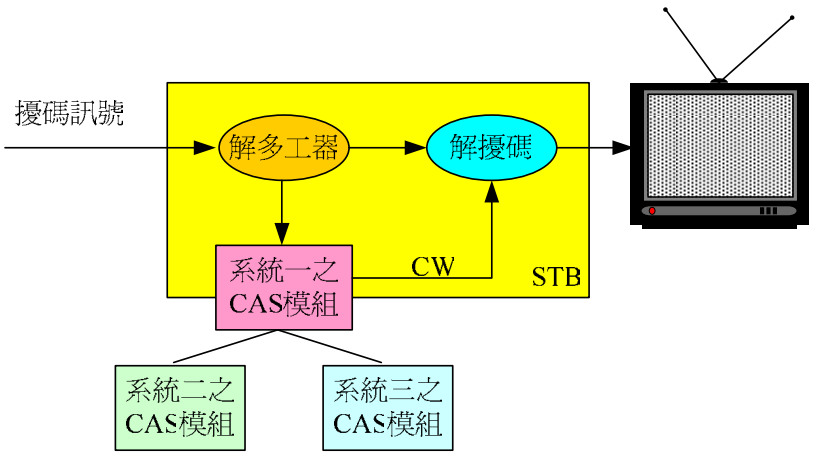

圖 3.6 多密示意圖

圖中所示之系統二之CAS模組使用時機為該使用者欲觀看系統二(另一家電視台業者)的節目時，必須進行更換的動作。在使用上相當不方便。另外，在接收端進行整合的另一種可行方式為更新軟體。可藉由DVB所規規管的DVB-Data

Download 來對機上盒中的中介軟體進行更新，使得只要更新後，就可以使用於新的 CAS 系統。此種方式相對於上述的更換 CI-Module 的方式更有彈性並操作方便，並且也有開放的標準，機上盒的製作會容易。

3.3 條件式接取技術討論與建議

目前台灣的廣播電視都還是 Free-on-Air，也就是都是免費收看。使用者目前並不需要在機上盒中插入智慧卡等身份辨識的卡片來進行訂閱及付費的功能。但是如果考慮之後要加入這些如 PPC 及 PPV 等加值功能時，智慧卡勢必成為相當重要的一個元件。除此之外，整合的問題也會隨之而來，不同的電視台業者所使用的 CAS 也會攸關機上盒的成本。在 4.3 節中討論的兩種整合方案各有優缺點，同密技術有成本的優勢，對於消費者來說有一定的吸引力，但有跨區的問題以及更換機上盒的風險是它的缺點。而多密技術的硬體整合方案將使成本大大的提高並轉嫁至消費者身上是其主要的缺點，但卻可以使得同一接收端接收不同 CAS 發出的 ECM 與 EMM 訊息。而多密的另一種為軟體解決方案則可以有效的降低機上盒的成本，操作也簡便，但是如果各家電視台所發行的智慧卡無法通用的話，此種方式依然無法順利的運作。以下為在使用通用的智慧卡時，同步加密及多重加密的比較表。

表 3.2 同步加密及多重加密比較表

智慧卡模式	使用通用的智慧卡		
採用整合方法	同步加密	多重加密	
		硬體方法	軟體方法
頭端成本	高	低	低
接收端成本	最低	高	低
機卡分離	無	有	有
跨區問題	有	無	無
操作方便	最好	差	好
使用者風險 (更換機上盒)	有	無	無
缺點	跨區問題 (接收端為單一個 CAS)	模組成本高並限制於 CAS 廠商	需常更換機上盒上的 CAS 軟體
規格	DVB-Sim	DVB-CI	DVB-Data Download

表中並無列舉沒有使用通用智慧卡的比較項目。如果無通用的智慧卡時，各家電視台業者都會發行屬於自己的智慧卡。對於消費者而言，這將造成一定程度的不方便；如果某消費者 A 只有購買某家電視業者的智慧卡時(目前台灣是免費收

看，所以也不會有智慧卡及機上盒問題)，他將無法付費收看其它電視台所播的節目。因為在付費的情況下，所購買的智慧卡勢必要和機上盒綁在一起，其它不同業者的 CAS 系統就無法以同一張智慧卡來解密並順利收看，必須依靠上述的三種方法來解決。根據以上討論及介紹，我們提出了一種最佳的建議以供參考。在之後有付費的數位廣播電視環境中：

1. 建議各家電視台業者成立相關單位來通用之智慧卡
2. 建議在頭端系統中，支援同步加密(SimulCrypt)
3. 建議在接收端(機上盒)，支援多重加密(MultiCrypt)，並以軟體方式為佳

如此一來，不僅可以解決跨區的問題，也可以避免頭端設備受制於 CAS 廠商的問題。重要的是，如果智慧卡可以通用的話，就算智慧卡上的 CAS 是不同的，也只要透過軟體方式來更改機上盒上的 CAS 軟體就可以繼續收看該 CAS 所擾碼的內容，並不需要更換機上盒。

3.4 數位智慧財產權管理介紹

由於數位內容非常容易在網際網路中傳播，這將造成數位內容的版權受到嚴重威脅。所以，內容供應商、技術公司和決策者開始想要解決有智慧財產權數位內容的保護和使用數位內容權利的管理。在1994年1月在網路多媒體中保護智慧財產權的技術會議(Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment conference)中，提出數位智慧財產權管理(Digital Rights Management, 簡稱DRM)這個名詞，之後慢慢的被商業採用。而數位智慧財產權管理主要是要使得數位內容在生命週期間（產生到消失）都受到保護和管理。所以數位內容的散佈有五個主要的角色：內容創作者、內容提供者(授權)、內容散佈者、內容消費者和加入DRM的平台製造商。如圖3.7所示。

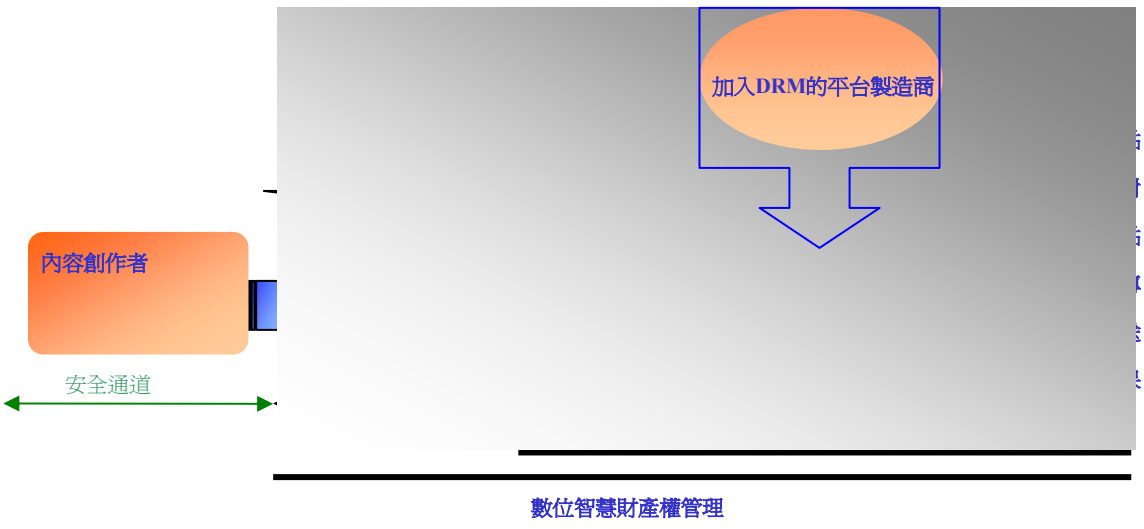

圖 3.7 數位內容散佈圖

- 內容創作者：創作物的產生者，如：作者、導演...等。
- 內容提供者(授權)：被創作者授權可以擁有創作物使用的權利，如：代理經銷商、三立電視台...等。
- 內容散佈者：擁有散佈器材去提供創作物的散佈，如：出版商、第四台業者。
- 內容消費者：消費創作物的人，如使用者...等。
- 加入DRM的平台製造商：製造有DRM功能，可以開啟數位內容的機器，如機上盒(set-top box)、手機、PDA…等。

而數位智慧財產權管理普遍有下列兩個定義：

- 狹義定義：為數位智慧財產權管理一開始的定義，主要集中在數位內容安全上的持續保護(persistent protection)。使用密碼學的技術來達到安全上的保護，通過加密技術來保護數位內容。若要存取數位內容，會先驗證該身份是否有存取權限，確定身份之後發給許可授權(License)，授權上會有對此數位內容權利的描述以及如何執行此數位內容。
- 廣義定義：這是目前的定義，不只是對數位內容做持續的保護，還要對數位內容進行交易、監控和追蹤。引述國際數據資訊(IDC)機構對數位智慧財產權管理的定義---"結合硬體與軟體的存取機制，將數位內容設定存取權限，並與儲存媒體結合，使得數位內容在生命週期間（產生到消失），不管使用過程中，是否被複製到別處，仍可以持續追蹤與管理數位內容的使用情況"。也就是說，在數位內容生命週期間，能提供完善的保護和管理的技術。數位智慧財產權管理的技術主要目的是為了能達到事前防護的安全管理，將數位內容加密、簽章，並設定使用者存取控制以及追蹤行為，在數位內容生命週期，不會被隨意複製、竄改、散佈，保障數位內容的完整性以及機密資訊的保密性。

3.4.1 數位權利管理模型

DRM 技術中最重要的就是權利模型的管理，權利上可以分為：

- 權利的使用和權限：保護了那些權利，有什麼權利可以使用，可不可以拷貝、列印、散佈...等。如圖3.8所示。
  - 使用的權利：列印、觀看、執行。
  - 傳播的權利：拷貝、移動、借。
  - 修改的權利：摘錄、編輯、嵌進。

- 權利的執行：若非法的存取內容，就有法律上的規範加上嚴懲。
- 權利的管理：使用權利的管理。
  - 法律上
    - 使用註冊的形式，取得許可授權來存取內容。

- 使用版權公告(Copyright Notice)或浮水印(Watermarking)來做以後爭議的查核足跡。

◆ 技術上

- 運用密碼學的技術，使用加密和身分認證的技術來保護內容，在描述嚴格的條件才能存取。
-

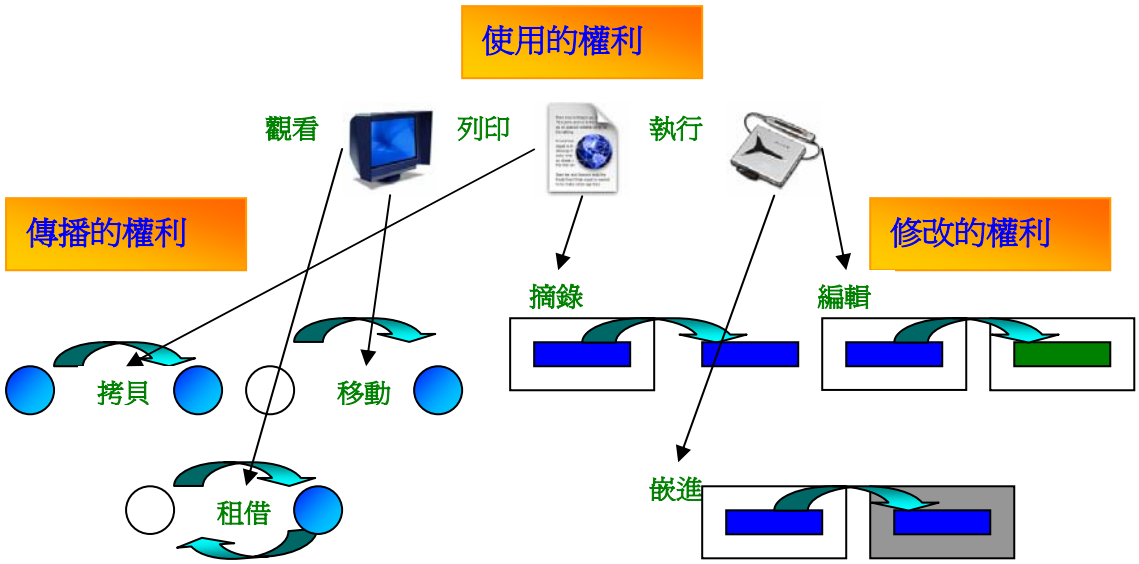

圖3.8 權利的基本類型

3.4.2 數位智慧財產權管理系統之基本架構

DRM 系統廣泛的來說包含內容和所連結權利的認證和使用限制執行，對每一個內容都要有唯一的識別符(Identifier)，就像實體書本的 ISBN，或在內容上嵌入標誌，就像圖片上的浮水印，都是為了要能夠認證內容，連結權利的描述依賴權利描述語言(Rights Expression Languages)來實現。而使用限制執行是靠著加密和金鑰的管理的技術，不同權限的人給予不同等級的金鑰，所以，所能使用的權利也就不同。

DRM系統是一連串硬體和軟體的服務技術在數位內容生命周期的管理，所以任何DRM系統架構都是由不同的標準化技術領域所組合起來的，可以從兩個觀點來看：

■ 結構觀點來看：有三個主要的技術元件分別在內容伺服器端、使用者端和認證伺服器端：如圖3.9所示。

◆ 封裝元件(Packagers)：放在內容伺服器端，由內容貯藏處取數位內容和描述資訊(metadata)封裝在一起的技術。描述資訊是描述數位內容的相關資訊，如產生時間，擁有者是誰...等。

◆ 控制元件(Controller)：放在使用者端，主要在做認證、存取控制、

解密...等技術。

- 許可元件(License Generator)：主要是創造和傳送加密的許可憑證，裡面會有解密金鑰和權利描述。

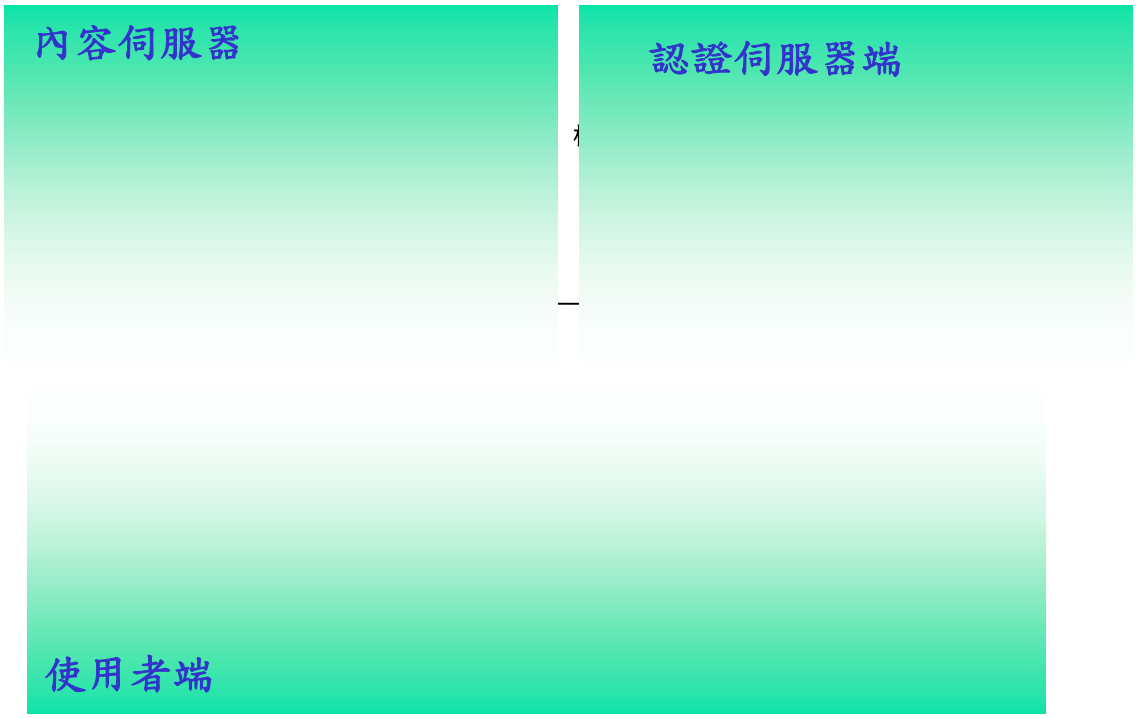

圖3.9 DRM系統基本結構示意圖

- 功能觀點來看：如圖3.10所示。
  - 內容的創造和取得：當內容第一次創造或再使用時，內容所連結的權利如何管理。
    - 權利的認證：對內容做認證的動作。
    - 權利的工作流程：對於權利的同意，允許內容在一連串工作流程中操作。
    - 權利的創作物：對新的內容分配權利，如描述權利擁有者和使用的允許。
  - 內容的管理：如何去管理內容和交易內容的技術。
    - 貯藏處：在可能在的幾個資料庫能夠去存取內容和描述資訊(Metadata)。
    - 交易：能夠去分配憑證(Licenses)，根據憑證進行付費的動作。
  - 內容的使用：如何去管理內容的使用。
    - 同意的管理：能夠在使用環境中去允許權利連結內容，如假如你只有權利去看文件，你就不能列印。
    - 追蹤的管理：能夠去追蹤內容的使用狀態，也要能跟交易系統做相容性，因為要去記錄使用狀態再進行付費機制。

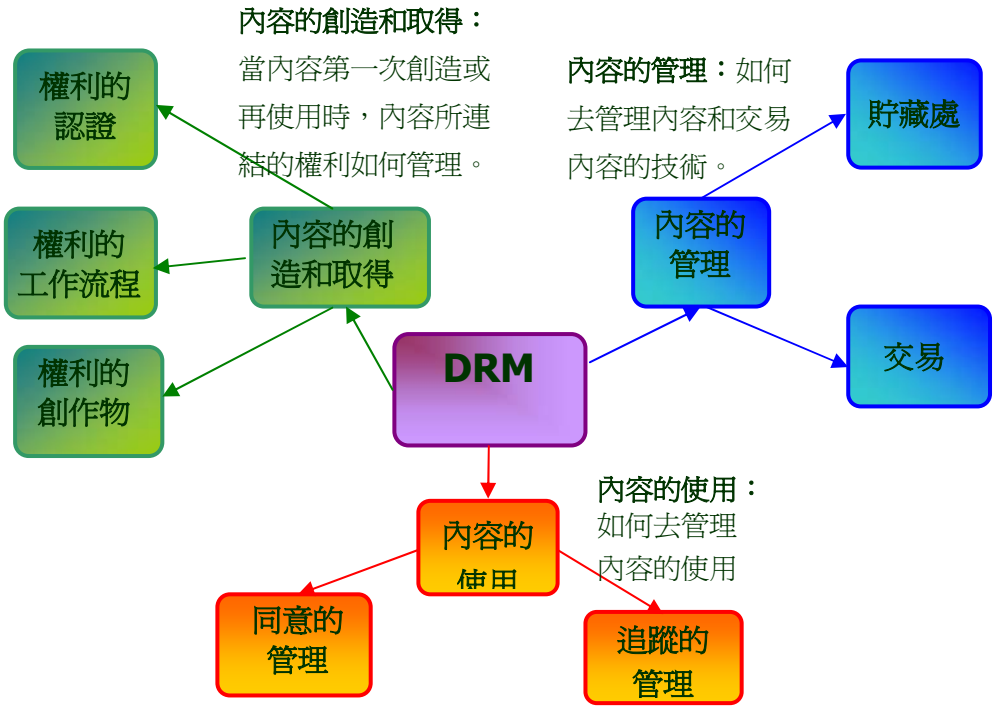

圖3.10 DRM系統功能結構

3.5 DRM核心技術

在 DRM 的核心技術中分為密碼技術和商業技術，其內容又分為：

- 保護機制：
  - 權利描述語言(Rights Expression Language,REL)：
    1. eXtensible Rights Markup Language (XrML)
    2. Open Digital Rights Language (ODRL)
  - 多媒體技術
    3. MPEG-2 CA (conditional access)
    4. MPEG-4 IPMPX (Intellectual Property Management and Protection eXtension)
    5. MPEG-21
  - 內容保護的整體架構(A Comprehensive Framework for Content Protection, CPSA)
    - 拷貝保護(Copy Protection)
      6. 內容加密系統(The Content Scrambling System, CSS)
      7. 事先儲存多媒體的內容保護(The Content protection for Prerecorded Media, CPPM)
      8. 重複儲存多媒體的內容保護(The Protection for Recordable Media, CPRM)
      9. 數位傳輸內容保護(The Digital Transmission Content

Protection, DTCP)

- 加解密技術(Encryption/Decryption)：
  10. 高等加密標準(Advanced Encryption Standard, AES)
- 盜拷追蹤與隱私權技術(Traitor Trace and Privacy)
  11. 浮水印和指紋技術(Watermarking/Fingerprinting)

◆ 條件存取(Conditional Access)

◆ 相容性技術

◆ 公開金鑰的基礎建設(Public Key Infrastructure, PKI)

- 金鑰分配技術(Key Management)
- 認證技術(Authentication/Identification/Signature)
  12. 訊息摘要演算法(Message-Digest Algorithm, MD5)
  13. 安全雜湊演算法(Secure Hash Algorithm, SHA)
  14. RSA數位簽章系統

■ 付費系統(Billing system)：

◆ SET

◆ 3-D Secure

◆ NetBill

◆ eCash

3.6 領導的標準與相關組織

隨著越來越數位化媒體的出現，擁有一個先進的多媒體解決方案就變得至關重要。這不僅是技術上的考慮，同時也是個人應用的需要。所有內容提供商都有共同的關注目標：內容的管理、版權的保護、對非授權接入和修改防範以及對於內容提供商和使用者隱私的保護。目前世界上有很多組織共同的來發展各類的DRM技術，包括了有軟硬體保護技術、數位內容案件研究、電子刊物、影音部份以及DRM的整合工作，如表3.3所示。

表3.3 各組織目前現況

組織名稱	國家	成立時間	研究方向	成果/標準	其它
SVP (Secure Video Processor)[13]	歐洲	2004	數位視訊硬體(set-top box)保護		實體保護為主
Electronic Frontier Foundation (Broadcast flat)[14]	美國	1990	研究政府及企業利用特殊技術來侵犯人權的事件	許多智慧財產權相關案件[15]	

Open eBook forum[16]	美國	1999	電子刊物之促銷與發行	1.Rights and Rules WG(技術報告)[17] 2.Publication Structure WG v1.2(技術報告)[18]	
cIDF (Content ID Forum)[19]	日本	1999	數位內容管理保護	cIDf2.0 Specifications (標準)[20]	
Coral Consortium [21]	美國	2004	DRM 整合技術	Coral Consortium v1.0 specifications (NEMO)	只能找到 NEMO white paper 版本[22]
The 4C/5C Entity	美國		5C Entity主要研究安全上的傳送，如IEEE 1394。而4C Entity主要研究安全上的儲存。		這組織是由IBM、Intel、Matsushita, Toshiba/ Hitachi所組成
Open Mobile Alliance (OMA)[7]	歐洲	2002	主要為移動產業發佈公開的規格說明書	OMA的DRM 1.0版和2.0版都定在2005年公佈[33]	
MPEG (Moving Picture Experts Group)[23]	歐洲	1988	主要是做數位影音的標準，對數位智慧財產權管理相關的標準有MPEG-2 CA和PART 11、MPEG-4 IPMP、MPEG-21	IPMP (Intellectual Property Management Protocol) [23]	
DMP (Digital Media Project)[24]	歐洲	2003	DRM整合技術	Interoperable DRM Platform (IDP)[25]的工作草案規格，目標有三個階段，在2005年五月已經發表了階段1	

3.7 現行產業發展現況

目前DRM的發展尚在起步階段，主要業者包括Microsoft、IBM、Nokia、RealNetworks、Sony、AOL、Yahooc！、DRM Network、SpeedEra、Verizon、Lerizon、Listen.com、Liquid、Audio、Lycos等。主要分為四類：

- DRM平台代理商(IBM、Microsoft)：提供DRM技術平台，讓使用者的網站或系統，能夠擁有部份的DRM功能，加以控管。
- DRM授權代理商(Intertrust、MPEG LA)：運用專利優勢，讓想涉入此領域者都需經過其公司授權，藉以收取權利金。

- DRM產品供應商(Authentica、Alchemedia、Neovue)：提供DRM產品。
- DRM服務供應商(ContentGuard)：提供伺服器端，利用對話方式讓使用者端可以透過該伺服器來運作DRM技術。

而以相關技術領域來分，可以分為幾個產業：

- 傳統多媒體產業：
- 網際網路服務產業：Microsoft、Apple、Sony、RealNetworks…等。
- 行動手機產業：Nokia、CoreMedia、DWS、Symbia、SDC…等。
- 數位電視廣播產業：Philips…等。

3.7.1 商業行為的DRM系統

市面上DRM系統產品或是商業上可接受的DRM系統。

3.7.1.1網際網路服務產業(線上音樂)

由於數位媒體檔案有可輕易地複製與分佈，並且不會流失任何內容品質的特性，在沒有妥善的安全性措施來保護內容時，盜版一直是令人擔憂的問題。因此，保護音樂檔案版權的問題更是顯得越來越重要。近來，MP3 撥放器多已加入 DRM 技術來保護音樂著作版權。如圖 2.11 所示。

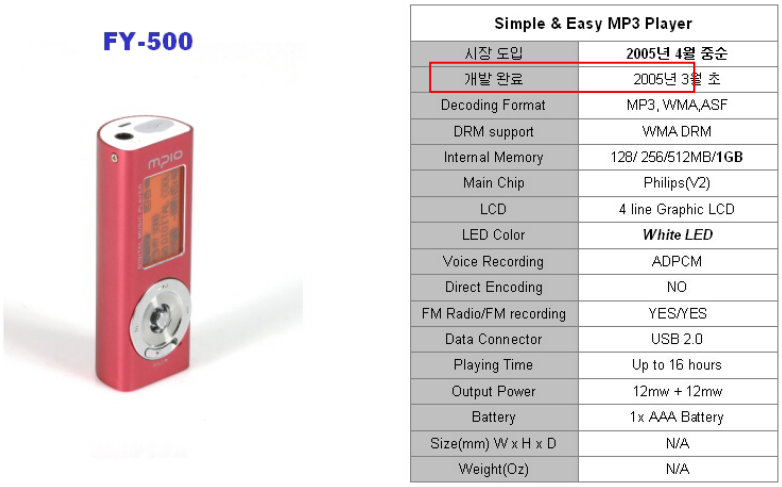

圖 3.11　MP3 撥放器規格圖(圖片來源：太平洋電腦網[31])

目前主要致力於線上音樂的 DRM (Digital Rights Management)技術的廠商有：微軟(Microsoft)、蘋果電腦(Apple)、RealNetworks 以及索尼(Sony)等幾間公司。下表為各公司開發的 DRM 平台技術。如表 3.4 所示。

表 3.4 各公司開發的 DRM 平台技術

公司	技術
Microsoft	WMDRM (Windows Media DRM)[12]
Apple	FairPlay(已被破解[26, 27])
RealNetworks	Helix DNA[28]
	Harmony*
Sony	OpenMG

*表中之 Harmony 為 Realnetworks 公司為了各個 DRM 技術(除了 Apple 公司之 FairPlay)所開發出來的平臺。

而在此期初報告中，由於 RealNetworks 公司之 Helix DNA、Harmony 以及 Sony 公司的 OpenMG 資料蒐集不易，所以我們將先針對 WMDRM (Microsoft)以及 FairPlay (Apple)兩個大廠的技術來分析比較，試著找出在線上音樂這個應用領域中，其主要的模型、交易流程以及所使用的密碼原件等等相關技術內容。

3.7.1.1.1 WMDRM

微軟的 WMDRM 技術始於 1999 年，發展至今已經是第五個版本了(WMDRM 10)。而著名的線上音樂供應商 Napster 也是採用此套 DRM 技術來保護該網站的數位音樂。如圖 3.12 所示。

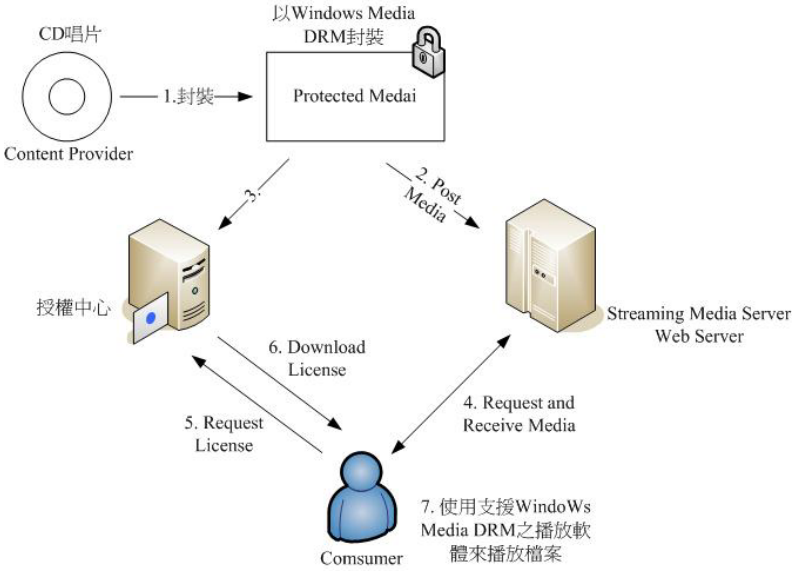

圖 3.12 WMDRM 流程示意圖

傳統的 CD 唱片經過封裝的程序封裝成副檔名為 wmv 或 wma 等型式的檔案後，分佈(Distribution)至串流媒體伺服器(Streaming Media Server)以及在網站伺服器(Web Server)提供該檔案的資訊(如歌曲演唱者)。接下來則會把相關的

授權資訊傳給授權中心。而消費者在瀏覽歌曲網頁(網站伺服器)時，購買他想要的歌曲後，消費者會被引導至授權中心去取得該歌曲的相關權限(可能透過帳號登入等方式來確認消費者身份後，給予權限)。最後消費者就能撥放該歌曲或是進行備份等動作(依授權中心所給的權限)。而 WMDRM 技術中最重要的封裝及解密過程。如圖 3.13 所示

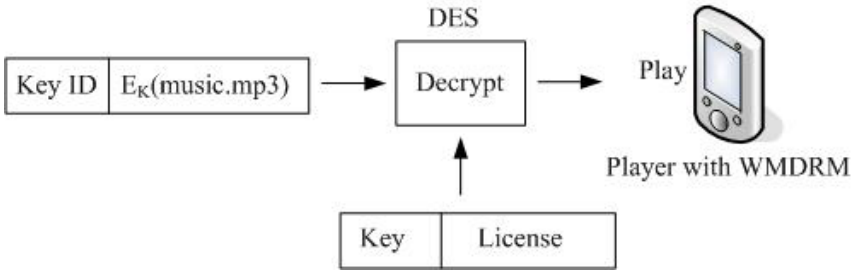

圖 3.13 封裝解密示意圖

封裝檔案時，Content Provider 利用 License key seed 及 Key ID 產生的 Key 來封裝欲保護的音樂檔案(music.mp3)。而授權中心會根據此 Key ID 及已知的 License key seed 來產生對應的加解密金鑰 Key。之後消費者根據所下載的 License(步驟六)來解開被保護的檔案，進行撥放等動作。以下為流程細節：

(1). 封裝：Windows Media Rights Manager 會先以金鑰封裝數位媒體檔案，這個金鑰會儲存於加密授權中，並且個別分佈。其他資訊也會新增至此數位媒體檔案。如：取得授權的 URL。

(2). 分佈：封裝檔案可放置在網站上以供下載、放在數位媒體伺服器上以供串流處理，以 CD 傳播，或是以電子郵件寄給消費者。Windows Media DRM 也允許消費者傳送具有「版權保護」的數位媒體檔案給朋友。

(3). 建立授權伺服器：授權交換中心的角色是用來驗證消費者對於授權的要求。數位媒體檔案與授權會個別分佈與儲存

(4). 取得授權：消費者必須先取得可將檔案解密的授權金鑰才能播放檔案。當消費者嘗試取得封裝數位媒體檔案、取得先前已傳送的授權，或是第一次播放檔案時，取得授權的程序就會自動開始。Windows Media Rights Manager 會將消費者帶至要求提供資訊或付款的註冊網站。

(5). 播放數位媒體檔案：若要播放數位媒體檔案，消費者需要有支援 Windows Media DRM 的播放程式。之後，消費者就可以根據包含在授權中的規則或權限(如：開始時間及日期、播放時間及計數作業等)播放檔案。而預設權限可能會允許消費者在特定的電腦上播放數位媒體檔案，以及將檔案複製到可攜式裝置中。若消費者將保護的檔案傳送給朋友，這個朋友必須取得他自己的授權才能播放該檔案。而在每台電腦逐一授權的配置，可確保唯有擁有封裝數位媒體檔案授權金鑰的電腦，才能播放該檔案。

3.7.1.1.2 FairPlay

蘋果電腦(Apple)是第一家致力於線上音樂保護的廠商，而該公司所販賣的數位音樂撥放器 iPod 更是眾所皆知，在美國的數位音樂撥放器市場更是佔了50%之多。Apple 的 iTunes 網路商店(iTMS)透過 Fairplay 將音樂檔案加密成 AAC 格式，而在 Apple iTMS 上購買的音樂，可以經由 Windows 或 Mac 平台的 iTunes 軟體下載到最多三台電腦的硬碟上，也可以自由下載到 iPod 上來進行撥放等動作。另外，除了 iPod 和 iTunes 之外，別的機器或軟體不能播放這個從 iTMS 合法購買而下載的音樂(限定在 Apple 的專屬產品領域內才能使用)。由此可知 Apple 不讓經由其它廠商的 DRM 加密過的合法下載音樂在 iPod 或 iTunes 上播放，Apple 在這個目前它幾乎獨霸的合法線上下載音樂的市場內，拒絕和其它廠商合作(如：RealNetworks，Apple)。FairPlay 的運作流程。如圖 3.14 所示。

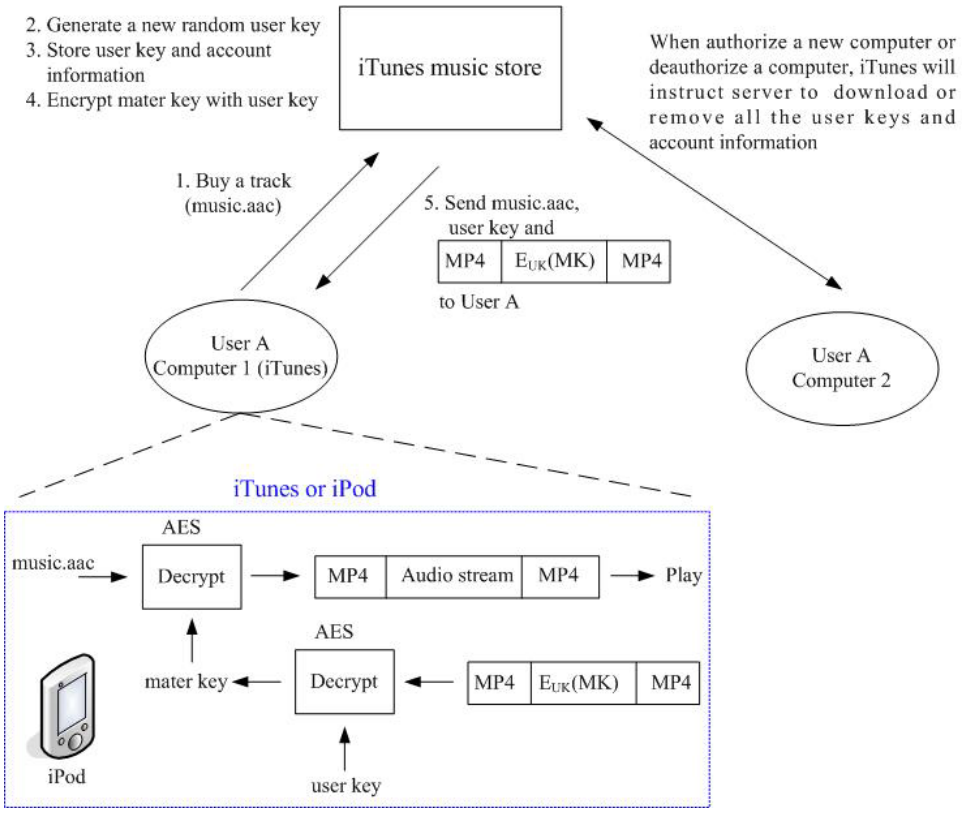

圖 3.14 FairPlay 流程示意圖

iTunes music store (iTMS)為蘋果的線上音樂交易的網路商店。而當使用者 A 在網路商店 iTMS 買了一首歌(music.aac)後，iTMS 會將 music.aac、user key 以及 E_{UK}(MK) 等資訊給使用者 A。一旦使用者 A 獲得上述資訊後，會先以 User Key 將 Master Key 解出來，再將 music.aac 檔案解開並進行撥放。使用者 A 如果之後在別台電腦(Computer 2)想要撥放已下載的檔案時，iTMS 會將該用戶的所有 User Key 及其它相關資訊一起送給該用戶，使得使用者 A 一樣能撥放已下載的檔案而不用再一次的付費。而這類的服務通常會限定同一個使用者能在幾台

不同的電腦(或裝置)上撥放。

表 3.5 WMDRM 及 FairPlay 比較表

公司	技術	資料加解密技術	相關權限內容
Microsoft	WMDRM	DES、RC4	1. 只允許不同的三台電腦(裝置)撥放 2. 只能在支援 WMDRM 的撥放器中撥放
Apple	FairPlay	AES、MD5	1. 只允許不同的五台電腦(裝置)撥放 2. 只能在支援 FairPlay 的撥放器中撥放(目前只有 iPod)

而目前在國內也已經有線上音樂商店的產生---Immusic。如圖 3.15 所示：

圖 3.15 Immusic 交易流程示意圖 http://www.imusic.com.tw/

由於這部份資料蒐集不易(未公開)，不過主要架構應與微軟的 DRM 技術(WMDRM)相去不遠，必須要有特定的撥放軟體(iPlayer)或硬體來支援此 DRM 技術。

3.7.1.2. OPERA

OPERA 平台的目的是為了介於各個不同 DRM 系統之間能夠相互溝通，而 OPERA 定義了許可證管理層，此層取代了現今 DRM 系統的許可證管理，而 OPERA 也整合了多個 DRM 系統，以及使用了它們的密碼與金鑰的管理工具。

在 OPERA 技術中，我們將保護層（或稱為執行層）和許可證管理層分開，並且用 Demonstrator（指示）表示技術的基本特徵。Demonstrator 的理論是 2003 年由柏林的 IFA、阿姆斯特丹的 IBC 和 Eurescom 所發表的。對於 Demonstrator 的發展現況，我們專注於 OPERA Proxy 和 OPERA Server 的說明。

OPERA Proxy 負責的是使用者環境的管理，包含了認證以及經由手機端認證方面。OPERA Server 主要在於負責獨立的許可證管理系統。對於 demonstrator 來說，有以下六點說明特徵：

（1） 使用者登錄
（2） 許可證的儲存
（3） DRM 系統產生許可證
（4） 監視使用者介面的許可證
（5） 購買內容的登錄
（6） 監視購買介面的許可證

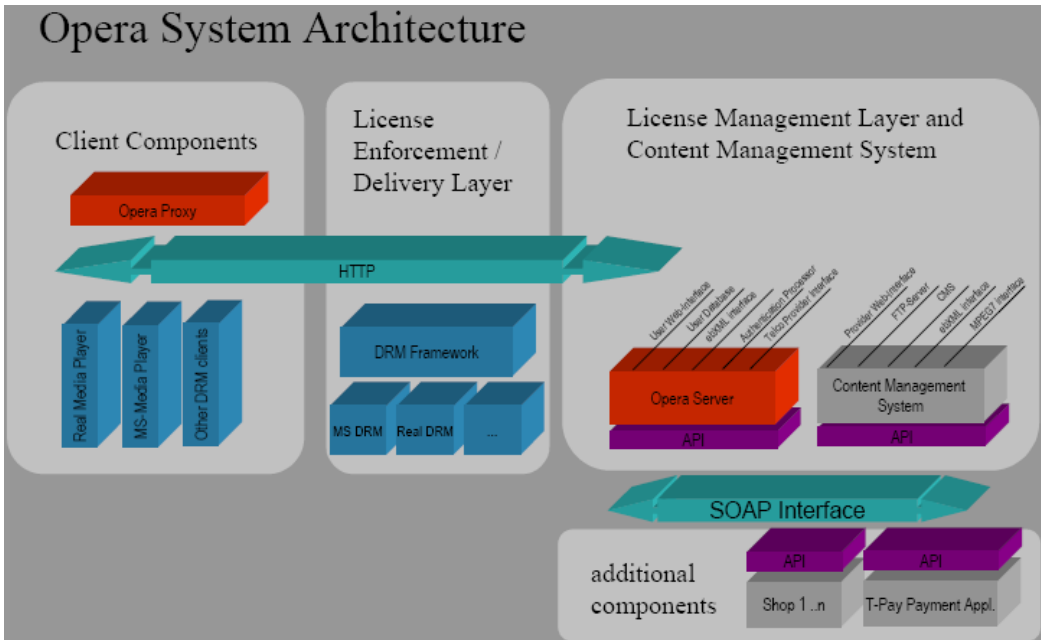

圖 3.16　OPERA 組成架構(取自[45])

（一）OPERA 技術：

OPERA 物件主要的目標是具體說明在不同 DRM 系統之間的功能，所以提供了兩點特徵：

（1） 使用許可證是獨立於 DRM 系統之下
（2） 許可證會被送到使用者的設備

為了達成這些功能，OPERA 整合了主要的 DRM 系統，或者使用可方便得到的 DRM 架構。在這些技術之上，OPERA 許可證管理也增加了兩點基本的想法：

（1） 使用者用 SIM-Card 或手機號碼進行安全性認證。

（2） 使用的規則是建立在每個 DRM 系統的許可證模組上。

也就是說我們區分了 DRM 系統下的許可證，以及 OPERA 的許可證。當 OPERA 許可證支援多個使用規則時，則必須要從 DRM 系統下得到『一次性』的許可證。如圖 3.16 所示

（1） 客戶端成員：

I. OPREA Proxy：主要負責使用者與 OPERA 伺服器間的連線。

II. DRM Player：可允許使用者觀賞它們所購買的內容。

（2） 伺服器端成員：

I. 許可證管理層：負責管理使用者得到的使用權。

II. 許可證傳輸和執行層：在 DRM 系統下傳送許可證，並且而送到正確的使用者手中。

III. 內容管理層：用來描述實用的介面，以及影音設備的管理系統。

（3） 額外的成員：

I. 購買機制：用來透過網路功能購買內容。

II. 付費機制：通常是屬於購買機制的一環，有時也會分開來使用。

III. 內容傳輸系統：支援內容的下載。

（二）OPERA 核心：

在 OPERA 物件中主要核心為 OPERA Proxy 及 Server。OPERA Proxy 使用 SIM-Card ID 或者伺服器資料庫來認證，並且將認證資訊送給 OPERA Server 進行確認的工作。如圖 3.17 所示。

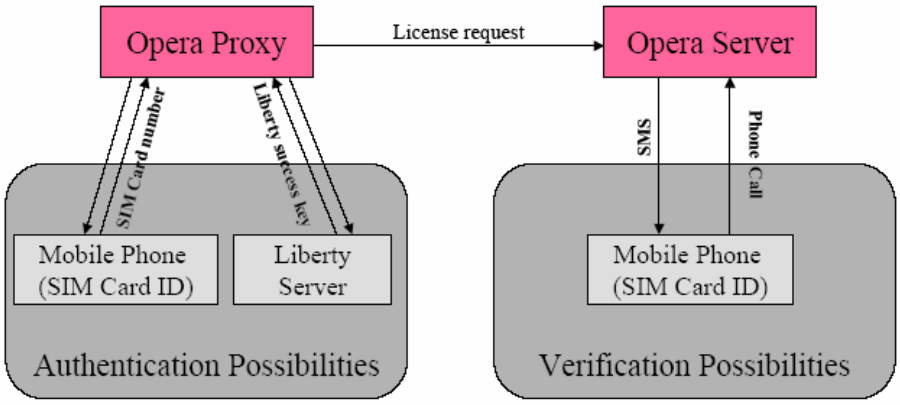

圖 3.17 核心示意圖(取自[45])

（三）Demonstrator 組成架構：(如 3.18 所示)

對於 Demonstrator 有兩個 OPERA 技術的核心成員：

（1） OPERA 許可證伺服器（又稱 OPERA 伺服器），屬於 Server 端的許可證管理層。

（2） 客戶端的 OPERA Proxy。

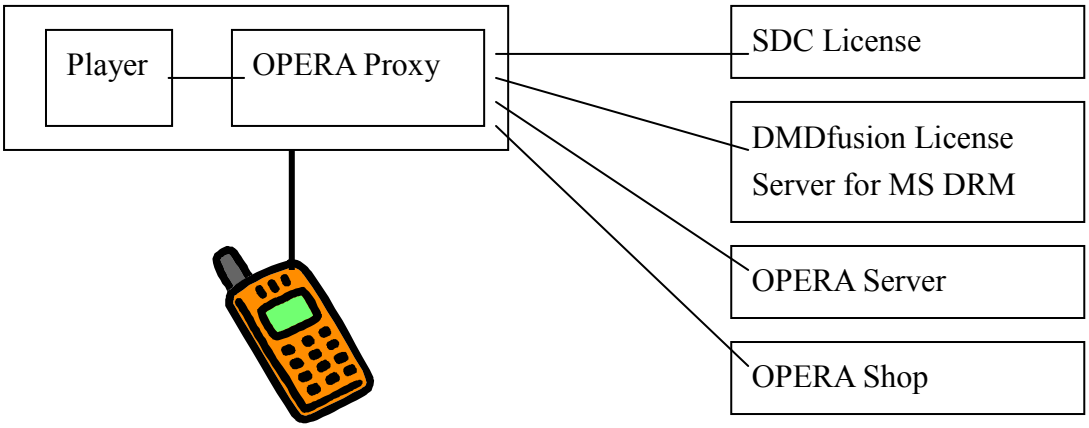

圖 3.18 Demonstrator 簡易架構圖

圖 3.19 為 Demonstrator 的工作流程。許可證伺服器是整合 DRM 系統的伺服器，DRM 的客戶端及播放器則是架設在使用者的環境下，而在此先假設使用者已經選定好想購買的內容，以及購買許可證，而許可證也已經登錄於 OPERA Server。

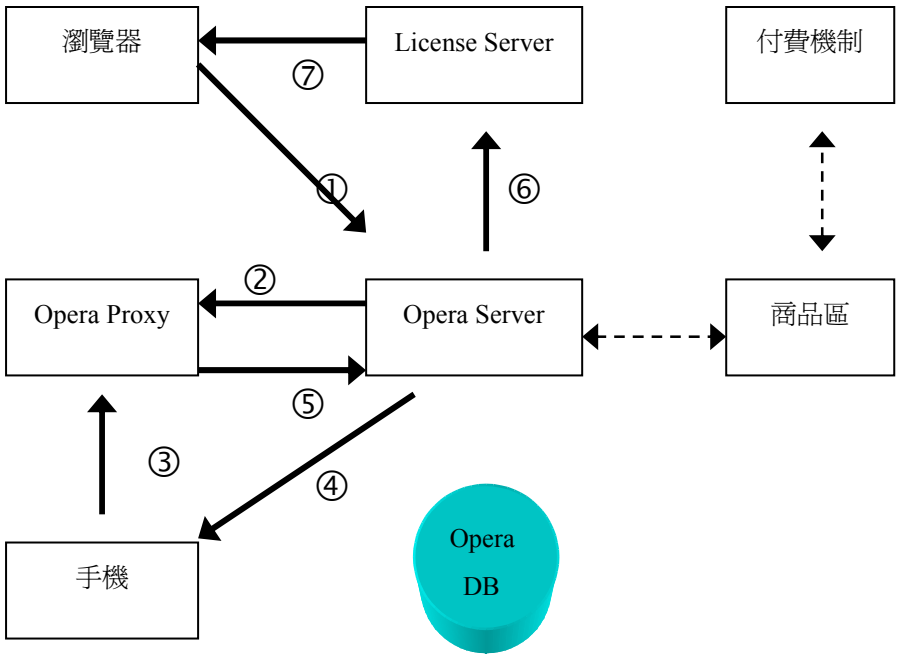

圖 3.19 Demonstrator 工作流程

Step：

1. 使用者在線上瀏覽內容，購買觀賞的許可證。
2. 客戶端的設備被要求確認使用者的身份。

3. 客戶端提供 SIM Card ID 給 Opera Server 來認證使用者身份。
4. Opera Server 產生一個金鑰，並且利用 SMS 送給手機。
5. 使用者的設備再將金鑰經由 Opera Proxy 送回 Opera Server。
6. Opera Server 承認使用者對內容的使用權，並且產生『一次性』的使用許可證。
7. License Server(例如 Real DRM)送『一次性』的使用許可證給播放設備。

（四）許可證管理協定：

OPERA Proxy 和 OPERA Server 是透過許可證管理協定相互聯繫，在此協定下，許可證的確認會被選取，並且執行。而 Demonstrator 是利用 SMS 的回傳機制來完成許可證的確認。

使用者藉由 OPERA Proxy 來要求許可證，而此時 OPERA Proxy 會讀取使用者的手機 SIM-ID 來確認身份，接著再向 OPERA Server 要求許可證。當使用者擁有許可證後，OPERA Server 會送出一串亂數給使用者端，並且用回傳亂數做確認的動作。圖 3.20 為 OPERA Proxy、Server 和手機端的聯繫方式。

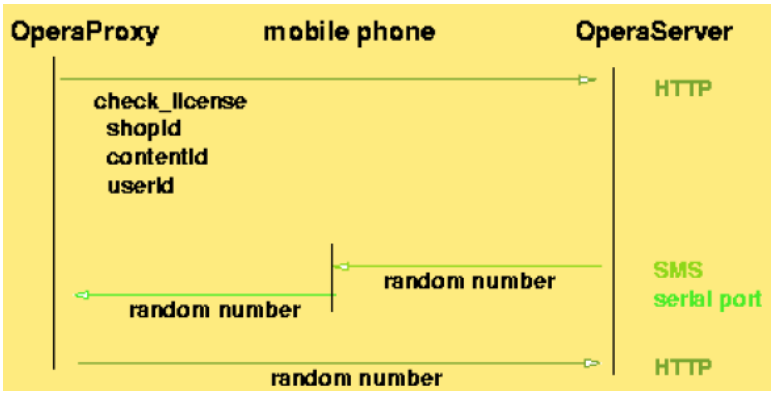

圖 3.20 OPERA Proxy、Server 和手機端的聯繫方式(取自[45])

（五）經由 HTTP 溝通的管道：

許可證確認的工作流程包含了幾個媒介：

（1） 播放器，是最初許可證要求者，以及最後接收解密金鑰。
（2） OPERA Proxy，居中協調手機與 OPERA Server 的聯繫。
（3） 手機，擁有 SIM-ID。
（4） OPERA Server，握有許可證資訊。
（5） 執行層的許可證伺服器，握有解密金鑰。

圖 3.21 為經由 HTTP 聯繫的過程。

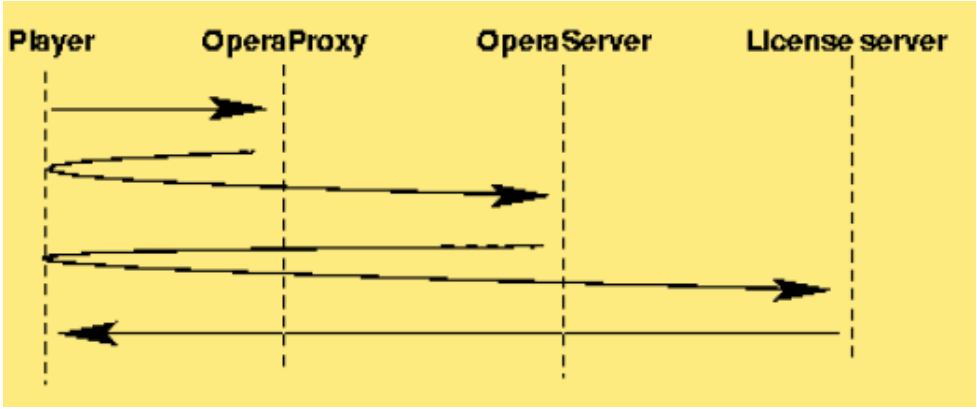

圖 3.21 經由 HTTP 聯繫的過程

大多聯繫是經由 HTTP，從播放器最初的要求，到執行層伺服器最後的回應，都是透過 HTTP 的協定完成。有一點不同的是，當 OPERA Server 和手機間亂數的傳送，是藉由 SMS 與 HTTP 的協定完成。

3.7.1.3 SmartRight

SmartRight 對數位家庭網路來說，是一個保護複製的系統，結合了條件存取系統(Condition Access System---CAS)，以及數位權利管理(Digital Right Management---DRM)系統，提供有效率的點對點方式，來解決數位內容保護的問題。

SmartRight 系統架構包含了個人私有網路(Personal Private Network，簡稱 PPN)，當中的設備是由個人或家庭所擁有的，而且不需要持續與網路連線，所以可以支援手機的設備。

SmartRight 的設備必須含有三個功能：

I. 存取功能：是用來保護從外面進入家庭網路的資料內容。

II. 顯示功能：是用來執行 SmartRight 系統保護的資料內容。

III.儲存功能：記錄網路上所運送的內容。

為了確保有效率的保護和安全更新，SmartRight 系統使用可移除的安全晶片卡，並且在卡片中嵌入安全金鑰，這類型的晶片卡可以用 ISO-7816 的 Smart Card，或者是可移除式的模組，用來對有線電視與 DVB-CI，NRSS 或 POD 連線。

在 SmartRight 技術中，存取功能使用了 Convert Card，而顯示功能使用了 Terminal Card，Convert Card 嵌入關鍵資訊到保護性的資料結構中，這些資料就是內容使用型態和擾碼金鑰。另一方看來，Terminal Card 會將這些資訊解碼，所以根據內容的使用型態，Terminal Card 也能將保護內容解擾碼。如圖 2.23 所示。

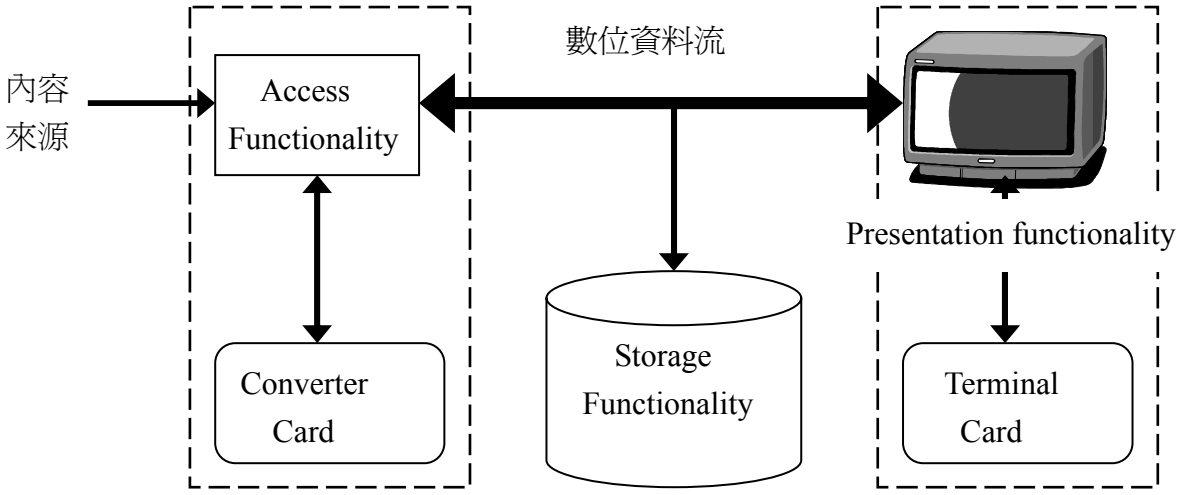

圖 3.23　個人私有網路架構

SmartRight 系統最主要的特徵是點對點的內容保護。以下有兩種存取功能的型態：

- 第一種存取功能型態是控制已擾碼的內容的存取，支援 SmartRight 的技術，而解擾碼的金鑰被封裝起來，置入在加密的 LECM（Local Enforcement Copy Management）訊息中，而此訊息也安全的被放入 Convert Card 裡。例如 DVB 的 Set Top Box 就是這類的方式。
- 第二種存取功能型態是控制已擾碼的內容的存取，但是不支援 SmartRight 的技術，這種方式是將內容重新擾碼，而重擾碼的金鑰被封裝起來置入在加密的 LECM 訊息中，而此訊息也安全的被放入 Convert Card 裡。例如 DVD 播放器就是這類方式。

個人私有網路(Personal Private Network，簡稱 PPN)是由 SmartRight 設備所組成的，所有在相同 PPN 上的 Terminal Card 都分享相同的網路金鑰，而兩個不同的 PPN 有不同的網路金鑰，所以他們不能共同分享受 SmartRight 保護的內容，甚至是複製的內容也不行。在 PPN 上的成員規模也有所限制，並不是無限的增加，每當一個有顯示功能的新設備加入同一個 PPN 時，計數器就會減少一，所以計數器主要是用來限制 PPN 的規模大小。

局部性執行複製管理（Local Enforcement Copy Management－LECM，簡稱 LECM）附帶了有關內容保護的資訊，CA/DRM 模組提供了相關的資訊來建置 LECM。包含了以下的資訊：

（1） 原文資訊。
（2） 內容型態。
（3） SmartRight 使用狀態。

（4） 對外來內容訂立的保護規則。
（5） 內容解擾碼資訊。
（6） 用具體的資訊處理純觀賞的內容。
（7） LECM 金鑰加密的數值。

LECM 包含了兩個部分：
（1） 保護部分：握有內容解擾碼及純觀賞的資訊，並且由一把 LECM 金鑰加密保護部分。
（2） 未保護的部分：總是處在明顯易懂的狀態下。

表 2.6 LECM 架構的簡易表。

		保護部分	
清楚的部分	LECM 金鑰	解擾碼資訊	純觀賞資訊

PPN、Terminal Card 和 Converter Card 的特徵：

- PPN 的特徵：
  - I. 所有的 Terminal Card 都享有相同的金鑰。
  - II. 最初的 Terminal Card 會亂數產生一把金鑰，並且同一時間只有一個 Terminal Card 能傳送金鑰給另一個 Terminal Card。
  - III.有限制的 PPN 成員規模。
  - IV. Converter Card 無法得取金鑰。

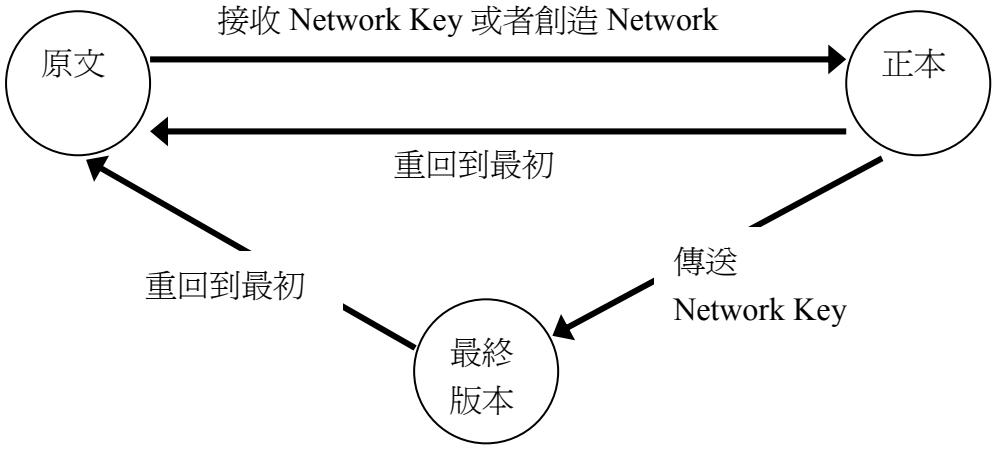

圖 3.24 Terminal 模組的三種狀態

- Terminal Card 的特徵：
  - Terminal 有三種不同的狀態(如圖 3.24)。
    - I. 原文，不含任何金鑰。

II. 正本，有一把金鑰，並且可以將金鑰傳送給原始的 Terminal 模組。

III.最終版本，有一把金鑰，但是不能將金鑰傳送到其他 Terminal 模組。

◆ 不同的狀態會遵循不同的規則。

I. 當被傳送時，Terminal 是屬於原文狀態。

II. 當原始的 Terminal 模組接收了從正本送來的金鑰，或者自己創造了一個新的 SmartRight PPN 時，就會轉變為正本的狀態。

III.當正本傳送自身的金鑰出去時，就會變為最終版本。

IV.當不再連上網路時，Terminal 模組便會維持在相同狀態。

■ Converter Card 的特徵：

每個 Converter 模組都有以下的資訊及資料：

I. SmartRight 憑證的公開金鑰，Converter 模組會使用此金鑰給有效的 Terminal 憑證。

II. 一個被選取的亂數 LECM 金鑰。

III.一個被網路金鑰加密的數值。

每當 Converter 模組改變自身的 LECM 金鑰時，便需要得到由新的金鑰加密的數值，而 Converter 模組便會從網路上的 Terminal 模組得到此數值。圖 3.25 為此協定的架構圖。

Converter 模組必須先知道 Terminal Card 的公開金鑰，當 Converter 模組得到公開金鑰後，首先會檢查金鑰的合法性，並且用此把公開金鑰加密自身的 LECM 金鑰，之後傳送加密後的金鑰給 Terminal Card，而 Terminal Card 會加其解密再回傳 LECM 金鑰給 Converter 模組，回傳時用網路金鑰來加密。而 Converter 模組得到值後，便將這些加密後的值置入每個 LECM 中。

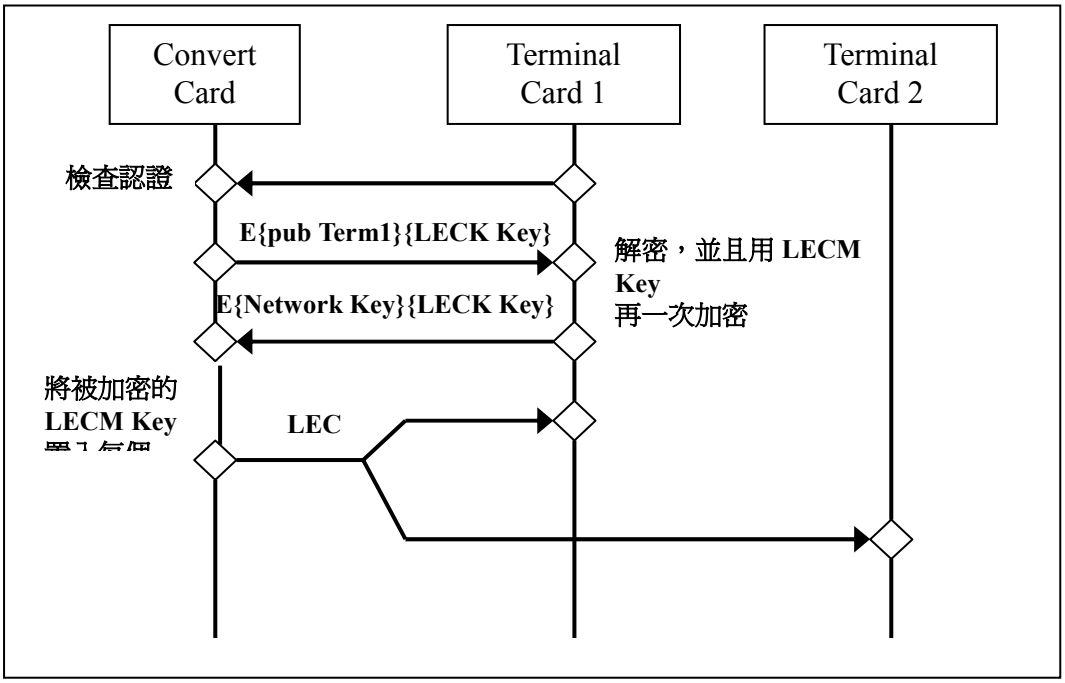

圖 3.25 LECM 金鑰交換協定架構

3.7.1.4 DMDFusion [39]

從 2000 年三月數位多媒體傳送安全公司(Digital Media Distribution Secure，簡稱 DMDSecure)已經在伺服器端上的 DRM 元件領先者，主要針對軟體供應商、廣播業者、行動業者和服務供應者有一個在伺服器端上的 DRM 問題解決方案。在 2005 年四月 SafeNet 公司併購 DMDSecure，而 SafeNet 公司在全球第七大資訊安全公司，已經有產品通訊上、智慧財權和數位身分的加密技術，以及硬體、軟體和晶片全領域的發展。SafeNet 已經成功的發展了版權管理商業的目光，SafeNet 強大安全技術和 DMDsecure 的內容 DRM 伺服器管理整合成對一個強大的安全標準，針對於數位多媒體內容傳送的產品，例如：軟體、語音檔、影像檔、遊戲檔…等。DMDsecure 發展了 DMDFusion、DMDLicenser、DMDPackager 和 DMDMobile 產品，目前要討論的是 DMDFusion 產品，針對於市面主流 DRM 系統上的整合，只要一個伺服器系統軟體可以封裝成多個 DRM 系統的產品。如圖 3.26 所示。

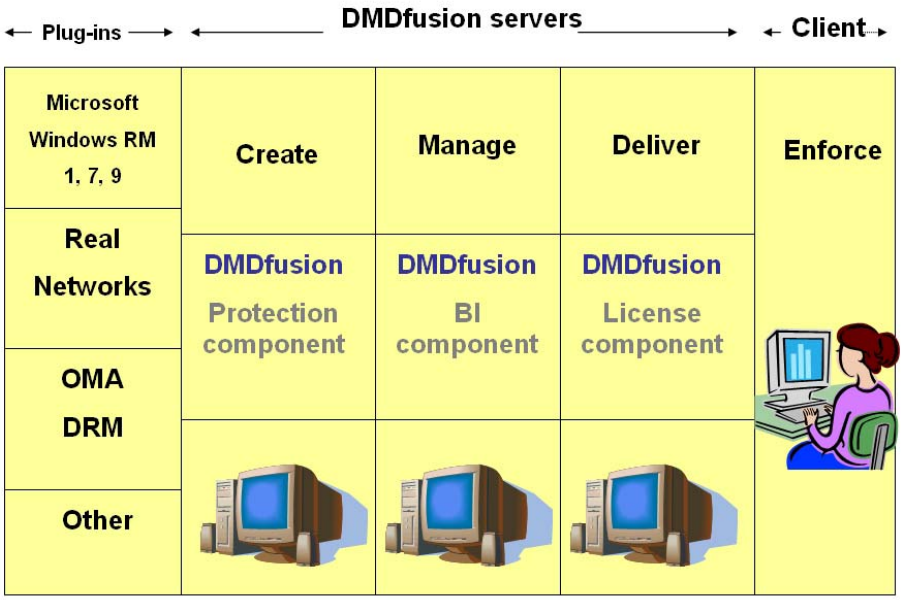

圖 3.26. DMDFusion 架構

- Protection Component
  - 用圖左裡的任意一種 DRM 系統去加密即時或是隨選視訊的內容
  - 擁有促進碼的整合的 API
- Rights Management Component
  - 提供一個圖形使用者介面(GUI)的網站
  - 使內容擁有者可以自訂一些使用權力，Server 端的條件和契約。
- Rights and License Delivery
  - License 的部分處理所有的 License 的請求組成以及傳送的程序。

- 用 Vouchers（是一個已經簽章的 URL 用來給予使用者取得 License 的權力） or 3rd Party 交易的解決方案。

3.7.1.4.1 DMDFusion 的一些主要特性

1. 公開和 pluggable 的架構：整合許多 DRM 的技術，他支援廣大範圍的資料類型與格式，這個系統支援 Windows Media Right Manager 1,7,9 系列，Real Networks, XrML、 MEPG REL 、OMA DRM。
2. 可以增加 DRM 功能於現有的架構中：可以增加 DRM 功能在現存的架構上，可以整合任何現存的解決方法，增加端點端對點的能力。
3. High-end , Scalable , Carrier Grade Platform：DMDFusion 主要是基於 J2EE 的技術。
4. End-to-End DRM solution：伺服端負責權力創造、管理和傳送。客戶端只需負責執行。
5. 使用工業界標準：PKI , XML 和網路服務。
6. 支援及時和隨選內容的 DRM 平台：可以保護以及使用 License
7. 能夠連接內容以及服務提供者：可以服務許多內容和服務的提供者以及在它們之間簽訂生意上的合約。
8. 公開的整合現有的架構：提供一個公開的網站服務的 APIs，確保於現有的電信及廣播架構整合的容易性。
9. 支援各種類型的商業模式：訂閱服務、Pay-Per-View、限制分送、預覽、限制裝置、Ppay-Per-Event…等。

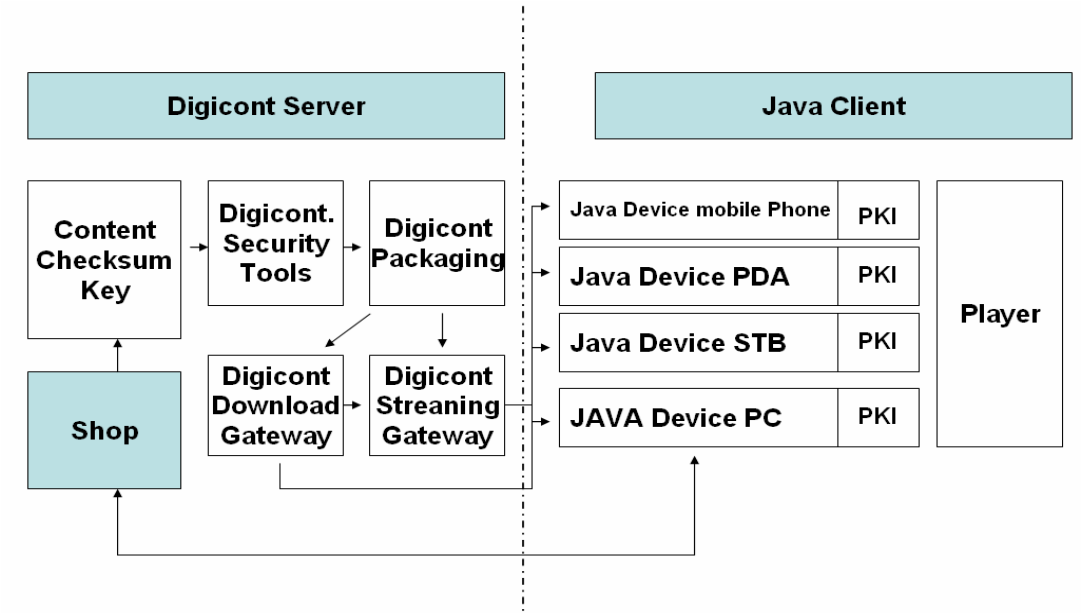

圖 3.27. SDC DRM 架構

(取自 http://www.digicont.ch/sdc_java_drm/core_technology/index.html)

3.7.1.5 SDC DRM [40]

SDC AG 公司的產品，是一家提供 JAVA DRM 的產品，以 Mobile Code 的架構為基礎。因為這個進階的架構可以把碼和內容封裝在同一個"數位貨櫃"(Digital Container)中(「數位貨櫃」是一個用來傳送內容, 軟體和程式碼的單位)。客戶端只需要在裝置上裝有 Java VM 而不需要安裝其餘的東西。

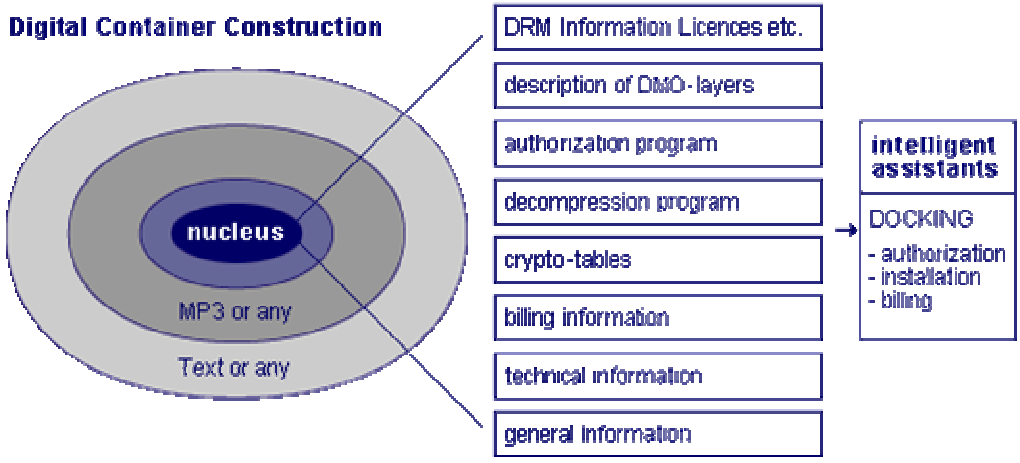

圖 3.28　SDC 數位貨櫃(Digital Container)架構

(取自 http://www.digicont.ch/sdc_java_drm/core_technology/index.html)

3.7.1.5.1 SDC DRM 的主要特徵

1. 客戶端不需要安裝設定：這個系統將內容和程式碼封裝於 Container（數位內容物件）。Container 本身含有用戶端應用程式所需的解密及播放內容 。因此用戶端不用額外安裝只需要 Java VM .
2. Multi-device and Multi-PKI：相同消費者購買的內容想要安全的轉換到其他屬於他的裝置需要不同的認證系統，SDC DRM 提供一致性的方法來解決。
3. Superdistribution：為了提供 Superdistribution 機制，把內容放到兩個 Container。
   - Container A：有 95%的內容負載，這個內容依舊能播放，剩餘的空間用於廣告的資訊或是提升音樂檔案的品質，是可以被分享的。
   - Container B：用於對 Container A 上內容作加密或是浮水印的資訊。
4. Security：
   - 內容用標準的 RSA 128bits 的鑰匙加密。
   - 內容使用唯一的 Session Key 加密。
   - Containers 用簽章防止駭客攻擊。
   - License 與使用者的私人鑰匙是高相關性的。

- 管理多把鑰匙。
- 只能在合法的裝置和正確的鑰匙才能夠播放內容。
- 使用混淆的技術為了避免反向工程。
- 使用個人化的浮水印以便追蹤。

3.7.1.6. VirtusosMedia [41]

VirtusosMedia 是一家主要是研究 DRM 的科技公司，重視保護影音的內容，VM DRM 是一個公開的標準，他的輸入可以是 XML, MPEG-1, MPEG-2, MPEG-4 或 MP3，他也支援 ISO/IEC 7816 智慧卡的使用，可以適用在各式平台：Windows , Linux，和支援各式硬體：PC, PDA, STB。

VM 是一套端點對端點的數位分送管理系統可以分為以下三個步驟：

1. Production：內容被創造, 編碼以及壓縮以及保護非法複製而加密。
2. Transport：使用在可控制的傳送通道。
3. Viewing ：使用認證確認使用者能不能使用內容，認證之後這個內容才會被解密以供使用。

3.7.1.6.1 四種 DRM (VM)的基本類型

1. **Conditional access DRM**：VM 所提供的最簡單 DRM 類型，提供一個"前門 Front Door"的保護不提供任何複製或分配的控制，主要用於只需低保護性的網站以及鄰近廣播系統。
2. **Transport Protection DRM**：主要用以保護傳送的通道，最常使用在像有線或衛星電視的廣播系統或是像網際網路 .ssl 連結，他是容易被實現的但是他難以抵擋 "Man in the Middle"的攻擊（因為認為通道是安全的 而有失防範）。
3. **Storage Protection DRM**：主要用於保護已存的資料例如：網站資料，他也用於保護儲存重要資料的 CD-ROM 或是一個封閉的硬體構造，通常是用軟體來做。
4. **Content Protection DRM**：包含之前的三種保護，使用資料加密和整個過程（儲存以及傳送）的加密，在端點用戶確認和認證後這個資料可以被即時解密以及觀賞。包含以下三個動作：
   - **Creator**：創造且加密內容。
   - **Client Portal 和 Subscription Manager**：儲存用於加密資料的鑰匙以及定義用戶規則。
   - **Integrated Player**：認證使用者和選擇鑰匙以及對於用戶管理者的使用規範。選擇了鑰匙之後解密內容以及執行。

3.7.1.7. InfoGate OnDema [42]

InfoGate 是一家提供架構在寬頻網路上進行隨選 IPTV、視頻點播和遊戲點播以及遠程教育的軟體解決方案提供商，是一家國際公司，總部設在以色列。InfoGate 推出的 OnDema 平台使電信和其他寬帶營運商有能力提供增值服務，如視頻點播、互動遊戲、電視頻道，並且可以通過電視和電腦間用戶提供現場直播服務。OnDema 平台具有內容發佈、控制、計費、用戶管理...等特色，能夠消除內容提供商和終端用戶之間存在的瓶頸問題，為各種寬帶業務提供了保障。因此，寬帶網路營運商只需通過一個 OnDema 平台，就可以為任意第三方內容提供商和寬帶用戶提供服務。

以下是 OnDema 系統的概括架構，而 OnDema 系統的架構可以分成三種基本的部分：

- Content Provider (CP)：上傳內容到 OnDema 系統用以提供各式的需求，也支援封包的創造（包含價錢，分送以及 Campaign 資訊。
- Master Access Provider(AP)：管理 CP 以及所有的 Edge 元件（to be analysed），提供管理 IT 系統功能。
- Edge Unit：用來存放端點用戶消費的內容，在靠近用戶端的位置(POP：point of presence)提供使用者的認證以及傳送遊戲以及影像的內容，所以可以確保高品質以及即時。

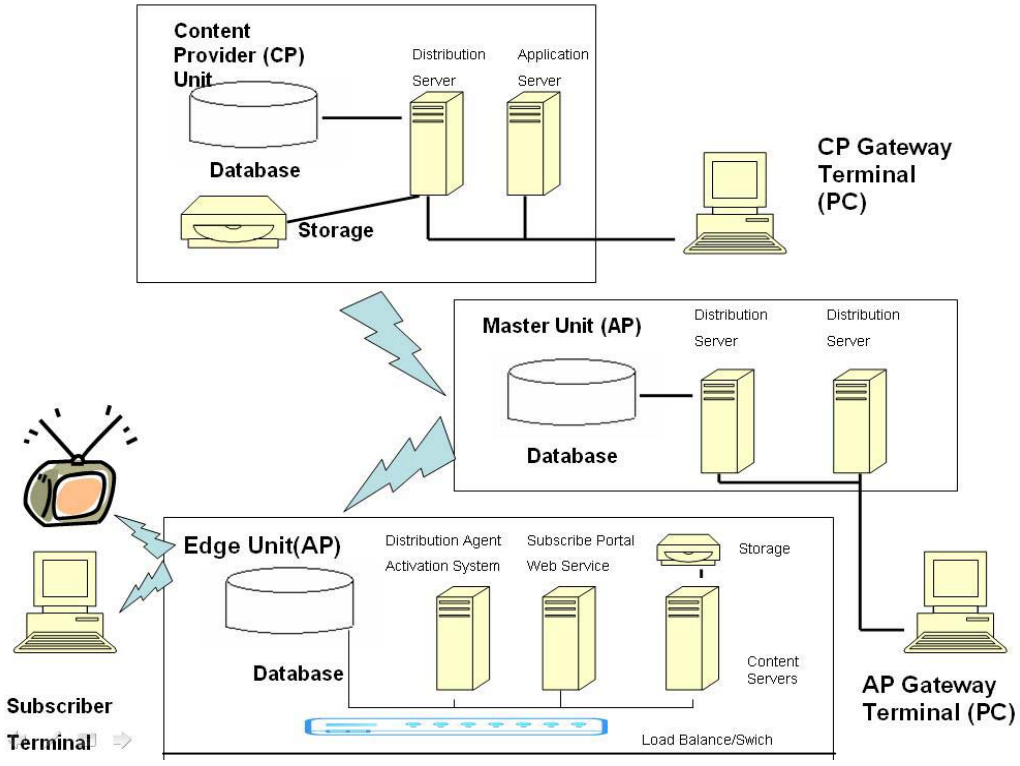

圖 3.29　The OnDema 系統架構

OnDema 系統的主要特徵

使用 Microsoft 的技術.　　(內容可從任何平台而來)，這系統提供：

- Content Management：可以處理一個多種內容格式以及 Metadata ，也包含工具以及進階管理 ，封裝 ，付費以及分類的能力。
- Subscriber Management：有效的處理不同層級以及類型的用戶， 用戶管理包含：清算帳目，個人化，追蹤，安全，隱私權以及 sub-account。
- Content Distribution：這系統可以處理以及分送來自內容的聚集者或是其他類型的內容提供者，分送的方式折是使用 POPs (points of presence) ，所以端點的用戶總是可以得到即時高品質的內容。
- Content Delivery：支援隨選視訊 ，隨選遊戲, IP 即時匯流串

3.7.1.8 Lockstream Catalyst

LockStream Catalyst DRM 服務平台提供預先編碼和傳送安全內容的綜合解決方案，所有的內容管理系統包含以下三種步驟：預先編碼、建立和傳送。在一個安全內容的工作情況下，所有的系統都必須綁上一個特別的 DRM 一起傳送。例如：內容加密和 Licensing。

Catalyst 平台是由五種不同的伺服器組成，有兩個主要核心伺服器和三個 domain 伺服器。Core 伺服器提供預先處理和控制存取安全內容的基本功能。Domain 伺服器需要利用 Business Process Requirement 提供了額外的能力。

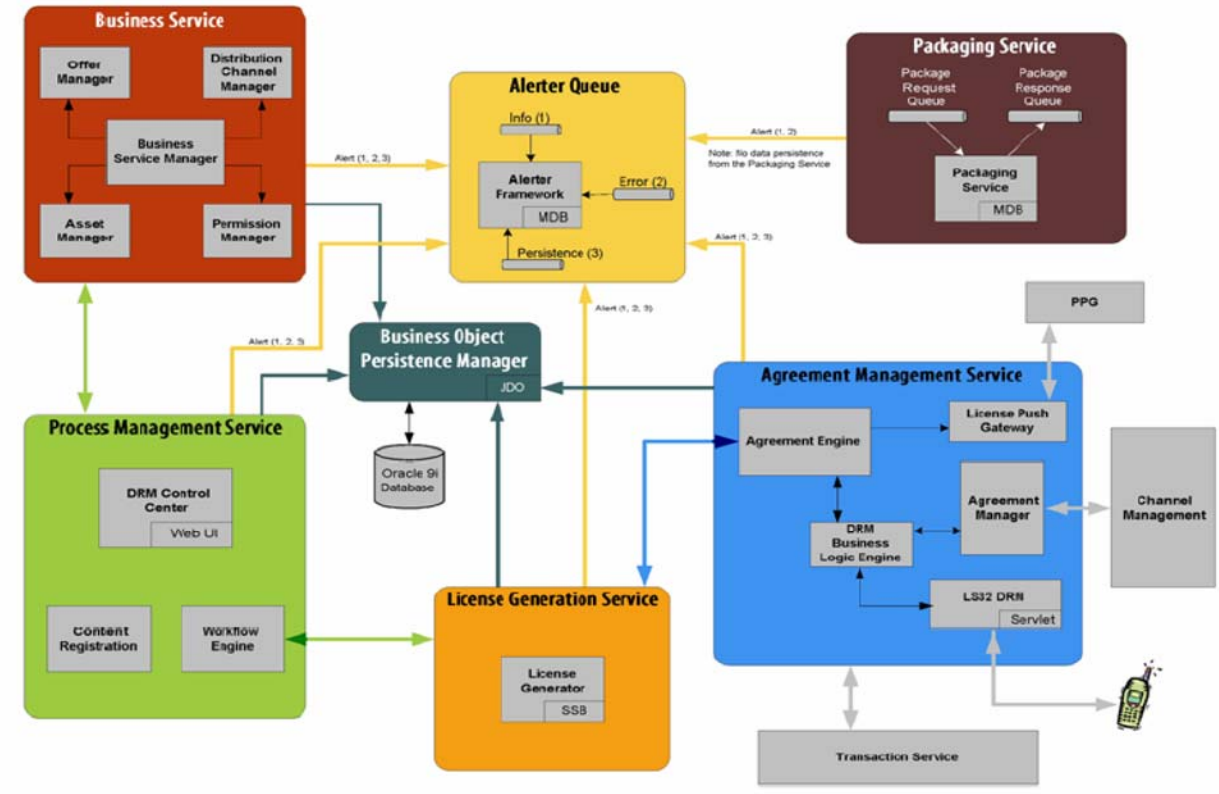

圖 3.30　Catalyst 架構(取自[37])

- Core Services:
  - Package Service：使用所選的 DRM 加密封裝數位內容和取得 license 的 URL。
  - License Generation Service : 產生內容的 License，使取得 License 才能有效的傳送。
- Domain Service:
  - Process Management Service：管理數位內容預先準備的程序和管理 Asset 和 Offer 的資料儲存。
  - Business Service ：提供創造產品報價的工具。
  - Agreement Management Service：管理內容的存取和 License，證實內容和 License 的請求，追蹤顧客存取的受保護內容。

3.7.1 R&D DRM 系統

此 DRM 系統平台是沒有要商業化，主要是為了發展和研究 DRM 系統。

3.7.2.1 OpenSDRM

3.7.2.1.1 OpenSDRM Component

OpenSDRM 權利管理平台是由一些分送的系統元件（Component）組合而成，他們在公開的網路上（例如：網路）交換標準的訊息。OpenSDRM 概念性的架構定義一個能夠處理於不同多樣化的商業模式分送內容的方案。

概念性的架構是基於三個不同的區塊元件（如圖 3.31）：
使用者角色(User Roles)、外部實體(External Entities)表示 DRM 的程序、內部實體(Internal Entities)提供 DRM 的功能。

- **User Roles**：OpenSDRM 的架構提供了下列幾種使用者角色
  - 作者/擁有者（Author / Owner Societies）
  - 內容提供者（Content Providers）
  - 裝置製造者 (Device Producers)：裝置製造商必須被 DRM 平台發給憑證。
  - 安全工具提供者 (Security Tools Providers)
  - 端點用戶 (End Users)
- **外部實體**：在架構上支援非 DRM 的功能，這些實體包括了
  - 付費機制 (Payment Infrastructure)： 負責處理所有財務上的交易，確保收入的正確性。

- 內容選擇單位 (Content Selection Module)：可以使用找尋, 瀏覽和選擇內容，例如：電子商店交易(Electronic Commerce Front-store)或是電子節目指南(EPG)。
- 裝置 (Devices)
- 傳送內容的伺服器 (Content Delivery Servers)
- 憑證系統 (Certificate System) ：它可以是一個外部實體，也可以是內部的實體，功能為發送適當的憑證給其他系統元件(Component)。

■ **DRM 實體：**這些元件（包括客戶端與伺服端）提供了必須的 DRM 功能，去保護內容和將內容與使用者之間的權利(Rights)做相關的整合，這些元件包括了有：

- 內容管理系統 (Content Management System)
- 付費匝道單位 (Payment Gateway Module)
- License 管理系統 (License Manager System)
- 內容保護工具認證與計費系統 (Content Protection Tools System)

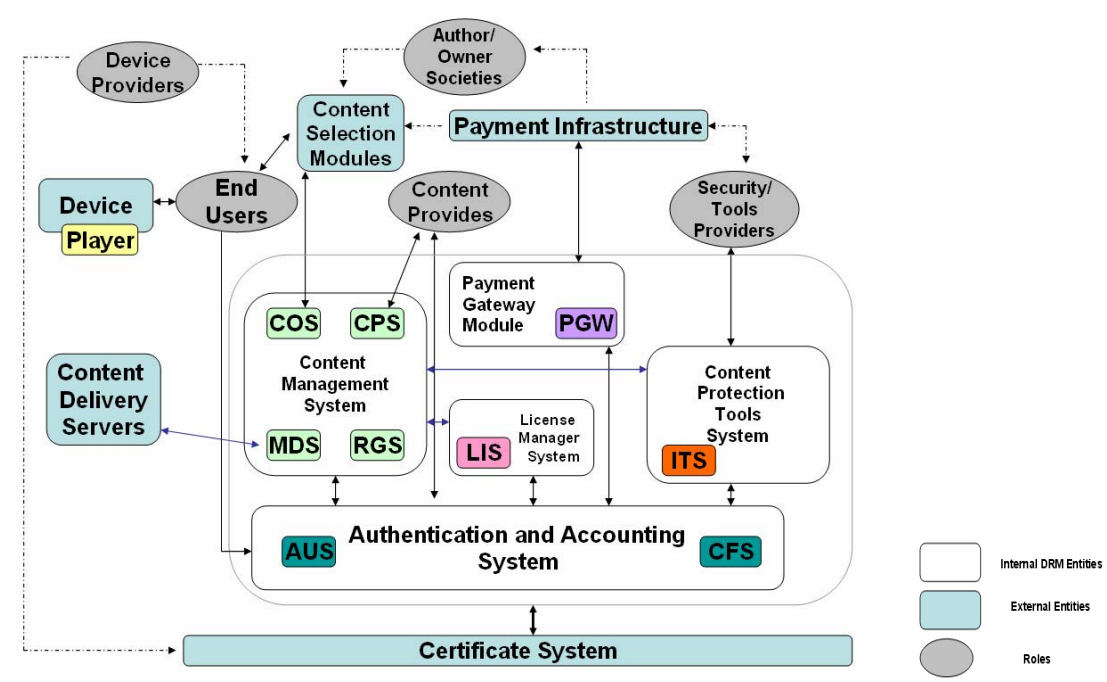

圖 3.31　OpenSDRM 主要區塊元件

外部的系統元件(External Component)與介面

這元件會詳述外部元件和 DRM 架構之間的互動：

■ 使用者：某位使用者他希望消費一段內容，這份內容不一定會被保護。無論如何這份內容必須在被保護的裝置，軟體和 License 的情況下使用才能存取和播放。使用者必須用以下的順序跟 OpenSDRM 做請求：確認使用者, 下

載 License 和使用網路瀏覽器或多媒體播放器播放內容，若不能播放內容 OpenSDRM 會給使用者報告為什麼他不能使用的原因。

- IPMP 工具的提供者：IPMP 工具提供者運用到加密、擾碼、浮水印和其他的方式保護內容，OpenSDRM 會運用這些工具去使用在內容權利的保護。這些工具必須滿足以下一些準則：內容提供者和 IPMP 工具提供者必須有商業上的轉換關係，也就是說內容製造者跟分送者可以選擇使用那種 IPMP 的工具去保護內容。
- 內容提供者：內容提供者主要是提供內容和可選擇一些 Metadata 資訊給 OpenSDRM 去做內容管理和散佈。
- 付費系統：付費系統有助於 OpenSDRM 去做一些電子商務的服務，而付費的方式要是獨立的，使得可以整合很多種付費方式的付費系統。
- 憑證當局(CA)：CA 負責發送憑證給實體，這些憑證將被實體使用來認證自己的合法性，憑證當局可以是內部系統，因此可以被某些實體全權管理，也可以是外部的交易實體，由第三方來控管。

內部的系統元件(Internal Component)與介面

- 內容準備伺服器 (Content Prearation Server，簡稱 CPS)：主要是接收原始內容，再做特定的編碼、保護和加上一些 Medadata
- 付費匝道 (Payment Gateway，簡稱 PGW)：主要是用在核對消費者的付費方式是否正確，再給予生效。
- 交易伺服器 (Content Server 簡稱 COS)：主要用來作內容的交易、內容定價資訊、伴隨內容的 Metadata 和最重要的內容使用權限的建立。
- 傳送多媒體伺服器 (Media Delivery Server，簡稱 MDS)：多媒體內容的散佈，使用一般的下載協定，例如：FTP、HTTP、RTSP…等。
- 註冊伺服器 (Registration Server，簡稱 RGS)：分配唯一的識別符給內容，而且要登記 metadata 資訊給特定的內容。此架構設計儘可能採用 ISO 標準。而 OpenSDRM 遵循 MPEG-21 的標準。
- 認證伺服器 (Authentication Server，簡稱 AUS)：主要是對 DRM 系統內外實體做合法性和安全性的鑑定，再給實體元件和提供者給於認證。
- License 伺服器 (License Server，簡稱 LIS)：針對使用者和內容給予存取權利，用權利描述語言寫成 License，取得 License 才可以使用相對應權利的內容。
- IPMP 工具伺服器 (IPMP Tools Server，簡稱 ITS)：CPS 在封裝內容時，有用到某個 IPMP 工具，當我們要解開此內容時，也是需要此 IPMP 的工具，所以，取得此 IPMP 工具伺服器的授權，則可下載使用。
- 媒體應用程式 (Media Application，簡稱 MPL)：內容播放程式。

3.7.2.1.2 OpenSDRM 的安全性

在 OpenSDRM 平台架構下，存在兩個安全層，一個是通訊層安全，另一個是應用層安全。

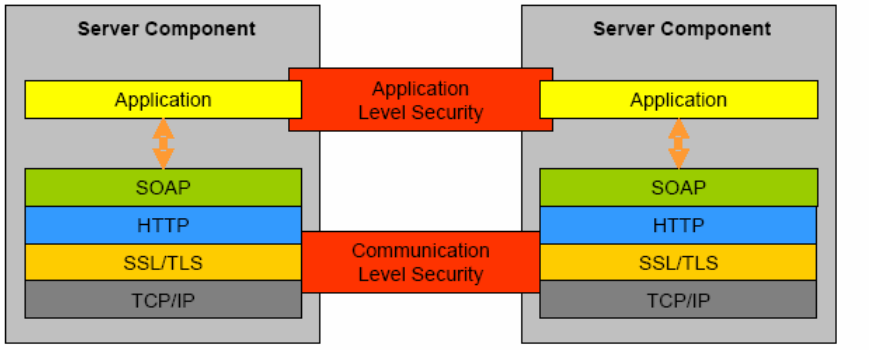

圖 3.32　OpenSDRM 安全層(Secure Layers)　(取自[38])

不同的系統元件彼此交換訊息時用同一個架構。訊息的格式組成如下

- 元件的 ID：一個 128 位元的確認器（由 MD5 雜湊演算法組成）
- 訊息內容：
- 數位簽章：預防訊息內容的竄改

圖 3.33　SOAP 交換訊息結構

裝置的確認性與認證性

一個裝置可以被只有一個使用者使用(例如手機)或是被多個使用者使用(例如 STB) 因此必須認證裝置必須有兩種層級，每個使用者必須要被認證才可以使用的裝置。

所有每個裝置製造商(Device Manufacturer，簡稱 DMan)放了屬於自己的憑證在裝置中。這個憑證是從一個可靠的憑證中心而來的 X.509 憑證。

第一步驟：每個 DMan 都必須被根憑證中心（ROOT CA，簡稱 rCA）發予憑證。

每個 DMan 擁有他自己的裝置製造商憑證：

$$Cert_{rCA}^{DMan[1]}, Cert_{rCA}^{DMan[2]}, \ldots, Cert_{rCA}^{DMan[n]}$$

每個裝置也有他自己的憑證：

$$Cert_{DMan[1]}^{Dev[1]}, Cert_{DMan[1]}^{Dev[2]}, \ldots, Cert_{DMan[1]}^{Dev[n]}$$

$$Cert_{DMan[2]}^{Dev[1]}, Cert_{DMan[2]}^{Dev[2]}, \ldots, Cert_{DMan[2]}^{Dev[n]}$$

$$\cdots$$

$$Cert_{DMan[n]}^{Dev[1]}, Cert_{DMan[n]}^{Dev[2]}, \ldots, Cert_{DMan[n]}^{Dev[n]}$$

若是當每個裝置想要通訊的時候或是一個裝置想要跟另一個元件通訊，他們可以秀出他們的憑證得到對方的信任（執行互相認證 Mutual Authentication），假如他們來自相同根憑證中心，互相認證成功。

這是一個現存的機制特別使用在網路上(SSL / TLS 協定)和使用 PKI 機制

互相認證機制是以以下步驟實現：

1. 裝置 A (Dev[a])寄出他的憑證($CertD_{Man[x]}^{Dev[a]}$)給裝置 B (Dev[b])
2. Dev[b]寄出他的憑證給 Dev[a] ($CertD_{Man[y]}^{Dev[b]}$)
3. Dev[b]以下步驟驗證
   - 是否有一個相同的 rCA 憑證在 Dev[a]的憑證串中
   - 有的話，使 Dev[a]的數位簽章有效化
   - 這個憑證為有效的
4. Dev[a]執行一個相同方式有效化 Dev[b]憑證
5. Dev[a]和 Dev[b]任選一數值互相測試，
6. 完成互相認證

伺服器元件的認證

為了建立安全的傳輸層，OpenSDRM 架構的軟體元件使用 SSL / TLS 協定，每個伺服器在他的軟體元件需要從憑證中心給予 X.509 憑證來安裝設定。OpenSDRM 可以建立一個安全和被認證的傳輸通道，可以允許一個訊息安全的從一個元件到另一個元件，用以下的方法：

- 每個元件計算出一對鑰匙（公開與私人）K_{pub}^{Server} , K_{priv}^{Server}，使用 RSA 演算法和使用自己的公開金鑰創造一個簽章憑證請求(Certificate Signing Request，簡稱 CSR)和一些額外的資訊在 CAU 後寄出。
- CAU 驗證 CSR 的有效性和發送 X.509 SSL 的憑證到適當的元件。
  $Cert_{X.509}^{server}$
- X.509 SSL 的憑證被安裝而且元件可以使用 SSL/TLS 來通訊，因此建立了安全的傳輸層。

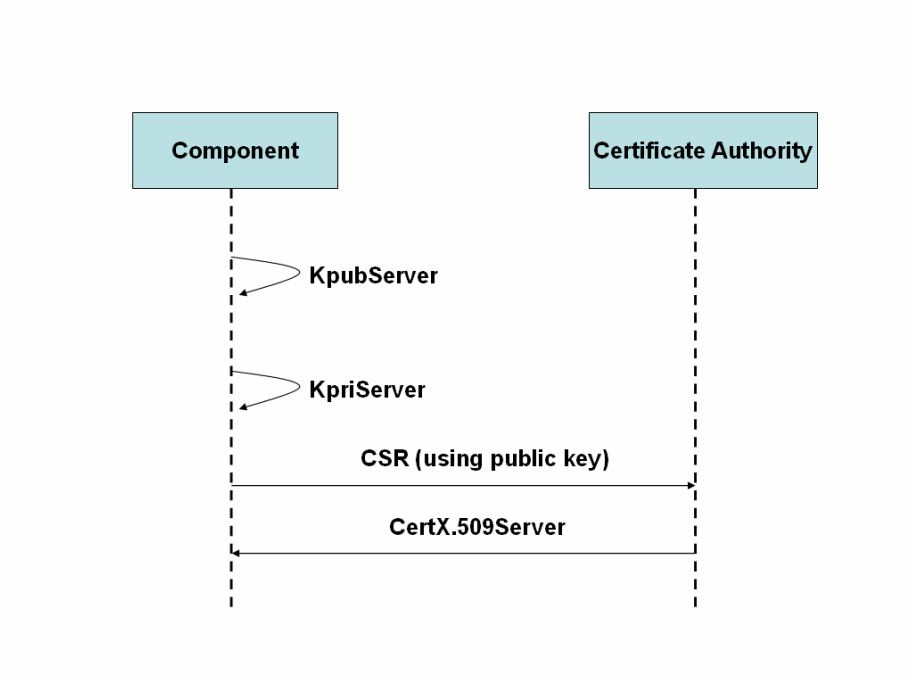

圖 3.34　Component Certificate Process

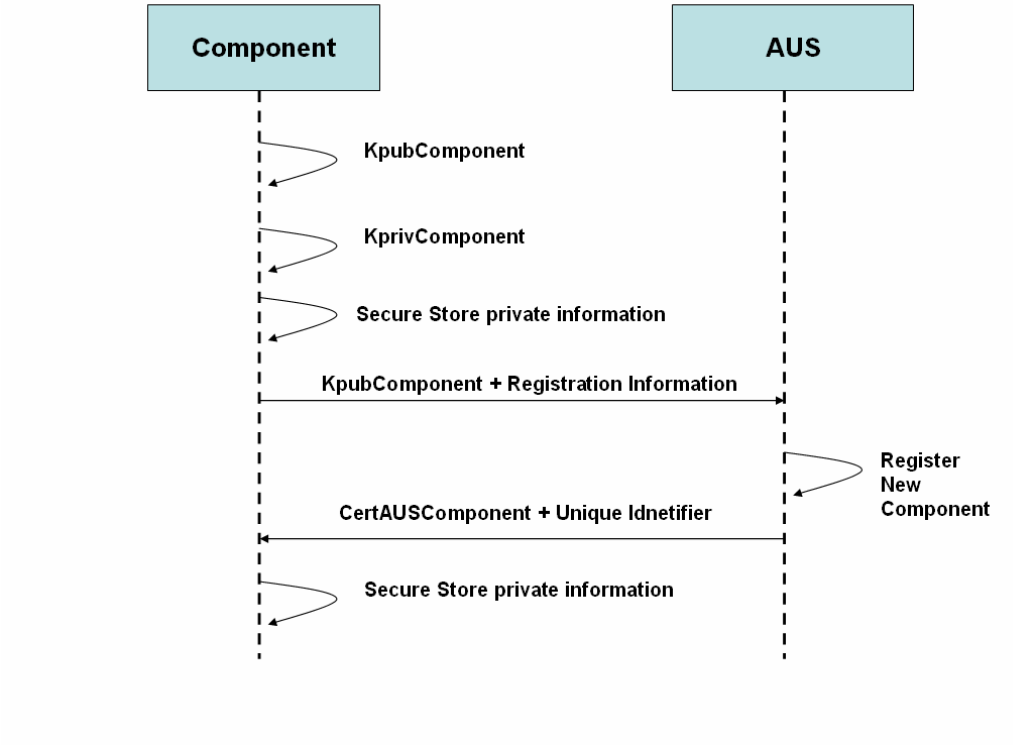

圖 3.35　Component Registration Process

OpenSDRM 中系統元件（Component）的註冊

- 每個元件計算出一對鑰匙（OpenSDRM 使用 1024 位元長度 RSA 的鑰匙，或是可以使用更高的位元），$Kpub^{Component}$, $Kpri^{Component}$ (各自有公開與私人金鑰)
- 元件管理者選擇一組登入帳號與密碼，使用 AES 加密 $Kpriv^{Copmonent}$ ，AES 的鑰匙會使用：K_{AES} = MD5 (Login + Password)，可以保護系統元件的私人金鑰：$K_{AES}[Kpri^{Component}]$
- AUS 認證從系統元件的資訊，註冊他以及有效化，然後為系統元件發送一組憑證：$Cert_{AUS}^{Component}$ 。這組憑證包含在其他資訊之中，系統元件的識別符和公開金鑰。然後憑證回傳給系統元件。

使用者在 OpenSDRM 平台的註冊

使用者包括了內容使用者, 內容提供者和 IPMP 工具提供者。

首先看一下內容提供者和 IPMP 工具提供者：

- 系統元件（ITS 和 CPS）收集新的註冊資訊和在 AUS 請求一個新的使用者的註冊
- 系統元件建構一個新的訊息：$SIGNKpri^{Component}\{Component_{ID}, Info\}$。這個訊息送給 AUS。
- AUS 檢驗和有效化這個訊息，註冊一個新的使用者和回傳一個唯一 $USER_{ID}$ 的給系統元件。

註冊內容使用者是一個更複雜的程序，這是由於內容提供者和 IPMP 工具提供者有儲存他們的資訊在遠端伺服器，內容使用者則是依靠他們自己的平台儲存資料，為了提供額外的安全層級，OpenSDRM 提供一個數位錢包(Digital Wallet)，能夠儲存敏感的資料例如加密的資料和 License，內容使用者的註冊程序可以表示為：

- 當使用者第一次執行電子錢包他創造給使用者一對 RSA 鑰匙（$Kpri^{User}$, $Kpub^{User}$），和要求使用者輸入一組帳號和密碼。
- 用使用輸入的帳號和密碼，創造一把鑰匙 K_{AES}=MD5(login+password)，用來加密敏感資訊，K_{AES}[Info]。
- 數位錢包要求使用者輸入一些個人資料($Person_{Data}$)和一些付費資料(Pay_{Data})（使用者付費資訊例如：信用卡號）。
- 錢包請求 AUS 註冊新的使用者，用 AUS_{Kpub}^{AUS} 加密所有的資訊並寄出 $Kpub^{AUS}[Person_{Data}, Pay_{Data}, KPriv^{User}, Kpub^{User}]$
- AUS 接受資料並解密他和註冊這位使用者。AUS 用一個為了使用者組成的新憑證回應錢包 $Cert_{AUS}^{User}$，包含在使用者的唯一確認器, 他的公開金鑰和確認 AUS 他的簽章的資訊中。

■ 這個錢包儲存所有重要的資訊，$K_{AES}[Cert_{AUS}^{User}]$

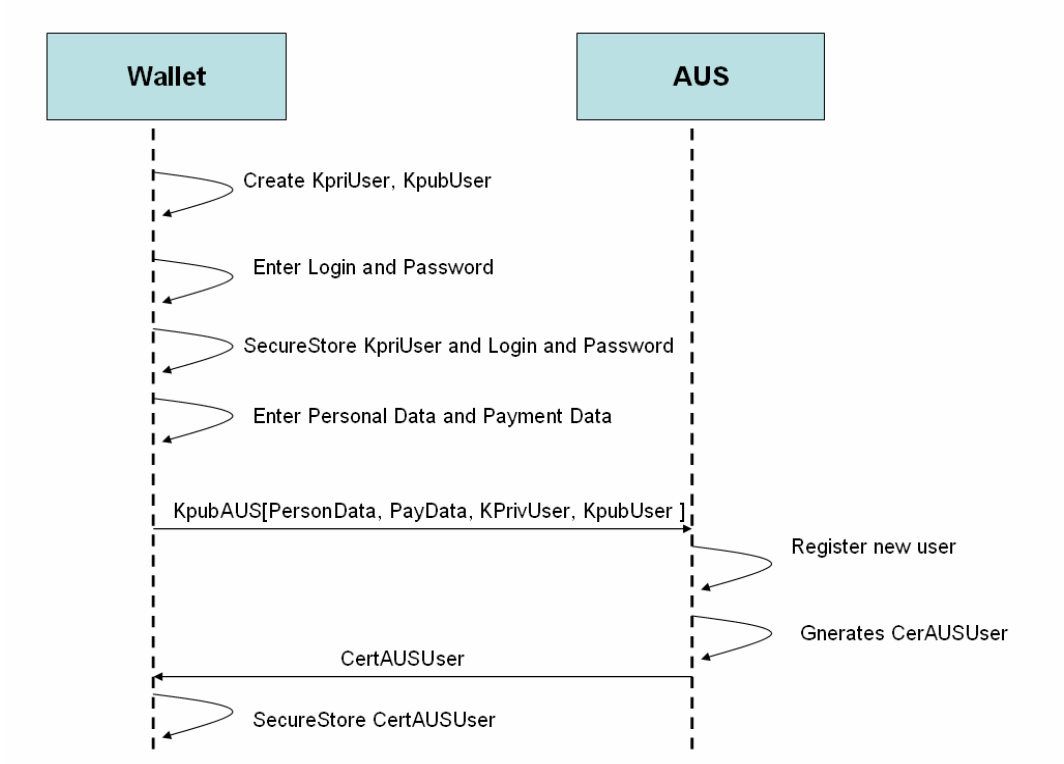

圖 3.36　Users Registration Process

系統元件的訊息交換

可以以下面的流程圖表示：

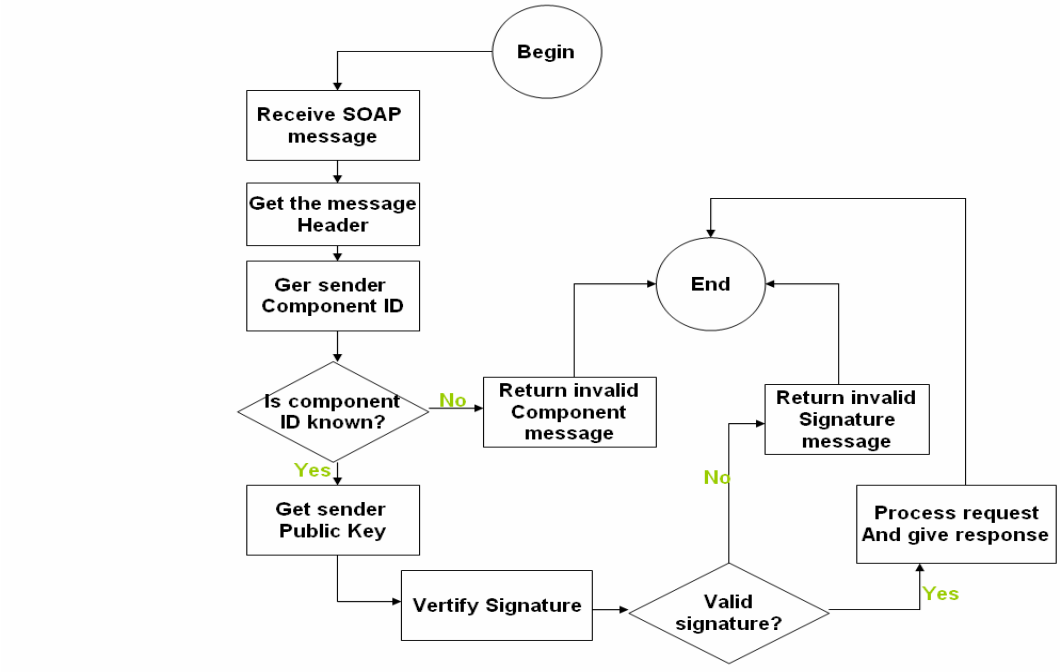

圖 3.37　Message Security and Integrity Vertification

付費資訊

OpenSDRM 定義了定義了具體化的內容付費機制，雖然付費方法在 OpenSDRM 的範圍之外。先必須在 COS 和 PGW 中建立可靠的關係。因此一個 COS 需要訂閱一個 PGW。可以用以下程序表示：

- COS 連接 AUS，和要求 AU 提供有效的 PGW。COS 寄了 **SignKpriCOS{COSID, RequestAvailablePGWs}給 AUS。**

- AUS 驗證這個訊息，回傳給 AUS 一個答案 **SignKpriAUS{<ListOfAvailablePGWs, CerAUSPGW>}**

- COS 選擇一個有效 PGW 和寄給他一個訂閱 PGW 的請求：**SignKpriCOS{AUSID, SubscribePGW, CertAUS^{COS}}**

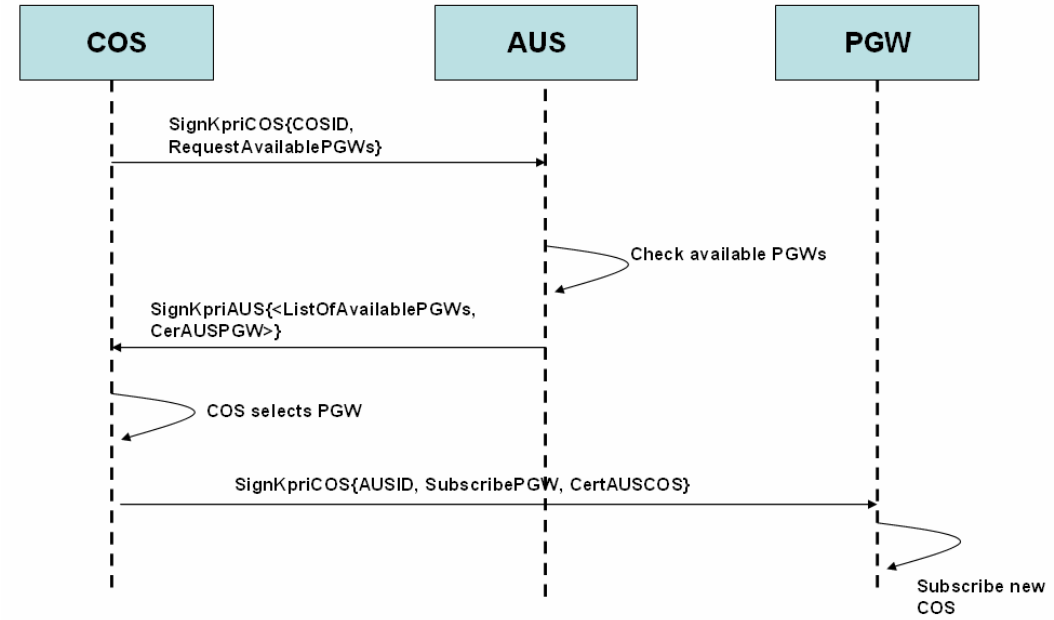

圖 3.38　Payment Gateway Subscription Process

使用 OpenSDRM 付費服務：

包含兩個步驟：使付費工具有效和得到消費的金額。
使付費工具有效在系統中是很重要的步驟，可以分為以下步驟：

- COS 寄出關於付費的詳細資訊，包括使用者的曾集合付費金額給 AUS，**SignKpri^{CO}S{COS$_{ID}$, U$_{ID}$, PGW$_{ID}$, PayData}**
- AUS 驗證和有效化 COS 的請求和檢查使用者 ID 為了從 AUS 上的使用者註冊資訊找尋適當適當付費方法。這個資料是用 PGW 的公開金鑰加密：**Kpub$_{PGW}$[PaymentClearence$_{U}$]**
- AUS 回傳給 COS 資訊，對他簽章：**SignKpriv$_{AUS}${Kpub$_{PGW}$[PaymentClearence$_{U}$]}**
- 再從 COS 送至 PGW，請求他有效化這個付費交易：**SignKpri$_{COS}${COS$_{ID}$, Kpub$_{PGW}$[PaymentClerence$_{U}$]}**
- PGW 有效化這個訊息以及加密使用者付費資訊，使用這個資訊去和相符合的付費架構通訊，並執行他之後，PGW 回傳有效付費的結果給 COS：**SignKpri$_{PGW}${PGW$_{ID}$, Transaction$_{ID}$ }**

付費程序的第二個階段包含了獲得金額。這個程序首先需要已經獲得這筆錢和皆下來 COS 必須持有有效的 TransactionID。獲得金額的過程可以描述為：

- COS 寄給 PGW 一個訊息：**SignKpriCOS{COSID, TransactionID }**
- PGW 有效化這個訊息和驗證 TransactionID 為了評估是否這個交易事實上是否成立和執行這個付費活動。
- PGW 回傳一個結果的狀態給 COS：**SignKpriv$_{PGW}${PGW$_{ID}$, Transaction$_{ID}$, Result}**

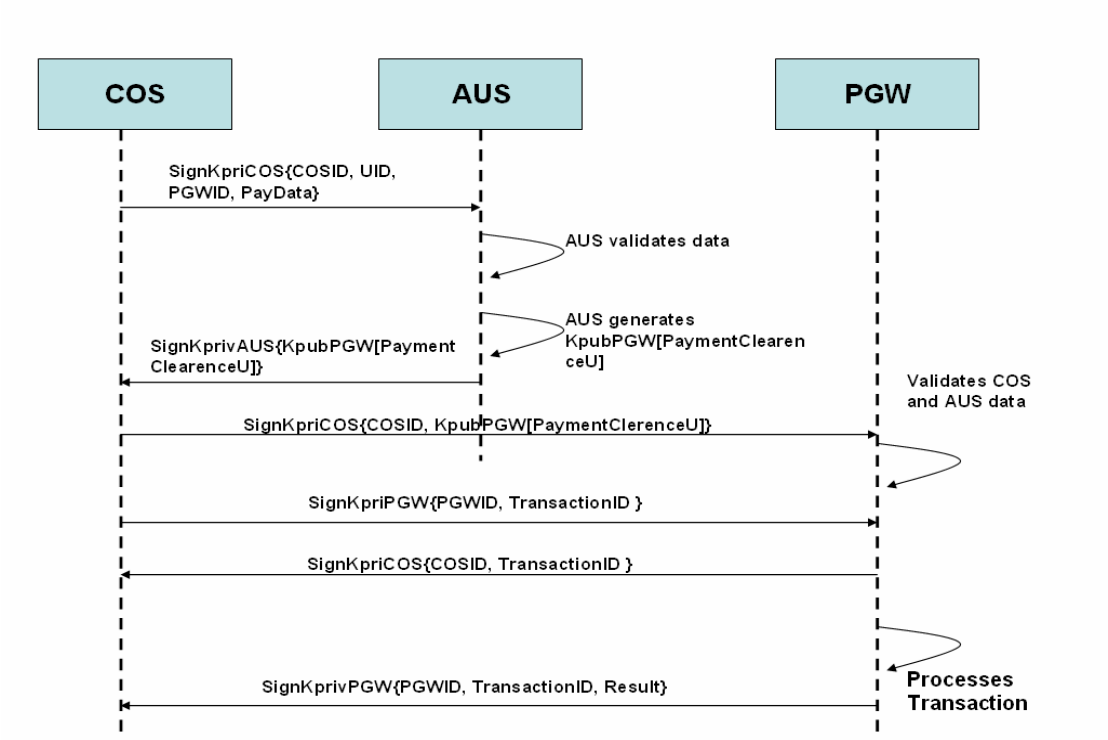

圖 3.39　Payment Process

3.8 DRM 建議規範

從上述的 DRM 基本架構跟 DRM 研究與產業界的發展，提出幾點建議規範：

- 使用者裝置端的 DRM 核心運算(DRM Agent)必需達到 Tamper-Prove 的安全性，而受到安全檢測，發給安全裝置證：因為所有 DRM 內容和權利描述之間的運算資料被取得，整個 DRM 系統就瓦解，DRM Agent 會處理 DRM 內容解密、權利的控管、暫存原始檔…等重要內容。
- 內容發佈者和權利發佈者應分開管理：因為權利發佈者是很重要的系統，除了讓他功能越簡單化越好，除了安全上較好管理，內容發佈者和權利發佈者應分開管理就可以運用 Superdistribution 技術，讓內容更快速的散佈。
- 權利發佈者與使用者裝置必需相互認證：此作用主要是為了讓雙方都是在合法者，防止有非法者從中破壞整個 DRM 系統。
- 內容與權利物件必需先加密才能傳送：先加密之後再傳送的話，內容和權利物件可以在任何無安全通道下傳送，而且也可以儲存，已經是固有的安全了。
- 為了適應各個不同的 DRM 系統，讓各個不同的 DRM 系統都能夠溝通，應該建立起一個國內 DRM 互通平台，以利版權內容的流動性，而國際上互通性 DRM 平台有 OPERA、DMDFusion、SmartRight、MPEG 4 IPMP-X，研究性的 DRM 系統有 OpenIPMP、Media-S 和 OpenSDRM，以及專門在探討 DRM 互通性的組織有 DMP 和 Coral Consortium，可以尋求專家去制定，研究一個有互通性、安全性、有彈性和更新性的 DRM 互通平台。

第四章 數位智財管理(DRM)之核心技術與數位電視多媒體共通平台建置研究

4.1 前言

在DRM的核心技術中分為密碼技術和商業技術，其內容又分為：

- 保護機制：
  - 權利描述語言
  - 多媒體技術
  - 加解密技術
  - 相容性技術
  - 認證與完整性技術
  - OMA-DRM技術
- 付費系統(Billing System)：
  - SET
  - 3-D Secure
  - NetBill
  - eCash

4.2 數位智財描述語言

在數位智慧財產權管理中，任何的權利都得透特定的語言來描述，如此一來才能使每個數位內容能受保護，有權限的使用者才能進行相對的存取執行動作。目前權利描述語言(Rights Expression Language, REL)以 XrML 及 ODRL 兩個標準為主，描述如下：如表 4.1 所示。

表4.1 權利描述語言比較

名稱	國家	主要組織採用	支持組織	其它
XrML	美國	MPEG-21	Adobe、Barnes&Noble、HP、Microsoft、Time Warner、Xreox…等。	目前ContentGuard用來設為音樂產業的通用標準
ODRL	澳洲	OMA	W3C、Adetti、iprsystems、NOKIA、purplecast、AARPA、marktek…等。	由The World Wide Web Consortium(W3C)共同發佈最新版本1.1

4.2.1 ODRL-Open Digital Rights Language[35][36]

為澳洲地區所延伸出來的標準，由 The World Wide Web Consortium (W3C)共同發佈最新版本 1.1，最主要被 Open Mobile Alliance (OMA)所採用，其相關支組織有 W3C、Adetti、iprsystems、NOKIA、purplecast、AARPA、Marktek…等。

4.2.2 XrML-Extensible Rights Markup Language [34]

美國所延伸出來的標準，以 XML 為基礎的程式語言，是從 Xerox's Digital Property Rights Language (DPRL)所發展出來的，目前 ContentGuard 用來設為音樂產業的通用標準,最主要被 MPEG-21 所採用,其相關支持組織有 Adobe、Barnes&Noble、HP、Microsoft、Time Warner、Xreox…等。

4.3 多媒體技術

4.3.1. MPEG (Moving Picture Experts Group)

在ISO/IEC下的非營利工作團體，主要是做數位影音的標準，對數位智慧財產權管理相關的標準有MPEG-2 CA和PART 11、MPEG-4 IPMP、MPEG-21。MPEG－21 Multimedia Framework的出現和發展正是致力於在大範圍的網路上實現透明的傳輸和對多媒體資源的充分利用，並且建構廣泛深入的多媒體框架，將解決付費/訂閱模式(線上及離線)、搜索、篩選、定位、檢索和存儲內容、消費者使用權、消費者隱私…等問題。其中與DRM相關的分支標準技術有下列三部份

- 權利描述語言(Rights Expression Language)
- 權利資料字典(Rights Data Dictionary)
- 智慧財產管理協定(Intellectual Property Management Protocol，為MPEG-21主要核心架構)

4.3.2. MPEG-4 IPMP

MEPG IPMP 一開始是在 MPEG 4 終端機(Terminal)裡被一些"HOOKS"集合所定義的，而MPEG-4 IPMP (Version 1) 的標準定義在IOS/IEC 14496-1；1999，之後，才又發展出更有彈性的技術，稱為IPMP eXtensions，簡稱IPMP-X。

4.3.3. MPEG IPMP "HOOKS"

HOOKS 最基本的定義是一組在解調過程中的點稱之為"控制點" (Control

Points)；在它們之中可以插入一個保護的機制，稱為 IPMP 系統。從解調緩衝區到提供者的媒體資料流中都可以執行 IPMP 的程序。而被 IPMP 系統以 stream 的方式傳送稱為 IPMP Stream。例如：加密金鑰，同調的資訊…等。HOOKS 允許多個 IPMP 系統共同存在相同的終端機(Terminal)，特定保護內容根據內容提供者制定 IPMP 系統在授權時間內才能執行。

"IPMP Hooks"提供智慧財產身分確認資訊 (Intellectual Property Identification Data Set，簡稱 IPIDS)，IPIDS 是各種內容識別符和影音物件(Audio-Visual Objects，簡稱 AVO)聯結起來，再一起包在 MPEG-4 位元匯流檔裡。IPMP HOOKS 可以允許適當的 DRM 系統被使用在順應 MPEG-4 規格的終端機上。靠著 IPMP 系統的 ID 聯結 AVO，而由註冊中心管理唯一 ID。這個 ID 指出那個 IPMP 系統去管理 AVO，除了 IPMP 系統 ID 之外，MPEG-4 IPMP 還提供了私人資料的空間，使 IPMP 系統能夠使用在傳送任何他們所需要的資料。

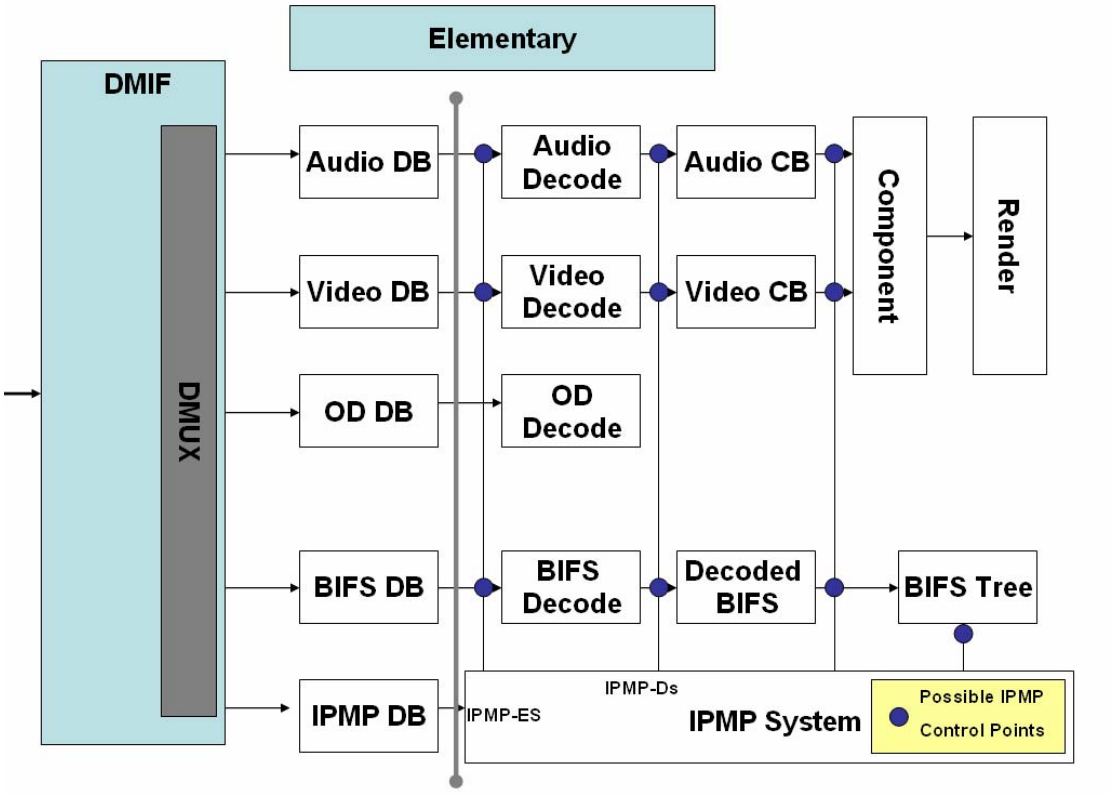

圖 4.1　MPEG "IPMP Hooks" Architecture

這個規格提供了第二個機制為了將 IPMP 系統 IDs 和私人的 IPMP 資料與 AVO 連接在一起：為了 IPMP 資料與 AVO 的同調。當 IPMP 的資訊需要被重送時，讓裝置開始接收和解碼內容，這個機制在 MPEG-4 串流中是很有用的。而機制也賦予一個服務提供者管理內容金鑰的變更，提供額外的安全等級。
無論如何 IPMP Hooks 還是有一些需要討論的問題

- 在沒有 MPEG-4 播放器製造商和 IPMP 系統提供者事先同意的情況下，目前沒有一個標準去具體說明一個 IPMP 系統是如何被"Hooked"在 MPEG-4 播放器中。
- IPMP 系統間互相認證間也沒有標準的機制。
- 無法簡單的取代一個已經損壞的 IPMP 系統。

4.3.4 MPEG IPMP Extensions

用來設計解答以上 Hooks 的"公開性問題"以及在 MPEG 與一些安全方法之中提供更完整的 DRM 架構。

MPEG 近年來架構了一個 IPMP-X (Intellectual Property Management and Protection eXtension)規格，他是最早的 DRM 解決方案去管理 MPEG 內容，提供了一個安全的架構。

MPEG IPMP eXtnesions 不破壞或是影響現存的應用，也就是 Hooks 的規格。一個確認器可以被定義為為了具體說明將使用的 IPMP 解決方案，MPEG-4 IPMP "hooks" 保護的內容可以被 MPEG-4 IPMP-X 終端機存取，當 MPEG-4 IPMP-X 保護的內容是被一個未知的 IPMP 系統保護可以設想成是由一個 IPMP "Hooks"來執行。

MPEG-4 IPMP-X 可以被使用在各式複雜度的成及下控制任何類型媒體的保護，需要使用一個特定的 DRM 系統在 MPEG-4 系統中來保護已知的資料。MPEG-4 IPMP-X 可以保護 MPEG-4 下任何類型的內容例如：影像，聲音，電腦圖檔，文字，互動的內容等等。

當使用者請求存取受 IPMP-X 保護的內容時，MPEG-4 終端機執行 IPMP 工具的列表(IPMP 工具是指可管理內容的存取)，然後找出適當的工具，用終端機中概念性的架構說明也就是工具的管理者，另一個概念性的實體：訊息路由器處理工具跟專端機之間的路由資訊。假如互相認證成功了以及達成所有的 IPMP 工具的請求，一個權力管理 IPMP 工具這個 license 對內容的有效性，然後開始個別執行每個部分的匯流。舉個例子：一個解密的工具解密了內容然後將內容寄到媒體解碼器，然後媒體解碼器解碼了匯流串並將他傳至一個浮水印工具，這個工具從內容中讀取或是在內容中寫入，最後交給內容提供者以供給使用者使用。

在 IPMP-X 和 IPMP 工具之間通訊或兩個 IPMP 工具間通訊，是基於在一種訊息的架構。這個規格定義了一組基準的訊號，IPMP 工具必須組合和傳送他們為了能夠與這個架構中的其他實體通訊，可以分類為以下幾種類型：

- IPMP 連線與斷線訊息 (IPMP Tool Connection and Disconnection Messages)
- 事件通告訊息 (Event Notification Messages)：提供 IPMP 工具有請求的能力和到事件的通告，例如：與其他工具連線或是中斷，偵測浮水印等等。

- IPMP 程序訊息 (IPMP Processing)：定義在 IPMP 程序中的各種行為，像是傳遞鑰匙，使用規則，用影音的浮水印工具溝通，配置可選的加密法等等。
- 認證訊息 (Authentication Messages)：驗證兩個實體（工具或是終端機）之間的可靠度，決定或是創造用來通訊的安全通道。
- 使用者互動訊息 (User Interaction Messages)：一位使用者需另一位使用者的資料，定義使用者與實體間的訊息交換。
- 消費訊息（Consumption Messages）

最後總結一下 IPMP eXtensions 帶來的幾個主要優點：

- 互動性（Interoperability）：兩個不同 IPMP 工具之間的互動是可行
- 安全性 (Security)
- 有彈性的 (Flexibility)：可以自由選擇演算法（用以互相認證，加密，浮水印管理等等）來管理內容。
- 更新能力 (Renewability)：可以簡單的更新舊的IPMP工具。

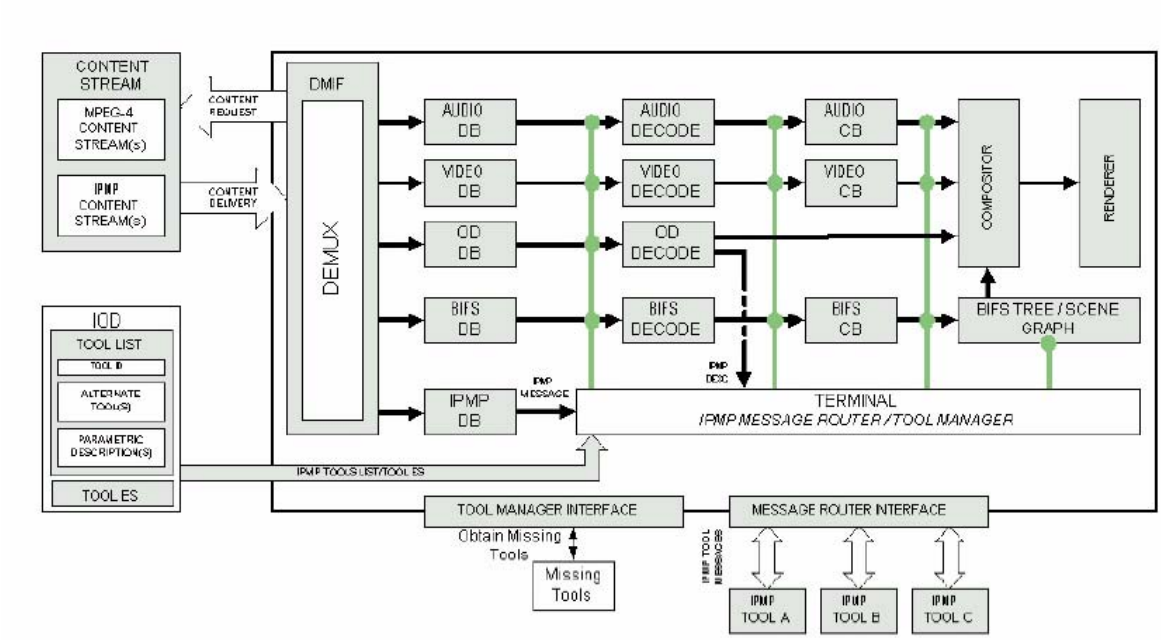

圖4.2 MPEG-4 IPMP Extensions(取自[9])

4.4 加解密技術

在數位內容而且網路發達的環境中，如何讓數位內容受到保護，使得只有經授權的用戶才能觀賞一部電影或是聆聽所訂閱的音樂是 DRM 中最關鍵的技術。勢必要將加解密相關的技術加入數位智財管理架構中來達成使用者付費的目地。在密碼學中，加解密系統可以概略的分為對稱式加解密系統(Symmetric Cryptosystem)以及非對稱加解密系統(Asymmetric Cryptosystem)。以下就兩種系統進行簡單的比較。對稱式系統又稱為 Secret Key Cryptosystem，以換位

(Permutation)以及取代(Substitution)為基本方式，運算速度快，用於大量資料之加解密。在對稱式密碼系統中，加密者(發送端)以及解密者(接收端)會事先共享一把祕密的金鑰。如此，當接收端收到經由發送端加密過後的密文(Ciphertext)時，解密者才能利用同樣的一把金鑰來將密文解開成明文(Plaintext)。重要的是，此把祕密金鑰是整個系統最重要的部份，一旦洩露，則此系統變得不安全，所以對稱式系統會有金鑰分配(Key Distribution)的問題。常使用的對稱式密碼系統如:DES、TripeDES 以及 AES 為主。另一方面，非對稱式密碼系統又稱為 Public Key Cryptosystem，不同於對稱式系統的是，非對稱式系統植基於數學難題，所以運算速度較對稱式系統慢，但無須考慮金鑰之分配，適合用於較少量之資料加解密，如保護對話金鑰或使用者之個人資訊。非對稱式密碼系統的金鑰不再是同一把祕密金鑰，而是會有一把私密金鑰(Private Key)以及一把公開金鑰(Public Key)，私密金鑰只有該使用者擁有，但是公開金鑰則是其它的人都可以獲得(經由 Certification Authority, CA)。如果使用者 A 想要加密明文 M 並發送給使用者 B，並且只想讓使用者 B 才能解開的話，A 可以將明文 M 用 B 的公開金鑰加密，並傳送給 B。當 B 收到加密過的明文後，B 可以藉由自己的私密金鑰來解開此一密文。值得一提的是，在非對稱式密碼系統中，使用者可以利用自己的私密金鑰來對訊息或內容簽章(Signature)，而這個簽章就可以代表簽章者的身份(其它人無法獲得簽章者的私密金鑰就不能仿冒相同的簽章，這點不同於對稱式加密系統)。常見的非對稱式系統為 RSA。兩種系統之簡單示意圖如下。如果 $K_1 = K_2$，則此一系統為對稱式加密系統，而 $K_1 \neq K_2$ 則系統為非對稱加密系統。

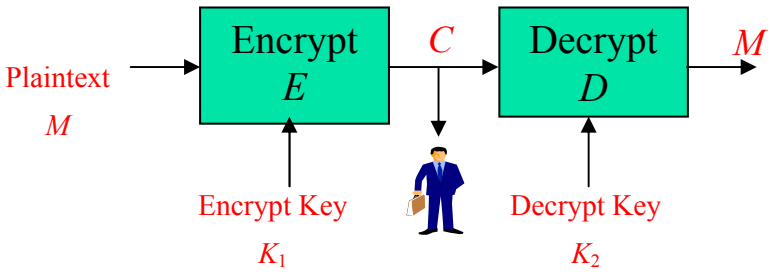

圖 4.3 加解密示意圖

4.5 認證與完整性技術

在4.4節中，我們提到了重要的加解密技術。在此一小節中，我們將討論另外兩個有關於使用者認證以及重要內容的完整性。首先，要對使用者認證可以使用3.4節提過的兩種加密技術，而一般在DRM系統架構中，是以非對稱式加密系統來完成使用者的認證，如OMA DRM等(見3.7節)。在使用者及權利發送者(Rights Issuer)之間，必定要透過適當的認證過程來讓使用者確定此權利發送者的身份以及讓權利發送者可以識別此使用者的身份，以便進行後續如付費的動

作。使用者端在收到由內容提供者(Content Provider)所傳送的內容時，一定得檢查內容的完整性以免該內容已被修改過或是傳送不完整等。而使用者在下載該內容所對應的權利物件時，也必須進行相同的完整性檢查。檢查完整性的技術通常由Hash Function (赫序函數)來完成，而一般常見的Hash Function則為MD5以及SHA-1兩種。Hash Function的功能為給定任一長度內容x，可以輸出成固定的長度h(x)，而且通常是單向的特性，亦即知道h(x)無法導出x的值。

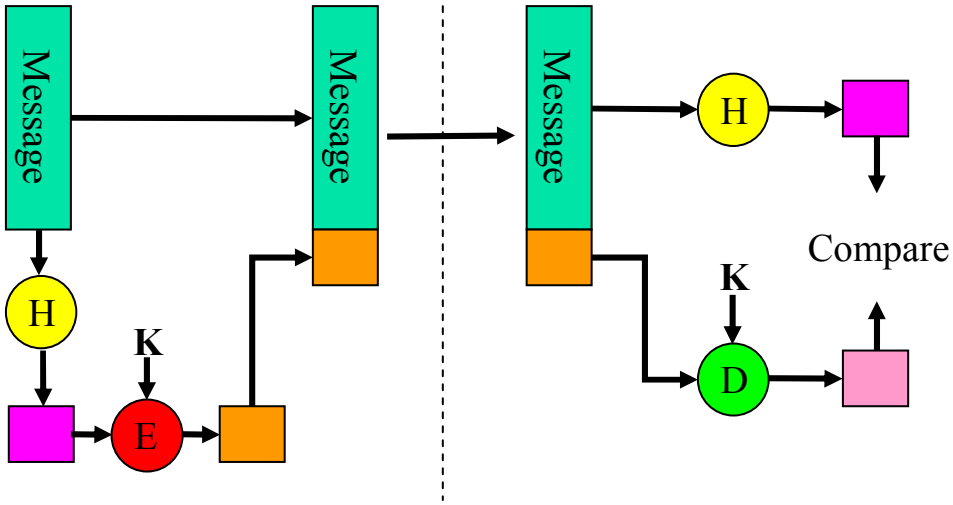

圖4.4 完整性檢查示意圖

由圖中可知，接收端只要將內容再進行一次hash後，再和解密出來的Hash值比較就可以知道內容完不完整。

4.6 互通性技術

DRM技術種類繁多，每家公司都會有自己的一套DRM技術，如何整合不同DRM技術來達到互通性，讓消費者及內容提供者使用上比較方便有效率是一項挑戰。在第二章已有說明幾個DRM系統做到互通性，如OPERA、DMDFusion…等。而目前從事互通性技術的組織有兩個，分別為DMP (Digital Media Project)以及Coral Consortium。分別介紹如下。

4.6.1 DMP (Digital Media Project)

數位媒體計畫(Digital Media Project, 簡稱 DMP)是在 2003 年 11 月正式成立，主要研究成員包括 GartnerG2 與 Berkman Center 的研究人員。目的在於將不同 DRM 系統的相容性訂定一套標準。在 2004 年十月，DMP 發展了互通 DRM 平臺(Interoperable DRM Platform, 簡稱 IDP)的工作草圖規格。DMP 期望在未

來IDP能被製造商和服務提供者當作DRM的軟硬體製作上的規範以利未來的相容性問題。而 IDP 的工作分為三個階段：

- 階段一：主要針對攜帶式影音裝置的技術描述規格，在2005年五月已經發表。
- 階段二：主要針對固定式裝置的技術描述規格，預定在2005年十月發表。
- 階段三：還沒有說明文件發表。

4.6.2 Coral Consortium

Coral Consortium 是一群企業的組合，包含了：InterTrust、Sony、Philips、HP、Fox Movie Studios、Matsushita、Samsung、NDS、STMicroelectronics 以及 DMDSecure。希望獨立於 DRM 技術實現內容的互通作業性。聯盟成員提出了一個支援多種共存 DRM 方案且對用戶透明的互通作業層，允許設備在用戶按下播放鍵後及時找到合適格式的內容。將為採用網際網路和家庭聯網設備的安全內容傳播提供互通作業性。而這個組織所發展的整合性技術為 NEMO (Networked Environment for Media Orchestration)。其主要架構如圖 4.5 所示。

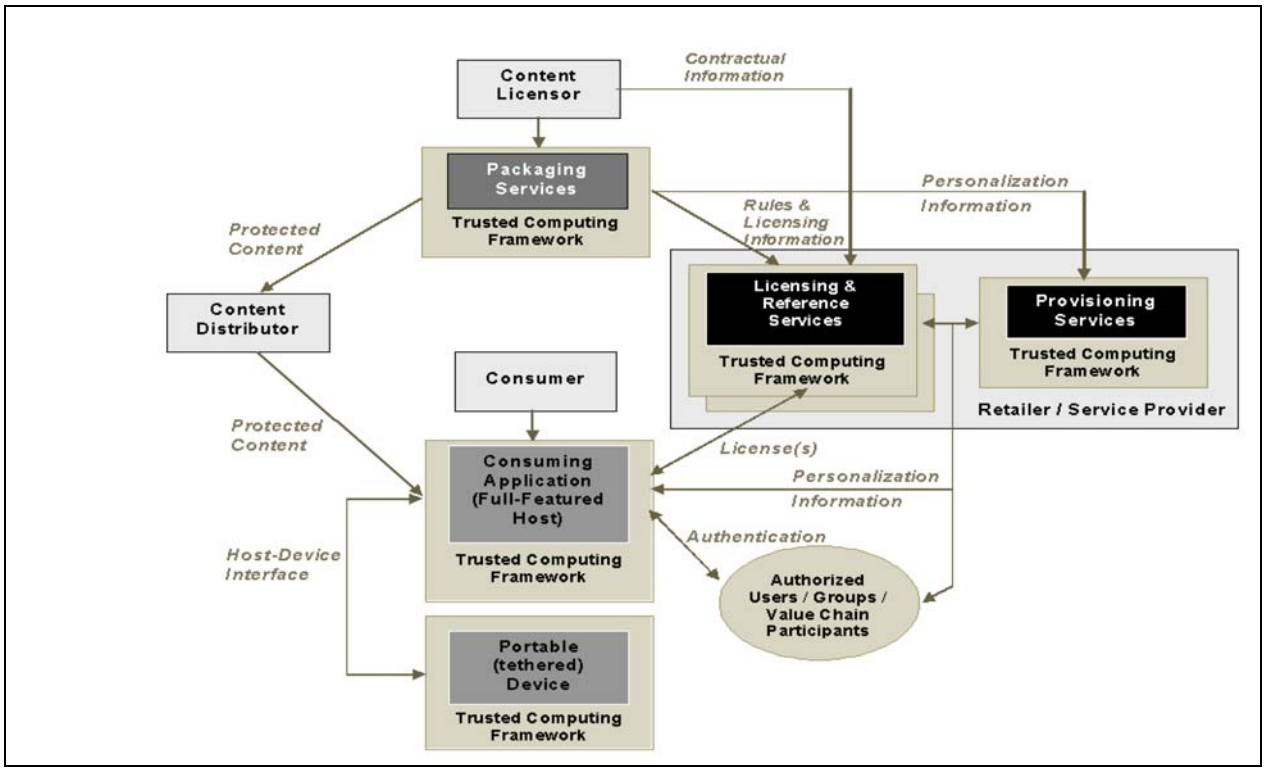

圖 4.5 NEMO 主要架構圖(圖片來源：http://www.coral-interop.org/)

詳細流程如下

Step1：封裝服務(Packaging Service)對數位內容進行封裝，並將契約資訊(Contractual Information)送至 Licensing & Reference Service。

Step2：封裝服務不但把封裝好的檔案送給內容發佈者(Content Distributor)，同

時也把該檔案的權限或規則等資訊送給 Licensing & Reference Service 以提供之後消費者所要求之權限。並且將權限分級，把這個分級資訊送給 Provisioning Service。

Step3：消費者會利用電腦內的交易軟體向 Licensing & Reference Service 查詢有沒有想要購買之數位內容。如果有的話，Licensing & Reference Service 會引導消費者前往該數位內容的來源位址(內容發佈者)來下載檔案。

Step4：Licensing & Reference Service 會向消費者驗證身份，並查詢該消費者的等級。驗證過後，即可對該數位內容進行權限內的操作。

Step5：受驗證過的數位內容也可以傳送至其它的系統(必須支援 DRM 技術)。

4.7 OMA-DRM技術

4.7.1 OMA (Open Mobile Alliance)

開放行動聯盟(OMA)為行動產業發佈和DRM技術有關的規格說明書，因應市場的需求，協助建立跨越國家、操作者和移動終點限制的相容和互動服務。為了擴大移動市場，支持開放行動聯盟的公司將致力於刺激多種更新更強的行動資訊、通訊和娛樂服務，使它們得到快速和廣泛的發展和使用。開放行動聯盟中有很多工作團隊，其中BROWSER&CONENT的團隊有研究Download與DRM的機制，主要已經發佈了四份文件，如圖4.6所示。

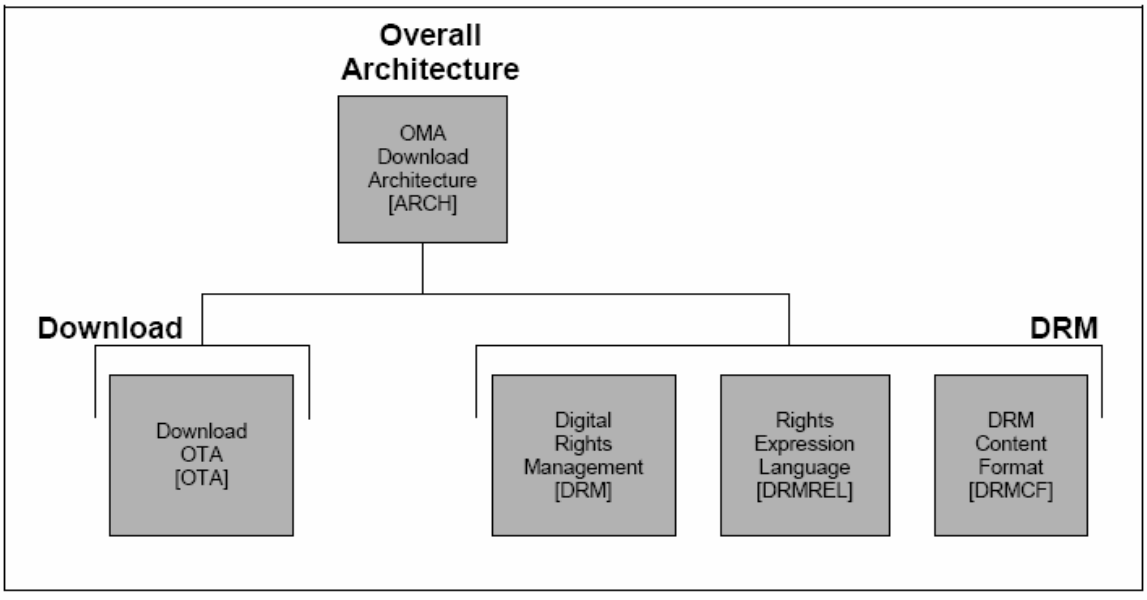

圖4.6 OMA Download與DRM的結構(取自[8])

其中OMA在DRM的方法有三個：如表4.2和圖4.7所示。

- 鎖住傳送(Forward-lock)：沒有DRM的方法，不設定權限，標準權限有播放、觀看、執行和列印多媒體物件，可以用HTTP 、WAP或MMS方式下載到裝

置上，但在裝置上設計不能再對外傳送多媒體物件。

- 結合傳送(Combined Delivery)：有DRM的方法，可以針對不同人給予不同的權限，把權利描述加到內容裡，結合在一起傳送，用鎖住傳送(Forward-lock)的方法一樣傳送，一樣在裝置上，不能再對外傳送內容。
- 分散傳送(Separate Delivery)：有DRM的方法，這是把內容跟權利描述分開不同地方來傳送，而內容允許用點對點(Peer to Peer)的超級傳送(Superdistribution)方式傳送，但權利描述一樣要鎖在裝置上不能傳送出去，主要是把內容用DCF(DRM Content Format)的方式加密封裝，而在權利描述裡放對應內容解密的金鑰，傳到裝置裡就可以解密播放，可權利描述可以針對不司人給予不同的權限。

表4.2 OMA DRM 的比較

名稱	DRM 方法	權限	對外傳送	其它
Forward-lock	無	不設定權限	不行	標準權限有播放、觀看、執行和列印多媒體物件
Combined delivery	有	給予不同權限	不行	結合在一起傳送
Separate delivery	有	給予不同權限	可以(權利描述不行)	這是把內容跟權利描述分開不同地方來傳送，而內容允許用點對點(peer to peer)的超級傳送(superdistribution)方式傳送
未來以PKI為基礎的技術				

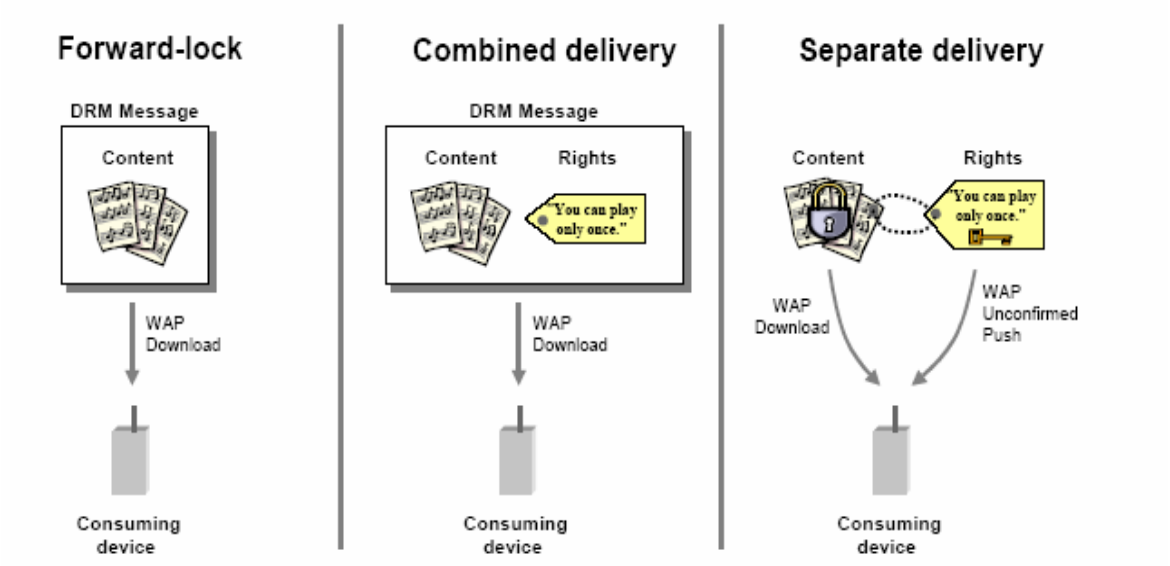

圖4.7 OMA DRM 的方法(取自[8])

4.7.2 OMA DRM核心技術

上一節已經稍微提到了OMA DRM的架構及技術。在此節中，我們將進一步探討OMA DRM(Version 2.0)的一些核心技術，如認證、權利物件的轉移、內容保護以及金鑰分配等等技術。下圖為OMA DRM整個的架構示意圖 [7]。

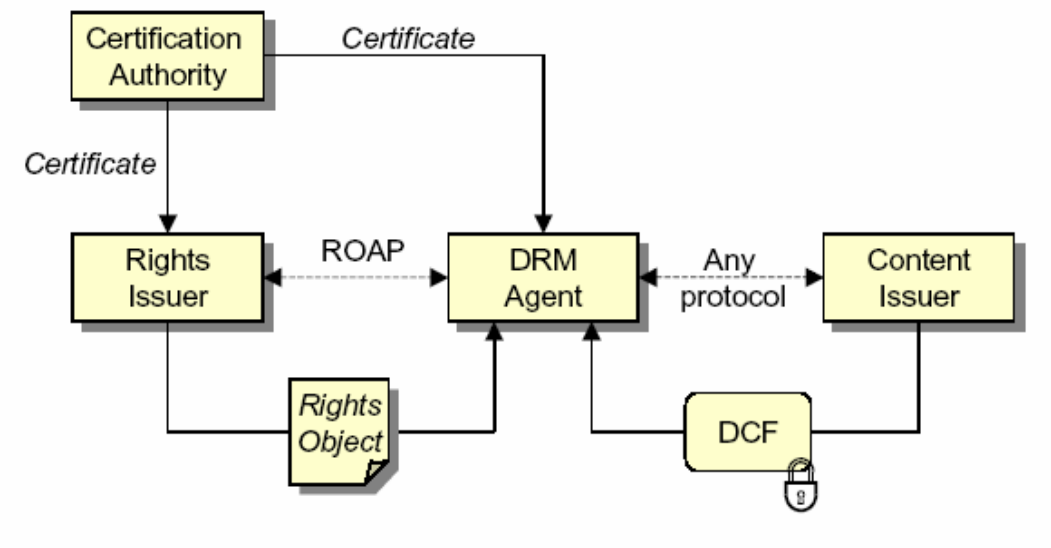

圖4.8 OMA DRM架構示意圖

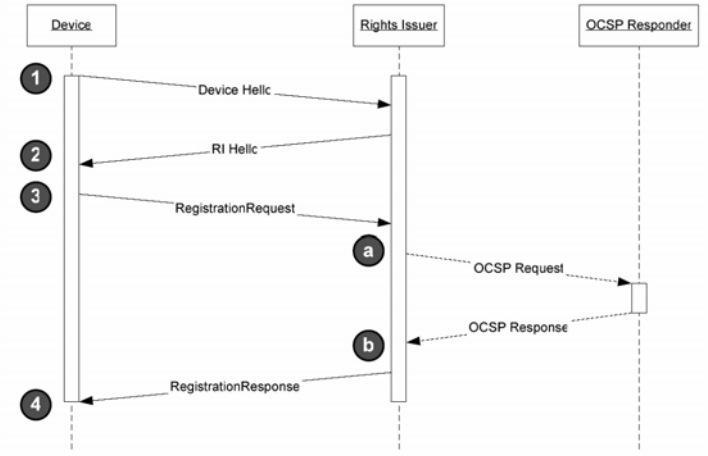

圖4.9. 4-Pass註冊示意圖

圖中清楚的定義了四個角色：Certification Authority(簡稱 CA)、Rights Issuer(簡稱 RI)、DRM Agent 以及 Content Issuer(又稱 Content Provider)。在系統運作前，RI 與 DRM Agent 必須跟 CA 取得合法的授權憑證(Certificate)。DRM Agent 在從 Content Issuer 端下載內容後(受 DRM 技術保護的內容, DCF, DRM

Content Format)，必須先跟 Rights Issuer 註冊並付費下載該內容的相關權利物件(Rights Object)後，才能將此 DCF 文件解密成可以播放的多媒體檔案。而 DRM Agent 與 RI 之間的通訊協定為 ROAP(Rights Object Acquisition Protocol)，包括註冊或是權利物件的下載都是以這個協定來進行通訊。圖 4.9 為 DRM Agent 與 RI 註冊的示意圖 [8]。

而圖中之OCSP(On-line Certificate Status Protocol)的目的在於可以即時讓 RI 確認 Device(DRM Agent) 的身份。如果驗證成功，RI 則會回應 RegistrationResponse訊息並在狀態欄註明"Success"。而在註冊完成以及內容下載完成後，最重要的事情即是下載對應的權利物件來打開該受保護的數位內容。權利物件的下載可以分成二種形式，一種為Pull，另一種則為Push。如圖4.10所示，在Pull形式中，使用者(Device)會跟RI發出某一權利物件的請求後，才下載該權利物件。另一種則較常發生在使用者訂購整個月的內容及權利物件時，RI會在某固定時間將所訂購的權利物件以Push(推)的方式送至使用者端，如圖4.11。

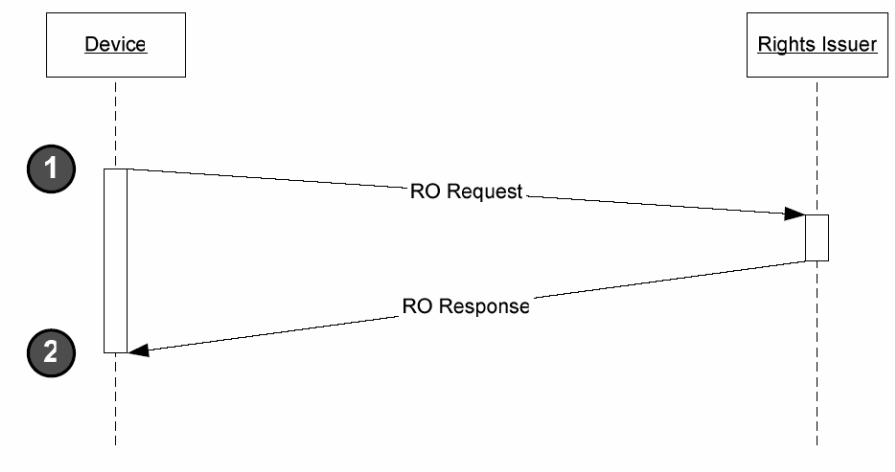

圖3.10 2-Pass ROAP

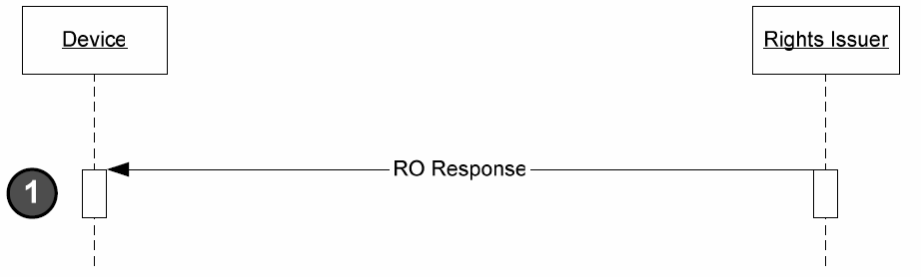

圖4.11 1-Pass ROAP

而在權利物件下載完成後，Device會檢查以下二個項目：1.權利物件的簽章是否為RI所簽。2.此權利物件是否完整(完整件檢查)。如果任一項驗證錯誤，則此物件將無法順利安裝並解開對應的數位內容。此時Device會再次跟RI要求新的

權利物件。

在內容的保護上，OMA DRM是以對稱式的密碼系統來對數位內容加密。首先，RI會先計算

$$C_2 = \text{AES-WRAP}(KEK, K_{MAC}||K_{REK}), C_1 = \text{RSA.ENCRYPT}(P,Z) \text{ ，}$$

其中KEK(Key Encryption Key)為RI利用所選之亂數Z經由金鑰產生函數(KDF, Key Derivation Function)所產生之金鑰；K_{MAC}為檢查權利物件及數位內容完整性的金鑰；K_{REK}為加密整個權利物件的金鑰。C_2為$K_{MAC}||K_{REK}$經過AES(金鑰為KEK)加密過的輸出密文。C_1為亂數Z經由RI的公開金鑰PS用RSA演算法加密後的輸出。最後將C_1、C_2、權利物件(已經以K_{REK}加密，並內含加密數容內容的金鑰CEK)送至Device端。解密過程如下圖所示。

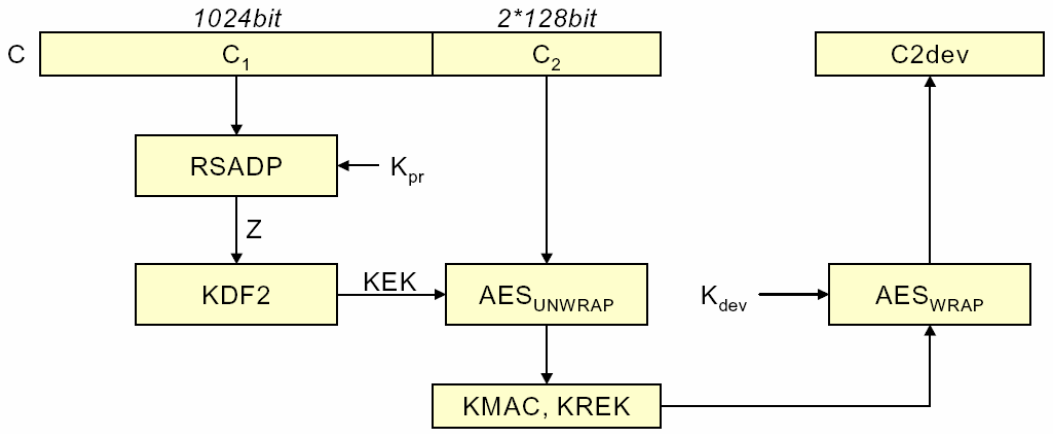

圖4.12 權利物件解密示意圖

由圖中所示，先將C1以使用者(Device)的私密金鑰來解開(只有他能解開)，輸出的亂數Z值再送入金鑰產生器KDF2來獲得KEK。之後就能利用KEK來解開C2並得到兩把金鑰K_{MAC}與K_{REK}。前者用於檢查權利物件的完整性，後者則用於解開權利物件並取出內容加密金鑰(CEK, Content Encryption Key)。如此一來則能解開對應的數位內容了。最後，圖中右側所示為K_{MAC}與K_{REK}兩把金鑰使用完後，馬上以Device的公開金鑰加密並存於記憶體中，這樣做的好處是降低這兩把重要的金鑰外洩的機會，使得此一系統更安全。

4.8 付費系統

4.8.1 線上交易簡介

目前在電子商務的研究方面已經有許多協定被實現，依照各種不同的考

量，如付款金額、可信任的第三者（TTP）型式、付款的時間、付款的元件等，可將電子交易協定分成以下幾個方面：

1. 高額交易及小額交易（Macro-payment vs. Micro-payment）

高額電子交易協定的安全主題主要為識別鑑定、資料完整性、機密性以及不可否認性等等，這樣的協定大部分採取公開金鑰密碼系統和高成本的線上查核；至於小額電子交易協定，因為交易的金額較小，不能提供高成本的密碼系統，取而代之的是低交易成本、高效率、匿名以及較低的安全需求。

2. 先付款及後付款（Prepay vs. Pay-later）

在網路上，買賣貨品需要有兩種傳送的機制：一個是將貨品從商家傳送到消費者的手中；另一則是消費者將錢傳送給商家。電子交易系統是屬於先付款還是後付款將大大的影響到傳送的公平性。目前多數的付款機制都是屬於先付款的方式為多，也造成線上交易常有爭議發生。

3. 線上及離線（On-line vs. Off-line）

當系統之TTP是在交易的時間內執行他的工作，比如說查核使用者的信用，則稱此系統是屬於線上的模式，反之就是離線的模式。線上的查核將降低系統的效率，不過卻能即時提供信用的確認。

4. 付款裝置（Payment Device）

電子交易元件主要可以分成三類：電子交易卡（Payment Card）、轉帳以及數位錢幣（Digital Cash）。電子交易卡是一種信用卡交易的延伸應用，由於當前許多金融機構的支持，電子交易卡已經有許多的使用者，目前在這方面，比較須要考量的是安全性的保證和隱私的保護。使用轉帳來做為付款的方式可以在網路上傳送即時的確認保證，在此我們可以使用數位簽章來代替傳統的簽章，對於這樣的電子交易系統，一個很重要的課題是在於金鑰的管理。電子錢包是基於盲簽章（Blind Digital Signature）的電子交易模式，為了避免數位錢幣的重複付款，數位錢幣的發行人必須維持一個龐大的資料庫以為線上的確認，這可能會是系統一個很大的負擔。

4.8.2 電子交易系統

在此小節中，我們將介紹幾種目前全世界比較有名的電子交易系統，包括有SET[4-6](已不用)、3-D Secure[1]、NetBill[3]以及eCash[2]等系統。

4.8.2.1 SET

SET是由Visa和MasterCard兩大信用卡集團所主導發展而成的，因此這個電子交易系統很自然的，其付款裝置就是使用電子交易卡來進行交易，使其在公開網路中能達到安全的目的。SET的交易結構如圖4.13所示。而由於SET太過於複雜，已被Visa等公司廢除，我們在此就不討論這個付費機制。

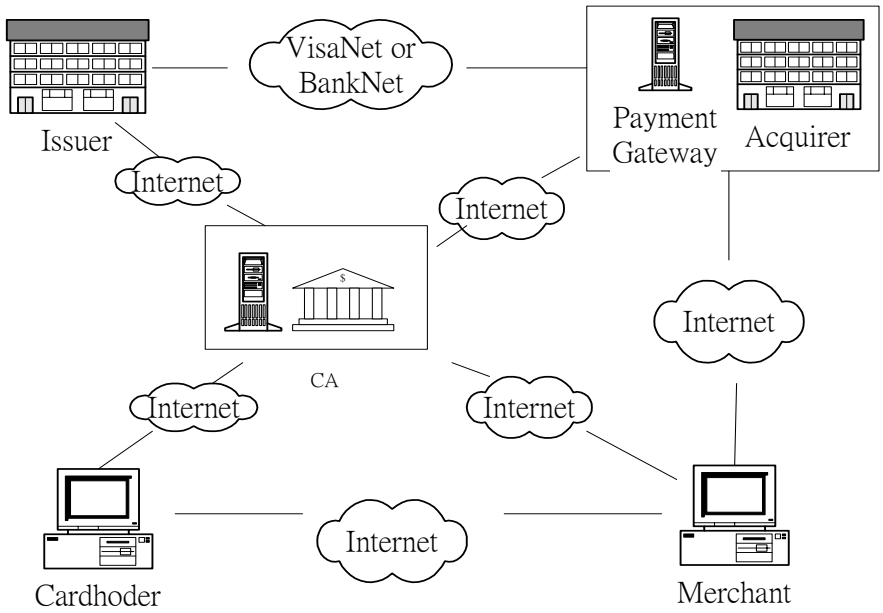

圖4.13 SET系統的交易架構

4.8.2.2 3-D Secure

以網路交易的安全性來主要考量的SET 認證驗證法，是須經由三方認證，本應為最安全與方便的交易模式，但最大的缺點在於使用與推廣不易，消費者端和特約商店端亦需安裝 CCA 及 MCA 憑證，是為最重大窒礙難行之處，故此機制目前 VISA 國際組織已予以廢除。3D-Secure 的模式是改良 SET 在推廣及運用上之不便，所衍生出來的機制，重新把現行網路信用卡交易架構區分為(1)發卡銀行區域(Issuer Domain);(2)收單銀行區域(Acquirer Domain);(3)跨作業系統區域(Interoperability Domain)。

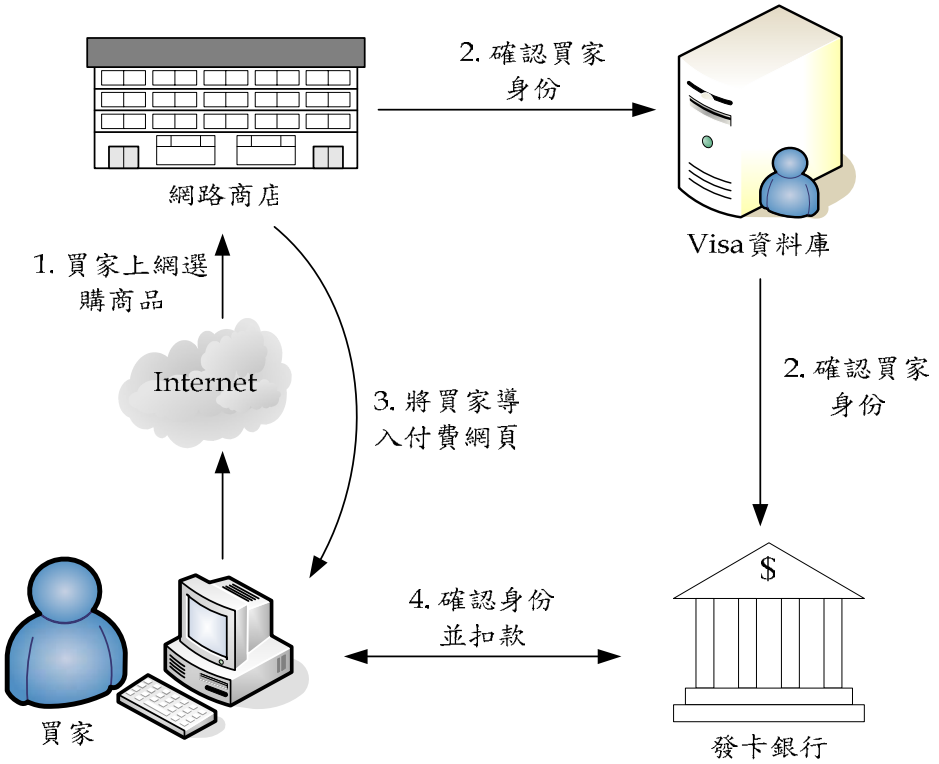

圖 4.14 3-D Secure 架構流程圖[1]

由圖 4.14 可知，整個架構及流程都比 SET 簡化了。持卡人在網路商店購買物品後，商店將會去確認持卡人的卡片真實性，並把持卡人導入發卡銀行確定持卡人身份以避免信用卡被冒用。之後再完成扣款動作，並將交易及認證資訊記錄起來。此時整個交易完成，持卡人將在之後收到由網路商店寄出的物品，而數位資料，如電子書等，則會以線上即時下載為主。

4.8.2.3 NetBill

NetBill 系統是由 Carnegie Mellon 大學聯合 Mellon 銀行和 CyberCash 公司研發而成的，它是屬於小額交易的系統，其交易的基本結構和交易協定如圖 4.14 所示。(EPO：Electroic Payment Order，為包含有顧客 ID，產品 ID、價錢、商家等產品相關資訊的明文)

首先，顧客要求商家報價，商家將貨物價格告知顧客，當顧客同意價格後，即要求商家出貨。商家將其產品資訊用對稱式金鑰K加密後傳給顧客，顧客便將簽章後的EPO傳回給商家，此時商家將其背書過的EPO送至NetBill伺服器，由伺服器判斷彼此的合法性，決定是否可繼續進行交易。並將其判斷結果簽章後送至商家，商家再轉送給顧客，完成小額電子交易。

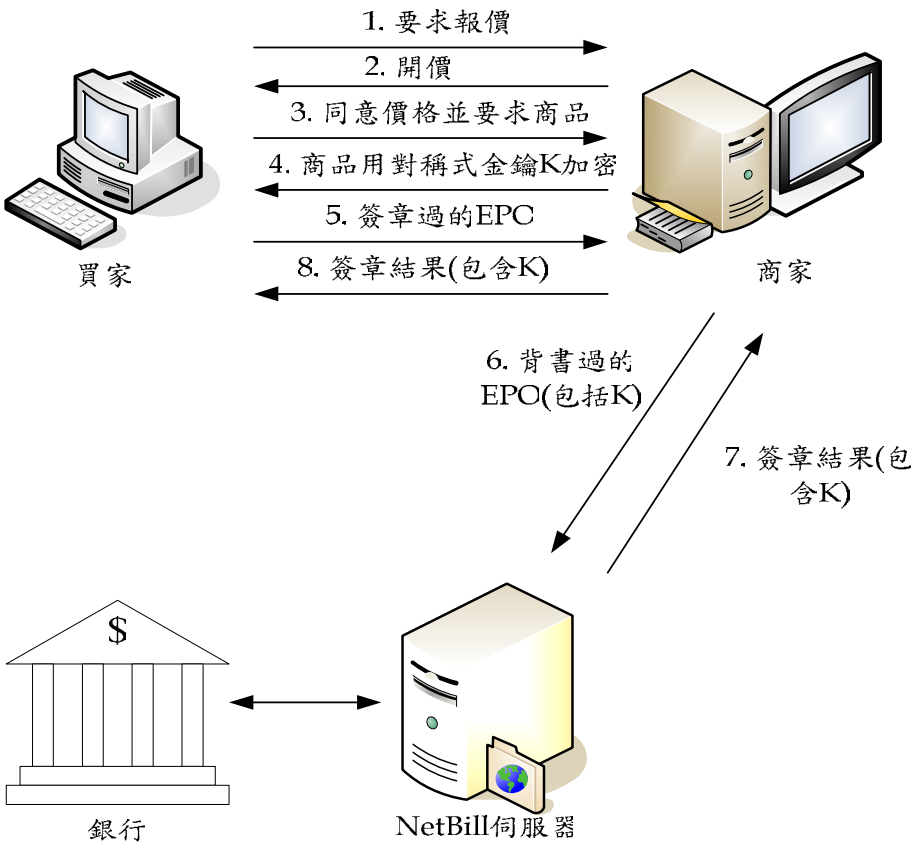

圖4.15 NetBill交易協定

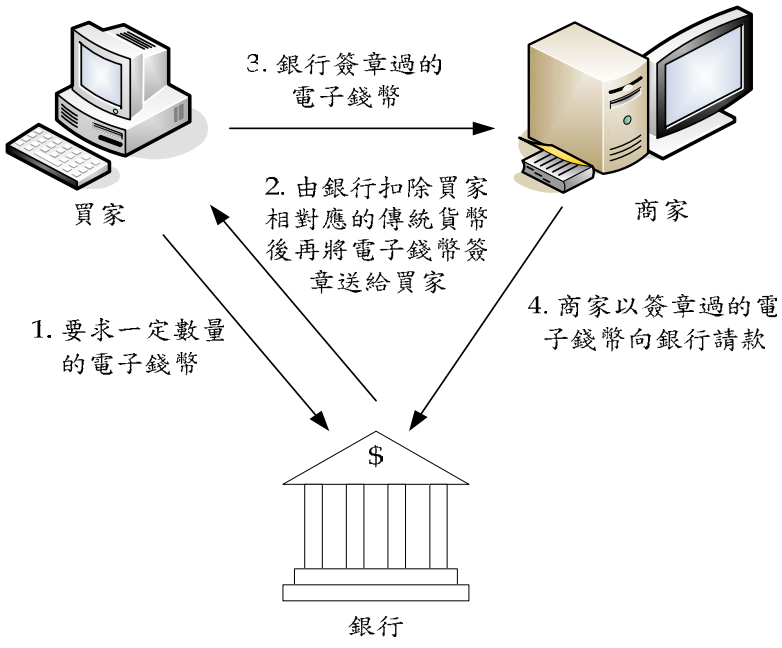

圖4.16 eCash交易流程

4.8.2.4 eCash

eCash是由DigiCash公司所發展出來的，它的付款裝置，就是數位錢幣。採用的密碼技術當然也是數位錢幣所根基的盲簽章技術，圖4.16就是eCash的交易流程圖。首先，由顧客產生一隨機亂數代表其「數位錢幣」，銀行收到顧客帳戶中的金額後，便對「數位錢幣」進行簽章(簽章演算法視情況而定)，顧客把經銀行簽章後的「數位錢幣」傳送給商家，商家再據此向銀行請款。

4.8.2.5 安全電子交易系統

以筆者所在實驗室自行提出的安全電子交易系統為例，說明電子交易系統的運作過程。主要的架構如圖3.17，除了憑証機構（CA）之外，最主要的參與者有三方：商家（Merchant）、消費者（Customer）和可信賴的第三者（TTP），TTP為系統的公平性所在，也是買賣雙方有爭議時的仲裁機構。為了執行的效率，我們將TTP採取離線（Off-line）處理的方式，除了一開始消費者必須先向TTP註冊外，只有在爭執（Dispute）發生時TTP才會介入交易中。

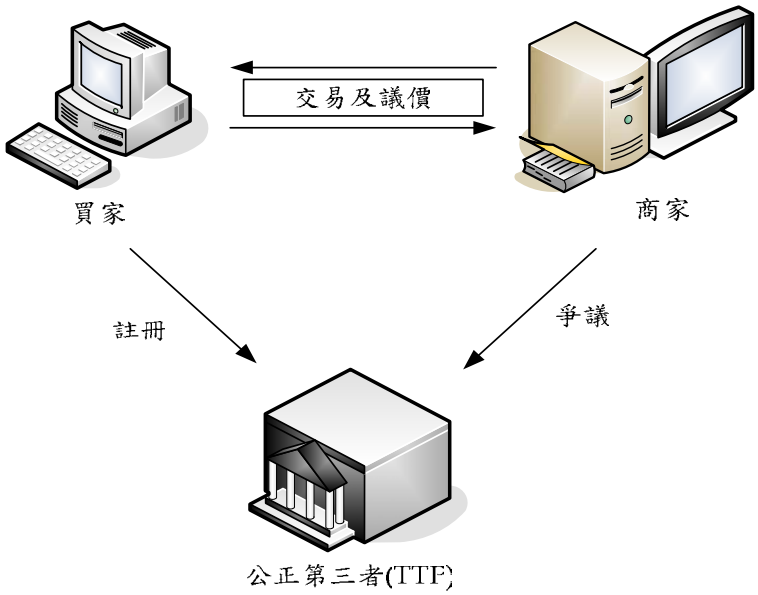

圖4.17 公平電子交易架構圖

1.公平機制

在現實生活中，所謂的公平機制係指「一手交錢，一手交貨」，然在網路交易環境中卻很難達到此一境界，一般的電子交易對消費者存在著不公平的現象，當消費者決定於網路上進行電子交易時，便利用其數位簽章進行網路交易，然若商家並未將貨品送出，則消費者必需透過申訴管道，才可能得到其訂購物品，達到網路公平原則。本節提出將數位簽章分成二部分（部分簽章），分別為簽章一與簽章二。在交易過程中，必須將簽章一與簽章二結合後才能得到完整簽章，利用完整簽章才能完成整個交易行為。

2.安全性和公平性

此架構的安全性是根基於下面的特性：

- 特性一：只有消費者（C）可以產生部份簽章S（m）。
- 特性二：只有商家（M）和信賴的第三者（TTP）可以驗証部份簽章S（m）的合法性，只有TTP可以轉換部份簽章S（m）為完整簽章Sig_C（m）。
- 特性三：如果商家（M）確認交易的合法性，則TTP可以轉換部份簽章S（m）為完整簽章Sig_C（m）。

3.交易系統運作

- 認証（Certification）

  每個在網路上的實體，包含可信賴的第三者（TTP）、商家（M）和消費者（C）都必須先進行這一個程序，為各個實體的公鑰作認証。

- 註冊（Registration）

  此程序的主要目的是要使消費者（C）先向可信賴的第三者（TTP）進行註冊驗証消費者的身份，並共同分享一個金鑰，此時消費者會交付部分秘密給TTP，使TTP有能力為產生消費者的第二份簽章（簽章二），即確保TTP可以將消費者的部份簽章$S（m）$轉換為完整的簽章$Sig_C（m）$。然TTP是無法產生消費者的簽章一，故無法代表消費者進行網路消費。

- 議價（Negotiation）

  此程序是為了使交易更具變通性，讓交易雙方有議價的空間，但是決定是否接受所出的價格可能需要人工處理。議價行為之進行直到雙方對交易金額達成協定或取消交易為止。

- 交易（Payment）

  當雙方都同意了協議的價格後便進入了這個程序，此時消費者使用其私鑰進行第一部分的簽章，簽章一便透過網路傳送到商家端，商家可用簽章一來判斷消費者的合法性，若簽章一正確，則商家便透過網路或實體通路進行貨品運送。當消費者查核此貨品的正確性後，便再利用其私鑰進行第二部分的簽章，並將其傳送給商家。商家便可將簽章一及簽章二組合成完整的簽章Sig_C（m），據此要求銀行從消費者的帳戶轉帳給商家。

- 爭議（Dispute）

  爭議有兩種情況，一種是商家（M）沒有將貨品傳給消費者（C），那麼商家將無法取得消費者的完整簽章Sig_C（m）；另一種情況是商家已經將貨品傳出，但是沒有收到消費者的完整簽章Sig_C（m），也就是說兩種狀況都必須經過TTP的幫忙商家（M）才能取得貨款。

解決方法：TTP將消費者（C）的完整章簽Sig_C（m）送給商家

（M），將貨品用消費者（C）的公鑰加密送給消費者（C）。那麼不論是情況一或二商家都能擁有消費者（C）的完整章簽$Sig_C(m)$和而消費者也必定擁有貨品，使得交易完成。由於我們的貨品是網路可傳輸之二進位元的資料，故即使重覆，消費者（C）沒有獲益，而商家（M）並沒有損失，至於如何防止電子貨品被拷貝賣出可用加密的方式，但此議題並不在此文討論。

這些特性使得消費者（C）相對於商家（M）沒有任何的優勢，確保交易可以公平地被完成。最後，比較所列舉的電子交易系統，如表4.3所示。

表4.3　電子交易系統比較表

	一般交易/小額交易	線上/離線	較有利方	付款時間	資料庫負荷	CA	付款裝置
NetBill	小額交易	線上	商家	先付款	高	無	轉帳
SET	一般交易	線上	商家	後付款	高	有	信用卡
3-D Secure	一般交易	線上	商家	先付款	高	無	信用卡
eCash	一般交易	線上	商家	先付款	高	無	數位錢幣
公平電子交易系統	一般交易	離線	公平的	後付款	低	有	轉帳

4.8.3 大學聯考分發系統及其收費機制

由於目前大學聯考演變成考招分離，就是考試與分發是獨立付費，考生考的成績不好時，可以選擇不參考志願分發，如此就可以省下此部份的費用。我們在此將此一特殊的付費機制拿出來討論，以供參考。線上報名分發的流程如圖 3.18 所示。線上報名系統中，如有考生有十二萬人的話，報名系統會在一開始時，先建置十二萬份的帳號及密碼組。如果有一考生聯考完後，準備參加志願分發，他會先跟銀行付費購買線上報名系統的帳號及密碼，此時銀行會通知線上報名系統，使得該帳號啟用。之後，該名考生再以該組帳號密碼登入線上報名系統並與該考生的身份連結在一起，最後就能開始選填志願的流程了。

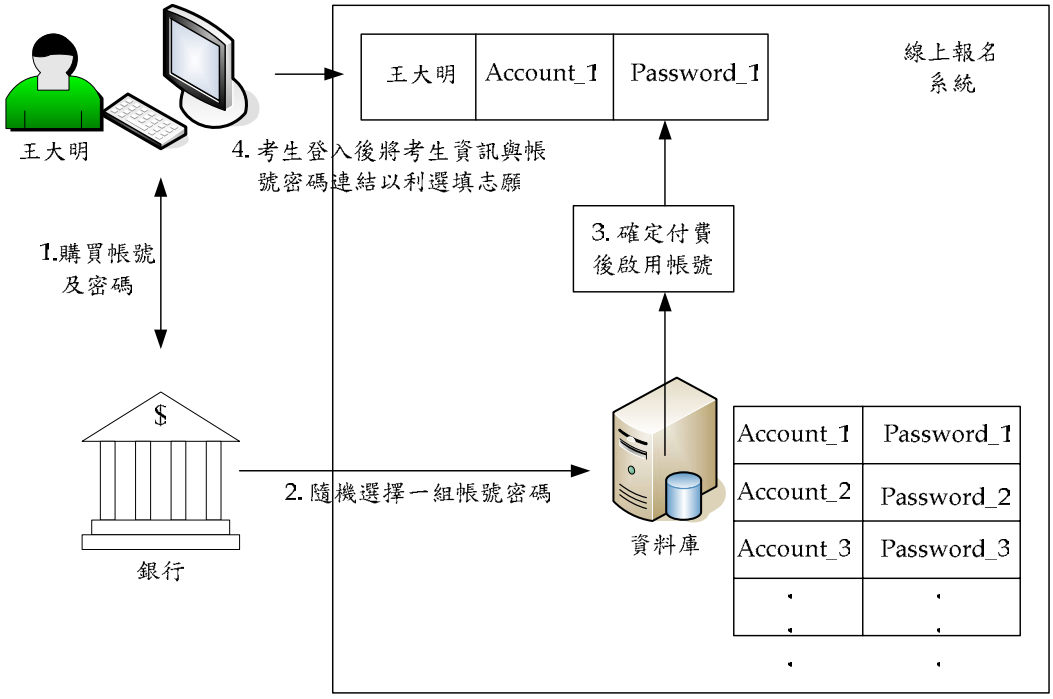

圖 4.18 大學分發流程示意圖

4.8.3 結合回傳通道之收費方式討論

用戶端可以利用此一方式來點閱所需要的節目或是利用回傳通道來進行互動節目，如線上投票及脫口秀等等。如何來完成付費並取得該有的授權是我們這小節的重點。我們在這期中報告會先提出幾種可行的方式進行討論，而在期末報告時，將會選擇一種最適合台灣目前的廣播及現有環境的付費方式以提供電信總局來參考。分別介紹如下，並參考圖 4.19 及圖 4.20。

1. 信用卡線上付費：

(a)付費方式

(i)事後付費：線上付費但是還未扣款，需要幾個工作天後，銀行才會將帳單寄至用戶端來繳費。此種方式類似於 3.8.1.2 節的 3-D Secure 的機制。

(ii)即時付費：線上直接進行扣款的動作，用戶端在此一方式必須輸入自己的帳戶號碼及一些身份確認的動作，之後即進行扣款的動作(約幾分鐘內)。

(b)付費架構：透過銀行來收錢

(i)單一銀行：所有電視台的節目相關付費皆由同一家銀行負責。缺點是：所有的用戶訂閱節目資訊以及所有電視台業者的營業額會被該銀行全數知悉，將會有相關的穩私權問題。

(ii)多家銀行：如果是由多家銀行來負責的話，上述的缺點將可以解決，也不會有隱私權的問題發生。但缺點是：各電視台業者需要和多家銀行簽約以利後續的付費。

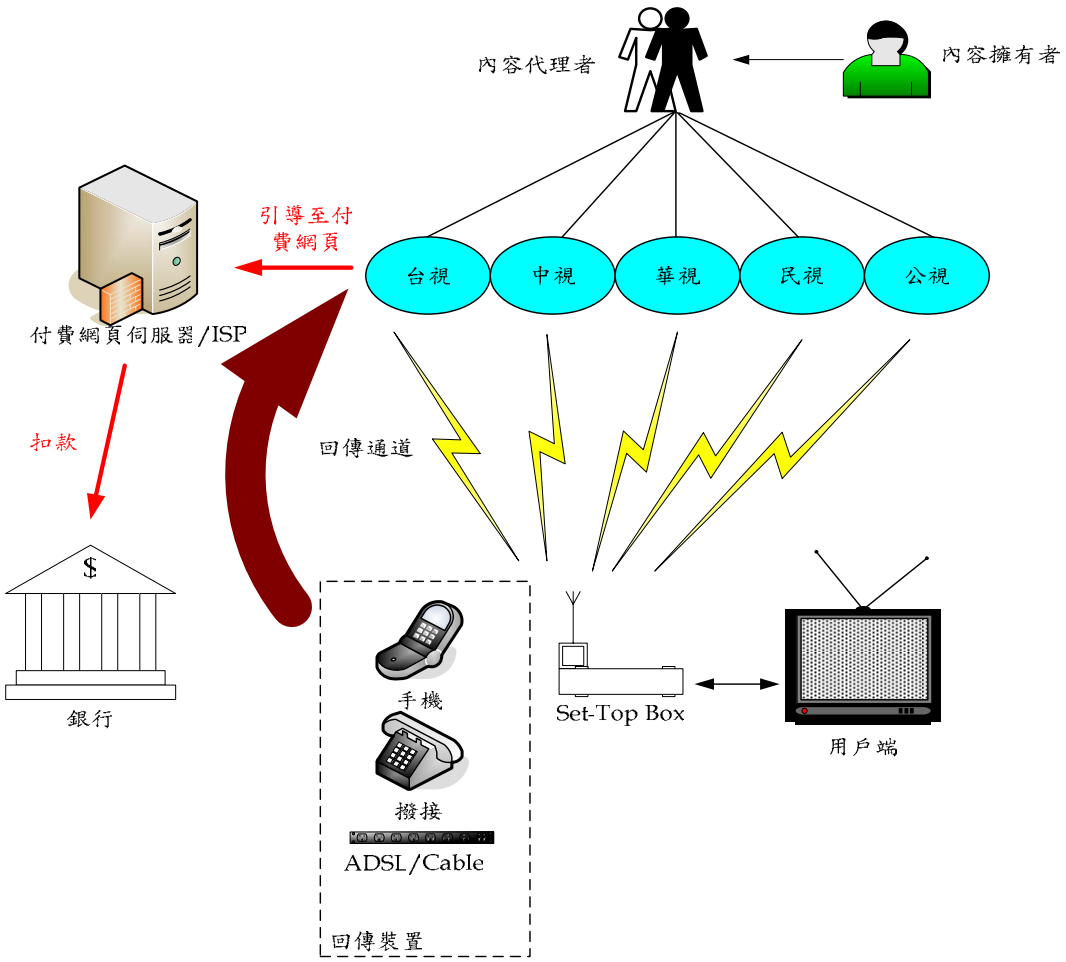

圖 4.19 線上付費及 ISP 直接收費架構圖

2. 由電視台直接收錢：

如圖 4.20，此種方式可以藉由電視台業者直接發卡，電視台業者經由卡上的點數直接對用戶進行扣點或扣款等動作，而電視台業者的資料庫也需一併更新。直接收費可以避免電視台業者的資訊被第三者獲得，不會洩露出自己(電視台)的敏感資訊。而缺點是：客戶很有可能無法以一家電視台發行的卡通用於另一家看視台。舉例來說，台視所發行的卡，就不能點閱中視的付費節目，用戶就必須一人多卡。

3. 透過 ISP 收錢：

各家電視台必須與網路服務供應業者(ISP)簽署合約，由 ISP 直接收錢，而台灣的 ISP 業者不只一家，如此一來將可以避免有一家 ISP 決定任何一家電視台的營業額。而經由 ISP 收費的話，也是要符合政府的相關規範才可以勝任代收的工作。

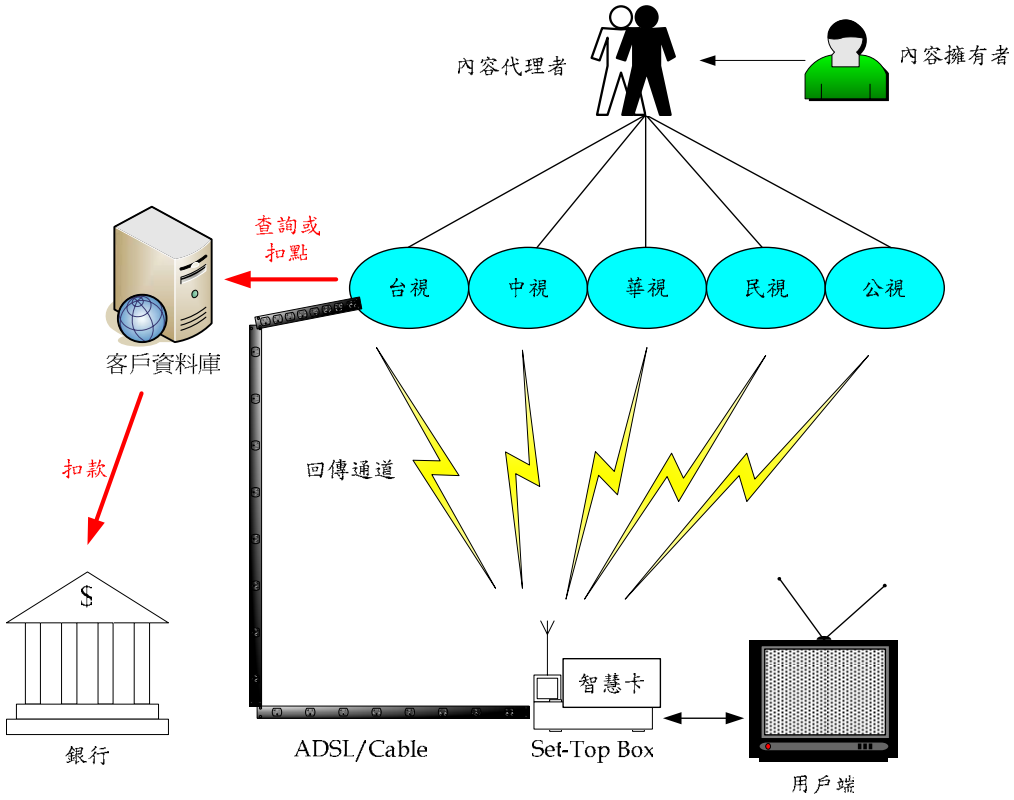

圖 4.20 電視台發行智慧卡扣點示意圖

上述的機制都必須注意一點，就是要避免全部都由一家銀行或者是 ISP 來代收錢，才能夠防止敏感資訊洩露以及電視台業者的資訊外洩。此外，任何代收的銀行或是 ISP 都應該是有相當的信譽才可以成為代收的機構。更重要的是，有關係到錢的機制都一定要關心的議題--爭議。舉例而言，如果某用戶點閱最新的影片欲觀賞，錢也付了，但是影片沒有廣播下來，那麼就會發生糾紛及爭議。所以我們建議應該由政府單成立適合的申訴的單位來解決此類問題，而且回傳的資料(包括訂閱的內容及是否付費等訊息)也必須存留一定時間以供檢查，並要注意偽造問題。如何防止偽造或是耍賴等問題也是付費機制裡必須要特別留意的。

4.9 DRM 與無線數位電視多媒體共通平台建置研究

4.9.1 DRM 與 IPDC 共通平台之研究

IPDC 為頭端廣播平台，由廣播方式傳送串流資料，IPDC 封裝成 MPEG -2 串流之前，資料來源檔由 DRM Issuer 先加密成 DRM 保護的型式，而 Rights Issuer 產生相對應的權利物件(Rights Object，簡稱 RO)，權利物件有解開 DRM 封裝的金鑰和描述內容檔案的權限，當消費者從廣播取得 DRM 檔時，再由 SMS 的方式取得 RO，並在 DRM Controller 控制播放，而在 MPEG-2 編碼時，也可以再加上 CAS 的裝置擾碼，加強廣播上的安全性。如圖 4.21 所示