

永豐紙業股份有限公司

數位版權(DRM)的平台技術與應用架構

永豐紙業 數位服務處

游勳鈞

2004/04



內容大綱

- 內容產業的改變
- **DRM**的技術研究
- 技術架構之介紹

內容產業改變





現有問題與挑戰

■ 消費者需求和供應需求者不同

消費者需求

- Any Time Any Place，內容取得即時、快捷。
- Cheapest，最低價格。
- Friendly UI，使用操作方便。
- Portable Copy Save，可攜帶，複製及轉移位置。
- On-Demand，不需購買附帶內容。

供應者需求

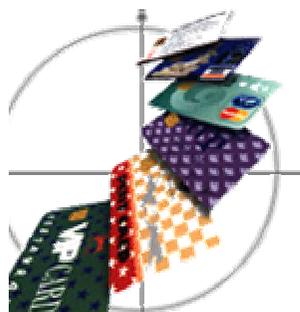
- Cost down，快速低成本行銷。
- No transfer，禁止消費者不當散播內容。
- Valuable，透過附加內容，擴增價值。



現有問題與挑戰

■ 現行保護機制與數位內容使用情境不符

現行保護機制



- 可正常使用
- 允許使用者複製
- 允許使用者傳遞
- 允許使用者修改

使用者會保護內容

數位內容使用情境



- 可正常使用
- 允許使用者複製
- 允許使用者散佈
- 允許使用者修改

使用者會破壞規定



數位內容保護概念

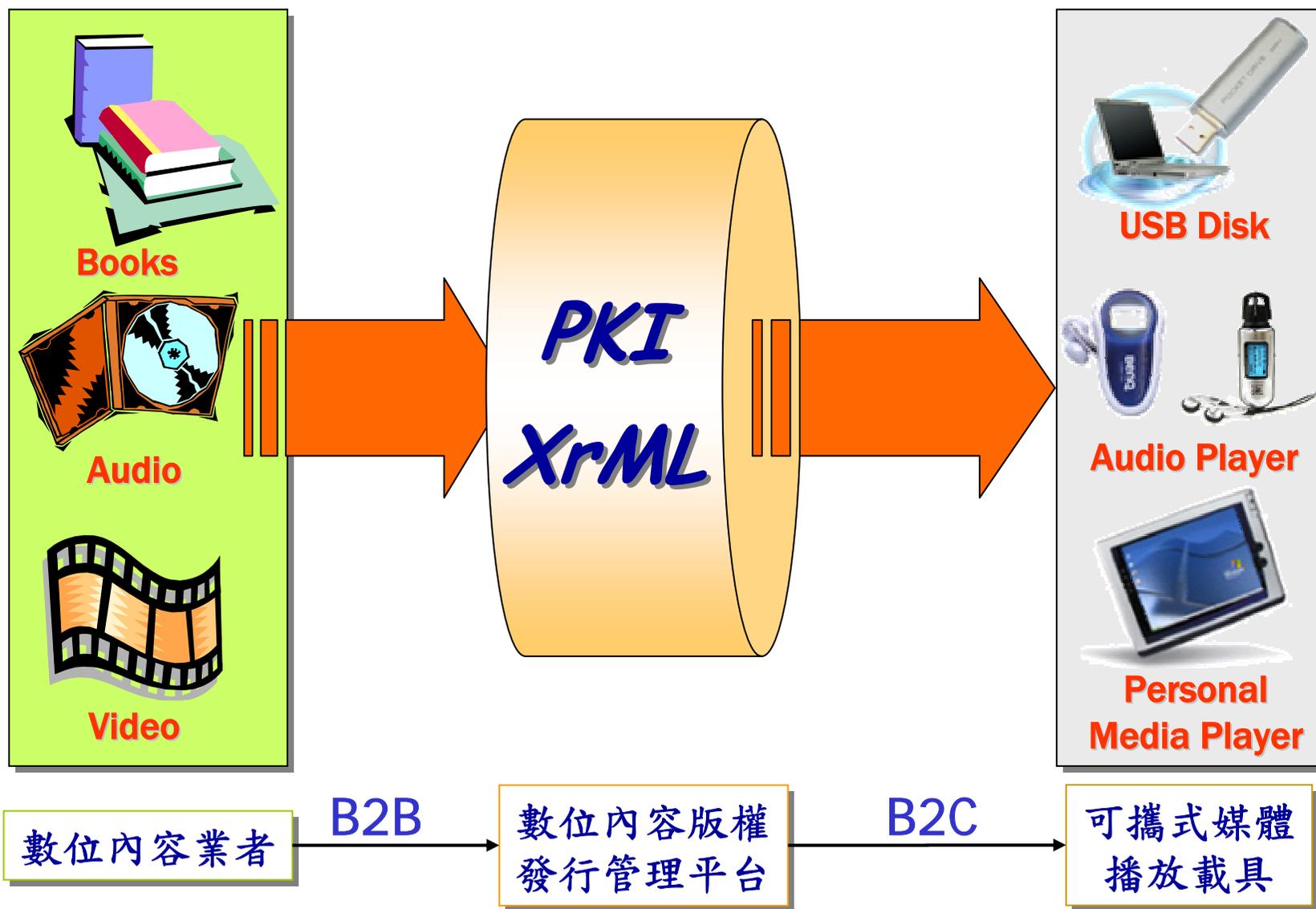
- 如何符合使用者需求，正常使用數位內容，又不能隨意複製散播？
- 如何保護出版者的權益，讓每次的傳遞都可以被掌握。
- **DRM**如何整合數位時代商業模式，創造效益。

DRM的技術研究





數位內容出版關鍵－版權管理





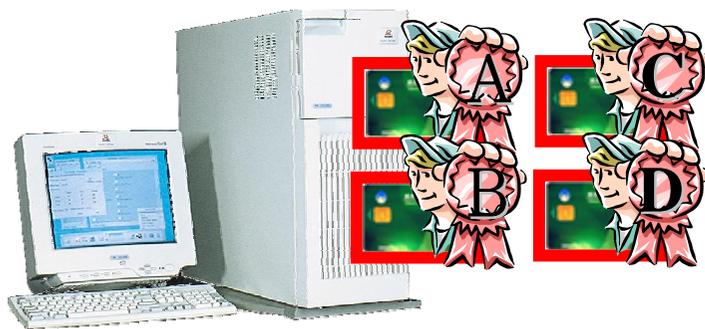
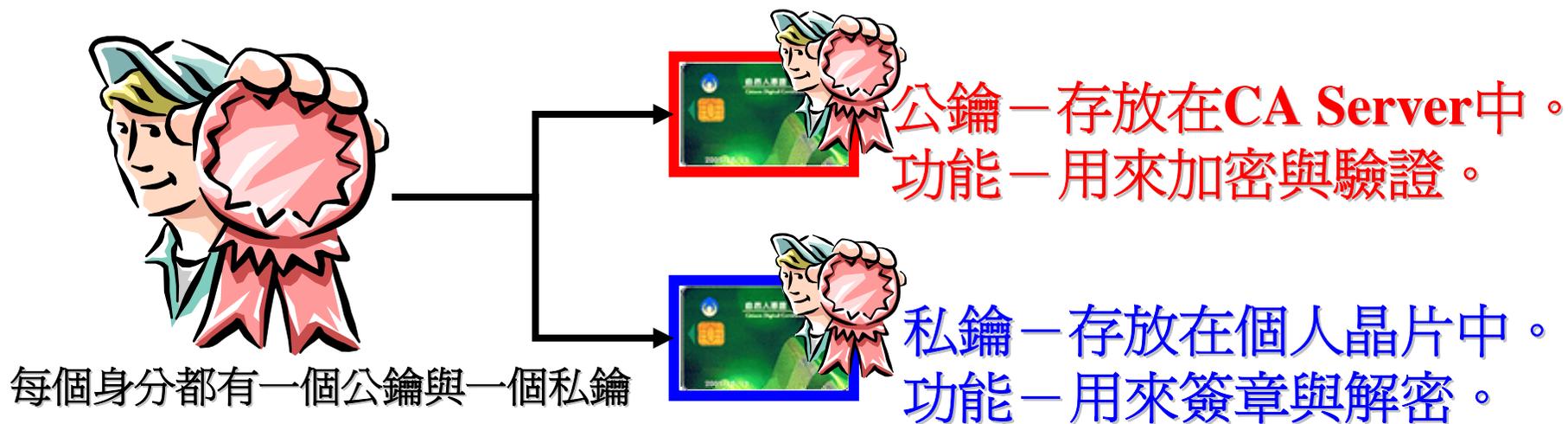
相關技術 PKI

■ 公開金鑰系統基礎建設(Public Key Infrastructure , PKI)

1. 可同時解決資料之隱密性、身份鑑識、訊息完整性與簽章資料之不可否認。
2. 被公認為目前解決上述資安需求最成熟之方案。



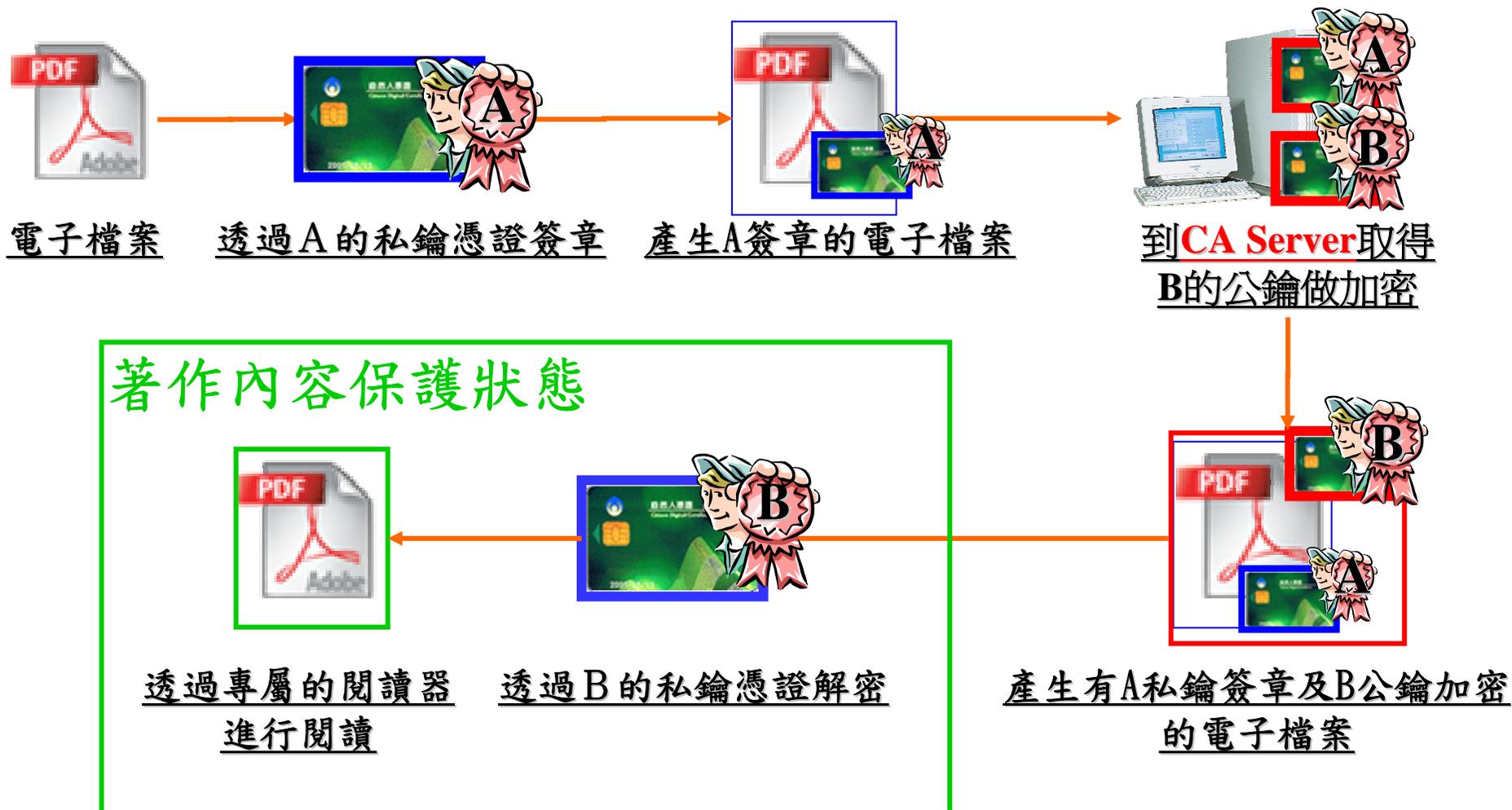
PKI原則說明



CA Server



PKI原則說明





相關技術 **XrML**

■ **XrML(Extensible Markup Right Language)**

XrML為各國國際標準組織作為數位版權描述語言標準，已有許多知名大廠諸如：**Microsoft**、**Adobe**、**Sony**、**HP**和**Xerox**等及一些著名出版商率先採用。

■ **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。

技術架構之介紹

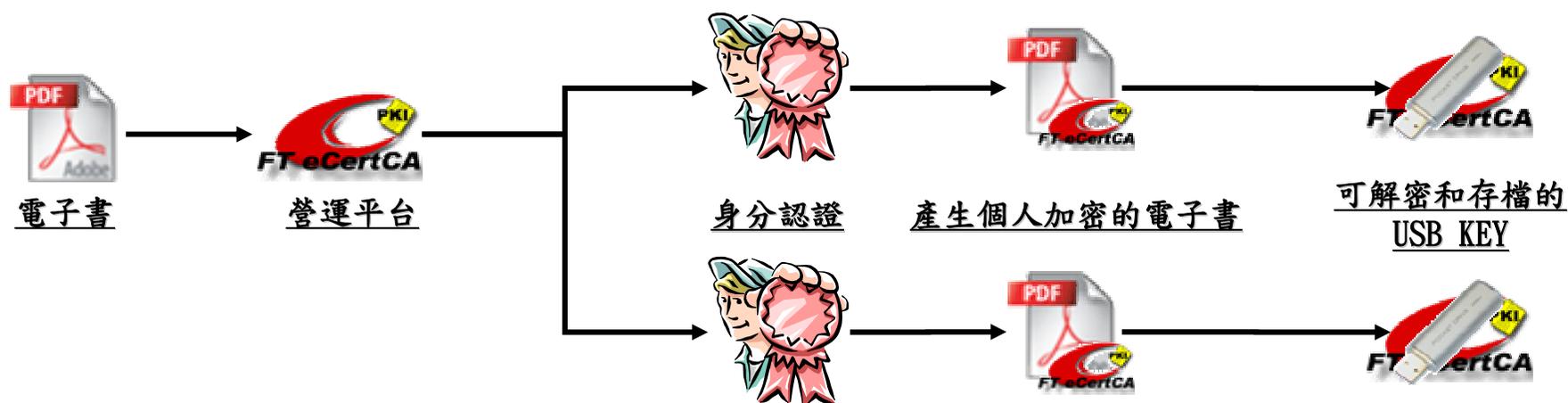
可攜式電子出版品





什麼是可攜式電子出版品

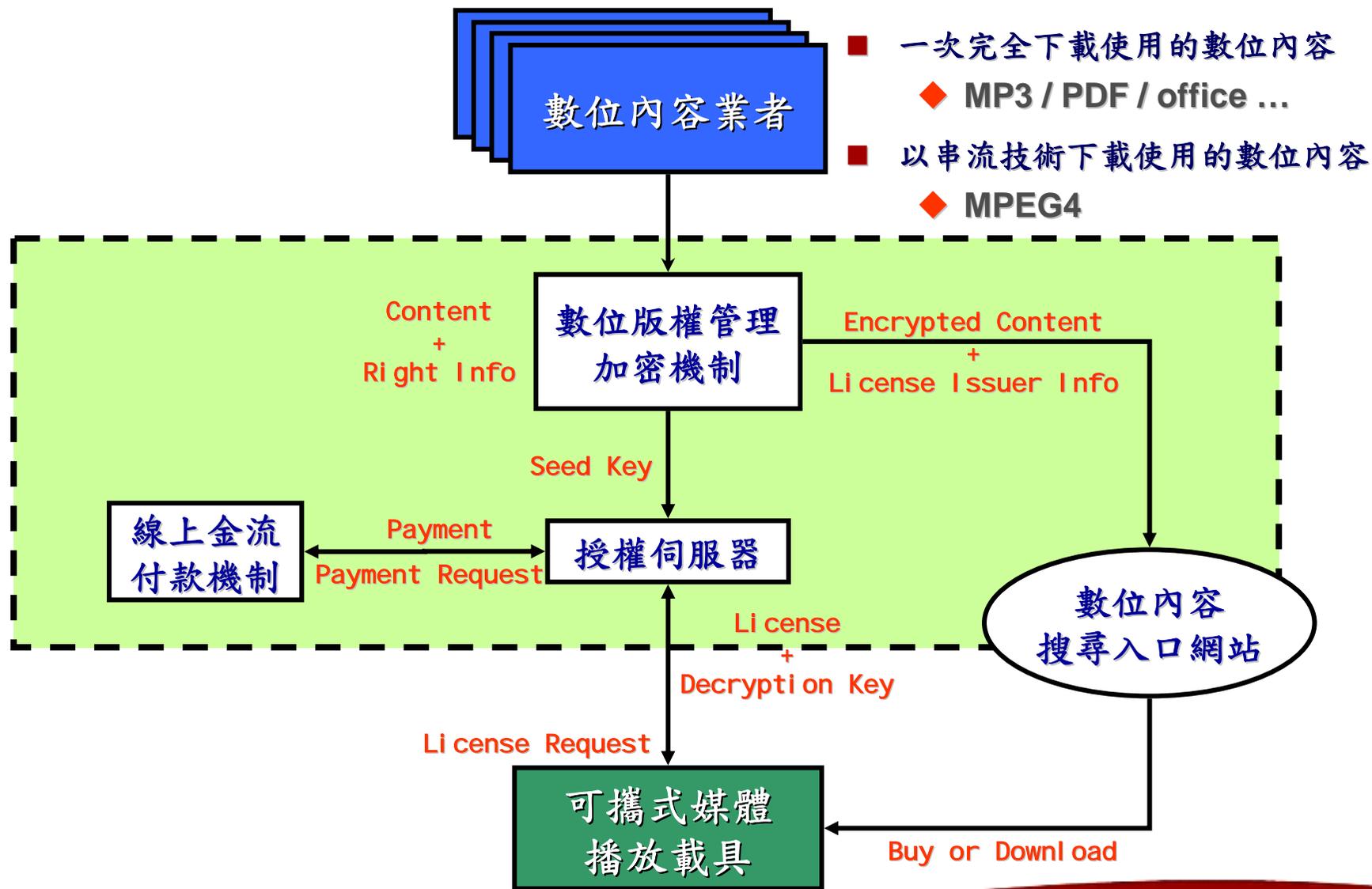
- 可攜式電子書的版權控制是依據〈USB Key〉，讓閱讀時的版權管理追尋一個可以隨身攜帶的KEY。
- 對同一份電子書內容，根據不同之讀者進行個人化的加密。這將使得不同使用者間，在 USB Key不借用之條件下，將無法解開其加密內容。





平台技術流程

數位內容版權發行管理平台





可攜式電子出版品的四大特色

PKI安全應用

- 利用 PKI 進行社群成員身份認證
- 以 PKI 為基礎之金鑰交換機制，進行同一電子文件不同使用者不同加密內容之『個人化加密』
- 數位內容中保留版權擁有者之數位簽章



儲存/安全/應用結合的 USB

- 整合市場之高容量之USB KEY的多工應用
- 整合使用來管理版權、儲存數位內容以及PLAYER之抽取式 USB 隨身碟



支援XRML的規範

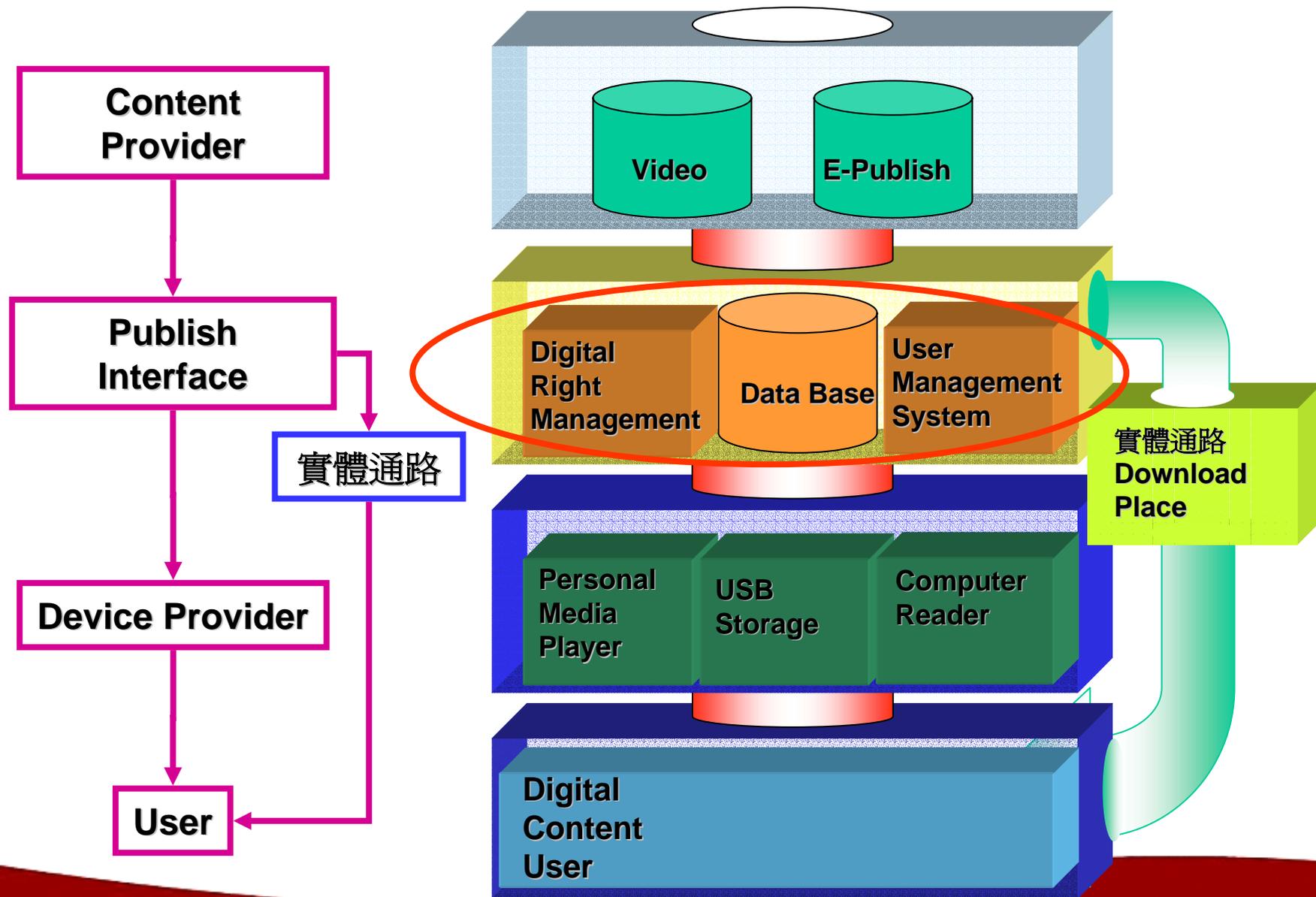
- 支援XRML規範，後端可自行開發搭配
- 透過XRML管理Player各版權使用的功能

數位內容的加密與數位簽章

- 建立數位內容與使用權限整合之完整檔案
- 以完整之數位內容之PLAY整合檔案管理之介面
- 與 USB Key 搭配解密保護數位內容

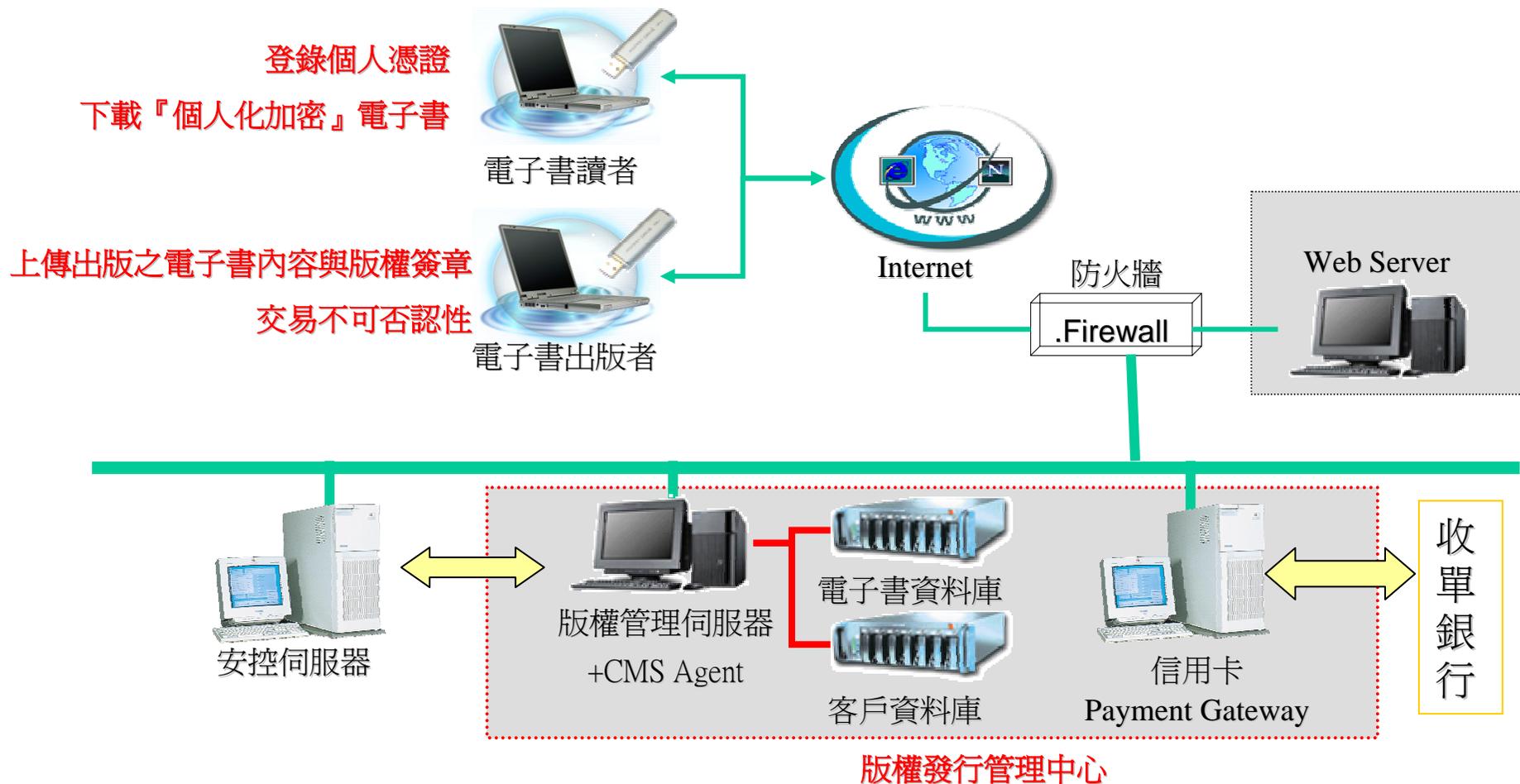


DRM 應用模組架構結合通路





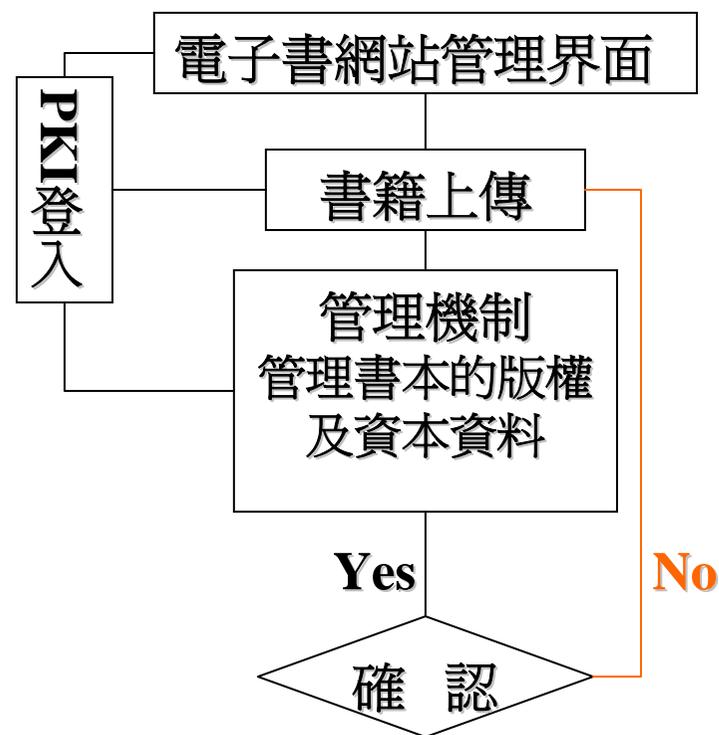
以電子書的營運模式為例





出版社端之使用流程

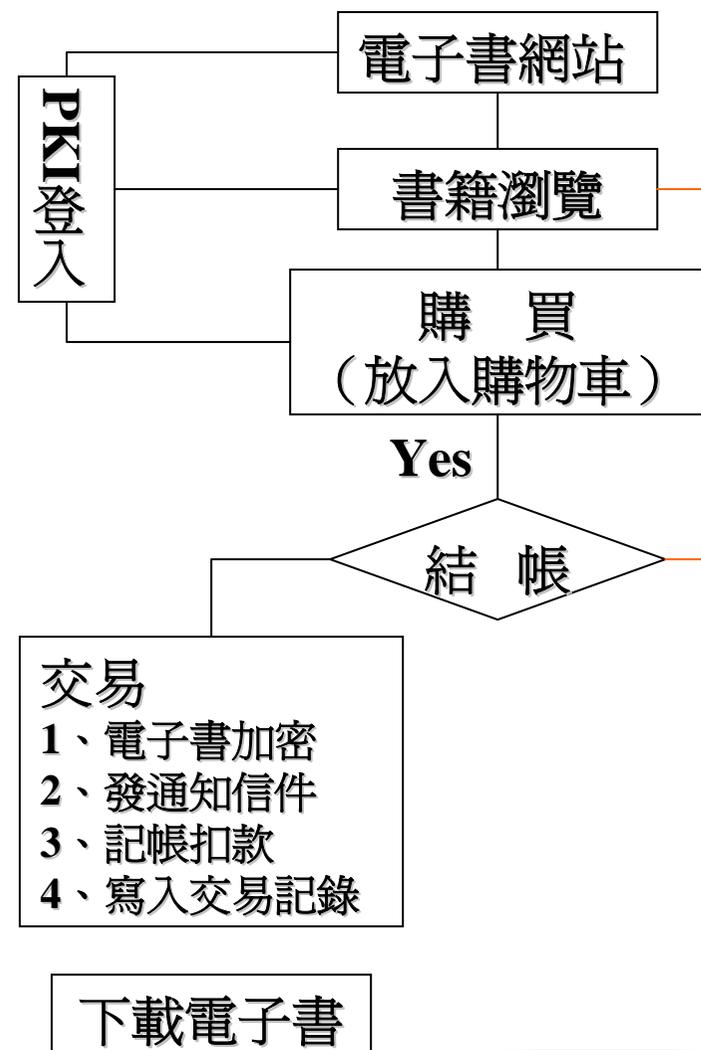
- 內容提供者建立其所有權(著作權)之數位簽章
- 內容提供者設定其 **Metadata** 的 **Rights** 授權使用方式





客戶端購買下載之流程

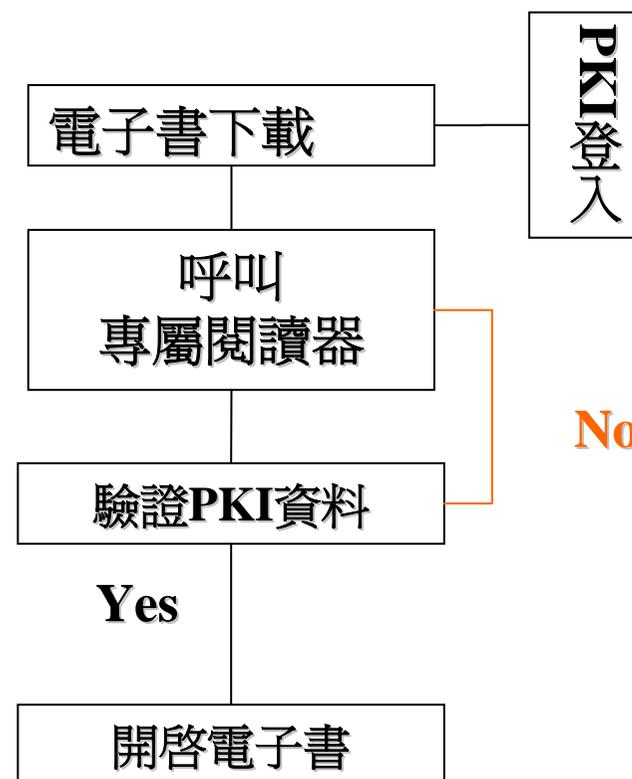
- 將所欲購買的數位內容做依照登入之身分做個人化的簽章並編寫成符合**XrML**規格的內文
- 依照交易條件對數位內容做**Rights**的授權





客戶端閱讀之流程

- 先行以**PKI**驗證消費者的身分，接著根據其中金鑰進行解密
- 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





數位版權管理平台介紹

■ 示範網站

[Http://www.handbox.com.tw](http://www.handbox.com.tw)



謝謝指教

邱迪先 happy@email.yfp.com

