基於 P2P-OSGi 服務取得機制之數位版權管理機制

林宸堂　　張志鴻
國立嘉義大學資訊管理系
{ ctlin, s0981497 }@mail.ncyu.edu.tw

摘要

隨著資訊科技的發展，讓數位家庭的概念也越來越熱門，OSGi 聯盟提出以家庭閘道器整合家電設備，讓各式各樣的設備間可以相互溝通、提供服務；因而有一些研究結合 OSGi 平台與傳輸更快速的 P2P 網路架構，來達到家庭間多媒體服務的共享。但在 P2P 的分享架構下卻一直存在著盜版的問題，因此我們必須有一套完整的機制，來幫助解決盜版的問題。

在過去已經有針對 P2P 的分享機制提出了數位版權管理機制，它們雖然提供了一定程度的安全性，但相對也讓版權控制系統伺服器的負載過於龐大，因此本研究在基於一 P2P-OSGi 服務取得機制的研究上，整合了數位版權管理機制，在本機制中，利用密碼學系統，為分享檔案的過程提供了一個安全的保護，也減輕了過去研究中版權控制系統伺服器的負載，更讓使用者可以很方便的利用本機制來販售其數位內容。

關鍵詞：OSGi、P2P、DRM。

Abstract

The concept of digital home becomes popular with the development of the information technology. The OSGi Alliance proposes the idea of integrating the household appliances with home gateway, in that case, the communication among appliances becomes possible. Many researches integrated of OSGi platforms and the P2P networking to share multimedia services. However, a digital rights management (DRM) mechanism is needed to solve the piracy problem due to P2P sharing system.

Although some DRM mechanisms for P2P sharing systems have been proposed, they often caused the DRM server overloaded. Therefore, in this paper, we propose a new DRM solution based on the P2P-OSGi system. Our solution uses PKI system involved in the OSGi standard to protect communication security and user authentication. Our DRM system is built on OSGi service gateways, hence, it is convenient for OSGi users to sell or buy the digital contents. In addition, the proposed DRM system is more efficiency since we do not need a central DRM server to encrypt content.

Keywords: OSGi、P2P、DRM

1. 前言

現今家庭中有越來越多的家用設備，而不同的設備各有不同的功能，若欲整合這些功能，一般使用者通常欠缺專業的知識來處理這些整合的問題，因此實現一個自動化設定硬體環境也就顯得更重要，家庭環境中的不同的多媒體裝置間之通訊就變成了一個很重要的議題。現在有許多廠商提出了各種家庭應用環境的標準，如 ECHONET、OSGi、UPnP、DLNA...等[1][2][3]，有了這些標準的支援，讓家庭環境中的各種設備間得以相互通訊，達到一個有助於發展家庭網路的環境。

其中 OSGi 的應用十分廣泛，從醫療照護至家庭娛樂，都可利用 OSGi 來達成自動化的環境，以方便使用者之使用。過去已有研究[4]利用 OSGi 平台建置 P2P 分享機制，以提升多媒體檔案的分享速度，透過 P2P，讓每個不同的家庭間可以透過該機制互相分享多媒體數位內容，使數位內容更容易地在不同家庭的 OSGi 平台間做更快速的共享，且達到自動化的視聽環境設定以及多媒體的播放。P2P 提供了一個很快速的檔案分享技術，但 P2P 也一直被認為是盜版的溫床，其原因是 P2P 本身就缺乏安全機制—其並未提供付款（Payment）、限制非授權存取…等相關機制。過去已有一些研究針對此議題提出基於 P2P 的 DRM 系統[5][6][7]，雖然這些研究都可以解決傳統 DRM 系統在數位內容在傳輸上的效率問題，且也提供了一定程度的安全性，但它們都過於依賴中心伺服器來提供每個使用者的加解密金鑰，如此會讓中心伺服器對於金鑰上的管控變得過於複雜，所以我們希望可以分散加解密的運算負載以及金鑰的管控到各個欲販售數位內容的使用者上，達到一個安全又有效率的 P2P 分享環境。

因此本研究在基於 OSGi 平台上設計一套 DRM 系統，目標是讓創作者可將自己欲販售之數位內容加密後再予以發佈至 P2P 網路上，下載完數位內容的使用者可在付費後向創作者要求使用執照（License），拿到使用執照後方可存取所下載的數位內容。而 License 會依使用者對數位內容的權限（如存取次數、存取時間等）來製作。同時，我們會對 License 做一完整的保護，其中包括：License 使用者的身份驗證、License 的完整性驗證、以及 License 的來源驗證。

2. 文獻探討

過去已有許多針對 OSGi 平台的研究，但由於 OSGi 的標準中缺乏自動化的 Content（多媒體）服務取得機制，所以有研究提出了一套以 Content 導向的 OSGi 服務取得機制[4]，且此研究為顧及 Content 的傳輸效率，因此又加入了 P2P 的網路架構，以加速服務的傳輸速度以及可靠度。由於本研究是以該機制為基礎來設計 DRM 系統，因此底下先簡略介紹該機制的內容。

2.1 P2P-OSGi 服務取得機制

該研究設計一個 Content 導向的相關服務取得機制，且將該機制整合於 OSGi 平台上，該機制內有 2 種主要的 Bundle，分別為：影音 Bundle（Content Bundle）以及相關服務 Bundle（Device Bundle），為了建立 Content Bundle 與 Device Bundle 間的關連性，以達到一個自動化的設定環境，作者重新設計了 OSGi 原始的 Bundle，但並未更動其結構，而是將 Content 放入原始 Bundle 的 Other Resource 欄位中，利用了原始 Bundle 的閒置空間，並且將關連性資訊設計成 Relationship Header（RH），分別放入 Content Bundle 以及 Device Bundle 中，以建立 Content Bundle 和 Device Bundle 的關聯。

而在 Content Bundle 的分享方面，因為 Content Bundle 中包含多媒體影音檔案，其檔案大小通常很大，若只單純透過 Client-Server 架構來傳送，會讓系統效率受阻，可能會降低使用者的使用意願，因此，該研究採用純分散式 P2P 的架構來做 Content Bundle 的分享，利用 P2P 傳輸速度上的優勢，讓 Content 的分享效率提升。

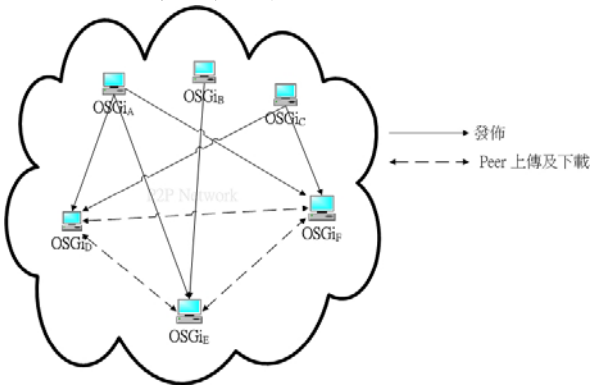

圖 1 P2P-OSGi 服務取得機制架構圖

2.2 P2P-DRM 系統相關研究探討

目前有許多知名的 P2P 分享軟體，如 BT、eMule…等，它們提供了分享檔案上的便利性，但這些分享軟體並未提供數位版權保護的機制。因此，Zhang 學者等人在 BT 的分享機制上提出了一套 DRM 系統[6]，其使用非對稱式加密來保護數位內容。

Zhang 等人所提出的雖然方法可以保證每一個資料區塊在網路上傳送的安全性，以及保護了其數位版權，但相對上也有一些缺點。該系統需要一個集中式的 Server 幫各個 Peer 產生 Re-Encryption Key，且從每一個 Peer 到其它 Peer 都會需要重新重送 Re-Encryption Key，如此 Server 的負載會過於龐大，以至於無法顧及其效率。Server 還需要保留每一次交換後的資訊，因為所有的 Public Key 和 Re-Encryption Key 都保留在 Server 中，這樣會嚴重拖累到 Server 的延展性。再者，將數位內容使用不同金鑰重新加密，在實質上並不會增加安全性，攻擊者只要能截走其中一個 Peer 的 key 攻擊即可，並不需要拿走所有 Peer 的 Key 才可破解，因此在實質上與只用一把金鑰加密的安全性並無差異。

3. P2P-OSGi DRM System

此章節我們將對我們所提出的 P2P-OSGi DRM 機制做一個介紹。

3.1 系統環境與假設

DRM 系統中最關鍵的要素為客戶端的平台中，需要有一個可信任的內容播放器（Player）或瀏覽器（Browser），主要預期它在解密的過程中不會將解密過後的明文外流，意即保護資料流，以及正確地強制執行並套用明定在 License 裡的使用權限[8][9]。本系統內的播放器或瀏覽器會自行判斷 Client 對於他拿的 License 是否具有讀取權限，若 License 中的資訊與其 OSGi 平台的 ID 不符，則不予讀取。意即，使用者收到其購買 License 後只能在其自己的系統上使用，無法移轉。因此本研究做了四個基本的假設：第一、用戶端的 OSGi 平台是可信任、且安全的，即在 Client 端的 OSGi 平台（使用者端的 OSGi 閘道器）內的播放器或瀏覽器，它們只負責解密 License，並且讀取出權限使用規則，且在播放期間不會將解密 Content 的金鑰以及解密後的 Content 外流；第二、我們假設我們架構內的 PMG 的角色是公證的第三方，可以很正確協助交易事宜，但本研究不干涉 PMG 及銀行間的金流方式，只確保交易雙方交易是否完成；第三、因本研究是架構在 OSGi 平台上，OSGi 的規格[2]中，就具有 PKI 的架構，因此本研究之後的協定會使用 PKI 機制，來達成本研究的交易協定；第四、使用者在加入 P2P-OSGi 分享機制之前，都需要取得一個 Token，其目的是提供使用者自身具唯一且唯讀的機密資訊，Token 的取得方式有許多種，而目前較常見的有 Smart Card（IC Card）、RFID、與手機的 SIM 卡[11]…等，都可以用來提供唯一性的資訊當作 Token 使用，在本研究中為了保持系統設計的彈性，不指定使用何種方式來取得 Token 資訊。

本研究基於以上之假設，為 P2P-OSGi 服務取得機制[4]設計了 DRM 系統（如下圖 2 的系統架構圖），架構中共包含了四個角色：

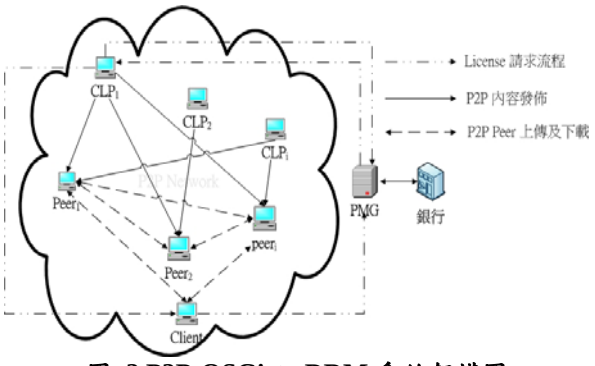

圖 2 P2P-OSGi 之 DRM 系統架構圖

- 原始檔案擁有者（Content and License Provider，簡稱 CLP）：在 P2P 分享機制下，任何一個 OSGi User 想透過本 DRM 機制販售商品，都可以成為 CLP 的角色。它同時也掌控消費者對 Content 的使用規則，意即每個 CLP 都是 DRM Server。
- 已擁有檔案的使用者（$Peer_1$~$Peer_{i-1}$,$Peer_i$）：已經經由 P2P 分享機制下載到 Content Bundle 區塊的 OSGi 平台，其在 DRM 的機制下並未參與任何角色，除非它想購買此 Content 的 License，若想購買，即成為上圖 2 中的消費者（Client）的角色。
- 消費者（Client）：即想購買 Content 的 Peer，它會向 PMG Server 請求付款，在做完付款動作後即可向 CLP 拿到 Content 的 License 來解密、存取 Content。
- 付款中心（Payment Gateway，簡稱 PMG）：協調買賣雙方交易的中介角色，負責與銀行處理雙方交易流程，但本研究不干涉 PMG 及銀行間的金流方式，只確保交易雙方交易是否完成。

3.2 符號定義

在詳細介紹 P2P-OSGi DRM 系統之前，為了簡化協定的表示方法，將之後所使用的每個符號加以定義，以提升可讀性，如表 1 所示：

表 1 符號說明表

符號	說明
ID_x	角色 X 的唯一識別碼
$Name_{Bundle}/ID_{Bundle}$	Content Bundle 的名稱及 ID，即商品的名稱以及商品的 ID。
PK_User/PR_User	在 PKI 機制下，User 的公開金鑰（Public Key）與私密金鑰（Private Key）
Token	硬體特徵碼，可經由多種方式取得，如 IC 卡、CPU 序號…
TS	時戳 (Time Stamp)，以 TS_1~TS_k 代表不同的時間
H()	單向雜湊函數
$E_{PK\_User}(M)$	使用公開金鑰 PK_User 對 M 做非對稱式加密
TID	交易單號碼
TD	詳細交易資訊，如 ID_{Bundle}、購買之存取等級、數量…等
PA	付款總金額
N	Nonce，以 N_1~N_k 代表不同的 Nonce
BA_{Client}	Client 的付款帳戶資訊
BA_{CLP}	CLP 在販售商品後的收款帳號資訊
$CERT_{OSGiUser}$	OSGi User 向 CA 註冊後，所得到的憑證（Certificate）
DR	PMG 所簽發給付款者的數位發票（Digital Receipt），用來記錄成功付款後商品的項目以及金額

3.3 系統流程與協定設計

在本節我們將詳細介紹本研究的交易機制。下圖 3 為系統流程圖，共分成 5 個階段。系統實際流程 5 個階段中的 P2P 下載階段，為第二章文獻探討中所提到之 P2P-OSGi 服務取得機制[4]，因此在下面的協定介紹中並不會針對此一階段多做說明，以下僅針對本研究中所新增 4 個新設計的流程做說明。因為本研究是架構在 PKI 的環境上，因此我們假設在交易開始前，不論是 CLP、Client 或是 PMG，都已經向 CA 取得各自的憑證（Certificate），供後面的交易過程中可驗證身份、以及加密交易資訊。憑證的時效性檢驗，也都會利用 PKI 的機制去處理，所以接下來的處理流程都不包括憑證的正確性與時效性的檢驗。

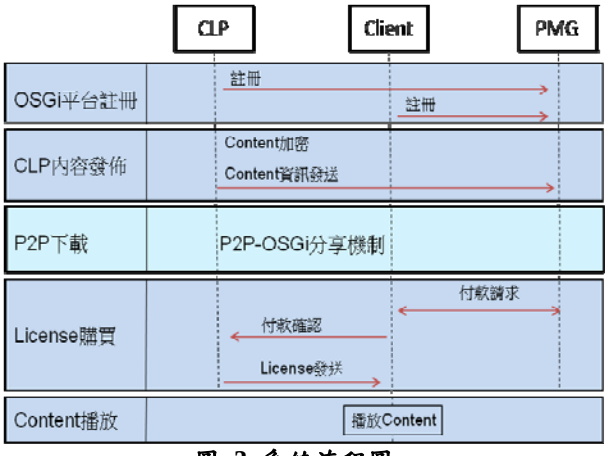

圖 3 系統流程圖

3.3.1 OSGi 平台註冊階段

CLP 或 Client（以下合稱 OSGiUser）要販售或購買商品前都必須向 PMG 註冊，註冊的動作主要是為了讓 PMG 可以知道有這一個使用者（Client/CLP）的存在，下圖 4 為 OSGiUser 註冊協

定）。

步驟1. OSGiUser 利用 Token 做雜湊運算，將運算結果當成自己的 ID。

步驟2. OSGiUser 利用上一步驟中利用 Token 所計算出來的 ID 向 PMG 做註冊的動作，並在訊息內會帶入 OSGiUser 的憑證，供 PMG 可利用憑證辨識第一次註冊的使用者，同時也將憑證與 $ID_{OSGiUser}$ 做關聯，讓日後 PMG 可依 ID 來查找對應的公開金鑰（PK_User）。訊息會使用 PMG 的公開金鑰加密，以保有其機密性。我們是利用密碼學的擴散（Diffusion）特性來達成訊息的完整性驗證[12]，我們將密文內第一個欄位 CLP/Client 的資訊，以明文的方式，附加在訊息中，讓 PMG 可以利用此明文來驗證解密後的訊息是否正確，以此判斷訊息是否有遭到竄改。同時，我們在訊息內會加入一 Time Stamp TS_1，讓 PMG 可依此 TS_1 來確認該訊息是即時訊息，不是重送攻擊。

步驟3. 註冊成功後，PMG 會回應一個成功註冊的訊息，告知 OSGiUser 註冊成功。PMG 會使用其私密金鑰將 N_1 加密，N_1 為上一步驟中，OSGiUser 所產生的一個 Nonce，OSGiUser 收到後利用 PMG 的公開金鑰解密訊息，比對 N_1 是否正確，若比對無誤，即表示此回覆訊息的發送者確實為 PMG，藉此達到身份確認，以及防止重送攻擊的問題發生。

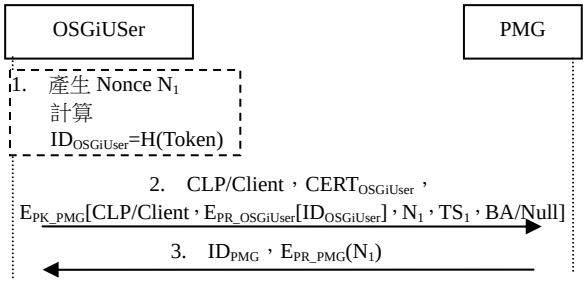

圖 4 OSGiUser 註冊協定

3.3.2 CLP 內容發佈階段

若 CLP 有 Content 欲販售前，CLP 會對欲販售的各個 Content，各自使用不同數位內容加密金鑰（Content Encryption Key，CEK）加密，一個 Content 僅加密一次，不會因使用者不同而再重新加密，完成加密後，再封裝成 Content Bundle。封裝完成後，其必須將商品（Content Bundle）的資訊告知 PMG，日後，若 Client 想購買商品時，即可向 PMG 要求商品資訊，下圖 5 為 CLP 商品資訊更新協定。

步驟1. 計算 H(CB_Manifest)，其為欲販售之 Content Bundle 的 Manifest 的雜湊值。

步驟2. 將商品資訊以及 CB_Manifest 雜湊值，傳送給 PMG，更新商品資訊。協定的設計也允許 CLP 在一次的流程中，傳送多筆商品資訊，在訊息中，$[ID_{Bundle}、H(CB\_Manifest)]_i$ 就代表某一筆商品的資訊，所以假定 CLP 同時間有 10 筆商品資訊欲更新，則 i 就會以 1 到 10 來表示。訊息會利用 CLP 的私密金鑰加密，讓 PMG 可以驗證訊息來源，PMG 可以使用 CLP 的公開金鑰正確的解密訊息，即可以確認是 CLP 所送過來的資訊，不是他人假造。

步驟3. 商品資訊更新成功後，會回傳更新成功訊息通知 CLP。

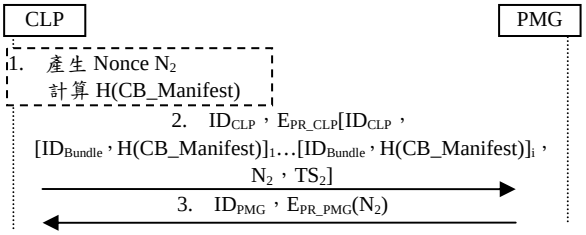

圖 5 CLP 商品資訊更新協定

3.3.3 License 購買階段

在 License 購買階段，Client 取得 Content Bundle 後，若 Client 有意購買 License，則 Client 的 OSGi 平台依 Bundle 的 Manifest 資訊，向 PMG 請求查詢正確的 Content Bundle Manifest 資訊，查詢成功後，即可向 CLP 購買 License，下圖 6 為 License 購買協定。

步驟1. Client 利用所下載的 Content Bundle，從 Content Bundle Manifest 中取出 Bundle 的擁有者 ID（ID_{CLP}），以及 Bundle 的 ID（ID_{Bundle}），向 PMG 發送「查詢 Content Bundle Manifest 的雜湊值」的請求，我們會將訊息利用 PMG 的公開金鑰加密，以保有該訊息的機密性，此步驟還未正式發出購買請求，所以不需要做身份的驗證，但我們需要做訊息的完整性驗證。

步驟2. PMG 收到 Client 的查詢請求訊息後，會依 ID_{CLP} 以及 ID_{Bundle} 開始查找資料庫內是否有符合之項目，若找到符合之項目，會回傳 Content Bundle 的 Manifest 雜湊值給 Client。此步驟 Client 需要去驗證該訊息是否是 PMG 所送過來，並檢驗訊息的來源以及完整性，因此 PMG 會將訊息以自己的私密金鑰加密，以達到來源驗證與訊息完整性。

步驟3. Client 收到訊息後，即可向 CLP 告知欲購買的商品資訊（包含 ID_{Bundle}、購買之存取權限名稱，統稱 TD），請求購買 License。Client 會將訊息利用 CLP 的公開金鑰加密，讓其購買訊息保有機密性，達到保護 Client 隱私的目的。

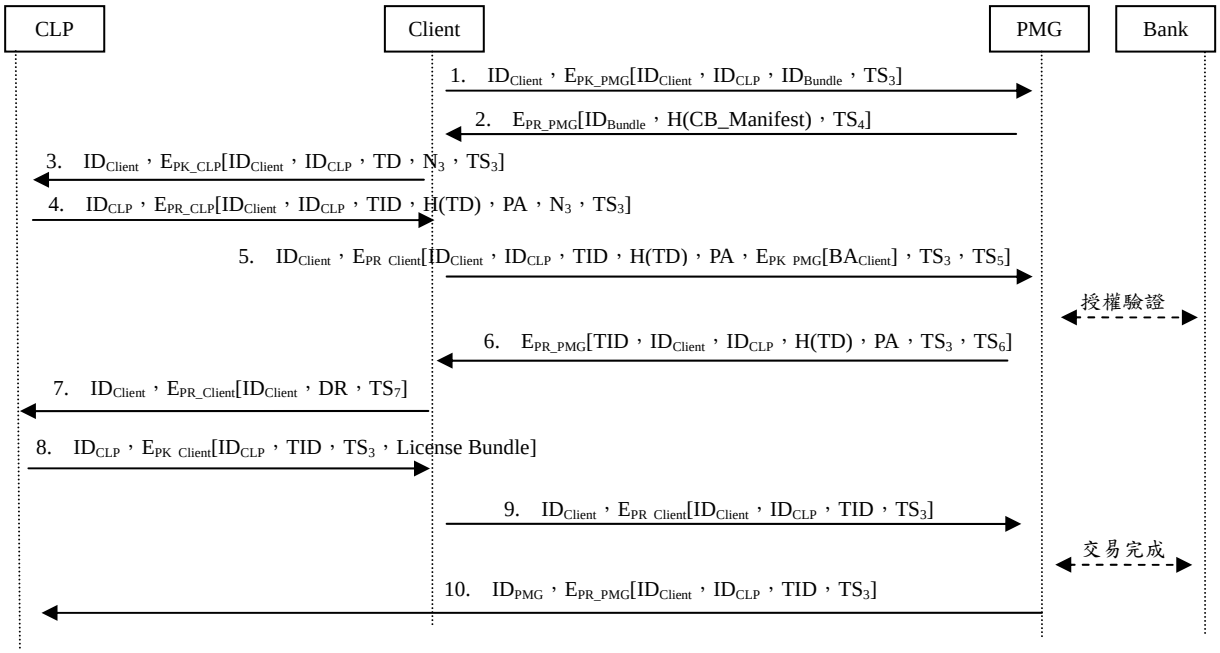

圖 6 License 購買協定

步驟4. CLP 收到 Client 的購買請求後，會依 Client 的購買需求，產生相對應的訂單號碼（TID），並將訂單編號 TID 以及訂單總金額 PA 回傳給 Client，讓 Client 做最後的訂單確認動作。CLP 會利用自己的私密金鑰將訊息加密，做簽署的動作，讓 Client 可以利用 CLP 的公開金鑰來檢驗訊息的來源以及完整性，同時 Client 也需要留存此訊息，若日後訂單上有爭議時，可利用此訊息來解決爭議。由於任何人都可以用 CLP 的公開金鑰來解密此訊息、並得知內容，而商品資訊（即 TD）為較私密的資料，因此我們是將 TD 做雜湊運算後，再加入密文中，如此 Client 仍可驗證其正確性，又不用擔心第三方知曉商品內容。

步驟5. Client 收到訂單資訊後，即會比對商品項目以及商品價格、總額是否正確，若比對無誤，則向 PMG 發送付款請求，同時會附上自己的付款帳號資訊（BA_{Client}）。我們會利用 PMG 的公開金鑰將付款帳號加密（BA_{Client}），因此無須擔心 Client 的付款帳號這種敏感資料會被他人竊知，並將訊息利用 Client 的私密金鑰加密，對訊息做簽署的動作，讓 PMG 收到訊息後，可以利用 Client 的公開金鑰解密訊息，來驗證訊息的完整性以及來源。

步驟6. PMG 收到付款帳號資訊後，即會向銀行確認 Client 所給的帳號是否具有付款能力。若 PMG 在向銀行確認付款帳號正確，即會向 Client 送出付款帳號確認成功的訊息。該訊息會使用 PMG 的私密金鑰加密，做簽署的動作，本系統將整個經 PMG 簽署過的訊息當作是一個數位發票（代稱 DR），Client 即可使用 DR 來證明自己所給的付款帳號確實是有付款能力，可以支付此次交易。

步驟7. Client 在收到 PMG 利用其私密金鑰所簽發的 DR 後，即可利用 DR 向 CLP 要求 License。Client 利用其私密金鑰加密做簽署的動作，讓 CLP 可以驗證此筆交易付款者（Client）的身份，證明 DR 確實是他本人的。

步驟8. CLP 收到 Client 所送來的 DR 後，即會依 Client 的購買需求，將對應的存取權限以及 Content 解密金鑰（CEK）封裝成 License。為了讓 Client 可以去檢驗 License 的來源以及完整性，CLP 必須對 License 做簽章，再一同寫入 License 中，產生 License 檔案，再將 License 檔案，封裝成完整的 License Bundle，再發送給 Client。為了保護 License，我們會使用 Client 的公開金鑰加密，以達到訊息的機密性。

步驟9. 在比對資料無誤後，Client 會傳送收到商品的確認訊息給 PMG，之後 PMG 再向銀行確認此筆交易已經完成，得以轉帳。

步驟10. PMG 確認交易都完成後，會再送一個轉帳成功的訊息給 CLP。

3.3.4 Content 播放

第五階段為 Content 播放階段，Client 已經擁有 Content Bundle 以及完成 License 購買的動作。

步驟1. OSGi 平台內的播放器或瀏覽器，會以 Client 自己的 Token 計算出 ID_{Client}，然後去讀取 License 的資訊，看是否與 License 內所記錄的 ID_{Client} 相符，相符則再繼續第 2 步驟的檢驗，否則不允許存取 License。

步驟2. 在完成第一階段的檢驗後，OSGi 平台即會

開始檢驗 License 的完整性，以確認其未被修改過。OSGi 平台是利用 License Bundle 裡的 CLP 簽章來驗證 License 的來源以及完整性，若驗證無誤，即表示 License 未被竄改過且來源是正確的，OSGi 平台即會再利用 Client 的私密金鑰解密 Content Encryption Key（CEK）取得 CEK，利用 CEK 將 Content Bundle 中的 Content 解密，同時播放器會配合 License 中所記載的存取權限來控制 Content 的存取。

4. 分析評估

本章節中，我們將會分析本研究中之協定，是否有達到一個交易機制所需要的各個安全需求，以及交易公平性問題。

- 訊息機密性
  在訊息機密性上，本研究採用了雜湊函數以及 PKI 的機制來達成。較機密的資料、如 License 購買協定訊息 5 中的付款帳號、訊息 8 傳送商品（License），或者在註冊協定中 OSGiUser 的 ID，我們會以訊息接收者的公開金鑰將訊息加密，以確保只有擁有相對應私密金鑰的接收者才可解密、取得訊息內容。若資訊是需要給第三方知道的（如使用者所購買的商品資訊，TD），我們會將 TD 使用雜湊函數計算，再將訊息傳送給第三方，用以保護使用者的隱私。
- 訊息來源驗證
  我們使用傳送者的私密金鑰將欲傳送的訊息加密，讓訊息接收者可以利用傳送者的公開金鑰來驗證訊息的來源，若可以成功解密，則表示訊息來源是正確的，例如 License 購買協定中訊息 1 即是採用此法。
- 訊息完整性
  在訊息完整性部分，我們分別以 PKI 機制，以及利用密碼學擴散（Diffusion）[12]的特性來達成訊息的完整性驗證。在 PKI 機制的完整性驗證部分，我們使用傳送者的私密金鑰將欲傳送的訊息加密，讓訊息接收者可以利用傳送者的公開金鑰來驗證訊息的來源，若可以正確的解密，則表示訊息是未被竄改的；利用密碼學擴散（Diffusion）的特性，讓攻擊者在不知解密金鑰的情況下，無法準確的修改密文中的資訊。而本研究協定設計中，每個訊息都會有一固定的欄位格式，若密文在傳送的過程中被修改，接收者可以很容易判斷出欄位是否有符合協定設計中的格式，因此，我們利用密文中可辨別身份或內容的欄位，以明文的方式放在訊息中，再一併傳送給訊息接收者，接收者就可透過該明文來間接驗證密文的完整性，比如 License 購買協定訊息 8 即是用此方法。
- 不可否認性
  我們利用簽章的技術來達成這個目的，當買家付款完成或者賣家送出的商品，都會利用其各自的私密金鑰將訊息加密，即對訊息做簽署的動作，若日後交易雙方有爭議時，即可使用這些經過簽署的訊息來證明，以解決爭議，藉此來達到不可否認性。
- 交易公平性若
  一套具公平性的交易機制，必須考量到交易雙方的利益，在交易公平性部分，即買方在付完款給賣方後，可以確實的收到商品；而賣方在收到錢後要確實的將商品送給買方。本系統在這點考量下，在加入了 PMG 這個角色，來協調雙方的交易。在 License 購買協定訊息 9 中，PMG 會待 Client 向他發送商品收到的訊息後，再向銀行確認此筆交易，再進行轉帳的動作；轉帳完成後，PMG 即會再向 CLP 告知轉帳成功，讓 CLP 可以確認帳款是否收到，以此來保證交易雙方的權益。

5. 結論

本研究提出一個整合了 P2P-OSGi 平台的 DRM 機制，不但解決了 P2P 架構分享機制的版權的問題，也讓家庭中的使用者以及創作者，有更便利的管道去存取、販售數位商品。因此，本研究提出的方法，不僅能確保買家的購買商品時的隱密性，也提供一套能有效解決交易上爭議的方法，以確保買賣雙方的權益。

參考文獻

[1] EchoNet. [Online]. Available: http://www.echonet.gr.jp/

[2] OSGi. [Online]. Available: http://www.osgi.org/

[3] DLNA. [Online]. Available: http://www.dlna.org/

[4] 陳一翔，基於 P2P 網路架構下 Content 導向 OSGi 服務取得之設計與實作，國立嘉義大學，2010。

[5] T. Kalker, H. J. Dick, H. Pieter, R. Hartel, L. Lagendijk, and V. S. Maarten, “Music2Share-Coypright-Compliant Music Sharing in P2P Systems,” Proceedings of the IEEE, Vol. 92, pp. 961-970, 2004.

[6] X. Zhang, D. Liu, S. Chen, and R. Sandhu, “Towards Digital Rights Protection in BitTorrent-like P2P Systems,” George Mason University, Fairfax, VA, USA.

[7] 林奕如，P2P 網路之可追蹤與公平交易的數位版權管理機制，國立中興大學，2011。

[8] J. Park, R. Sandhu, and J. Schifalacqua, “Security architectures for controlled digital information dissemination,” Proceedings of 16th Annual Computer Security Application Conference, pp. 224-233, 2000.

[9] J. E. Cohen, “DRM and Privacy,” Communications Of The ACM, Vol. 46, pp. 46-49, 2003.

[10] T. Lindholm and F. Yellin, “Java Virtual Machine Specification,” Addison-Wesley, 1999.

[11] K. U. Chen, C. Y. Lin, and T. W. Hou, “A Low-cost Secure Schemes for Authentications and Access Control with the Use of Multiple Public IC Cards,” 3rd International Conference on Advanced Computer Theory and Engineering, Vol. 3, pp. 609-613, 2010.

[12] S. Claude, “Communication theory of secrecy systems,” Bell Systems Technical Journal, Vol.28, pp. 656-715, 1949.