保障合理使用權的線上數位產權管理系統設計

The Design of Fair-use Online DRM System

陳育毅[1] 詹進科[2] 陳政潔[2]
Yu-Yi Chen Jinn-Ke Jan Cheng-Jie Chen

[1.]國立中興大學資訊管理系
Department of Management Information System
National Chung Hsing University
Taichung, Taiwan, Republic of China

[2.]國立中興大學資訊科學研究所
Department of Computer Science
National Chung Hsing University
Taichung, Taiwan, Republic of China

摘　要

數位產權管理系統是由資訊技術元件與服務組成的系統，符合相關法律、政策、商業模式的一種智慧財產發佈與有效控管產權的機制。現存的數位產權管理(Digital Right Management, DRM)系統，利用使用者電腦的硬體序號做為限制，數位內容只能在單一裝置使用，影響了消費者合法購買的數位內容之合理使用權(fair use)。所以我們更進一步研究，導入 Virtual Software Token 的方式，提高數位內容的可攜性，符合法律上的基本保障。

關鍵詞：數位產權管理、合理使用權、可攜性、虛擬軟體令牌

Abstract

Digital rights management is a system of information technology components and services along with corresponding law, policies and business models which strive to distribute and control intellectual property and its right. Most of the existing digital rights management system using the hardware serial number to bind the usage of digital contents, this kind of policy will against the consumer's fair use right. Therefore, we will design the protocols to achieve the portable digital content by using virtual software token.

Keywords：digital rights management, fair use, portable, virtual software token

1. 簡介

「數位產權管理系統(Digital Right Management)」為數位內容經營最重要的新趨勢，可運用在各種不同格式(文字、影像、聲音、多媒體)的數位內容服務，是因應數位化、網路化的傳播與使用行為所形成的產權管理與著作權議題之新興領域，主要提供數位內容加密保護且產權控管的機制，防止非法拷貝、竄改和散佈。在 2001 年，美國麻省理工學院於 Technology Review 雜誌將數位版權管理的技術，選為改變未來世界的十大創新技術之一。

依國際數據資訊(IDC)[7]的定義：「整合軟硬體之存取與控管機制，將數位內容賦予存取權限，於數位資訊之生命週期內(從產生到廢止)，不論其使用與複製之途徑，仍可持續追蹤與管理數位內容之使用狀況，以提供完善保護數位資訊與權限之管理技術，稱為數位產權管理」。另外，美國國立標準技術研究所(NIST)[15]則是這樣定義：「數位產權管理系統是由資訊技術元件與服務組成的系統，符合相關法律、政策、商業模式的一種智慧財產發佈與有效控管產權的機制」。兩大機構分別從技術層面與管理層面闡述何謂數位產權管理，綜合所述，我們知道數位產權管理系統的運作，除了需要有保護數位內容的密碼學技術外，還要有完整的產權控管機制。

數位產權管理系統的運作是整合多種軟硬體技術之實施，包括：數位內容的呈現、複雜的產權控管機制、數位內容與產權保護，使數位內容創作者能有效保護他們的數位內容產品，防止任何非法使用，使用者必須付費並取得使用執照後，依執照的權限來使用數位內容。為符合這樣的需求，一般數位產權管理系統的規劃，都是針對下列四種角色的互動來做設計：

一、數位內容創作者(Content Provider)：

數位內容創作者會先將數位內容進行加密，以限制數位內容的流通，並製作該數位內容相對應的產權，賦予數位內容使用上的限制。然後將封裝的數位內容和產權分別安全地傳送至數位內容經銷者和使用執照供應商。

二、使用執照供應商(License Server)：

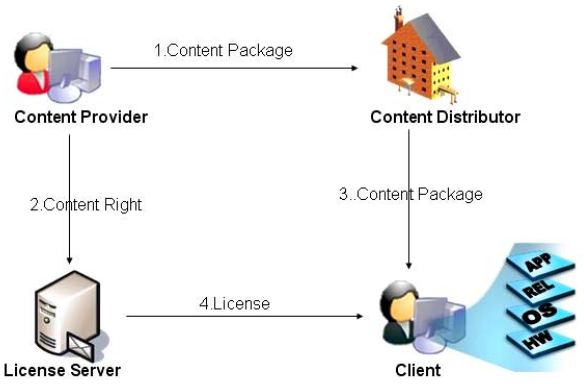
負責保管數位內容使用執照(內含產權與保護金鑰)的機構。

三、數位內容經銷者(Content Distributor)：

為數位內容創作者和使用者之間的媒介，主要提供一個傳播的管道，負責販賣或散佈由數位內容創作者合法加密過後的數位內容。

四、使用者端(Client)：

整個系統中，使用者是最不被信任的，因為任何一個使用者都有可能想要破解受保護的數位內容。所以為了要確保整個系統能夠安全運作，使用者端的數位產權執行軟硬體(DRM-enabled Application)必須具備 Tamper Proof 的特性，不致於讓惡意使用者能夠竄改軟硬體的保護措施，確保數位內容僅能依其權限使用。



圖一、數位產權管理系統的運作

數位產權管理系統的主要運作流程，是以密碼學的安全機制對數位內容進行保護，簡單說明如下：

Step1 數位內容創作者產生一把金鑰(Content Key)，以對稱式加密法(Symmetric Encryption)將數位內容加密，然後將封裝的數位內容(Content Package)，傳送至數位內容經銷者。

Step2 數位內容創作者制訂數位內容相對應的產權(Content Right)，賦予數位內容使用上的限制，然後將產權傳送至使用執照供應商。

Step3 使用者透過網路向數位內容經銷者購買合法的數位內容封裝。

Step4 使用者根據數位內容封裝內的資訊，向使用執照供應商請求對應的使用執照(License)。使用執照內包含了可解開數位內容的金鑰，在傳送給使用者的過程中，是以使用者端的公開公鑰做非對稱式加密(Asymmetric Encryption)。

Step5 要使用數位內容時，只有使用者端數位產權執行軟體(或硬體)的私密金鑰才能解開使用執照，得出數位內容的金鑰與產權，在產權規範下解密使用數位內容。這中間的過程，需要使用者端的應用層、產權解譯層、作業系統層和硬體層等共同合作，才能達到所需的安全性。

數位產權管理系統有時會被誤解成僅是利用加解密技術達成數位內容的保護，因為在整個流程來看，的確是數位內容創作者會先將數位內容進行加密，然後消費者從數位內容經銷者和使用執照供應商合法取得封裝的數位內容和產權，進一步解密得出數位內容。不過，若只以加解密技術做為數位產權管理系統的保護機制，其實無法確保使用者端的解密數位內容安全，使用者有可能將解密後的數位內容非法傳播出去。

2. 數位產權管理的五大安全技術

我們研究了現有的數位產權管理系統，如蘋果公司的 FairPlay[5]、微軟公司的 Windows Media Right Management[13]和 Window Right Management Services System [12]、InterTrust 公司的 Rights|System[3]，其安全機制不只是具備加解密技術，還包含獨特化機制、不可竄改性、數位浮水印、產權描述語言等五大安全技術[4,8,11]，才能確保數位內容的安全。

一、密碼學機制(Cryptographic)：

使用加密和簽章等密碼學技術，可以達成資料傳輸的保密性、完整性、不可否認性等，而在數位產權管理系統也都使用到這類的密碼學機制。

二、獨特化機制(Individualization)：

目前許多數位產權管理系統會使用不同的獨特化機制，確保使用者端的數位產權執行軟體(或硬體)是可唯一辨識的。通常是在初始階段先利用使用者端的硬體資訊或個人身份產生唯一的註冊碼，以此產生一組非對稱金鑰或憑證，保存在使用者端的數位產權執行軟體(或硬體)之安全空間。要使用數位內容時，只有使用者端數位產權執行軟體(或硬體)的私密金鑰才能解開使用執照，得出數位內容的解密金鑰與產權，在產權規範下解密使用數位內容。因為每個註冊的裝置或使用者都有不同的認證授權金鑰，一組使用執照因此限定由單一裝置或使用者解開，所以其數位內容也就能限定為單一裝置或使用者所使用。

三、不可竄改性(Tamper Resistance)：

使用者端的數位產權執行軟體(或硬體)除了具備獨特性，另外就是還要確保不可被竄改。為了避免惡意使用者破壞數位產權執行軟體(或硬體)，一個可充分抵抗惡意攻擊的技術是必須的，這樣才能確保整個系統運作中的使用者端是可信賴的。

四、數位浮水印(Digital Watertmarking)：

在數位產權管理系統的運作之中，數位浮水印也是相當重要的，其主要目的為：版權的保護、追蹤產權使用情形、數位內容的保護。

五、產權描述語言(Right Expression Language)：

產權利描述語言是為了能夠完整描述繁瑣、複雜的使用權限而產生的，為了跨平台與可攜性之目的，採用 XML(eXtensible Markup Language)來做設計。以產權描述語言來訂定數位內容的使用權限，像使用期限、存取頻率、產權移轉次數和授權對象等等。

3. 可攜性與合理使用權的問題

現在大部分數位產權管理系統對於數位內容的使用限制甚多，法律上賦予消費者在合理範圍內的使用原則幾乎都未受到保障，這會讓一般使用者對數位產權管理系統望而卻步。以我國的法律來說，根據著作權法[18]第五十一條之規定：「供個人或家庭為非營利之目的，在合理範圍內，得利用圖書館及非供公眾使用之機器重製已公開發表之著作」。舉例來說，消費者合法購買的 DVD 影片若在家裡予以備份不觸犯法律。另外，著作權法為了促進文化發展，平衡著作人及使用人的權利，還預留一些合理使用各項著作的空間，這在著作權法第四十四至六十五條有相關規定，只要符合其中任何一條，就可以在不經過著作人授權之情況下合理使用其著作。

當然，其他國家的著作權法也有類似的規定，例如在 2003 年 Mulligan 等人[14]以美國的法律和消費者個人合理使用範圍觀點提出「美國 Digital Consumer's 人權法案」，強調消費者擁有 space shift 與 time shift 等權利，也就是說，消費者合法購買的數位內容應該允許在任何個人的裝置使用(即 space shift)，且任何時間皆可使用(即 time shift)。因為就法律層面來說，在不侵害他人著作財產權、個人及家庭在非營利目的情況下，合理重製、暫時性重製、有條件移轉等，是對於消費者合理使用(fair use)的保障[4,6,17]。

目前數位產權管理系統下的數位內容使用缺乏可攜性，並不符合法律所賦予的個人合理使用權。例如 Apple 公司的 FairPlay 和微軟公司的 Windows Media Right Management，一開始都會對數位產權執行軟硬體進行獨特化的程序，以使用者端的硬體資訊產生唯一的金鑰，只有該台電腦或裝置才能解開使用執照，進一步解出數位內容，而這樣的設計實質上是把授權對象指定在裝置而不是使用者本身，致使數位內容是無法合理重製使用。例如消費者更新硬體後，由於硬體資訊序號改變了，消費者原先購買的合法數位內容將無法使用。

另外，在 Window Right Management Sevices System(RMS)的設計，是以憑證來確保數位內容的確是在被授權者使用的電腦上執行，與前述兩套系統最大的差別，在於以使用者憑證認定身份，數位內容的授權的確是針對使用者本身而非裝置，使用者可以在任何一台電腦再度使用有合法授權的數位內容，相較之下確實是對使用者的合理使用權有所保障。

數位產權管理系統的保護措施若嚴格限制產權的可攜性，不能讓消費者合法購買的數位內容可以合理使用，看似對數位內容業者較為

有利，因為數位內容不會被重製，有效保障數位內容業者的權益。但持續限制消費者的權益，不僅對消費者造成不便，更是違反相關法律規定，讓消費者不願意接納使用，反而造成數位產權管理系統的推廣不易。所以，如何有效保護數位內容，而同時又能兼顧消費者的合理使用權，是值得研究的方向。

目前有研究，提出不影響數位內容的安全性，以智慧卡提高數位內容的可攜性。將原本數位內容的授權對象指定在電腦轉到使用者隨身攜帶的智慧卡，便可在任何一個數位產權執行軟硬體播放自己合法購買的數位內容。也就是說，消費者可以在個人擁有的多台裝置上合法使用其購買的數位內容。而且因為智慧卡不可能被仿製，可保證數位內容在同一時間只在一個裝置使用，達成數位內容可攜性與合理使用之目的。

針對這個研究方向，Conrado 等人[2]在 2003 年提出如何導入智慧卡與數位產權執行軟硬體共同運作，讓消費者可在任何一個數位產權執行軟硬體播放自己合法購買的數位內容。在 2005 年，Hung-Min Sun 等人[16]針對 Conrado 的設計提出改進。

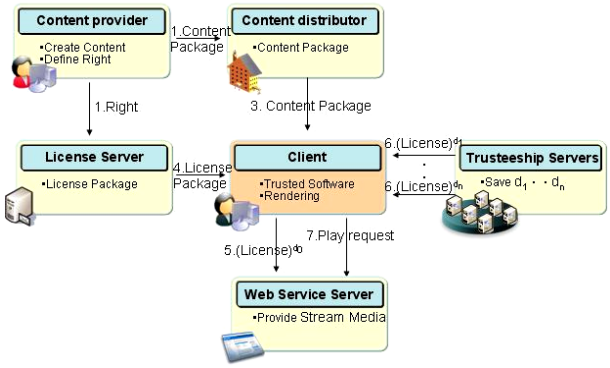
不過，在一般的電腦上，智慧卡並不夠普及，這樣的現象在 Chadwick[1]的文章中道出原因：1.需要額外裝置讀卡機、2.成本高、3.智慧卡的容量與運算能力有限、4.在一般電腦上，以智慧卡做為身份辨識有時比軟體方式的”Software Token”效率較差。所以，針對現實的環境，我們提出如何將 Virtual Software Token [9,10]導入數位產權管理系統，讓數位內容有更高的可攜性。

4. 我們的設計

使用者可以利用在不同裝置中的合法數位產權執行軟體(或硬體)執行 Virtual Software Token 機制，提高數位內容使用的可攜性，重點在於最關鍵的私密金鑰託管於伺服器，讓使用者無須攜帶任何設備，任何時間地點都可透過網路進行身份認證，合法存取數位內容。

如同一般數位產權管理系統，我們提出的架構有數位內容創作者、數位內容經銷者、使用執照供應商、使用者等四個角色，並配合設計所需，合理增加二個角色：

- 網路服務業者(Web Service Server)：提供串流技術的遠端服務。
- 託管伺服器(Trusteeship Server)：使用者私密金鑰的分割託管。



圖二、我們提出的架構

在我們設計的三個階段協定，使用下列的符號：

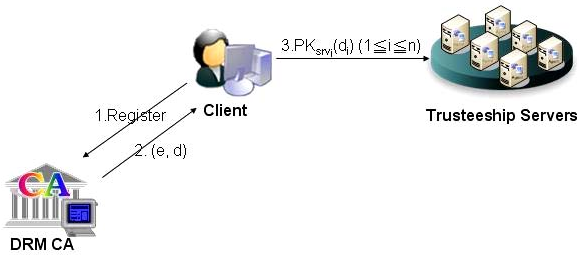
表一：使用符號

λ	1024 bit
N	$N=p*q$, $2^{\lambda-1} \leq N < 2^{\lambda}$
(e,d)	使用者RSA金鑰對且$e, d \in Z^*_{\psi(n)}$
(PK_{ws}, SK_{ws})	網路服務業者的 RSA 金鑰 $PK_{ws}, SK_{ws} \in Z^*_{\psi(n)}$
(PK_{srvi}, SK_{srvi})	託管伺服器的 RSA 金鑰對 $PK_{srvi}, SK_{srvi} \in Z^*_{\psi(n)}$
d_0	使用者端保留不託管分割金鑰 $d_0 \in Z^*_{\psi(n)}$
d_i	儲存在託管伺服器的分割金鑰 $d_i \in Z^*_{\psi(n)}$
ts	時戳
K_{temp}	使用者端與伺服器的暫時通訊金鑰

KeyID	數位內容的辨識碼
CK	加密數位內容的對稱式金鑰
License	含有產權和 CK 的使用執照
Content	數位內容

接下來，分別就系統運作的三個階段，做下列的設計：

[註冊與私鑰分割託管階段]



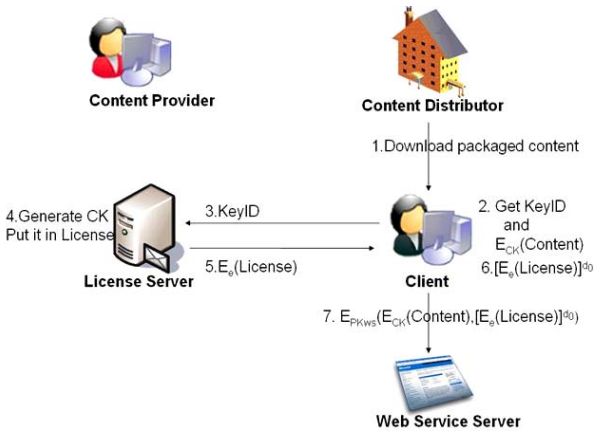
圖三、註冊與私鑰分割託管階段

Step 1 使用者端首先向提供數位產權管理憑證中心註冊。

Step 2 數位產權管理憑證中心即為使用者產生金鑰對(e,d)憑證，透過安全管道傳送至使用者端，儲存於不可竄改的數位產權執行軟體(硬體)內，確保不被非法存取。

Step 3 使用者端數位產權執行軟硬體利用PKCS#5 的Key Derivation Function 以密碼與一些容易記憶的種子參數產生強固金鑰d_0，再將私鑰d切割為$d=d_0+d_1+d_2+\ldots+d_n$。而使用者端的數位產權執行軟硬體將各個分割金鑰d_i $(1 \leqq i \leqq n)$，分別以各個託管伺服器的公鑰PK_{SRV_i}加密，傳送至n個託管伺服器。

[購買階段]



圖四、購買階段

Step 1 使用者向數位內容經銷商購買封裝過後的數位內容。

Step 2 使用者得到的數位內容封裝包含*keyID*和$E_{CK}(Content)$。

Step 3 使用者以 *keyID* 向使用執照供應商請求發佈相對應的使用執照。

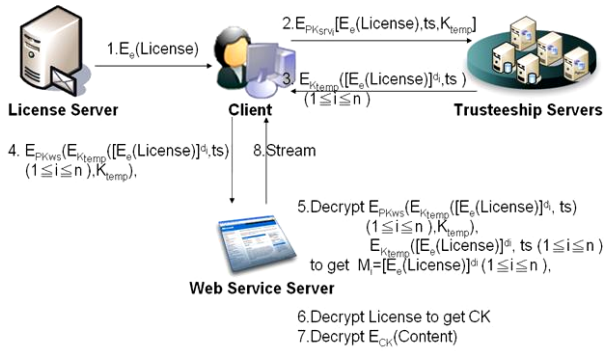
Step 4 使用執照供應商可藉由 *keyID* 查出對應的解密金鑰 *CK*，並將數位內容創作者事先制訂的產權一併封裝進使用執照。

Step 5 使用執照供應商可由數位產權管理憑證中心得知使用者公鑰 e，對使用執照加密，安全傳送給使用者。

Step 6 此時使用者擁有$E_e(License)$，利用其數位產權執行軟硬體保留的金鑰d_0，計算出$[E_e(License)]^{d0}$。

Step 7 最後，數位產權執行軟體(或硬體)將$[E_e(License)]^{d0}$和$E_{CK}(Content)$，以網路服務業者的公鑰PK_{WS}加密，安全傳送至網路服務業者。

[播放階段]



圖五、播放階段

Step 1 使用者端先前取得的$E_e(License)$，可隨時請求使用執照供應商提供。

Step 2 使用者端產生暫時通訊金鑰K_{temp}和時戳ts，連同$E_e(License)$，以各個託管伺服器的公鑰PK_{SRV_i}分別加密傳至n個不同的託管伺服器。

Step 3 各個託管伺服器以私鑰SK_{SRV_i}解開訊息後，檢查時戳在合理時限內，便以使用者託管的分割私鑰d_i計算出$[E_e(License)]^{di}$，並將此結果與時戳以暫時通訊金鑰K_{temp}加密，安全地傳回使用者端。

Step 4 使用者端數位產權執行軟硬體收到所有託管伺服器傳回的訊息$E_{K_{temp}}([E_e(License)]^{di},\ ts)\ (1 \leqq i \leqq n)$, 連同暫時通訊金鑰$K_{temp}$以網路服務業者的公鑰$PK_{WS}$加密，安全傳送至網路服務業者。

Step 5 網路服務業者以私鑰SK_{WS}將$E_{PK_{WS}}(K_{temp})$解密得到暫時通訊金鑰K_{tem}，然後用K_{temp}解出所有的$E_{K_{temp}}([E_e(License)]^{di},\ ts)\ (1 \leqq i \leqq n)$, 檢查時戳是否在合理時限內，並且得到：

$$M_1=[E_e(License)]^{d1}$$

$$M_2=[E_e(License)]^{d2}$$

$$\vdots$$

$$M_n=[E_e(License)]^{dn}$$

Step 6 網路服務業者的數位產權伺服軟體將先前保管的$[E_e(License)]^{d0}$與上述訊息進行下列運算：

$$[E_e(License)]^{d0} * M_1 * M_2 * \cdots * M_n$$
$$= [E_e(License)]^{d0+d1+\cdots+dn}$$
$$= [E_e(License)]^{d}$$
$$= License$$

合法解出使用執照，得出數位內容的解密金鑰CK與產權。

Step 7 在產權規範下，將$E_{CK}(Content)$解密得出數位內容。

Step 8 網路服務業者的數位產權伺服器，以串流技術將數位內容傳送，由使用者端的數位產權執行軟硬體同步接收，數位內容仍受數位浮水印保護，唯有在產權規範下才可合法使用。

5. 安全分析

在我們的設計，將 Virtual Software Token 導入數位產權管理機制，藉此改善許多數位產權管理系統設計不具可攜性的問題，而在安全機制上，同樣將加解密技術、獨特化機制、不可竄改性、數位浮水印、產權描述語言等五大安全技術加以整合，確保數位內容的安全。

一、密碼學機制：

在我們的設計中，使用對稱式加密法保護數位內容，再以非對稱式加密法保護使用執照。只有使用者端的私鑰d才能解出使用執照，取得數位內容的解密金鑰。然而私鑰d在初始階段即被數位產權執行軟(或硬體)分割託管於不同伺服器，因此不

論是內部攻擊者(在組織內部伺機竊取的人)或是外部攻擊者(試圖闖入攔截破解的人)，需破解所有的伺服器才有機會。而為了抵禦低指數攻擊(Low Exponent Attack)，我們建議使用者的公鑰e的大小至少要為$2^{16}+1$，而各個分割私鑰d_i也要符合$N^{1/4} < d_i < N^{2/3}$且$d_i \in Z_{\psi(n)}$，如此得以保障金鑰的安全性。

二、獨特化機制：

在我們的設計中，並非使用裝置硬體序號執行獨特化的動作，而是以憑證來確保數位內容的確是在被授權者所使用的電腦上執行，數位內容的授權是針對使用者本身而非裝置，使用者可在任何具有合法數位產權執行軟(或硬體)的電腦，使用合法授權的數位內容，合理使用權受到保障。

三、不可竄改性

在使用者端與網路服務業者端的數位產權執行軟體(或硬體)確保不被竄改的情況下，便可保障分割私鑰相關運算的安全性，並結合應用層、作業系統和硬體層的保護機制，就能使數位內容限定在產權規範下合法使用。

四、數位浮水印

網路服務業者的數位產權伺服器，在產權規範下，以串流技術將數位內容傳送，由使用者端的數位產權執行軟硬體同步接收，數位內容在傳輸過程仍應受數位浮水印保護，是數位內容創作者在加密之前就先嵌入浮水印，以達到保護效果。

五、產權描述語言：

產權利描述語言是為了能夠完整描述繁瑣、複雜的使用權限而產生的，為了跨平台與可攜性之目的，採用 XML 語法。而我們的設計雖然不討論這個部分，不過更具有可攜性的特性，是更為彰顯這方面的價值。

特別值得一提的，是我們的設計更具有實用價值，應用 Virtual Software Token 更較智慧卡具有可攜性，實質授權對象是使用者本身而非裝置，達到法律上賦予的合理使用權，也更適合應用於現今的網路環境。

現今網際網路頻寬的改善，各式的網路服務(Web Service)逐漸被開發出來並受到重視，大家越來越習慣透過瀏覽器上網處理事務，例如電子郵件、行事曆、網路硬碟等，網路服務已成為最受重視的技術，所以我們的設計是符合這樣的主流趨勢。也就是說，我們在整個架構中加入的網路服務業者與託管伺服器，確實是合乎網路環境的現狀。因此使用者可以在任何時間地點，不受裝置的限制(無需攜帶可驗證身份的智慧卡之類的隨身裝置)，只要使用的設備上具有合法的數位產權執行軟體(或硬體)，透過金鑰的託管伺服器與網路服務業者的協同運作，便可讓使用者在產權規範下隨時合理使用其購買的數位內容。

6. 結論

此篇主要是藉由 Virtual Software Token 的機制，將使用執照的實質授權對象指定在使用者本身而非裝置，有效改善一般數位產權管理中產權可攜性不足的缺點，且保障使用者的合理使用權。未來之研究將會進一步朝門檻式(threshold)的金鑰託管，使系統更具彈性。

參考文獻

1. D. Chadwick, "Smart Cards aren't always the Smart Choice", IEEE Computer, Volume 32, Issue 12, Dec. 1999, pp.142-143.
2. Claudine Conrado, Frank Kamperman, Geert

Jan Schrijen, and Willem Jonker, "Privacy in an Identity-based DRM System", IEEE Prceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03), Prague, September 2003, pp.389-395.

3. Jeffrey Dambrtowski, "InterTrust's Role in Information Assurance for Digital Media", http://www.acsu.buffalo.edu/~jwd/MGS602 project/intertrust.shtml, Nov. 20, 2003.
4. J. S. Erickson, "Fair use, DRM, and Trusted Computing", Communications of the ACM, Vol.46(4), 2003, pp.34-39.
5. "FairPlay: Effectiveness and Weak nesses of Apple's Digital Right Management Technology",http://e170.ex.com/p1/indigo.pdf
6. E. W. Felten, "A Skeptical View of DRM and Fair Use", Communications of the ACM, Vol. 46(4), 2003, pp.56-59.
7. IDC, http://www.idc.com
8. Mayur Kamat, "Security Requirements for Digital Rights Management", TRACK: Leading Edge and Emerging Technologies, October 14, 2003.
9. Taekyoung Kwon, "Virtual Software Tokens – A Practical Way to Secure PKI Roaming", Proceedings of the Infrastructure Security (InfraSec), Vol. 2437 of LNCS, Springer-Verlag, 2002, pp.288-302.
10. Taekyoung Kwon, "Refinement and Improvement of Virtual Software Token Protocols", IEEE Communica- tions Letters, Vol. 8, Issue 1, Jan. 2004, pp.75-77.
11. Qiong Liu, Reihaneh Safavi-Naini, and Nicholas Paul Sheppard, "Digital Rights Management for Content Distribution", Australasian Information Security Workshop, 2003.
12. Microsoft, "Microsoft Window Right Management Services System", http:// www.micrsoft.com/taiwan/windowsserver2003/technologies/rightsmgmt/default.mspx
13. Microsoft, "Windows Media Digital Rights Management", http://www.microsoft.com/windows/windowsmedia/tw/drm/default.aspx
14. D.K. Mulligan, J. Han, and A.J. Burstein, "How DRM-Based Content Delivery Systems Disrupt Expectations of Personal Use", ACM DRM 2003, Washington D.C., USA, October 27, 2003, pp.77-89.
15. National Institute of Standards and Technology, http://www.nist.org.
16. Hung-Min Sun, Chi-Fu Hung, and Bying-He Ku, "An Improved Identity- Based DRM System", 第十五屆資訊安全會議.
17. 陳育毅、蔡柏宏、詹進科, "建立家庭網路與個人合理使用的跨平台數位產權管理機制", 2005 商管與資訊研討會(Taiwan conference on Business and Information), Sep. 29-30, 2005.
18. "中華民國著作權法", http://www.cca.gov.tw/law/html/7-1.html