可攜式數位內容版權管理平台

邱迪先
永豐紙業股份有限公司

何君毅
永豐紙業股份有限公司

一、數位內容的推手與護法者—DRM

數位內容已為國家產業發展之重要政策，對印刷出版產業而言更是產業轉型的最佳契機，而電子書從發明到普及，版權的問題是相當重要的一件事，傳統書籍的版權會以怎麼樣的形式呈現在數位的世界，這是全球的人都在摸索的事情。然而在保障數位內容作者及數位內容提供業者權益的前提下，提供顧全兩方的需求是很重要的課題。也只有當數位內容作者及數位內容提供業者的權益被保障了，數位內容才能源源不絕的提供給使用者，使用者也才能享受到優質的數位內容。接著我們就來了解數位內容的推手與護法者—DRM。

1. 何謂 DRM？

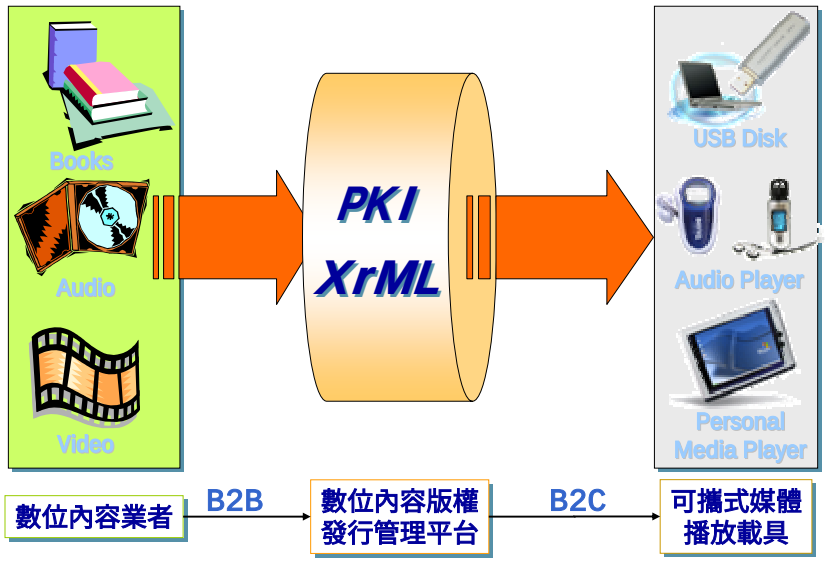
數位版權管理 (Digital Right Management) 簡稱 DRM，為目前國際先進的數位內容加密技術，保護電子文檔的安全性，實現電子文檔的使用過程可控、可跟蹤，防止電子文檔的非法拷貝，防止對電子文檔的篡改、控制電子文檔閱讀時間、列印份數限制等等。藉以保障數位內容作者及數位內容提供業者之權益，維護數位內容的智慧財產權。

2. DRM 的四大特色

網際網路急劇成長促成電子商務的快速起飛，然而數位化的內容卻是容易被複製，被傳播，原有的作者無法在既有的版權架構底下受到保障，所以資訊安全的考量便成為電子商務蓬勃發展的關鍵之一，數位內容版權發行平台的機制也因然而生。

二、數位內容版權發行平台的核心技術

數位內容版權發行平台就是在整合兩大技術 PKI 與 XrML，建立出數位內容出版業的新價值鏈。因此我們必須先行認識數位內容版權的左右護法—PKI 與 XrML。



1. 數位內容的左護法—PKI

密碼學原理中之『公開金鑰系統』因可同時解決資料之隱密性 （Confidentiality）、身份鑑識（Authentication）、訊息完整性（Integrity）與簽章資料之不可否認 （Non-repudiation），被公認為目前解決資安需求最成熟之方案。

公開金鑰系統之運作時參與者因必須擁有一對金鑰—公鑰（Public Key）與私鑰（Private Key）。大體而言，金鑰持有人必須謹慎保管代表個人身份之私鑰（有如個人之電子印鑑），並需透過某種公開與安全之機制發行其公鑰，以便與交易之另一方、用來以驗證持有人簽署之交易資料。因此，使用公開金鑰系統之組織，必須與其參與交易之使用者，共同建立一完整之運作環境，密碼學上稱建立此環境之所有規劃為『公開金鑰系統基礎建設』（Public Key Infrastructure，簡稱 PKI）

2. 數位內容的右護法—XrML

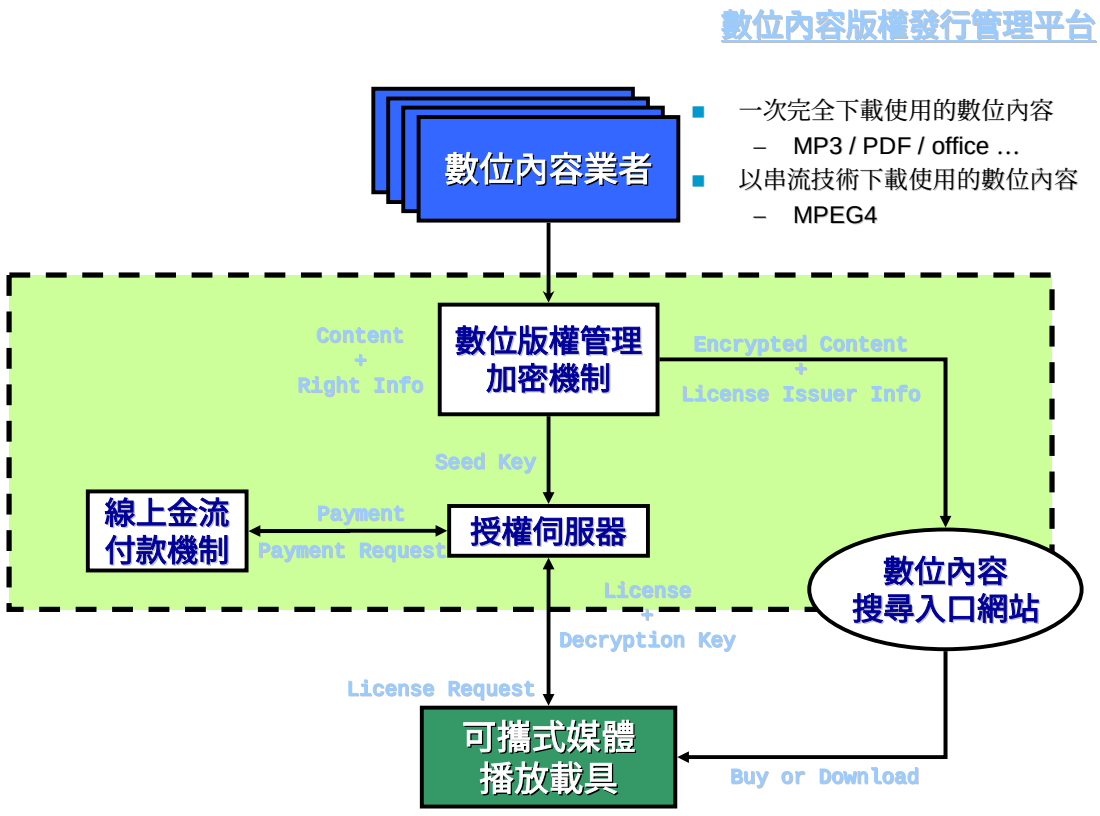
XrML 提供一個共通的描述方法來設定並管理數位內容和服務的使用權利及使用條件，而遵照 XrML 指定的內容在其所授權的範圍內來使用數位內容或服務，則由應用程式負責。將 XrML 內文與數位內容分開，一份數位內容、服務或軟體程式，可以有許多份 XrML 內文，每份內文可指定一種以上的使用授權，因此可以針對不同的使用對象，授與各種不同使用條件下方可使用的權利。XrML 雖然尚未成為工業標準，但事實上已經有許多的知名大廠諸如：Microsoft、Adobe、Sony、HP 和 Xerox 等及一些著名出版商率先採用，而且目前一些制定中的工業標準也採用 XrML 作為標準其中的一部分了。

三、**數位內容版權發行平台的技術架構**

首先系統將對使用者做身分的認證以為基礎，在數位內容版權管理部分，結合 PKI 技術，提供標準的憑證發行與管理機制，達到使用者身份認證及權限控管的整合應用功能，使得同一份數位內容對不同的使用者將會產生不同的簽章加密檔。

另一方面，數位內容版權發行平台可以依據消費者對於此數位內容的購買情況，進行版權控制資訊的產生。其中，版權控制資訊可以包括相應數位內容之授權期限、列印限制資訊、發行者資訊、數位簽章等等。因此每一檔案均具有相應之版權控制資訊來控制該檔案分區內數位內容的播放版權。

同時數位內容版權發行平台可以將版權控制資訊結合於加密數位內容中，編輯成一個個人化的數位內容簽章封包，並利用可擴展標記語言(Extensible Markup Language，XrML)來呈現。進而對應於數位內容交易的不同，數位內容版權發行平台對於消費者購買數位內容之行為亦有相應之計費與請款機制，以配合相對應之數位版權的交易模式。例如：提供內容移轉、內容複製及內容租賃等交易方式。



四、數位內容版權發行平台運作流程—以電子書為例

1. 出版社數位內容上傳

出版社數位內容上傳的過程，首先需透過 PKI 確認數位內容提供者之身分，接著數位內容提供者可以將所創作的數位內容上傳伺服器，伺服器除接受上傳檔案格式，並讓數位內容提供者預先設定 Metadata 的 Rights 授權使用方式；另外，對於系統同時以數位簽章的技術將數位內容提供者的智財權簽入檔案，將須保護的數位內容檔案儲存至內容伺服器中，並將 XrML 中 resource 指向數位內容管理伺服器中相對應的檔案，連同修改後之授權設定編寫成符合 XrML 規格的 XML 內文，儲存至版權管理伺服器。

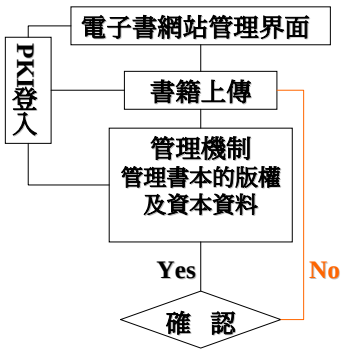
2. 客戶端網頁瀏覽購買

消費者購買數位內容的過程，首先一樣需透過 PKI 確認數位消費者之身分，接著版權管理伺服器將消費者可以將所欲購買的數位內容由數位內容管理伺服器取出，依照消費者的交易條件對數位內容做 Rights 的授權與個人化的簽章，編寫成符合 XrML 規格的 XML 內文，讓消費者下載使用。

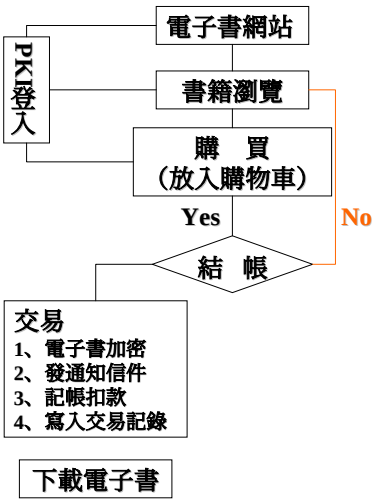
3. 客戶端閱讀數位內容

首先消費者利用客戶端的撥放器開啟數位內容檔案，此時撥放器會先行以 PKI 驗證消費者的身分，接著撥放器根據其中金鑰進行解密，最後根據內容授權中的權利義務關係資訊進行審核管控及播放呈現該內容。

- 出版社系統使用流程



- 客戶端系統使用流程



- 客戶端閱讀流程