

## 適用於行動設備的數位權利管理系統<sup>1</sup>

葉禾田\* 陳玉音

南台科技大學資訊傳播系

### 摘要

在這個資訊快速傳遞的時代，行動設備與通訊網路也日趨健全，人們可以不再受限於較大型的電腦設備及有線網路，透過行動設備與通訊網路的結合，可以讓更多的人不再因時間、地點與空間的限制，更快速取得所需資訊進行娛樂、商務、學習等各項活動。而在這些活動之中，經由數位權利管理的保護，讓使用者在利用各式的行動設備擷取數位內容時更加安全。

本研究主要目的為利用行動設備所使用串流傳輸的特性，簡化已購買過的串流媒體再度播放流程與接續上一次多媒體播放的時間點，且當使用者們在取得串流傳輸的數位內容後，可以隨心所欲使用已購買的數位內容以及如何去鞏固使用者自身的權利，另外，保障數位內容提供者的權益，免除數位內容被惡意的傳播造成利益的損害。透過本系統，行動設備可以更加便捷取得所需資訊，同時也讓數位內容的使用可以更加的安全與有彈性。

關鍵詞：數位權利、數位權利管理機制、串流、數位內容

---

## Digital Right Management Suitable for Mobile Equipments

Her-Tyan Yeh Yu-Yin Chen

Department of Information and Communication, Southern Taiwan University

### Abstract

In this rapidly information transferred era, the development of mobile devices and communication network has become mature. Individuals are no longer restricted by time, location and space in obtaining online information due to the use of larger personal computer and cable networks. Instead, users are now able to obtain information more quickly and effectively.

---

<sup>1</sup> 本研究承蒙國科會提供計畫經費補助（計畫編號：NSC 96-2221-E-218-017），特此致謝。

\* 通訊作者

電子郵件：htyeh@mail.stut.edu.tw



ely to undertake entertainment, business and learning activities through the consolidation of mobile devices and wireless communication network.? In these behaviors, the transferred digital contexts are protected by the digital rights management, which provides better security to users capturing the digital information with various mobile devices.

The purpose of this study is to utilize the characteristics of streaming identity of mobile devices to reduce the time of replaying purchased streaming media and continuing broadcasting previous play for multimedia players. In addition, after users obtain streaming digital contents they could use these purchased digital contents as their desire, and protect the rights of users and content providers in order to avoid the malicious content spreading and the benefit loss. The digital right management system not only enables the mobile devices to obtain information more conveniently and effectively, but also improves the safety and flexibility of the use of digital contents.

*Key Words: Digital Rights, Digital Rights Management System, Streaming, Digital Content*

## 1. 緒論

行動設備與通訊網路日益健全，使得資訊可以迅速的發展與傳遞，人們可以不再需要侷限在於較大型的電腦設備以及有線網路，並且因為行動設備與通訊網路的結合，使得更多的人們不再因時間、地點與空間的限制而受到影響，可以更快速的取得各項所需要資訊與數位內容，來進行娛樂、商務、學習等各項活動，因資訊科技的技術成長，也讓行動設備取得資訊的使用頻率漸漸趨於頻繁。

數位權利管理 DRM (Digital Rights Management) 又稱為數位版權管理，主要是用來保護數位內容不會被惡意的拷貝、變更以及散播，以保障數位內容本身著作權利以及制定數位內容的使用規範，讓數位內容提供者可以受到權利的保護，數位內容使用者也可以較安心，且有規範的去使用受到保護的數位內容。

最近幾年，很多學者及研究人員已經對數位權利管理 DRM 提出相關解決方案 (Arnab and Hutchison, 2005; Mulligan et al., 2003; Thomas, 2003; Sun et al., 2007; Yang et al., 2009; 陳金鈴, 2007)，而且目前已有幾家公司包括 Adobe、IBM、Microsoft、Intel...等等，已經針對數位權利管理發展出相關產品。但在現今市面上多數的數位權利管理系統，都是比較偏向運用在於一般的較大型個人電腦設備之中，比較少是專門提供給行動設備去使用的數位權利管理系統，所以勉強的去提供給行動設備使用的時候，常會因為各類型的設備本身一開始所規劃的需求不同而造成使用上的限制，像是



行動設備本身的運算量較低、可以儲存的記憶體空間較小等。

而當行動設備在取得多媒體資訊的時候，因為行動設備本身儲存空間較小的關係，所以通常以透過串流傳輸的方式來進行，而一般串流傳輸會將多媒體資訊存放於緩衝區（buffer）之中，所以當多媒體資訊播放完關閉之後，就會直接將多媒體的檔案從緩衝區中刪除，不會再繼續存放於行動設備之中，所以當使用者在觀看多媒體影片時，如果遇到了觀看到某一個時間點，而因為各種不可抗拒因素，被迫關閉掉未觀看完的多媒體影片，於下一次再度播放的時候，又必須再重頭下載播放一次，無法直接從指定的時間定點來進行播放觀看的動作。

另外當使用者們在取得這些串流傳輸的數位內容之後，不外乎是想要可以隨心所欲去使用這些已購買過的數位內容，以及如何去鞏固自身使用者的權利，而換個立場來想，數位內容提供者最在意的也不外乎是對於所提供的數位內容，是否可以被妥善的保護，免除被惡意的傳播，造成自身利益的損害。針對授權使用者及數位內容提供者角色的需求，本研究欲達到的目標如下：

(1)授權使用者：

- ①如何讓授權使用者可隨心所欲使用數位內容？
- ②當授權使用者將設備損毀或遺失時如何鞏固使用者權利？
- ③如何簡化串流媒體再次播放動作？
- ④如何讓串流媒體接續上一次的播放時間點？

(2)數位內容提供者：

- ①如何保護數位內容不被惡意傳播？

## 2. 文獻探討

### 2.1 A license management protocol for protecting user privacy and digital contents in digital rights management systems

由 Park 等學者所提出，此研究主要是為了可以確保數位權利內容的安全與使用者的隱私，如圖 1 方法架構圖（Park et al., 2005）所示。

此協定將使用者匿名，並且利用 Elliptic Curve Diffie-Hellman algorithm 方法去建立用來保護數位憑證（License）的 Session Key，鞏固在傳輸時的安全性。在此協定中，主要分為憑證取得與憑證認證這兩個階段，透過所提出的憑證管理協定，可以去保障使用者身分的隱私與確保數位內容的安全性。

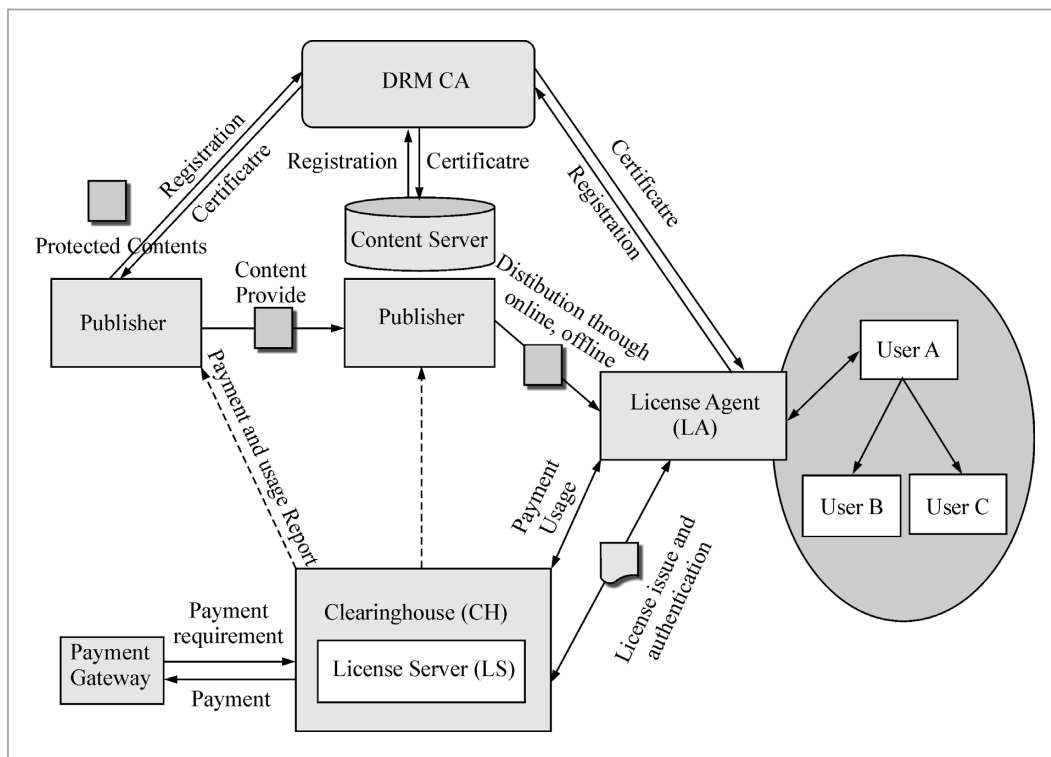


圖 1 Park 等學者提出方法架構圖

## 2.2 行動數位權利管理環境下的認證機制

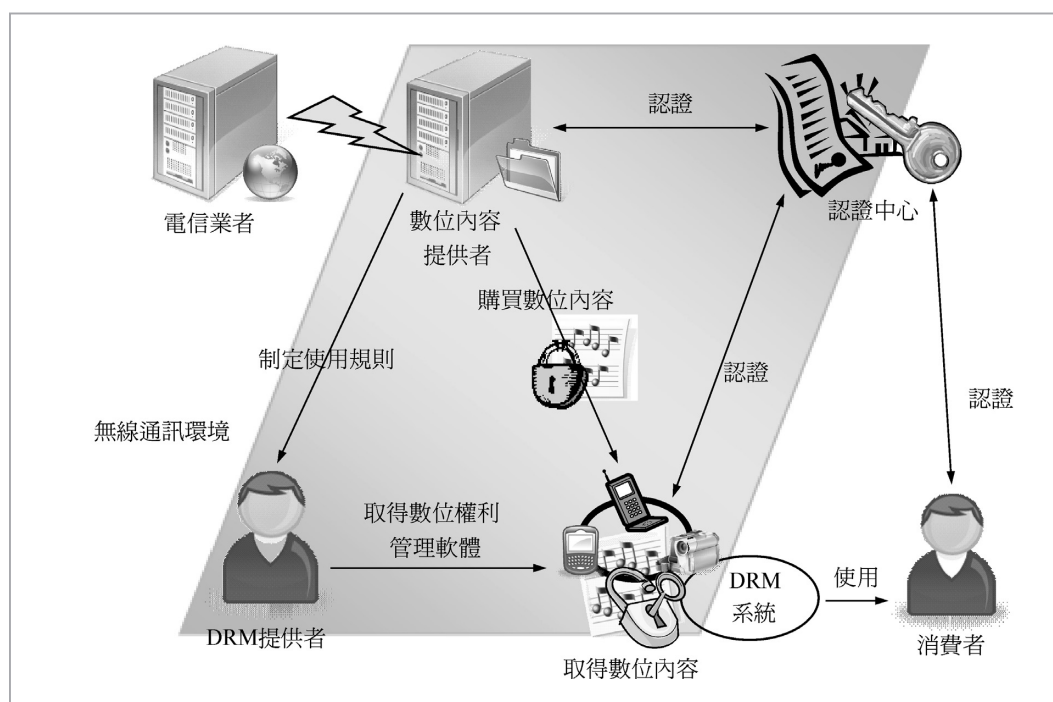
2007 年薛夙珍與學建仁兩位學者提出了一個在行動環境下的認證機制（薛夙珍與學建仁，2007），如圖 2 所示。首先消費者會先透過電信業者所提供的無線通訊網路，然後形成一個行動商務的環境，而數位內容提供者將制定的使用規則傳給數位權利管理提供者，並且提供可以被購買的數位內容給 DRM 系統。

而在消費者取得數位內容與 DRM 系統之前，還必須要先向認證中心來進行認證的動作，認證中心會與數位內容提供者和消費者來進行身份的確認，再和 DRM 系統做認證確認，消費者可以透過 DRM 提供者去取得數位權利管理軟體 DRM 系統，並且再透過 DRM 系統去取得數位內容來進行使用。

## 2.3 A secure and traceable E-DRM System based on mobile device

2008 年 Chen 學者提出了一種植基於手持設備之行動產權管理系統（Chen, 2008），應用了對稱密碼系統、非對稱密碼系統、數位簽章和單向赫序函數等機制來設計系統，所提出之協定分成三個階段(1)內容封裝階段：由封裝伺服器將數位內容做封裝、加密然後儲存到內容儲存伺服器的公開目錄中供使用者下載；並把解密的對稱





▲ 圖 2 行動數位權利管理程序

性金鑰 KEYCID 送到執照伺服器中存放。(2)註冊階段：行動使用者必須提出其個人身分憑證向授權機構註冊（此授權機構可能由企業內部相關主管組成），並建立相關系統參數以做為獲取解密金鑰階段交互驗證之工具。(3)獲取解密金鑰階段：行動使用者必須提出其個人身分憑證及一次使用有效的通行碼（經由授權機構選定的亂數種子，配合國際行動設備身分碼、個人身分憑證、時戳進行赫序函數運算後得到）供授權機構驗證，授權機構再依據使用者的身分決定是否同意發出其解密金鑰，最後以解密金鑰解開數位內容。

## 2.4 串流媒體接續中斷時間播放機制

黃國安與張裕榮兩位學者所提出的串流媒體的播放機制（黃國安與張裕榮，2006），可以在不特定的時間點，快速的去找尋到先前影片的中斷位址，並且接續播放中斷的影片然後繼續觀賞。使用者只需要利用 Windows Media Player 就可以直接去觀看到媒體伺服器上的各項資訊。

網際網路的使用者們通常是把網站當作一個存取多媒體資訊的介面，並透過 Web 網頁及使用者帳號管理來對多媒體伺服器進行存取的動作。而在該研究之中，還提出 Web Server 認證、記錄機制的設計，系統提供一個 Web 的網頁，當使用者在登入該系



統網站的時候，必須要先經過帳號、密碼的認證，才可以進行登入的動作。

資料庫會去記錄使用者曾經觀賞過的各個影片清單，當使用者每次登入系統網站之後，就可以明確知道自己曾經瀏覽觀賞過的每一部影片是否都已經結束傳送，如果尚未傳送完畢的影片要接續去觀看時，系統資料庫內也有著各個影片的時/分/秒記錄，WEB Server 可以提供 SMIL 格式的播放清單，讓使用者可以再次由 Media Services 去接收影片的串流媒體，以接續未觀看完畢的串流媒體。

## 2.5 相關數位權利管理系統議題

針對上面所介紹的各個數位權利管理系統，其中 Park 等學者（2005）所提出方法是將使用者進行匿名的動作，並且利用 Elliptic Curve Diffie-Hellman algorithm 的方式來建立加密用的 Session Key，對數位內容及數位憑證（License）進行保護，而在所提出的方法架構之中，當憑證代理人（License Agent）向 DRM System 要求取得數位憑證時，必須要先向 DRM System 中的數位憑證伺服器（License Server）做身分確認，如果身分確認無誤才會去發佈數位憑證，再去計算 Session Key，將這兩個資訊回報給憑證代理人，憑證代理人利用這些資料去計算認證的訊息，再利用所計算出來認證的訊息向數位憑證交換中心（License Clearinghouse）做認證確認，認證確認完成後，會由數位憑證交換中心發送一個內容金鑰給憑證代理人，才可以進行播放內容與描述權利，並且憑證代理人還會去權利交換中心進行權利追蹤，對權利來進行管理的動作，才算完全結束憑證代理人的工作，而這整個流程動作對於行動設備而言太過於繁雜，所需要付出的成本花費也就相對的高出不少。

薛夙珍與學建仁（2007）兩位學者所提出之行動數位權利管理環境下的認證機制，此認證機制是專門針對行動設備所提出，利用無線通訊網路來達成行動電子商務的環境，但在執行購買數位內容及認證階段加密的時候，卻沒有去考量到行動設備的運算能力不足的問題，在加密的過程裡使用了四次非對稱式的加密法與四次雜湊函式運算，大大增加了行動設備的負擔。

Chen（2008）學者所提出一種植基於手持設備之行動產權管理系統應用了對稱密碼系統、非對稱密碼系統、數位簽章和單向赫序函數等機制來設計，複雜度依然偏高，且並未考慮到如何簡化接續上一次的播放時間點的問題。

黃國安與張裕榮（2006）兩位學者所提出之串流媒體接續中斷時間播放機制，此機制提出了訂定使用者播放時間點記錄的觀點，但是卻只是利用未傳輸出去的多媒體資料量，來做為該時間點的一個依據指標，卻並沒有去考量到使用者本身觀看的進度問題，容易造成伺服器與使用者之間有著時間差的問題存在，進而無法確切的去掌控使用者自身播放觀看的時間。

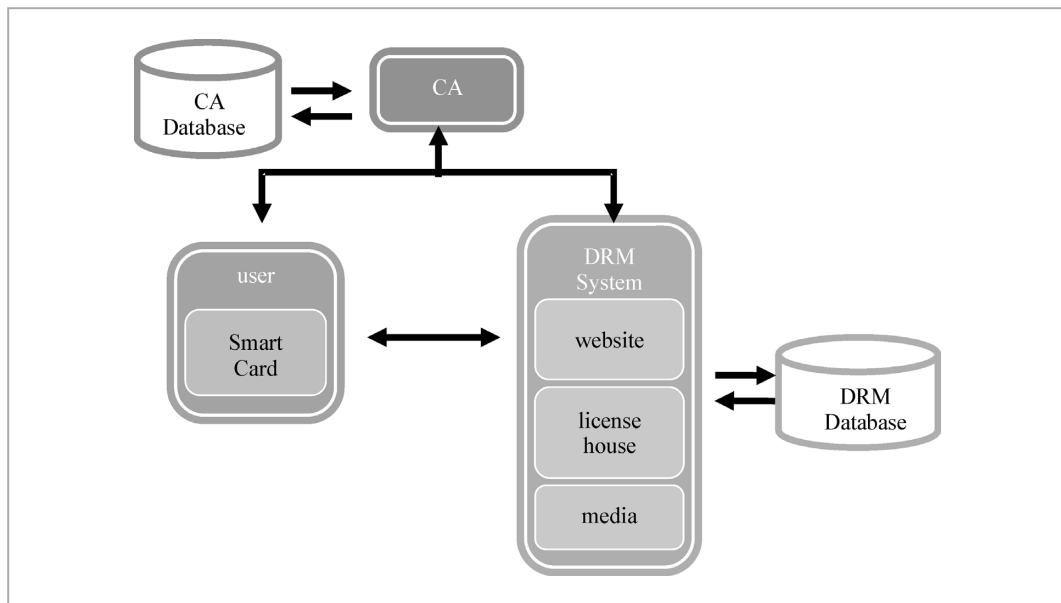


### 3. 適用於行動設備的數位權利管理系統

對於數位內容的使用者們而言，往往最重要的還是在於自己如何可以自由安全的使用數位內容以及如何鞏固自己所擁有的權利，透過數位權利管理可以讓使用者安全取得所有需要的資訊，也可以讓數位內容提供者保障自己所提供的數位內容，不被惡意散播出去。

#### 3.1 系統架構

如圖 3 系統環境架構所示，認證中心 CA 為一個可被信任公正的第三方，使用者 user 與 DRM System 皆須先行向認證中心 CA 進行註冊，使用者會以一組自選的帳號、密碼來向認證中心 CA 註冊，註冊完畢後認證中心 CA 會給予使用者一張內含兩把對稱式金鑰的 Smart Card，用來與認證中心 CA 和 DRM System 進行溝通使用的共享私密金鑰，而 DRM System 也會得到兩把對稱式金鑰，這兩把金鑰是用來與認證中心 CA 和使用者進行溝通使用的共享私密金鑰。



▲ 圖 3 系統環境架構

當使用者想要取得數位內容播放使用的時候，可以連至 DRM System 所提供的 website 去選取自身所想要的數位內容。在確認選取時，需先以個人自選的帳號、密碼和與 DRM System 溝通的金鑰加密，才可進行登入購買數位內容的動作。而这三項資訊，在使用者向認證中心 CA 註冊確認後，認證中心 CA 就會將資訊傳送給 DRM Sys-



tem 作為後續登入的依據。

當確認購買者的身分之後，DRM System 再向認證中心 CA 提出購買的申請，並由認證中心 CA 去處理購買付款的動作，當使用者付款完畢取得收據之後，數位內容才會根據 license 來進行加密動作，再將加密後數位內容傳至給使用者使用。當使用者接收到加密的數位內容後，必須再以與 DRM System 互相搭配的播放器 player 才可進行播放的動作。

### 3.1.1 角色說明

- (1)使用者 user：泛指欲購買數位內容來播放觀看者。
- (2)DRM System：用來提供使用者選取數位內容並且將數位內容進行加密動作，保障數位內容提供者的權益，其中 DRM System 由 website、license house、media 所組成。
  - ①website：由 DRM System 所提供的網站，讓使用者可以去瀏覽所需要的數位內容，並且在此進行選取動作。
  - ②license house：用來製造、存放與數位內容相對應的數位憑證 license。
  - ③media：用來存放原始未加密與已加密過的數位內容。
  - ④DRM Database：DRM System 所使用的資料庫，用來存放使用者個人與購買的相關資訊。
- (3)憑證中心（CA）：公平公正可被信任的第三方，所有成員皆須向此註冊。CA Database 為憑證中心 CA 所使用的資料庫，用來存放各個註冊者相關資料。

## 3.2 DRM System 符號說明表

表 1 針對本研究裡面所使用到的各個符號進行簡易說明。

▼ 表 1 DRM System 符號說明	
符號	說明
$u_{id}$	使用者自訂帳號
$u_{pw}$	使用者自訂密碼
$m_{id}$	行動設備唯一識別碼
$drm_{id}$	DRM System 帳號
$cp_{id}$	數位內容提供者帳號
$p_{id}$	數位內容產品識別碼
$K_{uca}$	使用者與憑證中心共享金鑰
$K_{ud}$	使用者與 DRM System 共享金鑰



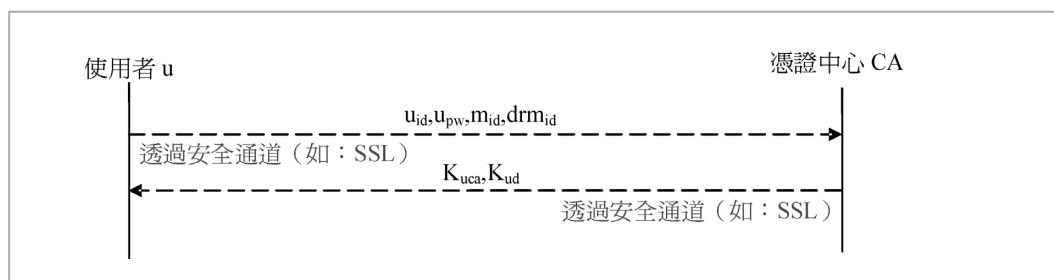
$K_{den}$	DRM System 與憑證中心共享金鑰
$K_u$	使用者獨自擁有的私有金鑰
$K_d$	DRM System 獨自擁有的私有密鑰
$N_u$	使用者隨選亂數值
$N_{u2}$	使用者購買後再次播放所選的隨選亂數值
$N_d$	DRM System 隨選亂數值
Index	記錄使用者下一次使用數位內容依據
Count	使用者購買次數
Price	該購買的數位內容單價
Total	記錄單次所購買的總金額
Receipt	使用者購買繳費後銀行所給予的依據
Ro	數位內容
Uro	接續傳輸未播放完畢的數位內容
C	加密後數位內容
New	要求數位內容重頭再次播放
Continue	要求數位內容接續上一時間點再次播放
Time	使用者端結束數位內容觀看所產生的時間點記錄

### 3.3 DRM System 運作階段

使用者  $u$  要進行一連串的數位內容使用，其中在個人的行動設備之中，必須要擁有著與 DRM System 相互搭配的播放器 player 才可以進行播放觀看動作。

#### 3.3.1 使用者 $u$ 向憑證中心 CA 註冊

當使用者  $u$  想要使用 DRM System  $D$  的時候，必須要先向憑證中心 CA 去進行註冊動作，並且在註冊動作之後憑證中心 CA 會發給註冊使用者  $u$  後續認證使用的加密金鑰。



▲ 圖 4 使用者  $u$  向憑證中心 CA 註冊



圖 4 流程步驟說明：

step1：透過安全通道傳送  $u_{id}, u_{pw}, m_{id}, drmid$

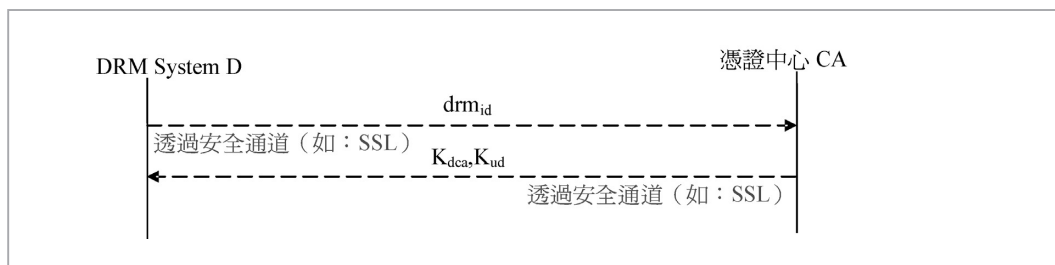
使用者  $u$  會將使用者自訂帳號  $u_{id}$ 、自訂密碼  $u_{pw}$ 、行動設備唯一識別碼  $m_{id}$ 、DRM System 帳號  $drmid$  透過安全通道，傳送至憑證中心 CA 來進行註冊動作。

step2：透過安全通道傳送  $K_{uca}, K_{ud}$

當憑證中心 CA 確認註冊資訊後，透過安全通道（如：SSL）傳送認證資料給使用者  $u$ ，使用者  $u$  就可以將這些傳送過來的資訊直接寫入到實體的 Smart Card 中包含兩組對稱式金鑰，一為與憑證中心 CA 共享的對稱式金鑰  $K_{uca}$ ，另一為與 DRM System D 共享的對稱式金鑰  $K_{ud}$ ，為往後認證溝通加密時使用。

### 3.3.2 DRM System D 向憑證中心 CA 註冊

在 DRM System D 運作之前，必須要先向憑證中心 CA 進行註冊認證的動作，註冊後可以讓 DRM System D 在與使用者  $u$  進行溝通時多一層認證的保護，且憑證中心 CA 會給予 DRM System D 後續用來與使用者  $u$  相互認證的加密金鑰。



▲ 圖 5 DRM System D 向憑證中心 CA 註冊

圖 5 流程步驟說明：

step1：透過安全通道傳送  $drmid$

DRM System D 將自己帳號  $drmid$  透過安全通道傳送至憑證中心 CA 進行註冊動作。

step2：透過安全通道傳送  $K_{dca}, K_{ud}$

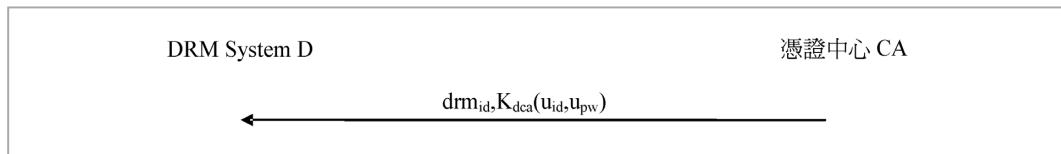
當憑證中心 CA 確認註冊資訊後，會發送兩把對稱式金鑰給 DRM System D，一為與憑證中心 CA 共用金鑰  $K_{dca}$ ，另一為與使用者  $u$  共享金鑰  $K_{ud}$  做為往後認證加密的時候使用。





### 3.3.3 憑證中心 CA 傳送使用者 u 登入認證資料給 DRM System D

每當新的使用者 u 註冊完畢後，憑證中心 CA 就會將使用者 u 與 DRM System D 之後要進行溝通使用的資訊，傳送給 DRM System D 作為後續兩者溝通認證使用的依據。



▲ 圖 6 憑證中心 CA 傳送使用者 u 登入認證資料給 DRM System D

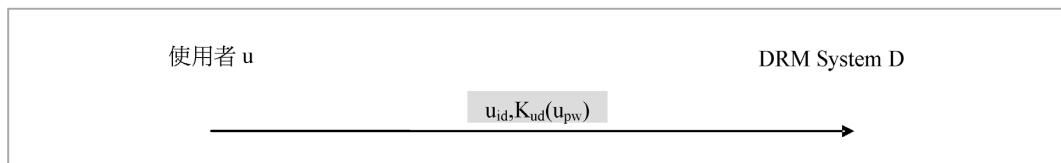
圖 6 流程步驟說明：

step :  $\text{drm}_{id}, K_{dca}(u_{id}, u_{pw})$

當使用者 u 向憑證中心 CA 註冊完畢後，憑證中心 CA 會將使用者 u 的自訂帳號  $u_{id}$  與密碼  $u_{pw}$ ，利用與 DRM System D 共享的金鑰  $K_{dca}$  加密傳送給 DRM System D。

### 3.3.4 使用者 u 登入 DRM System D

當使用者 u 要對 DRM System D 所提供的各項服務進行使用的時候，都必須先以個人的帳號、密碼來進行登入動作，方可開始使用各項資源。



▲ 圖 7 使用者 u 登入 DRM System D

圖 7 流程步驟說明：

step :  $u_{id}, K_{ud}(u_{pw})$

當使用者 u 要登入 DRM System D 時，只需鍵入個人的自訂帳號  $u_{id}$  與密碼  $u_{pw}$ ，再以 Smart Card 中的  $K_{ud}$  來進行加密動作後，傳送給 DRM System D 就可進行認證登入的動作。



### 3.3.5 首次購買及播放數位內容

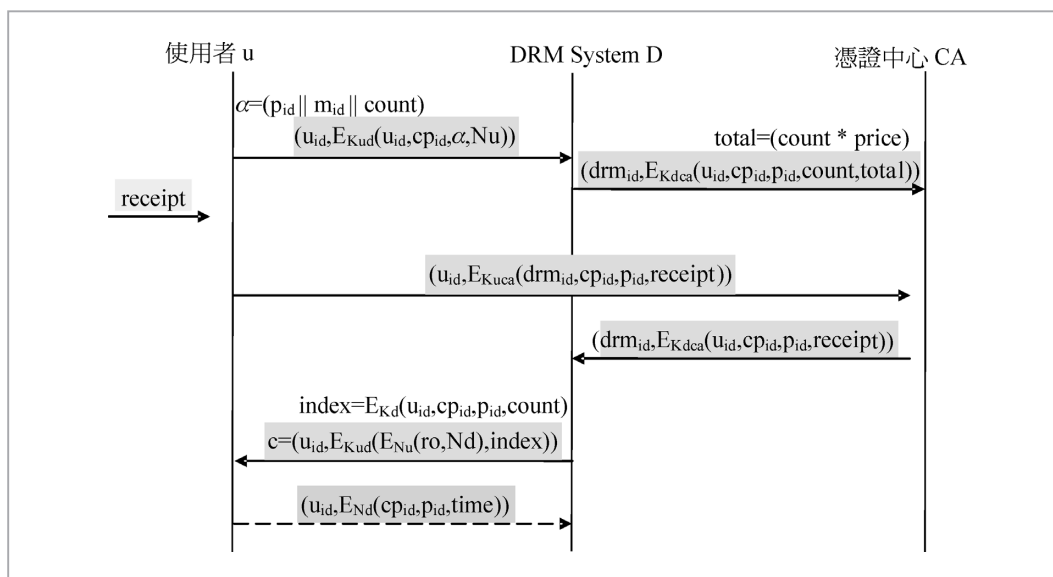
圖 8 流程步驟說明：

step1 :  $(u_{id}, E_{K_{ud}}(u_{id}, cp_{id}, \alpha, Nu))$ , where  $\alpha = (p_{id} \parallel m_{id} \parallel count)$

當使用者  $u$  第一次購買數位內容時，必須先登入 DRM System D，登入後再透過使用者  $u$  與 DRM System D 共享的對稱式金鑰  $K_{ud}$  將使用者帳號  $u_{id}$ 、數位內容提供者帳號  $cp_{id}$ 、 $\alpha$  { 數位內容識別碼  $p_{id}$ 、行動設備唯一識別碼  $m_{id}$ 、數位內容購買數量  $count$  } 與隨機亂數  $Nu$  加密後傳送給 DRM System D。

step2 :  $(drm_{id}, E_{K_{dca}}(u_{id}, cp_{id}, p_{id}, count, total))$ , where  $total = (count * price)$

當 DRM System D 收到該使用者  $u$  所傳送過來的訊息後，會先確認使用者  $u$  的身分，將其內容解密後，再將使用者帳號  $u_{id}$ 、數位內容提供者帳號  $cp_{id}$ 、數位內容識別碼  $p_{id}$ 、數位內容購買數量  $count$  與數位內容購買總金額  $total$  {  $total = \text{數位內容訂購數量 } count * \text{單價 } price$  } 以與憑證中心 CA 共用金鑰  $K_{dca}$  加密後，傳至給憑證中心 CA。



▲ 圖 8 首次購買及播放數位內容

step3 : receipt

當使用者  $u$  在訂購數位內容時會取得相對應的付款資訊，只要去銀行完成付款動作之後，銀行就會給予使用者  $u$  一個付款完成的依據 receipt，讓使用者  $u$  作為付款完成的證明。



step4 :  $(u_{id}, E_{K_{uca}}(drm_{id}, cp_{id}, p_{id}, receipt))$

在完成付款動作並取得付款依據 receipt 之後，使用者 u 會將 DRM System D 的帳號  $drm_{id}$ 、數位內容提供者帳號  $cp_{id}$ 、數位內容識別碼  $p_{id}$  以及使用者購買繳費後銀行所給予的依據 receipt，用使用者 u 與憑證中心 CA 共用私密金鑰來進行加密後，再傳輸給憑證中心 CA 做為後續確認可以播放數位內容的依據。

step5 :  $(drm_{id}, E_{K_{dca}}(u_{id}, cp_{id}, p_{id}, receipt))$

當憑證中心 CA 取得使用者 u 所傳輸過來付款依據的資訊後，就會將使用者帳號  $u_{id}$ 、數位內容提供者帳號  $cp_{id}$ 、數位內容識別碼  $p_{id}$ 、使用者購買繳費後銀行所給予的依據 receipt，用與 DRM System D 共享私密金鑰來進行加密，再傳輸給 DRM System D 告知此次數位內容的訂購繳費已完成，可以將數位內容傳輸給使用者 u。

step6 :  $c = (u_{id}, E_{K_{ud}}(E_{N_u}(ro, Nd), index)), \text{ where } index = E_{K_d}(u_{id}, cp_{id}, p_{id}, count)$

當 DRM System D 收到憑證中心 CA 送來的確認付款資訊後，先將其資訊進行解密，再將數位內容 ro 與 DRM System D 隨選亂數值 Nd，以使用者 u 先前自選的隨機亂數值 Nu 來進行加密，再與記錄使用者下一次使用數位內容的依據 index { 將使用者帳號  $u_{id}$ 、數位內容提供者帳號  $cp_{id}$ 、數位內容識別碼  $p_{id}$ 、數位內容購買次數 count，以 DRM System D 的私有金鑰  $K_d$  進行加密 }，以使用者 u 與 DRM System D 共享的金鑰  $K_{ud}$  來進行加密得到密文 c 再將其傳送給使用者 u。

step7 :  $(u_{id}, E_{N_d}(cp_{id}, p_{id}, time))$

當使用者 u 要關閉播放器的同時，播放器將會主動的把數位內容提供者帳號  $cp_{id}$ 、數位內容識別碼  $p_{id}$  與播放時間點記錄 time，一起以 DRM System D 隨選亂數值 Nd 來進行加密，再回傳給 DRM System D 來做記錄的動作。

### 3.3.6 已購買-從頭再次播放已購買數位內容

圖 9 流程步驟說明：

step1 :  $(u_{id}, E_{K_{ud}}(index, Nu2, new))$

使用者 u 將先前購買時所取得用來記錄使用者下一次使用數位內容依據 index、使用者 u 自選的亂數值 Nu2 與要求數位內容重頭再次播放 new，以使用者 u 與 DRM System D 共享金鑰  $K_{ud}$  加密傳送給 DRM System D。



▲ 圖 9 已購買-從頭再次播放已購買數位內容

step2 :  $\text{count}=\text{count}-1$ 、 $\text{index}=E_{K_d}(u_{id}, cp_{id}, p_{id}, \text{count})$ 、 $c=(u_{id}, E_{Nu2}(ro, Nd, \text{index}))$

當 DRM System D 收到該使用者 u 送來的訊息之後，會先確認使用者 u 的身分，將其內容解密後，再將使用者帳號  $u_{id}$ 、數位內容提供者帳號  $cp_{id}$ 、數位內容識別碼  $p_{id}$  與數位內容購買數量  $\text{count}$  { 此處的  $\text{count}$  會先將購買的數位內容次數減去一 }，以 DRM System D 私有的金鑰  $K_d$  加密製成新的  $\text{index}$ ，再將數位內容  $ro$ 、DRM System D 隨選亂數值  $Nd$  與  $\text{index}$ ，以使用者 u 自選的加密密碼  $Nu2$  來進行加密形成密文  $c$  再傳送給使用者 u。

step3 :  $(u_{id}, E_{Nd}(cp_{id}, p_{id}, \text{time}))$

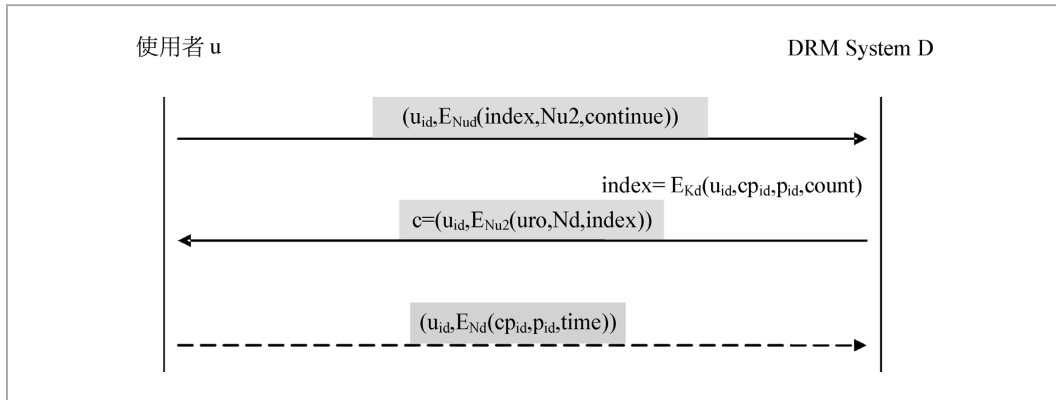
當使用者 u 將關閉播放器之時，播放器就會主動的將數位內容提供者帳號  $cp_{id}$ 、數位內容帳號  $p_{id}$  與播放時間點記錄  $\text{time}$ ，一起以 DRM System D 隨選的亂數值  $Nd$  來進行加密的動作，再回傳給 DRM System D 去做記錄的動作。

### 3.3.7 已購買-接續時間點播放已購買數位內容

圖 10 流程步驟說明：

step1 :  $(u_{id}, E_{Nu_d}(\text{index}, Nu2, \text{continue}))$

使用者 u 將先前購買時所取得的  $\text{index}$ 、自選亂數值  $Nu2$  和要求再次播放接續上一次未觀看完畢的數位內容時間點  $\text{continue}$ ，以使用者 u 與 DRM System D 共享的金鑰  $K_{ud}$  加密傳送給 DRM System D。



▲ 圖 10 已購買-接續時間點播放已購買數位內容

step2 :  $c = (u_{id}, E_{Nu_2}(u_{ro}, Nd, index))$ , where  $index = E_{K_d}(u_{id}, cp_{id}, p_{id}, count)$

當 DRM System D 收到該使用者  $u$  傳送過來的訊息後，會先確認使用者  $u$  的身分，將其內容解密之後，再去搜尋此數位內容上一次播放的時間節點，將接續傳輸未播放完畢的數位內容  $u_{ro}$ 、DRM System D 隨選亂數值  $Nd$  與  $index$  {將使用者帳號  $u_{id}$ 、數位內容提供者帳號  $cp_{id}$ 、數位內容識別碼  $p_{id}$  與數位內容購買次數  $count$ ，以 DRM System D 私有的金鑰  $K_d$  加密}，以使用者  $u$  自選的亂數值  $Nu_2$  進行加密，形成密文  $c$  傳送給使用者  $u$ 。

step3 :  $(u_{id}, E_{Nd}(cp_{id}, p_{id}, time))$

當使用者  $u$  關閉播放器時，播放器將會主動的把數位內容提供者帳號  $cp_{id}$ 、數位內容帳號  $p_{id}$  與播放時間點記錄  $time$ ，一起以 DRM System D 隨選的亂數值  $Nd$  加密，再回傳給 DRM System D 去做記錄的動作。

## 4. 安全性分析

### 4.1 隨心所欲使用數位內容且不失安全性

當授權使用者  $u$  取得數位內容的使用權利之後，想當然會希望可以在自身所擁有的行動設備裡面，自由自在的使用已取得授權之數位內容，透過 DRM System D 可以針對各個數位內容，使用對稱式金鑰加密法來進行對數位內容加密的動作，也可用來確保存放在 DRM System D 之中的數位內容在傳送給授權使用者  $u$  後，保障對於數位內容的安全保護。

而在 DRM System D 之中，授權使用者  $u$  可以連線到 DRM System D 所提供的



website 之中做個人行動設備設備碼的記錄，在每次購買下載數位內容的時候，就會將加密後的數位內容以設備碼來進行包覆，再傳輸給授權使用者  $u$  使用，最後已獲得授權的使用者  $u$ ，也才可以繼續進行數位內容下載的動作，且在下載完畢之後還必須搭配專屬的播放器  $player$  以及相對應的數位憑證  $License$ ，數位內容才可以順利的進行播放使用，讓使用者  $u$  可以自由的在自己所擁有的個人裝置之中自由的使用數位內容。

#### 4.2 設備損毀或遺失也可鞏固使用權利

當使用者不慎將個人的行動設備損壞或是遺失時，這常常會讓使用者們感到極大的困擾，因為每一個數位內容在傳送給使用者進行下載播放之前，都會先行利用各個使用者  $u$  所提供個人行動設備的專屬設備碼，來對數位內容進行包覆的動作，當使用者下載後要進行播放觀看該數位內容的時候，用來播放的行動設備就必須要是與一開始包覆數位內容時相同，必須要有相符的設備碼才可以再接續進行播放觀看的動作。

每一個使用者可以利用個人的帳號與密碼，自行登入到  $DRM$  System  $D$  所提供的 website 之中，並且可以將自己所擁有的行動設備設備碼進行登錄與刪除動作，且在每次播放數位內容的時候，還需要搭配上與憑證中心  $CA$  註冊時所寫入到  $Smart Card$  之中的私密金鑰才可進行觀看播放動作，這樣一來無論是使用者的設備損毀或是遺失，只要即刻登入到 website 之中進行更改，不但可以保障使用者們自身的權益，也可以讓使用者自由隨意選擇自己所要使用的行動裝置來進行播放觀看，並且也不會有使用者  $u$  隨意增加非自身設備，而造成數位內容被隨意傳輸的問題。

#### 4.3 簡化串流媒體再次播放及接續上一次的播放時間點

黃國安與張裕榮（2006）兩位學者所提出串流媒體接續中斷時間播放機制，此機制提出了訂定使用者播放時間點記錄的觀點，但是卻只是利用未傳輸出去的多媒體資料量，來做為該時間點的一個依據指標，並沒有考量到使用者本身觀看的進度問題，容易造成伺服器與使用者之間有著時間差的問題存在，進而無法確切的去掌控使用者自身播放觀看的時間。

本論文中當使用者關閉播放器之時，播放器就會主動的將數位內容提供者帳號、數位內容帳號與播放時間點記錄，一起以  $DRM$  System  $D$  隨選的亂數值  $N_d$  來進行加密的動作，再回傳給  $DRM$  System  $D$  去做記錄的動作。因此可以準確紀錄使用者關閉時間點，不會有時間差的問題存在。

#### 4.4 保護數位內容不被惡意傳播

如何防止數位內容不被惡意的傳播一直都是一個很重要的課題，可分兩方面說明：

(1)當使用者  $u$  要確認購買該數位內容的時候，必須要先行輸入在憑證中心  $CA$  註





冊時個人帳號以及密碼，來進行登入的動作。而 DRM System D 在傳送數位內容給授權使用者 u 之前，會先將數位內容以各個授權使用者 u 所提供的亂數值來進行第一次的加密動作，與相關資訊一起封裝之後，再利用使用者 u 與 DRM System D 共享的對稱式加密金鑰進行完整的加密動作，並與使用者 u 所提供的個人裝置設備碼進行整個訊息的包裹，完成後再傳送包裹完全的數位內容給使用者 u，而當使用者 u 每一次想要對該數位內容進行播放之時，還必須要跟 DRM System 取得該數位內容相對應的數位憑證 License，最後還要搭配上專屬的播放器 player，這樣數位內容才得以順利的進行播放動作。

透過這樣的方式，可以讓數位內容與使用者 u 無論是身分或是設備，都相互的緊緊扣在一起，即使數位內容不小心的被傳播出去，也會因為其他的使用者無法取得相對應的數位憑證 License 以及非原始的授權使用者 u 的設備，對於數位內容而言相對的也是一種保護。

- (2)在行動設備之中，利用串流傳輸本身的特性，對於數位內容來說也是一個安全性的保障，在播放之前會先行預載一些資料量放至於行動設備的暫存區之中，當資料量到達一定可播放的程度之後，就可以馬上進行播放，並且在播放的同時繼續下載後續所需要使用到的播放資料。

而進行播放觀看動作的同時，行動設備也會因為暫存區空間較小，會先將前面所下載且已播放觀看完畢的串流媒體內容先行予以刪除，讓儲存空間得以釋放再持續下載的串流媒體資訊，再進行播放的動作。並在媒體播放完畢後，直接將媒體資訊從暫存區之中完全的刪除，讓媒體可以免除留存於使用者 u 設備之中，讓數位內容得以免除於傳播的危機之中。

#### 4.5 功能性比較

表 2 將使用者所用加解密方式複雜度、數位內容安全保護、License 安全保護與數位內容播放這四項功能，針對各個學者們與本研究所提方法來進行功能性比較。由表 2 可以看出本系統無使用高運算成本的非對稱式加密與簽章，而是以較低運算成本去達成其安全目標。另外也有效的簡化串流媒體接續中斷時間播放機制。

### 5. 結論

在現今生活環境之下，越來越多的人們透過行動設備與通訊網路的結合，快速自由的取得各項資源，不再受限於時間、地點、空間這些因素，讓學習、休閒、娛樂、辦公、資料搜尋等，都可以隨心所欲的達成，讓使用者對於數位內容資源的取得更加



▼ 表 2 各相關機制功能性比較表

	複雜度	數位內容安全保護	License 安全保護接	續上一次的數位內容播放時間點
Park et al. (2005)	在 License 加密之中，使用 2 次非對稱式加密、5 次雜湊函式運算與 3 次數位簽章。	—	提出使用者匿名，並再利用 Elliptic Curve Diffie-Hellman algorithm 去建立 Session Key 來保護傳輸時的 License。	否
薛夙珍與學建仁 (2007)	在使用者購買數位內容與認證階段之中，使用 4 次非對稱式加密與 4 次雜湊函式運算。	以使用者 SIM 卡內的無線識別模組帳號與行動裝置身份序號，並搭配上提供者帳號、時間識別碼與產品識別碼，來對數位內容進行加密動作。	—	否
Chen (2008)	在內容封裝階段使用 3 次簽章及 1 次對稱式加密。	行動使用者必須提出個人身分憑證及一次使用有效的通行碼供授權機構驗證，授權機構再依使用者的身分決定是否同意發出其解密金鑰，最後再由 DRM-AP 以解密金鑰解開數位內容。	一旦 DRM-AP 每次嘗試開啟被保護的數位內容之後，獲取解密金鑰的必要驗證步驟就會自動被啟動。	否
黃國安與張裕榮 (2006)	—	利用使用者個人帳號、密碼進行登入認證，運用權限管理來對數位內容進行管控。	—	是 存在時間差的問題
本研究	在本研究之中，在購買及播放階段共使用 7 次對稱式加密，可以較低運算成本去達成其安全目標。	使用者必須使用個人帳號、密碼登入後，才可進行數位內容挑選、購買或播放，並以使用者隨選亂數值與對稱式金鑰，來向相關資訊進行加密，讓數位內容除了原本的共享金鑰，在每一層隨選亂數的加密保護。	使用者播放數位內容前，會先檢查是否擁有權利，當已確認擁有權利時，會將相關資訊回傳給 DRM System 去取得下一次是否還可以播放的最新 License，並利用使用者隨選亂數值與共享金鑰來進行加密。	是 無時間差的問題

的快速便捷。

而在取得這些資源的時候，也必須要鞏固使用者與提供者的權利與安全，並且讓整個認證流程快速完成，本研究提出適用於行動設備的數位權利管理系統，讓使用者在利用行動設備進行數位內容取得時可以更加的便捷。而針對授權使用者與數位內容



提供者，提出設備碼記錄讓使用者可更加無拘束的在個人設備中使用數位內容，不會因個人設備毀損或遺失造成權利受損，並在每次播放數位內容時，會先管控是否擁有播放權力，在確認取得允許播放認證才可進行播放，且將串流媒體再次播放的繁複程序進行適當簡化，並提供時間點記錄讓使用者可選擇未播放完畢的地方繼續進行觀看，讓使用者在觀看上更加的有彈性。

透過上述的各項改善，讓整個數位權利管理環境可依循著較適用於行動設備的環境來進行服務的提供，並使授權使用者與數位內容提供者都可以在更加方便與完善的環境之中，完成數位內容資訊的取得與傳輸，不再因行動設備本身特性等問題造成使用上的困擾，所有參與者都可以保障自己本身權利，並讓行動數位權利管理系統更臻至完善。

## 參考文獻

- 陳金鈴（2007），“一種植基於手持設備之行動產權管理系統”，《朝陽學報》，1（12），395-415。
- 黃國安、張裕榮（2006），“串流媒體接續中斷時間播放機制”，刊於《第五屆離島資訊技術與應用研討會論文集》，36-40。
- 薛夙珍、學建仁（2007），“行動數位權利管理環境下的認證機制”，刊於《第十八屆國際資訊管理學術研討會論文集》，編號 p0204。
- Arnab, A. and Hutchison, A. (2005), "Requirement analysis of enterprise DRM systems," in *Proceedings of Information Security South Africa (ISSA) conference*, Johannesburg, South Africa, 1-14.
- Chen, C. (2008), "A secure and traceable E-DRM system based on mobile device," *Expert Systems with Applications*, 35(3), 878-886.
- Mulligan, D., Han, J., and Burstein, A. (2003), "How DRM based content delivery systems disrupt expectations of personal use," in *Proceedings of the 2003 ACM workshop on Digital Rights Management*, Washington, DC, USA, 77-89.
- Park, B., Kim, J., and Lee, W. (2005), "A license management protocol for protecting user privacy and digital contents in digital rights management systems," *IEICE - Transactions on Information and Systems*, E88-D(8), 1958-1965.
- Sun, H., Hung, C., and Chen, C. (2007), "An improved digital rights management system based on smart cards," in *Proceedings of the 2007 Inaugural IEEE International Conference on Digital Ecosystems and Technologies*, Cairns, Australia, 308-313.



- Thomas, S. M. (2003), "Digital management in a 3G mobile phone and beyond," in *Proceedings of the 2003 ACM workshop on Digital rights management*, Washington, DC, USA, 27-34.
- Yang, Z., Fan, K., and Lai, Y. (2009), "Trusted computing based mobile DRM authentication scheme," in *Proceedings of the Fifth International Conference on Information Assurance and Security*, Xi' An, China, 7-10.