

數位家庭之數位權利管理與分享機制

薛夙珍

schsueh@cyut.edu.tw

朝陽科技大學資訊管理系

楊志宏

s9314629@cyut.edu.tw

朝陽科技大學資訊管理系

摘要

數位權利管理(Digital Rights Management, DRM)已廣泛應用於網路多媒體交易，現行的數位權利管理模式多採用一份數位內容搭配一張授權證(License)，而一張授權證只能使用於一台設備上。因此，當消費者想要在其他設備上播放數位內容時，就必需再向授權中心購買授權證。此外，當使用者想要在不同設備上播放同一首數位內容時，也必須和 DRMs 保持連線以取得不斷的服務，一旦使用者離線後播放數位內容的服務就會被中斷。這不但限制了使用者的使用自由，也間接阻礙數位權利發展空間(通常使用者不會願意對同一件商品進行重覆消費)。因此，本論文基於數位權利管理架構，提出了一個建置於數位家庭環境中的家用數位權利管理系統(Home Digital Rights Management, HDRM)，透過 HDRM 進行數位內容的管理與使用權限設定，並發放可以使用在數位家庭中的授權證。如此一來，不但讓使用者可以將數位內容使用於數位家庭中的任何設備，又可不需經常與 DRMs 連線即可取得播放權利進行離線播放，同時達成數位內容共享並保護該內容使用不侵權的雙重目標。

關鍵字：數位家庭、數位內容、數位權利管理

Abstract

The technology of Digital Rights Management (DRM) is used in transactions of multimedia products in the Internet. The digital content is associated with a unique license that limits the usage to a designated device. Thus, a consumer must purchase another license for the playback

of the same digital content in another device. Furthermore, the consumer has to keep the device connected online with the DRMs providers in order to re-new the license. Once the connection is broken, the playback of the digital content will be stopped. Consequently, current DRM technology restricts the freedom of using the digital contents of the rights-owner and hinders the development of digital rights. The concept of digital family has been proposed by Intel, Microsoft, IBM and so on recently. The goal of digital family aims at sharing digital contents for all the devices in the family. If the digital content is protected by current DRM technology, the sharing can hardly be achieved in digital family. Therefore, we propose a new scheme to provide fair use of digital contents in the digital family. The Home Digital Rights Management (HDRM) is created to manage the digital content. The usage and the rights of the digital contents can now be shared under the Home License (HLicense) in a digital family. Consumers of the same family can share the purchased digital contents in other devices and play the digital contents offline by the services of the proposed HDRM scheme.

Keyword: digital family, digital content, digital rights management

1. 前言

多媒體產品在傳統的銷售模式中，商家必須花費大量生產成本製作成實體產品進行

銷售。消費者購買了實體型式的多媒體商品，即可在任何設備上進行播放，亦可輕易地將商品的移轉或買賣，卻也衍生了非法複製或移轉的問題，侵犯了商家與著作人的權益。多媒體商品數位化趨勢雖然讓商家降低了重製與銷售成本，但也讓使用者便利地透過網路取得非法的數位商品，更加劇了盜版的問題。因此，導入數位權利管理(Digital Rights Management, DRM)概念是重要的改善方法。

然而，數位產品的保護與權利管理在使用上有相當的限制，所購買的數位商品經常只能在特定設備上播放，也不能隨意將數位內容轉移或買賣，對使用者造成了種種的不便。傳統多媒體與數位內容的比較，如表 1 所示。因此，在廠商追求最大獲利下，如何兼顧消費者權益，達到合理使用(Fair Use)原則，是重要的研究議題。

合理使用議題必須在廠商與消費者雙方需求中取得平衡，廠商希望使用者必需取得合法的使用授權才能使用該數位內容，並依照授權權利使用數位內容，而不能擅自以自由意識使用數位內容，也禁止非法複製、使用。然而，消費者卻希望廠商所提供的數位商品，不需要連線也不需搭配特定軟硬體，便可播放數位內容，且能夠提供數位內容復原與轉移的權利。

基於合理使用原則，本協定在數位家庭環境中，建立一個家用數位權利管理系統(HDRM)，透過 HDRM 以群組方式向 DRMs 進行註冊，再經由 HDRM 管理數位內容和控制數位內容播放權限，讓使用者能在不同設備播放數位內容，又不需要經常與 DRMs 進行連線，而能夠確保數位內容不會被侵權。以下將在第二章節介紹 DRM 的相關文獻，第三章節說明所提出的協定架構與方法，第四章節進行分析與討論，第五章節進行最後結論。

表 1、傳統多媒體與數位內容比較分析

	傳統多媒體	數位內容
出版方式	光碟、卡帶	數位化資料透過網路傳輸至使用者播放設備中
消費方式	需購買整張光碟、卡帶	可依自己喜好選購
保護方式	CSS、CDS、LaserLock...	數位權利管理技術
播放方式	CD/DVD播放器、音響、隨身聽	特定的播放程式、設備
播放限制	無限制	依提供者授與的播放權限為依據
其他	也有其他學者將CSS等防拷技術視為是數位權利管理的技術、方法	使用者需要時常online更新數位內容授權，確保能夠持續播放數位內容

CSS (Content Scramble System) 利用資料擾亂方式，防止使用者複製檔案
CDS (Cactus Data Shield) 在光碟中加入修改技術，造成檔案在複製時產生錯誤
LaserLock 在光碟中隱藏錯誤檔案

2. 文獻回顧

數位家庭是由 Intel 等 17 家國際大廠成立組成的數位生活網路聯盟(Digital Living Network Alliance, DLNA)[6]所提出的一個概念，目的在於統一數位家庭的規格與標準，例如有線/無線網路協定、數位內容格式、傳輸協定、隨插即用設備標準和數位權利管理標準等，提供數位家庭中的家電皆能共享數位內容。

在 DLNA 中定義了數位家庭中數位設備的分類，包含了需要接上線路家庭網路設備(Home Network Device, HND)、無線手持行動通訊設備(Mobile Handheld Device, MHD)和協調有線和無線之間溝通橋樑的家庭基礎架構設備(Home Infrastructure Device, HID)三大類。透過這些家電和標準化的協定，使用者可以隨心所欲的在家中使用數位內容，例如在煮飯時可以透過冰箱播放出美妙的音樂，在泡澡時能夠觀看當天的即時新聞等，如圖 1 所示。



圖 1、數位家庭架構[6]

有了數位家庭中數位設備的統一規格，即可進行進一步的數位權利管理 (Digital Rights Management, DRM)。Digital Rights Management: Business and Technology[2]這本書中，對 DRM 的定義是「DRM 負責控制和管理權利(Rights)來保護智慧財產權」，IDC White Paper[11]對 DRM 定義則是「運用軟體服務和保護技術在數位內容的生命周期內，來控制和管理數位內容的使用者授權和數位內容的使用規範」。數位權利管理是對數位內容進行保護、控制及管理的一種概念。數位內容泛指所有可以被數位化之事、物，例如聲音、圖像、影像、文件等。透過保護技術的運用，數位內容發行者可以對數位內容進行加密保護、權利宣告，以達到保護智慧財產權的目的。

Koenen、Lacy 和 Mackay 學者曾在 “The Long March to Interoperable Digital Rights Management”[12]文中提出數位權利管理的架構如圖 2 所示，相關個體包括了內容提供者(Content Provider)、內容分派者(Content Distributor)和使用者(Customer)三個實體，內容提供者將內容封裝產生受保護的內容、憑證(License)規則及相關的契約資訊，透過可信任的環境下將受保護的數位內容交由內容分派者進行傳輸分派，並由授權證伺服器管理憑證。當顧客想要取得數位內容時，需向內容分派者要求取得數位內容，再由授權證伺服器和提供服務的供應商溝通取得使用者購買權限的方式、付款與否，產生授權證並傳給使用者，交由可信任的應用軟體進行解密、播放，最後再由服務提供商將獲利分給各個實體，達成利益共享的目標。

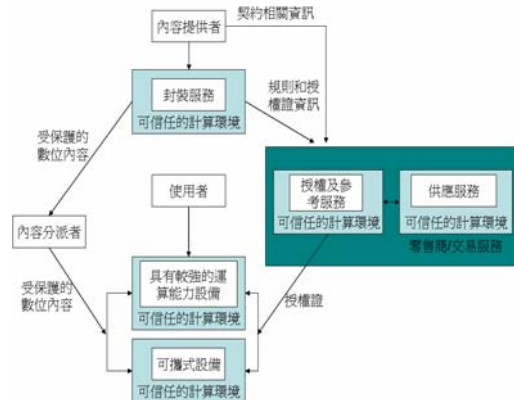


圖 2、數位權利管理架構[12]

有了 DRM 架構後，需要 DRM 權利表示語言來說明、解釋數位內容的使用規則(Usage Rule)，通常這些規則會被包含在 License 中，例如數位內容的金鑰、發行者的數位簽章及使用規則，而使用規則必需清楚明確地說明數位內容的使用規則。在 DRM 中常見的權利表示語言有 Open Digital Rights Language (ORDL)[14]、Digital Property Rights Language(DPRL)[7] 及 eXtension Rights Markup Language(XrML)[8]。

ORDL 是以 XML 為基礎而發展運用在 DRM 系統的權利語言，擁有較高彈性權利宣告方式和支援許多不同格式的數位內容規格支援，例如圖像、聲音、電影等，其中包含了資產(Assets)、權利(Rights)和群組(Parties)三個核心實體。資產包含所有的數位內容，權利被用來建立資產被同意可以使用的規則，群組則是包含了顧客和權利擁有者。DPRL 同樣是以 XML 表示語言發展而成的權利表示語言，由 Xerox 公司所開發，著重於控制主要和衍生而出的使用者中權利的建立。DPRL 主要的目標為適當描述權利與將權利說明訂定標準，提供操作上的定義說明，並提供可延伸的方式來支援新的語言。XrML 是由 DPRL 所延伸的一種語言，也是以 XML 描述語法為基礎的權利語言，提供了更多的說明能力和功能，例如整合、實體(Entities)的驗證和增加了結構(Structure)和語義(Semantic)標記的後資料

(Metadata)說明。此外 XrML 更進一步的提供了使用位置與追蹤情況的具體說明能力。

除了 DRM 架構與權利表示語言外，微軟開發了 Windows Media Rights Manager (WMRM)[9]，當使用者欲播放數位內容時，需要連線至 DRMs 取得 License 授權才能進行播放。WMRM 架構允許同一個數位內容在 10 台不同設備上進行播放。由於 License 採集中化管理方式，每一台設備都需要連線至 DRMs 取得授權，讓 WMRM 可方便管理、偵測使用者可否有侵權之行為。WMRM 架構，如圖.3 所示，來源端(Seed)會將產生的數位內容經過編碼後，傳給內容提供者(Content Provider)，再由內容提供者將數位內容進行加密、封裝。當使用者取得被加密後的數位內容，需透過應用軟體(Windows Media Play)進行播放，當應用軟體偵測到該內容有版權時，便會啟動多媒體權利管理(Windows Media Rights Management)機制向授權證發行商(License Issuer)要求取得授權證，當授權證發行商接受到要求後，會針對使用者提供的資訊(包含使用者的硬體資訊、購買的權利…等。)產生一張專屬的授權證，當取得授權證後，再由應用軟體負責解開受保護的數位內容，進行播放。

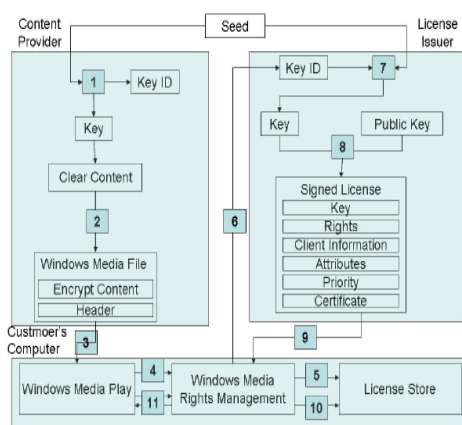


圖 3、WMRM 架構圖[9]

IBM 的 Xcp (eXtensible Content Protection)[13] 則依循內容保護系統架構(Content Protection System Architecture,

CPSA)[3]所定義的規範，建立一個在家用網路中數位內容分享的架構。家用網路中數位內容採用廣播式加密(Broadcast Encryption)，在家用網路內的每一種設備皆可自由傳輸與使用數位內容(如圖 4 所示)。當數位內容被傳輸至網路外時，數位內容會受到加密保護(例如採用 Content Protection for Recordable Media (CPRM) / Content Protection for Pre-Record Media (CPPM) [4, 5])，或以 Content Protection System Architecture (CPSA)公認的輸出方式(例如 DTCP)，防止家用網路以外的其他人在未被授權的情況下使用數位內容。

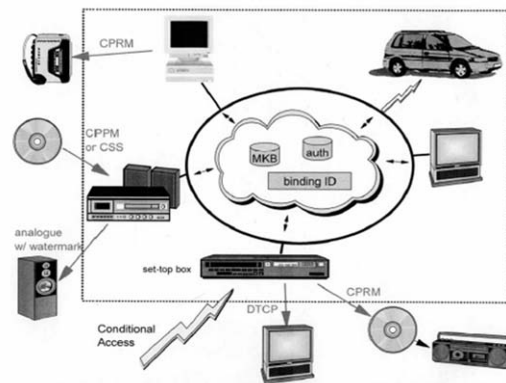


圖 4、採用 CPSA 架構的 Xcp 群組

Helix DRM[10] 是由 Real Network 所發展的 DRM，採用 Media Commerce Suite Technical (RMCS)[10]技術，藉由與硬體廠的配合嵌入 Helix DRM 達到安全共享的目的，並提供多種格式的支援，例如 Real Media(RM)、MP3、MP4 等。此架構包含二種模式：(1)Native Support 模式，當產品嵌入 Helix DRM 的 Helix DRM Client 和 Helix DNA Client 後，便可以啟動此模式，尋找鄰近的設備進行連結溝通。(2)Transfer to secure memory 模式，當確定要進行數位內容傳輸後，便會啟動此一模式，確定數位內容在傳輸過程中不被入侵，圖 5 為 Helix DRM 架構。

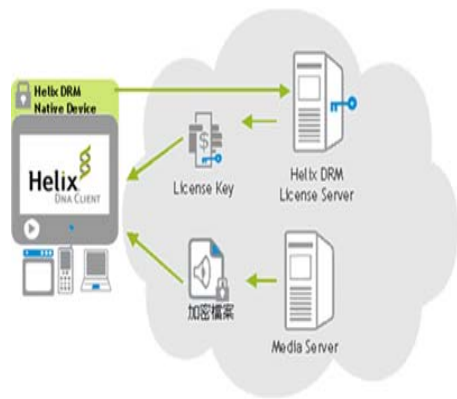


圖 5、Helix DRM 架構[10]

3. 協定設

在我們協定的設計中，透過數位家庭權利管理系統(Home Digital Rights Management，以下簡稱為 HDRM)進行權利管理，其可以是一部電腦或數位機上盒等設備，需定期與 DRM 中心進行連線更新 License 及應用軟體，並負責設備的註冊、檔案管理及 License 的協助更新。整個數位內容的加密、解密之活動，皆需要經由安全的硬體(例如安全的儲存區域或加解密晶片)或軟體協助完成。每當設備與 DRM 中心進行連線時，DRM 便會檢查使用者的硬體是否符合安全要求、應用軟體是否符合 DRM 接受的版本、檢查設備的硬體安全性。此外，當授權方式為無限制授權時，使用者在取得數位內容後可以自己使用，而不受到 HDRM 的理管，也不需要再與 HDRM 進行授權證更新，因此，可能造成使用者不願意將無限制授權的數位內容權利轉給其他家庭內的成員使用，只能待使用者再向 HDRM 連線時取回授權權利，所以，本協定在運行上適合於計時或計次的授權方式，較不適合無限制授權的使用方式。

在 HDRM 架構中，數位家庭之設備皆需符合 DLNA 提出的數位家庭設備規格，而每一設備在加入數位家庭環境之前，需先向 HDRM 進行註冊，取得在數位家庭中的群組識別碼(GID)。此外需要向 DRM 進行購買新

的數位內容時，必需透過 HDRM 連至 DRM 來進行購買，藉此確保在數位家庭中 License 及檔案能夠被適當的管理、分派。在數位家庭中有各種類型的家用設備(如圖 6 所示)，彼此可以透過有線或無線的區域網路分享數位內容。當需要購買新的數位內容或取得 License 時，便會連線到 HDRM 再由 HDRM 連線到 DRM 取得需要的服務。

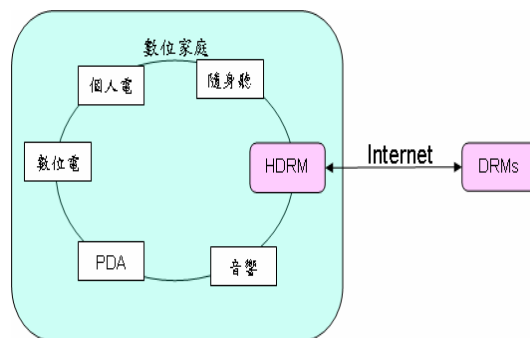
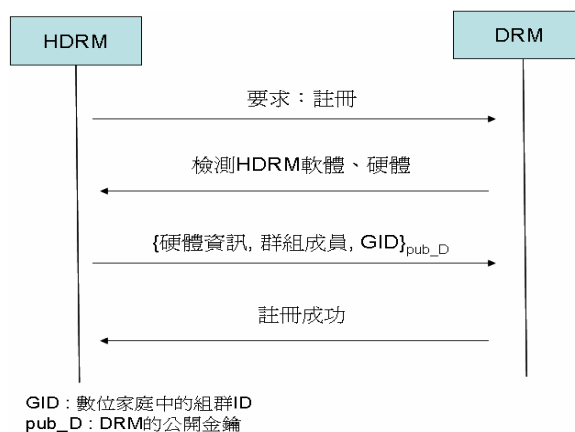


圖 6、HDRM 架構

當 HDRM 第一次向 DRM 中心要求服務時，必需先註冊取得認可，DRM 對 HDRM 進行硬體及軟體檢測，確定符合標準後，HDRM 將硬體資訊、群組識別碼(GID)和組群內成員資訊告知 DRM，確定資訊無誤，通知 HDRM 註冊成功，此時 HDRM 即可向 DRM 要求服務。詳細流程，如圖 7 所示，



GID：數位家庭中的群組ID
pub_D：DRM的公開金鑰

圖 7、HDRM 向 DRM 註冊

當使用者以手持設備進行數位內容的購買、License 取得及更新等相關流程時，必須透過應用程式與 HDRM 進行連線，如圖 8 所示。當設備與 HDRM 連線後，HDRM 先針對

設備硬體的安全性及應用程式的版本進行檢查，並確定該設備是否已經向 HDRM 註冊，完成檢測後 HDRM 會依照使用者的需求協助使用者取得相關的服務。接下來，將針對流程中註冊、購買、取得數位內容及更新進行說明。

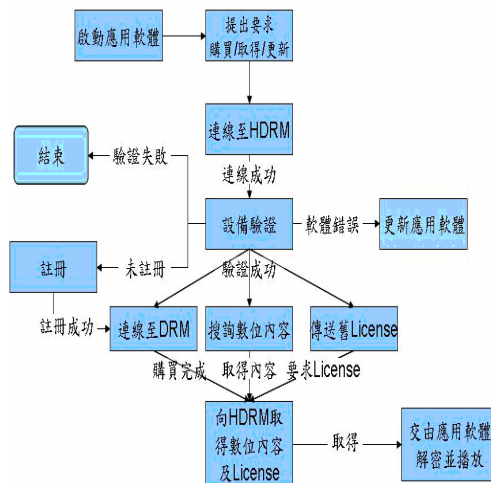


圖 8、HDRM 架構下之工作流程

(一) 註冊：當使用的設備尚未向 HDRM 註冊時，將被要求先作註冊，設備必需將本身的硬體資訊告知 HDRM，此時 HDRM 會連線至 DRM 要求更新群組，DRM 會透過 HDRM 來檢查設備的硬體及軟體是否合法。當確定設備的合法性後，HDRM 會將群組識別碼(GID)、設備識別碼(LID)及一把共享的秘密金鑰 SK 傳給設備，完成註冊程序。詳細流程，如圖 9 所示。

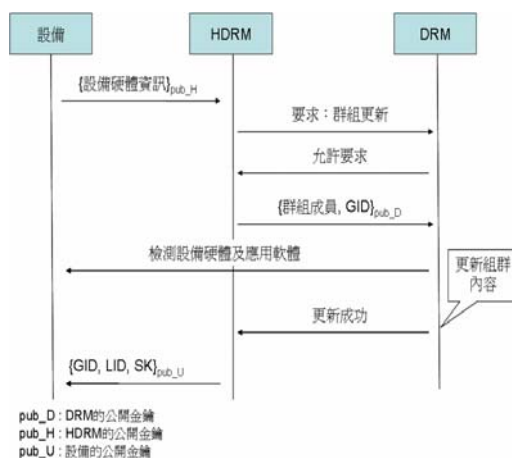


圖 9、設備向 HDRM 進行註冊

(二) 購買數位內容：當註冊與驗證程序完成後，使用者要求購買數位內容時，HDRM 連線至 DRM，並提供使用者瀏覽可購買的數位內容。使用者確定要購買的數位內容後，便會將群組識別碼(GID)、設備識別碼(LID)及欲購買的數位內容編號(SID)傳給 HDRM。當 HDRM 確定 GID 及 LID 皆無誤後，便會將 GID 及 SID 傳給 DRM 進行購買，DRM 依 HDRM 的購買發給 HDRM 已加密數位內容及 License，最後由 HDRM 將已加密的數位內容及修改過後產生的 HLicense 傳給使用者，再經由應用程式解密並播放，如圖 10 所示。

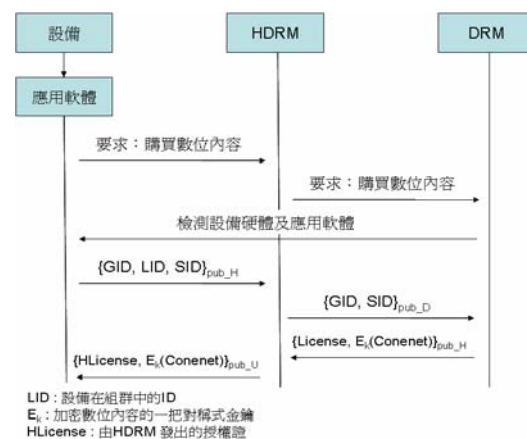


圖 10、購買數位內容

(三) 要求取得數位內容及播放：使用者亦可以直接向 HDRM 要求取得目前在數位家庭裡擁有的數位內容，此時 HDRM 會提供使用者瀏覽目前在家庭中所有的數位內容。當使用者確定要取得數位內容後，將 GID、LID 及 SID 傳給 HDRM，如圖 11 所示。

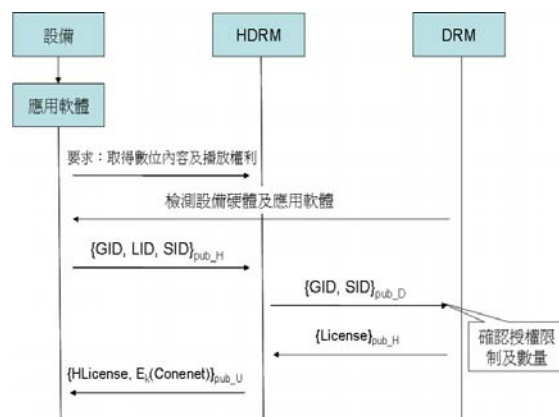


圖 11、要求取得數位內容

(四) **更新 License**：每一張 License 均記錄了播放到期日或可播放次數，當到期日或播放次數用完後，使用者便需要向 HDRM 要求取得新的 License。若使用者從其他設備取得加密的數位內容，此時使用者取得的 License 並不符合該設備使用，則需要向 HDRM 取得 License，如圖 12 所示。使用者必需將 GID、LID、SID 及過期的 License 傳給 HDRM，再由 HDRM 向 DRM 要求取得新的 License，當 HDRM 取得新的 License 後再修改成為家庭 License 傳給傳用者，再由應用軟體軟進行播放。

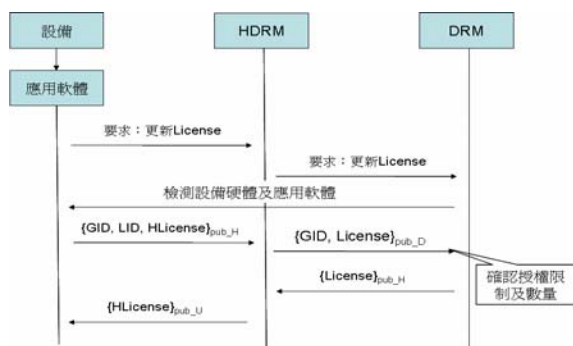


圖 12、要求更新 License

(五) License 管理不論在購買、取得數位內容及更新 License 的流程中，HDRM 都扮演了重要的中繼及 License 管理的角色，接下來將對憑證管理作說明。

(1) 設備加入群組與退出

當新設備要加入群組時，便會向 HDRM 進行註冊，HDRM 則向 DRM 告訴新設備加入之訊息，註冊完成後便可自由在群組內設備使用數位內容，亦可將數位內容帶出家庭外使用(設備離開數位家庭後，其仍屬於群組成員)。當群組要加入另一群組時，由於該設備已經在本群組註冊，該設備必需先回本組群進行退出動作，由 HDRM 告知 DRM 設備退出訊息，才能加入其他群組。當設備退出組群後，HDRM 便會向 DRM 更新資訊，因此該設備便無法再使用本群組中新的 License，但退出前的 License 使用至到期日或次數用完為

止。

(2) License 內容

當完成購買手續後，DRM 依 HDRM 群組購買權限(同時多少設備播放、播放次數、到期日)產生 License (如圖 13)。MetaData 被用來說明在 Usage Rule 中宣告的權利內容，例如，到期日的計算方式、權利歸屬的判定...等。Usage Rule 用來宣告權利，Signature(DRM) 是發行者針對 License 及權利宣告據有不可否認性的簽章驗證，Hash(Protect Content) 則是驗證已加密的數位內容完整性及 $E_k(\text{Content key})$ 被用來解開已加密的數位內容。

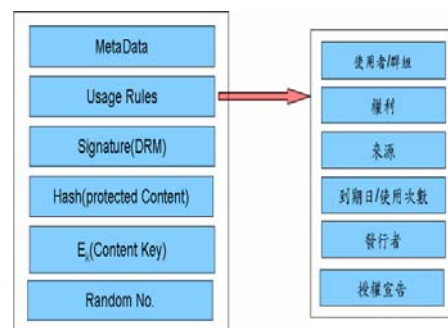


圖 13、DRM 產生的 License

當 HDRM 取得 License 後，利用 RD 及事先彼此分享的秘密金鑰 SK 進行運算取得一把金鑰 K_1 ，並利用 K_1 將解開數位內容金鑰(Content Key)的 E_k 加密為 $k_1(E_k)$ ，最後附加至 License 產生在數位家庭中使用的授權證 HLicense，如圖 14。

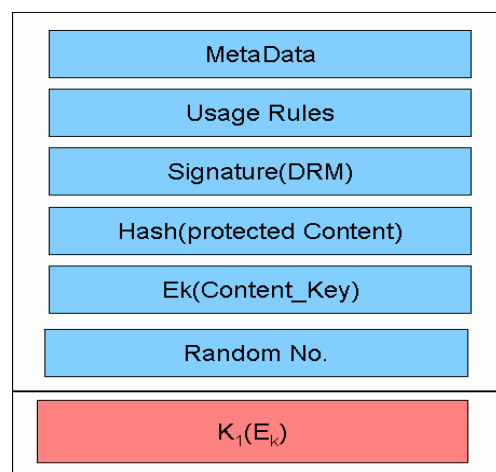


圖 14、HDRM 產生的 HLicense

(3) 加密與解密

當HDRM取得DRM傳送的License後，將隨機亂數RD取出和事先已經分享的秘密金鑰SK進行雜湊函數運數 $\text{Hash}(\text{RD}, \text{SK})=\text{S}$ 值，再利用DES[1]的概念將S擴張為 64Bits的金鑰 K_1 ，再利用 K_1 加密解開Content Key的 E_K 成為 $K_1(E_K)$ ，最後再將 $K_1(E_K)$ 嵌入到License產生HLicense並傳給使用者。以下以例子來說明加密方法：

假設RD為Rights，SK為Trust，經由雜湊演算法($\text{Hash}(\text{Rights}, \text{Turst})$)產生S，S的值为science，將science轉換為ASCII碼： $[\text{science}] = [(01110011) (01100011) (01101001) (01100101) (01101110) (01100011) (01100101)]$ 共 56 位元，再加入同位元檢查碼： $[\text{science}] = [(01110011) (10110000) (11011010) (00101100) (01010111)(01110011) (10001100) (11001011)]$ 產生共 64 位元，利用金鑰排列表-KP(見表 2)進行做金鑰初始排列。

金鑰初始排列後產生 $[\text{science}] = [(11000110) (10110101) (00101011) (00111011) (01010101) (10001100) (11000111)]$ ，再將排列後的值由中間切割為二個部份， $KL = [(11000110) (10110101) (00101011) (0011)]$ 與 $KR = [(10110101) (01011000) (11001100) (0111)]$ ，再透過位移表進行位移(見表 3)。

經過位移程序後產生 $KL' = [(10001101) (01101010) (01010110) (0111)]$ 與 $KR' = [(01101010) (10110001) (10011000) (1111)]$ ，最後透過金鑰壓縮表CP(見表 4)將 KL' 及 KR' 壓縮合併，經過壓縮後即產生第一把金鑰 $K_1 = [(00101101) (11011000) (11001110) (00110111) (01111111) (01000000)]$ ，最後利用 K_1 與 E_K 進行XOR來加密 E_K 。

DES演算法能產生 16 把金鑰，利用產生的第一把金鑰來加密 E_K ，並再將 K_1 以 DES 演算法產生第二把金鑰 K_2 ， K_2 經 DES 演算法產生 K_3 ，如此每一個循環便能產生 16 把

加密金鑰。

表 2、金鑰初始排列表 KP

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

表 3、位移表

回合數	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
左移位數	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

表 4、金鑰壓縮表 CP

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

解密程序則是在使用者取得License後，透過應用軟體算出 $S = \text{Hash}(\text{RD}, \text{SK})$ ，並將S以DES演算法求出 K_1 ，再利用XOR函數便可以算出 E_K 。當解密完後，應用程式也會將 K_1 以DES演算法算出 K_2 ，再利用 K_2 與 E_K 進行XOR來加密，如此進行 16 次的加解密運算。當 16 把金鑰均已使用後，軟體會再將S再以雜湊函數運算產生 S' ，再將 S' 以DES計算便能再產生 16 把金鑰，依此類推，不斷重覆變更加密金鑰。當使用次數到達規定次數後，應用程式會隨機產生一 64bits的亂數金鑰，並對 E_K 進行加密，當使用者在下一次播放數位內容時，因解不開金鑰，應用軟體便會要求再向HDRM連線，更新 License。

License中Usage Rule內包含了到期日及使用次數原則，當採用到期日方式時，DRM會先與設備進行時脈校正，確定設備中的時脈是在可容忍誤差之中。採用次數方式時，可使用次數以 16 的倍數為佳，因每進行一次雜湊值，便能產生 16 把金鑰來保護 E_K ，當可使用

次數為 16 的位數時，應用軟體可以輕易的判別是否已經到達規定的使用次數。例如：使用的次數為 128 次，再第進行第六次雜湊後，便不會再產生第七次雜湊，而改以亂數金鑰加密 E_K 。當數位內容無法被解開播放時，應用程式便會要求向 HDRM 連線取得 License 更新。

4. 分析與討論

在數位家庭環境下，使用者可以自由的轉移數位內容到其他設備播放而不需要特定硬體支援，而在軟體方面，仍需要符合 DRMs 信任的應用軟體才能執行播放行為。在本協定下不需要時常與 DRMs 連線進行授權取得或 License 更新之動作，只需在第一次購買、要求數位內容時和使用次數或期限到期時才需要再與 HDRM 進行連線溝通。至於 License 備分由 HDRM 負責 License 和數位內容的管理，因此當使用者發現 License 遺失時，只需向 HDRM 連線再要求一張新的 License。因此在合理使用議題上，達到了下列目標，如表 5 所示。

表 5、本協定達到的目標

項目	解決情形	說明
需搭配特定軟體、硬體	△	本協定仍需要可信任的軟體來協助播放數位內容，但不需額外硬體支援
數位內容可否轉移	◎	在合法使用情形下，可將數位內容轉移至其他設備
是否需時常與 DRM 進行連線	◎	不需要經常與 HDRM 或 DRM 進行連線，只要在 License 到期時才需進行連線
是否允許 License 備份	◎	除了設備內儲存一份數位內容及 hlicense 外，在 HDRM 也會另外儲存一份，以防止數位內容或 License 遺失
◎：已解決		
△：能夠達成一半要求		

本協定是透過不斷改變加密金鑰來防止惡意攻擊者破解受保護的數位內容。攻擊者如果要透過硬體來攻擊時，由於在註冊於連線時，皆需要進行檢測動作，因為不論採用硬體或軟體都會事先被偵測出，當設備有惡意攻擊意圖時，DRM 將會要求 HDRM 撤消在群組中的註冊，DRM 本身亦會將讓設備列入黑名單

中，防止該設備有二次攻擊之可能。

當數位內容及 License 已傳入設備後，設備再進行攻擊行為時，首先攻擊者必需事先破解 License 的編碼方式取得 RD 值，當攻擊者有能力取出 RD 值算出 S 值時，仍必需破解 DES 演算法，才能成功算出 E_K 。

5. 結論

數位家庭是未來的家庭生活娛樂發展趨勢，透過數位家庭的建立，使用者不但可以享受到高品質的影像、音樂，更可以建立許多數位環境集中化控管便利生活。本協定是以使用者在合理使用原則下進行研究，未來研究方向希望將公平使用原則中，賣方對於公平使用原則的議題加入進行研究。此外採用 XOR 方式進行加密，在安全性上較為不足，因此將針對此方面研究，找出一個對稱式加密法來保護 E_K 。另外本協定是以設備為基礎來進行數位內容共享，但如果以人為基礎，當購買者購買了數位內容後，便可在數位家庭內甚至於家庭之外都能播放數位內容，而不受硬體、軟體和需要連線等限制，播放數位內容。

參考文獻

- [1] 鐘慶豐，近代密碼學與其應用，儒林，ISBN 957-499-730-8。
- [2] B. Rosenblatt, B. Trippe and S. Mooney, *Digital Rights Management: Business and Technology*, John Wiley & Sons, 2001, ISBN 076-454-889-1.
- [3] Content Protection System Architecture (CPSA), 2006/10/28, <http://www.4centity.com/data/tech/cpsa/cpsa081.pdf>
- [4] Content Protection for Recordable Media (CPRM), 2006/10/8, <http://www.4centity.com/tech/cprm/>
- [5] Content Protection for Pre-Record Media (CPPM), 2006/10/8,

- <http://www.4centity.com/tech/cppm/>
- [6] Digital Living Network Alliance (DLNA), 2006/10/18, <http://www.dlna.org>
 - [7] Digital Property Rights Language (DPRL), 2006/10/18, <http://www.oasis-open.org/cover/dprl.html>
 - [8] Extensible Rights Markup Language (XrML), 2006/10/18, <http://www.xrml.org>
 - [9] Microsoft: Windows Media Rights Manager (WMRM), 2006/10/18, <http://www.microsoft.com/windows/windowsmedia/drm/default.aspx>
 - [10] RealNetwork: Digital Rights Management (DRM), 2006/10/18, <http://www.realnetworks.com/products/drm/index.html/>
 - [11] J. Dubl and S. Kevorkian, "Understanding DRM System: An IDC White paper," IDC, 2001.
 - [12] R. H. Koenen, J. Lacy and M. Mackay, "Ten Long March to Interoperable Digital Rights Management," *Proceedings of the IEEE*, Vol. 92, Isu. 6, pp. 883-897, June 2004.
 - [13] J. Lotspiech, S. Nusser, and F. Pestoni, "Anonymous Trust : Digital Rights Management using broadcast encryption," *Proceedings of the IEEE*, Vol. 92, Isu. 6, pp.898-909, June 2004.
 - [14] R. Iannella, "Then Open Digital Right Language: XML for Digital Rights Management," *Information Security Technical Report*, Vol. 9, Isu. 3, pp. 47-55, July-September, 2004.