數位內容版權發行管理機制

林昱仁
Yu-Jen Lin
工研院電通所
helios@itri.org.tw

徐和謙
Ho-Chien Hsu
工研院電通所
v3@itri.org.tw

葉文熙
Wen-Hsi Yeh
工研院電通所
Willy@itri.org.tw

1. 摘要

近年電腦科技的發展，各種影音紙本等傳統媒體數位化成為一種趨勢。但隨著網際傳輸技術的進步、寬頻環境的普及，彼此間分享檔案變得很方便；同樣的，數位化後的內容檔案如果沒有經過妥善的保護，也容易經由網路途徑散佈，造成未經合法授權使用的情形發生。因此，數位化後的檔案版權保護，便成為十分重要的課題。

另外數位內容的檔案受保護後，必須保持使用上的便利性，也必須要滿足多種授權使用模式。

本文提出一個兼顧各種授權使用模式及確保數位內容檔案安全性的數位版權發行機制，來達到數位內容版權的保護。並搭配多種付費機制，使得購買版權時的付費過程更加有彈性。不同的數位內容廠商也可透過此機制互相合作，出版共同版權的數位內容，以促進數位內容流通及使用率。

關鍵字

數位版權管理、數位版權發行

2. 前言

近年來隨著網際網路蓬勃發展及寬頻網路逐漸普及，不論是在校學生或是校外人士，透過網路來取得數位內容變得方便、可行，且逐漸成為一種趨勢。但伴隨著各種檔案交換軟體及點對點傳輸工具(Peer to Peer-P2P)的盛行，使得在網路上取得未合法授權檔案變成非常容易，版權不易控管的結果會變成苦心開發好的數位內容無法獲得收益，造成想投入數位內容市場大餅的業者為之卻步。

以目前 APPLE 所提供的數位音樂下載服務為例，其讓使用者能以每首歌不到一塊錢美金(0.99)的代價下載單曲，而不需要為了一首歌而去花費十首歌的價錢購買整張專輯，下載的音樂透過軟體控制管理(iTunes.)，無法無限複製，只能在下載的 PC 上或 iPod 上使用。唱片公司因為有安全機制的保護，所以願意將旗下的音樂授權給 APPLE 販售。iPod 第一年內就賣出超過七千萬首歌，產值驚人。可見只要有合理的售價及完善的數位內容保護機制，是可以創造數位內容廠商及消費者雙贏的局面。

當數位內容產業開始興起，單一公司將難以提供一完整的數位內容產業供應鏈上所需的所有服務，產業分工的需求便開始興起，數位內容產業逐漸形成數位內容製作、數位內容加值與數位內容營運等不同階段，然而，各階段間彼此的資源交流受到業者對於內容版權使用的限制與擔心，難以真正達成廣泛的流通與分享。因此，如何在此產業分工的環境中提供各階段的資源可以在具備版權發行管理的機制下，提供既安全又符合彈性的交易功能，便成為一重要的議題。

本篇文章重點在於提出一種數位內容版權發行及交易機制來達成數位內容產

業鏈下的數位內容流通，同時兼顧數位內容保護版權管理及內容使用者在使用上的便利性，讓數位內容得以再利用，創造出更大的利益。

3. 數位內容保護與數位版權管理

傳統數位內容保護，大部分都是採用以下兩種作法：一是把內容檔案全部加密，取得授權後獲得解密金鑰，進而解開整個檔案；二是用密碼驗證方式驗證使用者身份後，就將整個檔案全部開放使用。不過以往的保護方式比較薄弱，且用途上受限制，最大的缺點是無法控管使用者獲得數位內容檔案後的行為。

因此，現今的數位版權管理機制，除了數位內容保護的需求外，還必須包含以下功能：

- 使用者認證：確認合法使用者身份，未經合法授權，就算獲得該檔案，也絕對無法使用。
- 存取限制：同一份數位內容檔案，依授權身份不同，可制訂不同的存取限制。例如部分數位內容不提供未付費的使用者瀏覽，必須付費以取得授權，才可以瀏覽整個內容。
-
- 用途限制：依授權內容不同，授予不同的用途限制，例如：限制複製、列印等操作功能，授權中未明白指名的其他操作動作就無法使用，除非另外取得合法授權。
- 時間限制：依授權內容不同，授予不同的使用期間，例如：一個月、一週等，使用時間一到，就無法再利用原先合法取得的內容，除非再取得合法授權。

以上功能可依需要組合出授權內容，例如：授權給 Bob 在一個月內只能瀏覽該份數位內容最多不超過十次，且無法列印或複製該數位內容。

4. XrML 版權描述語言

為了達成數位版權管理所提供的諸多功能，勢必需要將數位版權的授權內容轉成文件格式以方便作為遵循之用，在本機制規劃採用 eXtensible rights Markup Language (XrML)，這是一種專門設計來描述數位內容版權及版權使用限制的 XML 語言。XrML 可針對不同對象，提供多種授權方式及限定各種使用限制。XrML 並使用了數位簽章技術，讓收到版權描述檔的數位內容使用者無法私自竄改版權描述檔內容。由於 XrML 是標準 XML 語言，基本上除了能應用在描述數位內容版權的權利事項外，還能讓這些與權利事項有關的資訊能在不同的應用與系統之間互通有無。

5. 數位版權管理需求

整合上述所介紹之 XrML 數位版權描述語言，並搭配數位憑證(Certificate)及公開金鑰(Public Key)技術，可以達成下列數位版權管理的需求：

一、身分認證：利用公開金鑰及憑證比對 XrML 中記載的授權使用者 ID，來認證使用者，只有 XrML 中紀錄的合法身分者才能使用該數位內容。即便使用者將授權檔案未經同意”分享”給朋友，沒有通過身分認證，就無法瀏覽或使用該數位內容檔案。

二、XrML 檔案完整性：廠商在發行數位版權時，利用自己的私密金鑰(Private Key)對 XrML 檔案簽署數位簽章，假若使用者私自竄改 XrML 檔案，在檢查比對授權檔案的雜湊值及簽章時就會發現 XrML 檔案被竄改

過，就無法瀏覽/使用該數位內容檔案，也就無法藉此以改變授權權限。

三、數位內容檔案保護：數位內容檔案用秘密金鑰(Secret Key)加密，秘密金鑰再以使用者的公開金鑰加密，將數位內容密文記載在 XrML 版權描述檔中，使用者在瀏覽/使用前，瀏覽程式會用使用者的私密金鑰先解出秘密金鑰，這樣一來合法授權使用者便可以成功解出數位內容檔案。

四、使用條件限制：在使用數位內容檔案前，瀏覽程式會先檢查 XrML 檔案記載的使用權限，並決定使用者可瀏覽/使用的權限。

五、使用時間/次數限制：數位內容廠商可以將 Ticket 資訊用秘密金鑰加密，秘密金鑰再以使用者的公開金鑰加密，將密文記載在 XrML 版權描述檔中，使用者在瀏覽/使用時，必須將 Ticket 資訊送往數位內容廠商，廠商比對資料庫中 Ticket 權限/次數等資訊，如果合法，使用者便可成功取得數位內容檔案，如果屬於次數授權，便在資料庫中維護 Ticket。這個方法有幾個好處：

i. 時限內授權使用：例如授權在期限一個月內使用。

ii. 固定次數授權使用：例如個人使用 30 次。

iii. 時限和固定次數授權使用：例如限制一個月內使用 30 次。

iv. 共享固定使用次數授權：例如授權給校園，一年內限制瀏覽次數一萬次。

v. 計次收費授權：使用者可以計次使用，先享受後付款。廠商可在固定時間依照 Ticket 記錄請款(例如：月結)。

vi. 版權移轉機制：使用者 Alice 如果要把版權移轉給 Bob，廠商收到 Alice 的申請後，只需簽發新的 XrML 檔給 Bob(內含新的 Ticket)，這樣 Alice 所持有的 XrML 檔自動失效(因為內含的 Ticket 已經無效)，版權已經成功轉移給 Bob。

vii. 贖回機制：使用者 Alice 如果要把版權贖回，廠商收到 Alice 的申請後，只需把原先的 Ticket 資訊設定為不合法，Alice 所持有的 XrML 檔自動失效。

viii. 補發/更新版權：使用者 Alice 版權檔案遺失或私密金鑰對更新，廠商收到 Alice 的申請後，只需把原先的 ticket 資訊設定為不合法，並簽發新的 XrML 檔回傳給 Alice，Alice 所持有的舊 XrML 檔自動失效。

六、離線使用：廠商將數位內容用秘密金鑰加密後，連同發行的授權憑證 XrML 檔案一同交給使用者。使用者端的瀏覽程式或元件在認證使用者合法授權身分後，從 XrML 檔中解出秘密金鑰，再用秘密金鑰解出數位內容檔案，再呈現在瀏覽程式或元件上。

而數位內容營運單位則可以透過發行 XrML 授權文件來描述數位內容授權範圍，輔以適當的版權管理元件或程式，於使用者實際使用數位內容時強制使用者於授權的範圍內使用數位內容。

6. 數位版權發行機制

本章所要介紹的是數位內容檔案的保護機制，滿足前一章所介紹的各種需求及使用到的技術，共分成數位版權發行、使用者使用數位內容、和其他內容業者使

用該數位內容發行新的數位內容三大部分：

一、數位版權發行階段：

本節闡述數位內容廠商發行數位內容的版權，並到數位內容檢索平台註冊。詳細說明如下：

圖一：業者發行數位內容版權

i. 如圖一中的步驟 0 及步驟 1，內容提供業者至交易平台註冊帳戶資訊並到內容搜尋平台註冊一數位內容

ii. 內容提供業者可針對每份數位內容制定數種授權模式，如：

a. 預覽/試用
b. 單次瀏覽/使用
c. 期限內瀏覽/使用
d. 限定瀏覽/使用次數
e. 限定期限內可瀏覽/使用的次數
f. 是否提供使用者轉移版權服務
g. 是否提供使用者贖回服務
h. 是否提供其他廠商利用該數位內容包裝新數位內容服務

iii. 將制定好的授權模式、內容廠商資訊及付款資訊(包含廠商間拆帳等資訊)包裝成 XrML 交易授權文件檔案

iv. 如圖一中的步驟 2，將包裝好的 XrML 交易授權文件檔案上傳至搜尋平台

二、使用者使用數位內容階段：

本節闡述使用者使用數位內容的各種可能模式及付費方式詳細說明如下：。

i. 數位內容使用者透過搜尋平台找尋到合適的內容。

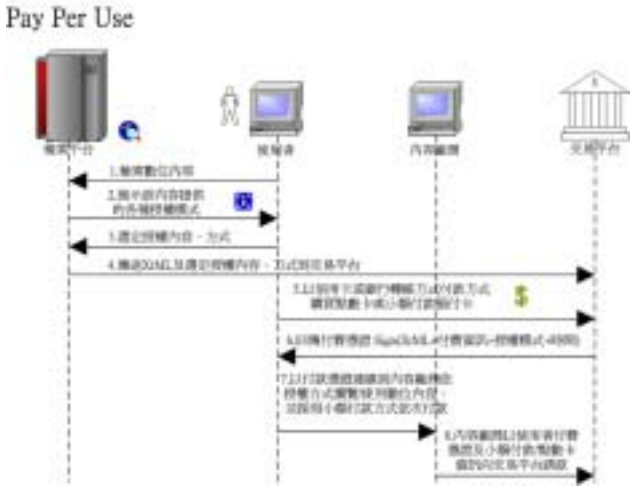
ii. 系統解析該 XrML 交易授權文件檔案，依照原內容提供業者設定的各種交易授權模式，以文字或圖形等形式的描述呈現給使用者選擇。

iii. 數位內容使用者選擇中意的模式，在此則分為下列交易型態

圖二：Prepaid 購買使用模式

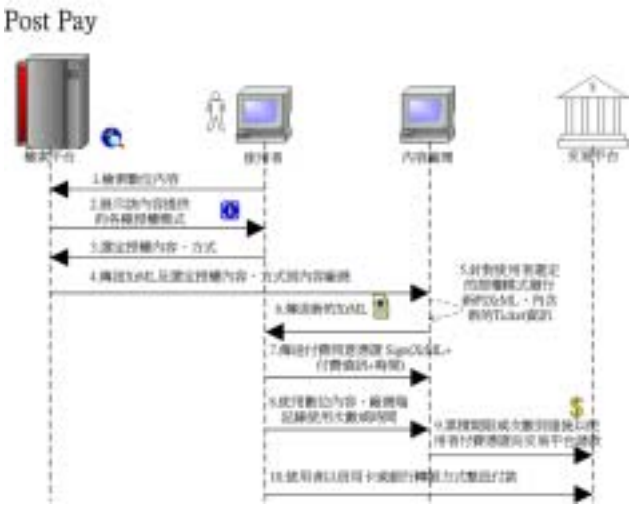
a. Prepaid：如圖二步驟 5 至步驟 7，使用者先連到交易平台，採用信用卡或銀行轉帳等方式付款後，取得付款收據，使用者再依此收據連到

內容廠商，依購買內容瀏覽/使用該數位內容。內容廠商如步驟 8 所示，依使用者付款收據向交易平台請款。



圖三：Pay Per Use 使用模式

b. PayPerUse：如圖三步驟 5 到步驟 7，使用者連到交易平台，以信用卡或是銀行轉帳方式購買點數卡或小額付款機制之電子錢。交易平台發給使用者付款憑證及點數卡/電子錢。使用者在每次使用/瀏覽該數位內容前，再以點數卡或電子錢付款。內容廠商如步驟 8 所示，每隔固定時間或固定次數一到，便依使用者付款收據及收到的電子錢/點數等向交易平台請款。

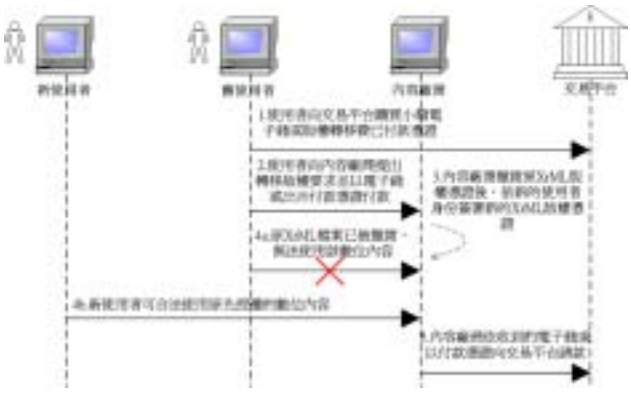


圖四：Post Pay 使用模式

c. Post Pay：如圖四步驟 4 到步驟 6，搜尋平台在使用者選定採用 Postpay 付款方式後，將購買資訊傳送到內容廠商端，廠商依使用者選定的交易授權模式，另外發行一個 XrML 使用授權文件檔案並傳給使用者。在步驟 7 中，使用者對收到的 XrML 及其他相關資訊，簽署付款同意憑證並傳送到內容廠商端。步驟 8 到步驟 9 說明了使用者每次使用數位內容，都會在廠商端留下屬於自己的 Ticket 相關資訊，等到固定期限或固定次數一到，廠商一次向交易平台請款。步驟 10 說明使用者以採用信用卡或銀行轉帳向交易平台付款。

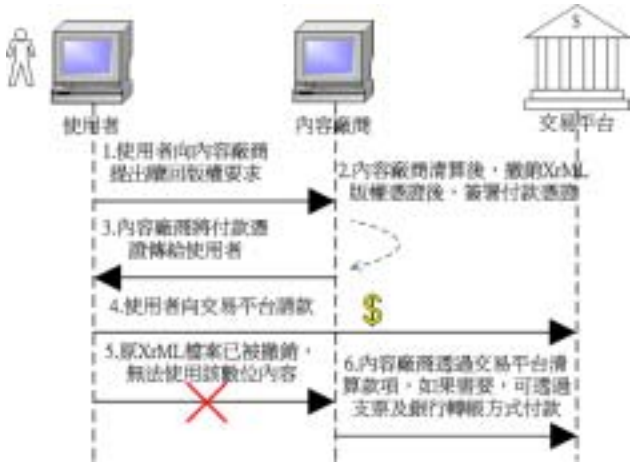
圖五：Offline Use 使用模式

d. Offline Use：如圖五步驟 5 及步驟 6，使用者以信用卡或銀行轉帳方式付款後，交易平台簽署付款憑證給使用者。使用者連線到內容廠商端，出示付款憑證，廠商便針對使用者購買內容，發行新的 XrML 使用授權憑證，並將數位內容檔案打包，供使用者下載。步驟 10 中，廠商依使用者付款憑證向交易平台請款。



圖六：版權轉移

iv. 如果允許轉移版權，如圖六所示，由版權目前合法使用者先向交易平台購買小額電子錢或轉帳購買已付費憑證，再向業者提出轉移版權申請，並提供新的使用者資訊給該內容業者，業者先廢止之前核發的 XrML 使用授權文件檔案並重新簽發 XrML 使用授權文件檔案。在步驟 4a 中因為舊的 XrML 檔案已被撤銷，所以原先使用者無法再使用該數位內容。步驟 5 說明內容業者可依收到的電子錢或已付款憑證向交易平台請款。



圖七：版權贖回

v. 如果允許贖回版權，如圖七所示，由目前該數位內容的使用者對目前仍然有效的數位內容使用憑證，向業者提出贖回版權申請。在步驟 2 到步驟 3 中，廠商先廢止之前核發的 XrML 使用授權文件檔案，再簽署退款憑證，並將退款憑證傳給使用者。在步驟 5 中說明使用者因為 XrML 檔案已被撤銷，所以無法再使用該數位內容。步驟 6 說明使用者依廠商退款憑證向交易平台請款。

三、其他內容業者使用該數位內容發行新數位內容階段：

本節闡述其他數位內容業者透過搜尋平台尋找到其他內容業者所擁有的數位內容檔案，並透過合作方式，產生新的數位內容，詳述如下：。

i. 內容業者透過搜尋平台找尋到合適的內容。

ii. 系統呈現該內容提供業者針對該數位內容所授權的各種授權模式。

iii. 內容業者選擇中意的模式

a. Prepaid：內容業者連到交易平台透過銀行轉帳或支票付款後取得付款憑證憑證，並連線到原內容廠商並出示付款憑證，原內容廠商依廠商選定的交易授權模式，另外發行一個 XrML 授權文件檔案，以後使用者連線使用該廠商的數位內容，只要其中有其他廠商的數位內容，就可以連回到原廠商處使用。

b. Pay Per use：不必付款直接取得專屬授權憑證，使用時才從每筆使用者支付的小額付款或點數卡由雙方協議透過交易平台拆帳。

c. Post Pay：先取得專屬授權憑證，然後利用其 Ticket 控制期限和次數，期限或次數到期後整批轉帳，例如月結。

d. Offline Use：廠商採用前一節提到的使用者 Offline Use 機制，下載數位內容檔，並將檔案加入自己的數位內容檔，組合成新的數位內容檔案。

iv. 將取得授權之 XrML 檔案包裝進自己的數位內容中

v. 針對此份數位內容制定數種授權模式。

vi. 將制定好的授權模式、內容廠商資訊及付款資訊(包含廠商拆帳資訊)包裝成 XrML 檔案。

vii. 將包裝好的 XrML 檔案上傳至搜尋平台。

7. 衍生交易行為模式

使用第六章介紹的數位內容保護機制，可以衍生出下列以往數位內容檔案無法辦到的交易使用模式，可使得購買使用方式更有彈性：：

一、買斷：即第六章提到的 Offline Use，類似傳統的數位內容交易模式，與傳統的差別是，雖然使用者可以自由的使用所購買的數位內容檔案，但該數位內容仍然可以受到有效的控管流向，無法任意複製流通。

二、租賃：即第六章提到的 Online Use(Prepaid、Pay Per Use、Post Pay)，使用者可以用較低的價格在期限內自由使用所租賃的數位內容檔案，期限一過，授權自動失效，也不必將數位內容檔案歸還，不像傳統出租方式，逾期歸還還會被罰款。

三、版權轉移(二手市場)：提供使用者方便轉移版權的機制，開創廠商另一種收益途徑，使用者也可以將購買金額作最大的利用。

四、版權贖回：提供版權贖回機制，保障使用者利益，且使用者可以選擇將退款再購買其他數位內容，可以提高數位內容的使用率。

五、合作發行：各業者合作發行新的數位內容，以提高數位內容的使用率，並透過拆帳方式創造雙方更高的利益。

8. 結論

數位內容版權保護的缺乏一直是各家廠商遲遲不願意大量投入數位內容市場的主要原因。在數位內容蓬勃發展的年代，如何兼顧便利的使用及數位內容的安全性，是市場可否健全發展的一大關鍵。本篇文章提出了一個針對數位內容檔案各種交易授權模式的解決方案，並採用 XrML、加解密技術、Ticket 提供了多種便利的使用方式之外，仍能確保數位內容檔案的安全性。另外透過合作機制，使得各廠商數位內容元件利用率提高、出版品更多元化。期望在安全性的顧慮消失後，廠商可以無後顧之憂的情形下，投入數位內容市場，使得數位內容市場更加的蓬勃發展。

9. 參考資料

一. XrML / http://www.xrml.org

二. XML Signature / http://www.w3.org/Signature/

三. 「近代密碼學及其應用」 / 賴溪松、韓亮、張真誠著 ： 松崗[1997]

四. 「以數位權利為基礎的商品交易機制」 / 廖鴻圖、莊文勝、陳煜文、吳威震 ： 2003 年數位內容創意加值研討會論文集 I P.40~P.47

五. 「數位圖書館與 DRM」。陳映后、何佳欣、黃崇瑋 ： 2003 年數位內容創意加值研討會論文集 II P.17~P.25

六. APPLE iPod+itunes http://www.apple.com/itunes/