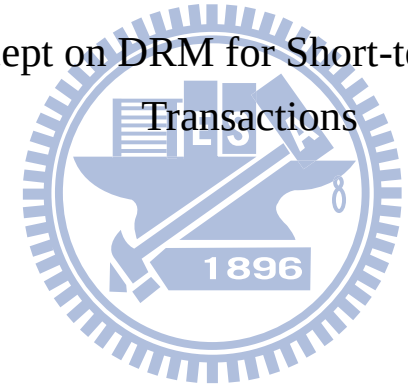
國 立 交 通 大 學

資訊學院　資訊學程

碩 士 論 文

以 SSO (Single Sing On)實現頻繁交易或短期租賃之 DRM 系統

Applied SSO Concept on DRM for Short-term Renting or Frequent Transactions



研 究 生：徐國峰

指導教授：陳登吉　教授

中 華 民 國 九 十 九 年 七 月

以 SSO (Single Sign On)實現頻繁交易或短期租賃之 DRM 系統

Applied SSO Concept on DRM for Short-term Renting or Frequent Transactions

研 究 生：徐國峰　　Student：Kuo-Fong Hsu

指導教授：陳登吉　　Advisor：Deng-Jyi Chen

國 立 交 通 大 學

資訊學院 資訊學程

碩 士 論 文

A Thesis

Submitted to College of Computer Science

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Computer Science

Jul 2010

Hsinchu, Taiwan, Republic of China

中 華 民 國 九 十 九 年 七 月

以 SSO (Single Sign On)實現頻繁交易或短期租賃之 DRM 系統

學生：徐國峰　　指導教授：陳登吉　博士

國 立 交 通 大 學　　資 訊 學 院　　資 訊 學 程 碩 士 班

摘要

近年來，隨著網路的蓬勃發展，帶動了全球數位內容出版業(電子書、電子報、電子雜誌、網路小說、數位學習等)，但也由於網路的普及，造成有價的數位內容被刻意或不經意的廣為流傳，嚴重危害到數位內容版權擁有者的利益，間接也影響了數位內容產業的正常發展

數位版權管理(Digital Right Management, DRM)可用來保護數位內容業者及數位內容。廣義上來說，數位版權管理是利用各種資訊技術，來控制特定的數位內容(如:音樂、電子書、軟體、多媒體檔案等)的使用。這些技術除提供防止消費者任意把內容複製到其他未經授權的設備或未經授權的使用者功能，且對授權內容的操作做了某些特定的限制。

數位版權管理系統通常是設計用來保護大金額、高價值的消費市場或聚焦於保護企業內部有價值之數位資產，在小額消費的普羅市場上，數位版權嚴謹的憑證取得與驗證流程卻反而成為其絆腳石，在本研究中，我們提出了針對小額消費普羅市場的解決方案。

本論文提出了類似悠遊卡機制及應用單點登入(Single Sign On)技術的SAML-based DRM，使得使用者可透過一匿名代號使用。

最後再介紹以 SAML-based DRM 為基礎，未來可能的發展及研究方向。

Applied SSO Concept on DRM for Short-term Renting or Frequent Transcations

Student：Kuo-Fong Hsu　　Advisor：Dr. Deng-Jyi Chen

Degree Program of Computer Science
National Chiao Tung University

ABSTRACT

In recent year, internet is very popular , and there are many e-publishers (like e-book, e-news, e-magazine, e-learning.....etc.) setting up in internet in the world.

However, following by the internet blooming, the problem of copy right is indeed challenged directly or indirectly by illegal download and illegal free share which disintegrate the profit, benefit, and the business growing for the e-publishers .

Now! Digital Right Management, DRM can help those e-publishers solve these situations. Basically, Digital Right Management, DRM is used to control the using of special e-service (like e-music, e-book, software, e-file...etc.) by various information technology which could provide e-publishers to prevent illegal download or illegal free share from internet, and which could also provide e-publishers to limit consumers' behavior. The purpose of Digital Right Management, DRM is focusing on protecting the valuable of e-asset for business and the high profit in the consumer market.

However, the processing of Digital Right may be not easy and take too long time to attract new customers in the low-price consumer market. In our thesis, we provide a model to solve this problem.We figure out a new architecture, SAML-based DRM with a similar concept of Single Sign On, which can help users log-in by an anonymous code.
In final, we will introduce and analyse the development in the future of this technology, which will be based on the concept of SAML-based DRM .

誌謝

本論文得以完成，由衷感謝指導老師陳登吉教授細心的指導與博班鎮宇學長平日的提點及家人的支持。

目錄

摘要 i
誌謝 iii
目錄 iv
圖目錄 v
一、 緒論 1
1.1 研究背景與動機 1
1.2 研究目的 1
1.3 章節概要 4
二、 文獻探討 5
2.1 數位版權管理系統(Digital Right Management, DRM) 5
2.2 裝置式數位版權管理系統(Device-based DRM)－Windows Media DRM 7
2.3 身份認證式數位版權管理系統(Identity-based DRM) 11
2.4 單點登入 (Single Sign On, SSO) 14
2.5 SAML 15
三、 SAML-based DRM 22
3.1 悠遊卡機制 23
3.2 SAML-based DRM運作原理 25
3.3 SAML-based DRM特色 26
3.4 系統架構 27
3.5 系統原理 28
四、 系統實作與成果 37
4.1 系統環境 37
4.2 情境展示-短期租賃 37
4.3 情境展示-頻繁交易 40
五、 結論 43
5.1 總結 43
六、 參考文獻 45

圖目錄

圖 1：典型數位版權管理系統模型[1] 3
圖 2：數位版權管理系統基本架構圖 6
圖 3：Windows Media DRM 架構圖 8
圖 4：購買數位內容流程 12
圖 5：播放數位內容流程 13
圖 6：單點登入示意圖 15
圖 7：SAML 組成元件圖 17
圖 8：SAML 單點登入使用情境圖 18
圖 9：SAML 授權服務使用情境圖 19
圖 10：SAML 後援交易使用情境圖 19
圖 11：SAML 架構圖 20
圖 12：SAML 的使用案例 21
圖 13：iTunes 註冊及購買流程 23
圖 14：悠遊卡的世界 24
圖 14：傳統 DRM 運作模式 25
圖 16：SAML-based DRM 運作模式 26
圖 17：SAML-based DRM 架構 27
圖 18：SAML-based DRM 循序圖 28
圖 19：SAML-based DRM 運作模型圖 31
圖 20：SAML-based DRM 資料交換協定 32
圖 21：虛擬商店登入畫面 38
圖 22：身份認證伺服器登入畫面 38
圖 23：數位版權管理系統使用者主畫面 39
圖 22：購買數位內容畫面 39
圖 24：使用者已購買的數位內容清單畫面 39
圖 25：使用者點選 Play 進行數位內容播放 40
圖 26：虛擬商店登入畫面 40
圖 27：身份認證伺服器登入畫面 41
圖 28：數位版權管理系統使用者主畫面 41
圖 29：購買數位內容畫面 42
圖 30：使用者已購買的數位內容清單畫面 42
圖 31：使用者點選 Play 進行數位內容播放 42
圖 32：Advanced SAML-based DRM 架構 44

一、 緒論

1.1 研究背景與動機

近年來，隨著網路的蓬勃發展，帶動了全球數位內容出版業(電子書、電子報、電子雜誌、網路小說、數位學習等)的商機，但也由於網路的普及，造成有價的數位內容被刻意或不經意的廣為流傳，嚴重危害到數位內容版權擁有者的利益，間接也影響了數位內容產業的正常發展

數位版權管理(Digital Right Management, DRM)可用來保護數位內容業者及數位內容。廣義上來說，數位版權管理是利用各種資訊技術，來控制特定數位內容(如:音樂、電子書、軟體、多媒體檔案等)的使用。這些技術除提供防止消費者任意把內容複製到其他未經授權的設備或未經授權的使用者功能外，也對授權內容的操作做了某些特定的限制。

數位版權管理系統原意是設計用來保護大金額、高價值的消費市場或聚焦於保護企業內部有價值之數位資產，在小額消費的普羅市場上，數位版權嚴謹的憑證(License)取得與驗證流程卻反而成為其普及化的絆腳石。

因此在本研究中，我們試著思考現有數位版權管理系統在小額消費普羅市場中頻繁交易與短期租賃這兩種消費行為模式遭遇到的問題，並探討如何在確保數位內容版權擁有者的權益下，如何提高消費者的接受度，強化數位版權管理系統在小額消費市場的競爭力。

1.2 研究目的

數位版權管理系統，原是為了解決因網際網路(Internet)與全球資訊網(WWW)的快速發展，衍生而出的機密或隱私資訊外洩等資安問題而產生的，圖 1 是一個典型的數位

版權管理系統模型[1]，依照功能我們將其分成數位內容擁有者(Content Owner)、消費者(Consumer)、授權管理中心(License Server)及發行者(Disturber)等四個角色，每個角色的作用如下：

1. 數位內容擁有者

   即數位文件作者或版權擁有者，數位內容擁有者負責將已加入保護的數位文件提供給發行者。

2. 消費者

   即欲購買數位文件的終端使用者，透過向授權管理中心提出需求並支付相當的費用後，即可獲得受保護的檔案與數位憑證，進行合法權限內的使用。

3. 發行者

   發行者為數位內容擁有者與消費者之間的媒介，管理數位內容發佈中心。當發行者收到來自授權管理中心的訊息之後，即將消費者所購買的數位內容傳給消費者。

4. 授權管理中心

   負責管控數位內容權限與交易事宜。當消費者支付相當的費用後，授權管理中心會核發數位權限(digital rights)給消費者，並且記下消費者的執行權限及交易記錄。

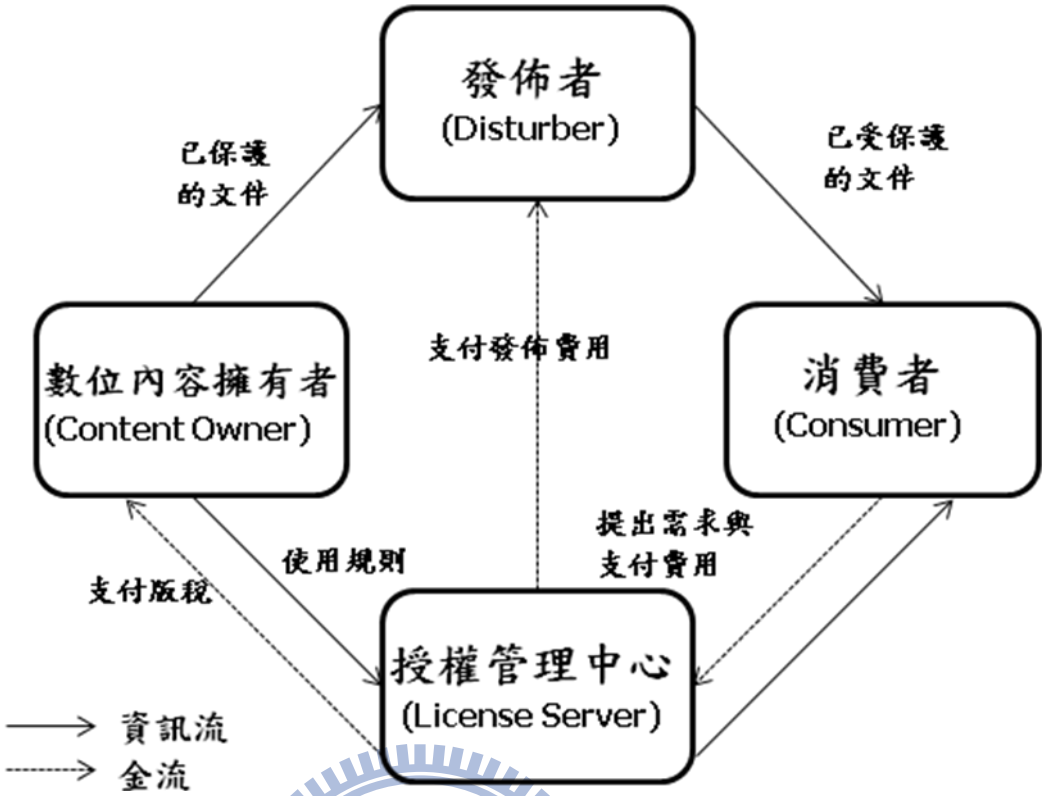


圖1：典型數位版權管理系統模型[1]

大致上，數位版權管理系統廠商，均依循此模型設計並依據不同的數位內容進行開發，以發展不同需求的管理系統，如：Microsoft[2]、Apple[3]、智勝國際[4]、優碩科技[5]等。

這些數位版權管理系統，一般都是為了保護高價值的數位內容或企業內部有價值之數位智權或資產，為達到極致保護的目的，數位版權管理系統提供了較複雜的數位權限發放與繁瑣的授權認證的機制，且每一個數位內容均須要一份獨特的數位權限；使用者在購買前也須出示並提供身份資料及信用卡資料，才能完成交易，取得數位內容。有些系統甚至將數位內容綁定在特定的硬體設備上，消費者在付出相當費用後，仍必須受限於特定硬體才能使用其購買之數位內容。例如：Apple 的 iPod。當將這些看似有效嚴謹的保護機制，應用在小金額消費的普羅市場時，例如：消費者想試閱多本最新的電子小說其中某些章節，再挑選感興趣的電子小說購買。因為這些繁瑣的保護措施，消費者可能會因此而降低購買意願。

SAML (Security Assertion Markup Language) [6][13]是由 OASIS(Organization for the

Advancement of Structured Information Standards)制定的一個解決單點登入(Single Sign On, SSO)需求的規範。在遍尋各大論文後，我們發現，並無研究先進針對 SAML 機制與 DRM 這兩個主題進行整合研究。因此，本論文針對小金額頻繁交易的普羅市場，經由悠遊卡及 SAML 機制，以代號或間接命名機制取代消費者資訊，簡化數位版權管理系統繁瑣的憑證發放及認證過程，提出一個新型態的數位版權管理系統架構，並於本論文第四章中實作一個雛型以驗證本架構之可行性與實用性。

1.3 章節概要

本論文共分五個部份，其內容簡述如下：

第一部份「緒論」，說明本論文研究機動的描述與希望達成之研究目的，並對論文章節做簡單的介紹。

第二部份「文獻探討」，探討與本研究相關的背景知識與文獻，如數位版權管理系統基本技術，並討論其中部份技術的優缺點、再對SSO機制，做一完整的探討。

第三部份「SAML-based DRM」，藉由架構圖，說明結合悠遊卡及SSO機制的數位版權管理的DRM系統設計、架構流程。

第四部份「雛型系統展示」，以實例說明如何應用 SAML-based DRM 在短期租賃及頻繁交易上。

第五部份「結論與未來研究方向」，說明本研究的貢獻及結論，並對未來研究方向提出建議。

二、 文獻探討

本章將詳述數位版權管理系統之基本架構與在系統上會使用到的技術，同時我們也分別探討依認證方式分類的裝置式數位版權管理系統(Device-based DRM)及身份認證式數位版權管理系統(Identity-based DRM)，並提出這兩種數位版權管理系統在小金額頻繁交易市場上遇到的阻礙。

2.1 數位版權管理系統(Digital Right Management, DRM)

在數位化時代裡，由於通訊技術及網路技術的蓬勃發展，加上數位儲存及播放裝置的普及，數位內容已廣為大眾接受，我們所熟知的媒體，如：聲音、唱片、圖片、文字、影像、書籍等，已全數從傳統保存方式走向數位化。藉由網際網路的深化，虛擬化的數位媒體交易也成為新興的商業模式，但也因為網際網路開放的空間，如果這些使用虛擬交易取得的數位媒體內容若沒有特別保護，很容易造成有價的數位內容被刻意或不經意的竊取，嚴重危害到數位內容版權擁有者的利益與數位內容產業的正常發展。

為了保護數位內容出版者權益，數位版權管理(Digital Right Management, DRM)因此順勢而生，它利用各種資訊技術，來控制特定的數位內容(如:音樂、電子書、軟體、多媒體檔案等)的使用。防止消費者任意把內容複製到其他未經授權的設備或未經授權的使用者，並對授權內容的操作權做了某些特定的限制，成為保護數位內容的利器。

2.1.1 數位版權管理系統基本架構

圖 2 為 Intertrust 建構的數位版權管理系統架構[7]，雖然每一家廠商的架構會有所差異，但在設計上都會遵循 Intertrust 定義的架構。

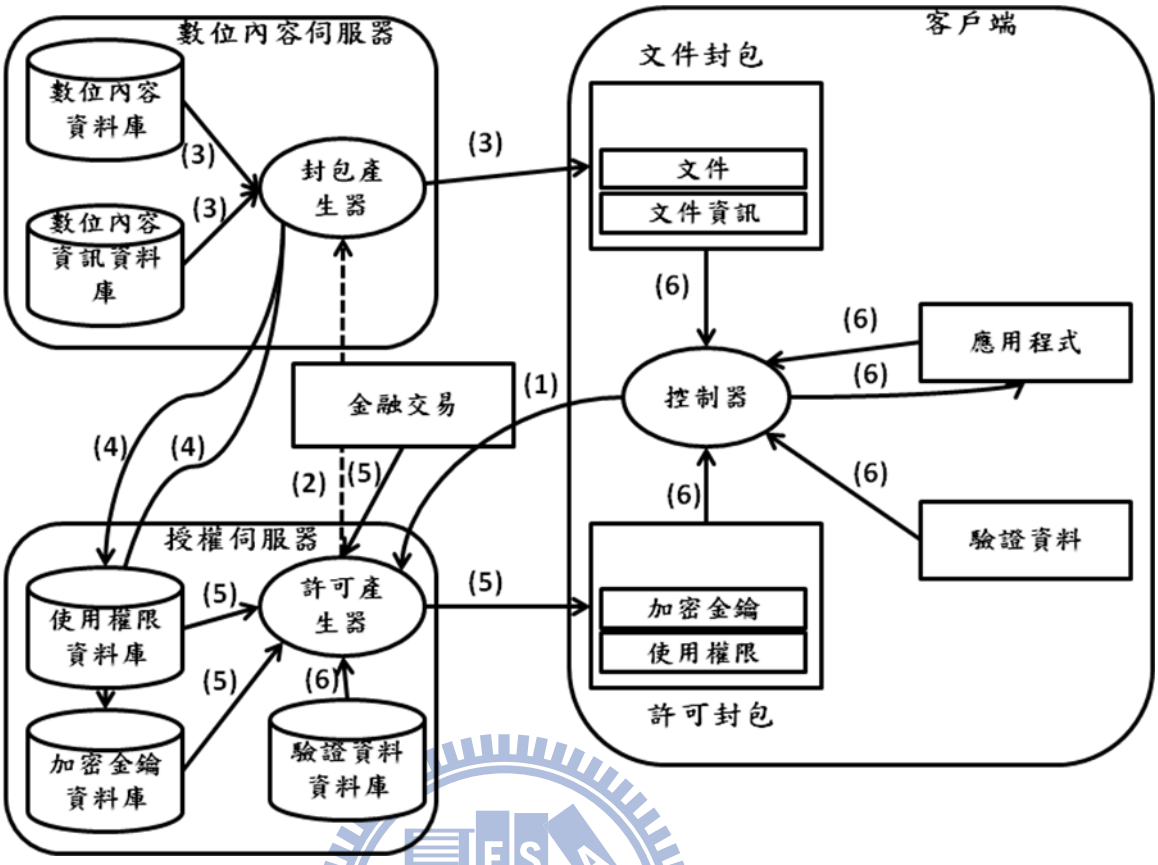


圖2：數位版權管理系統基本架構圖

在 Intertrust 的基本架構中，其運作流程如下：

(1) 使用者向授權伺服器(License Server)購買文件。

(2) 授權伺服器將使用者購買的數位內容資訊傳送給數位內容伺服器(Content Server) 。

(3) 數位內容伺服器將使用者購買的數位內容及數位內容資訊從資料庫取出、加密封裝成文件封包(Content package)，供使用者下載。

(4) 數位內容伺服器將使用權限(Right)及加密金鑰(Encryption Key)傳送給授權伺服器。

(5) 授權伺服器確認使用者已完成付費動作後，即利用前述(4)之使用權限及加密金鑰製作版權管理檔案，並將版權管理檔案封裝成授權封包(License Package)傳送給使用者。

(6) 客戶端的數位版權管理系統控制器(DRM Controller)會將下載的數位內容封包

與授權封包解開並進行驗證，待驗證無誤後，使用者即可依照授權封包賦予之使用權限使用數位內容。

2.2 裝置式數位版權管理系統(Device-based DRM) – Windows Media DRM

以綁定硬體裝置進行認證的數位版權系統常稱為裝置式數位版權系統(Device-based DRM system)或封閉式數位版權系統，數位內容只被允許於此數位內容的特定的裝置上使用，不允許分享或轉移數位內容到其他裝置上，數位內容可攜性極低，此種系統以微軟 Windows Media DRM 為代表。

微軟於 1994 年 4 月推出第一個版本的 Windows Media DRM[8]，目前最新版是 Windows Media DRM。因為微軟在 X86 市場上的地位，Windows Media DRM 也成為相當著名的數位版權管理系統。

2.2.1 系統架構

在微軟的 DRM 系統中有三個主要的角色，分別為數位內容伺服器(Content Provider)、許可證伺服器(License Server)及客戶端(Client)；數位內容伺服器(Content Provider)將已受保護的音樂、影像等其它數位媒體封裝並上傳至網站或串流內容主機，許可證伺服器(License Server)則負責電子交易及授權憑證(License)管理。

其運作流程如下圖：

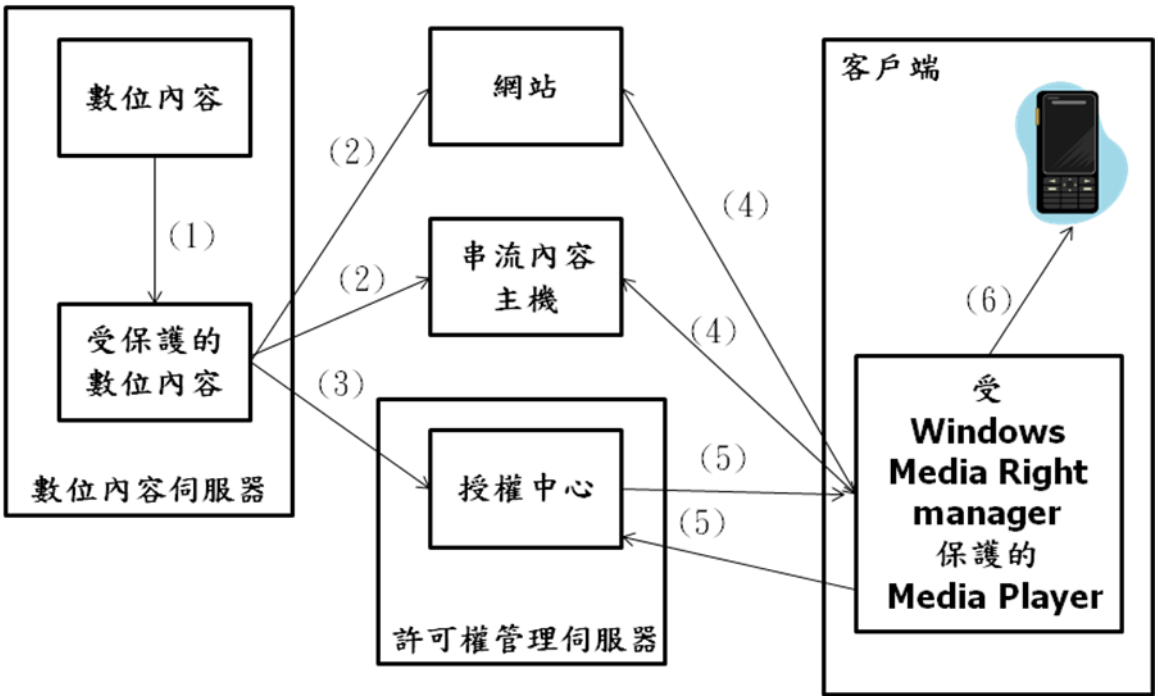


圖3：Windows Media DRM架構圖

資料來源：
http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx

1. 打包(Packaging)

Windows Media 數位內容伺服器將對數位媒體檔進行打包。打包的檔除了被加密外也使用一個“金鑰”鎖定。該金鑰儲存在一個加密許可證中，該許可證將單獨分發。(這是 Windows Media許可權管理器所獨有的功能)，它還會在數位媒體檔中添加其他資訊，例如用於獲取許可證的URL。打包的數位媒體檔將保存為Windows Media Audio格式(檔案副檔名為 .wma)或Windows Media Video 格式(檔案副檔名為.wmv)。

2. 分發(Distribution)

打包後的數位內容檔可放在網站下載或數位媒體伺服器上以串流方式處理、通過CD進行分發或使用電子郵件發送給消費者。Windows Media DRM還允許消費者將受版權保護的數位媒體檔發送給朋友。

3. 建立許可證伺服器(Establishing a License Server)

數位內容提供者可選擇許可證交換中心，該交換中心將儲存許可證的特定許可權或規則並提供Windows Media許可權管理器許可證服務。交換中心的作用是對請求許可證的消費者進行身份驗證。且數位媒體檔和許可證是分開儲存和分發的，因

此更便於管理整個系統。

4. 使用者要求並取得已受DRM保護的數位媒體(Request & Receive Media)

使用者向網站或串流內容主機要求並取得已受DRM保護的數位媒體。

5. 要求並獲取許可證(Request & Download License)

要播放打包的數字媒體檔，消費者首先必須獲取一個許可證金鑰，為該檔解鎖。當消費者試圖獲取打包的數字媒體檔、獲取一個預先傳遞的許可證或首次播放該數字媒體檔時，都將自動啟動獲取許可證的過程。Windows Media 許可權管理器會引導用戶進入註冊頁（要求輸入帳號資訊或完成線上付費），或者從交換中心檢索一個許可證而不提示任何問題。

6. 播放數位媒體檔(Playing Media)

要播放數位媒體檔，消費者需要能支援 Windows Media DRM 的播放機。消費者即可根據許可證中所提供的規則或許可權來播放媒體檔。許可證可提供多種不同許可權，如開始時間和日期、持續時間以及對操作計數。例如：預設許可權可能允許消費者在特定電腦上播放數位媒體檔並可將該檔複製到可攜式裝置。但是，許可證是不可轉讓的。如果消費者將打包的數字媒體檔，發送給一位朋友，則該朋友必須獲取自己的許可證，然後才能播放該檔。這種按 PC 頒發許可證的模式可確保打包的數位媒體檔，只能在已獲得該檔的許可證金鑰的電腦上播放。

2.2.2 功能

Windows Media Digital Rights Management (DRM) 是一種彈性的平台，可讓您保護和安全地傳送儲存庫及訂閱的內容，以便在電腦、可攜式裝置或網路裝置上播放。

Windows Media Rights Manager 為 Windows Media DRM 平台的元件之一，是一種有助於保護內容擁有者權限，同時讓消費者輕鬆且合法地取得數位內容的技術，提供了下列功能。

1. 永久保護

Windows Media Rights Manager 會使用授權碼來「鎖定」數位媒體檔，以維護

內容保護，即使這些檔案已廣泛分佈也一樣。每一個授權只會指派給一部電腦。這樣就能夠防止非法分佈數位媒體檔。

2. 增強式加密

Windows Media Rights Manager 包含經過實證的加密配置，可確保分佈的數位媒體檔不會侵犯隱私或涉入其他非法的使用。

3. 個別化

Windows Media Rights Manager 是透過將每個播放程式連結到主機電腦，讓它成為唯一的播放程式。如此就能夠防止讓受約束的播放程式在網際網路上廣為散佈。藉由個別化，即可在授權程序中識別和停用所有受約束的播放程式。

4. 個別分佈的授權及內容

將授權與實際的數位媒體檔分開發行，可提供最大的彈性並允許廣泛地分佈內容。每當播放數位媒體檔時，Windows Media Rights Manager 就會檢查消費者的電腦是否有授權。不具有效授權的消費者將被導向授權註冊頁面。

5. 安全的音訊路徑

Windows Media Rights Manager 可在Windows Millennium Edition 及Windows XP 作業系統中，確保從播放程式到音效卡驅動程式內容的安全。這種安全關係可降低任何未授權的程式擷取電腦中的數位媒體串流的可能性。

6. 改良的撤銷及更新功能

當有新的播放程式可供使用時，Windows Media Rights Manager 會撤銷受約束的播放程式。

7. 易於變更的授權條款

由於授權和數位媒體檔是分開存放的，因此能夠變更授權伺服器上的授權條款，而不需重新分佈或重新封裝數位媒體檔。

8. 即時加密內容

利用 Windows Media Rights Manager 9 系列及更新版本，內容擁有者可在受保護的即時數位媒體內容 (例如新聞、搖滾演唱會或主要的體育賽事) 正在進行時，透過網際網路來傳送這些事件，而不需先批次處理並儲存這些內容。這種新功能可同時編碼和加密「即時」內容，並避免未經授權的使用，同時可讓消費者透過網際網路體驗到即時廣播的魅力。

2.2.3 使用於小金額頻繁交易的情境

Windows Media Right Manager 強調了「永久保護」(Windows Media Rights Manager 使用授權碼來「鎖定」數位媒體檔，每一個授權只會指派給一部電腦或硬體裝置)及「個別化」(Windows Media Rights Manager 透過將每個播放程式連結到主機電腦，讓它成為唯一的播放程式)。在小金額頻繁交易行為上，例如：消費者利用 PC 在電子交易平台上(如：Amazon)購買了多本最新的電子小說其中某些章節。當消費者在網站上購買電子小說後，其認可權將與使用者購買時使用的硬體綁定，當使用者想將已付費之電子小說複製到行動裝置(如：Android、iPod)上時，消費者將面臨已付費購買的數位媒體內容，僅能限定在某個裝置上播放，雖然使用者可額外購買可移轉至行動裝置的許可權，但行動裝置上的播放程式必須為 Windows Media Player，消費者有可能成功將電子小說複製到 Android 或 iPod 上，卻無法撥放的窘境。對消費者而言，花了錢購買一些非高價值的數位媒體內容，卻必須受限於這種緊密保護數位媒體的方式，將大幅降低消費者消費意願。

2.3 身份認證式數位版權管理系統(Identity-based DRM)

有別於以綁定硬體裝置進行認證的裝置式數位版權系統(Device-based DRM system)，身份認證式數位版權管理系統使用了智慧卡(Smart Card)這種裝置儲存使用者資訊，並以此類裝置裡的資訊進行身份驗證，以提高裝置式數位版權系統裡較弱的數位媒體可攜性。

2.3.1 系統流程

Conrado *et al*'s[9]在 2003 年提出了身份認證式數位版權系統，他整合了 DRM 基本架構中的數位內容伺服器(Content Provider)及許可權管理伺服器(License Provider)，並在

使用端提出以智慧卡(Smart Card)方式進行身份認證，只要將智慧卡(Smart Card)裝置在任何裝置上，即可隨時隨地播放已購買的數位內容。

與裝置式數位版權系統不同的部分[10]分別在使用者購買數位內容及播放這兩個行為上[10]，請參閱下方說明。

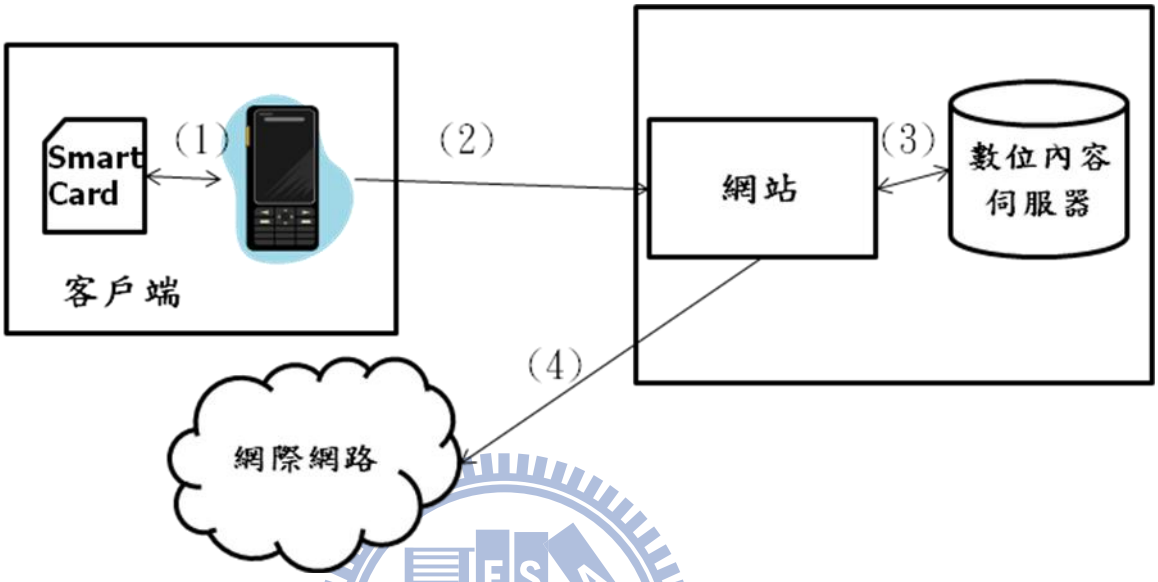


圖4：購買數位內容流程

當使用者透過網站購買數位內容時，身份認證式數位版權管理的流程如下：

1. 智慧卡計算使用者認證資訊

使用者透過智慧卡產生一組亂數(RAN)，並利用存在智慧卡裡的公用金鑰(PK)及產出之亂數(RAN)產生一專供認證此使用者的認證資訊。

2. 向數位內容伺服器(Content Provider)傳送訊息

使用者傳送 SSI(Secret Security Identifier, 通常為電子金融交易上常用的安全認證機制)、欲購買的數位內容資訊及步驟 1 產生的認證資訊給數位內容伺服器。

3. 驗證及產生授權

數位內容伺服器在收到客戶端傳送之資訊後，會先確認 SSI 資訊是否有效。待確認無誤後，數位內容伺服器將產生使用者授權。

4. 透過網際網路發佈使用者授權資訊

數位內容伺服器利用網際網路發佈使用者授權資訊，使使用者可輕易的取得。

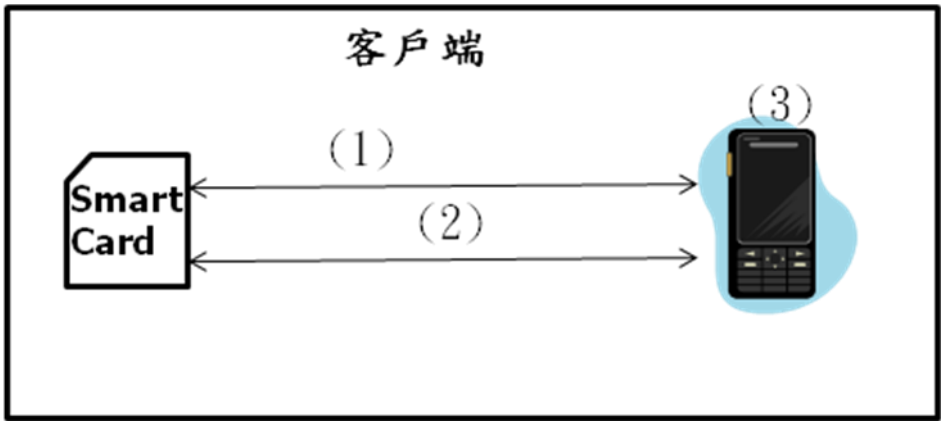


圖5：播放數位內容流程

當使用者想撥放已購買的數位內容時，身份認證式數位版權管理的流程如下：

1. 驗證

透過儲存使用者公用金鑰(PK)及私用金鑰(RK)的智慧卡進行身份驗證，如果使用者通過驗證，則可要求下載播放數位內容，否則將無法要求下載。

2. 要求數位內容

使用者透過撥放裝置傳送欲撥放的數位內容，並等待使用權下載。

3. 檢核使用者授權

如果使用者從未購買此數位內容，撥放裝置將無法取得相關的使用者授權。反之，撥放裝置將檢查使用授權是否與智慧卡在購買此數位內容時產生的認證資訊是否一致，如通過檢核，撥放裝置即可撥放此數位內容。

2.3.2 衍生問題

在身份認證式數位版權管理系統上，數位內容是不會被加密的，數位內容存取驗證及檢核身份認證的動作完全由撥放裝置與智慧卡掌控。當使用者使用非法的撥放裝置撥放時，非法存取將無可避免的，這種方式將危害到數位版權擁有者的權益。

身份認證式數位版權管理系統，僅有數位內容伺服器與使用者等 2 種角色，授權伺服器在此模型中，其功能已與數位內容伺服器合併，通常在眾多數位版權管理系統中，授權伺服器與數位內容伺服器各有其功能。

由於身份認證式數位版權管理系統使用了智慧卡儲存公、私金鑰，使用者若想在不

同撥放裝置上播放數位內容時，必須隨時備妥智慧卡，除了攜帶不便外，若智慧卡不慎遺失，使用者購買的數位內容將完全被不當人士盜用，對使用者來說也沒有任何保障。

2.4 單點登入 (Single Sign On, SSO)

在企業裡，常會有網站服務系統，如：EIP(企業入口網站)、ERP(企業資源規劃平台)、CRM(客戶關係管理平台)、KM(知識管理平台)、PLM(產品生命週期管理系統)等，提供使用者日常作業相關的服務。當網站服務的系統隨著需求不斷增多時，如果每個使用者在每個網站服務系統上都有使用權限，且均有一組帳號密碼，對使用者而言，他必須記憶多組帳號密碼，且在不同網站服務系統作業時，常須要重新進行身份驗證(通常為 username/password)，這樣將造成使用者的困擾與不便。為了簡化多系統的身份驗證問題，因此產生了 Single Sign On 的需求，使用者僅需經過一次身份驗證後，即可自由存取受信任網域內其它主機上的服務系統而不需要再次進行身份驗證的步驟，如此可帶來下列效益：

1. 簡化身份驗證流程：無論訪問幾個網站服務系統，均只須進行一次身份驗證。
2. 易於使用：減少使用者登入時出錯的可能性。
3. 易於管理：不再須要處理和保存多套系統使用者的認證資訊，大幅縮減系統管理者在維護(新增、刪除及修改使用者權限)時間，且可一次直接停用使用者登入所有網站的權限。
4. 增加安全性。

2.4.1 系統架構

單點登入的架構如圖 6[11]所示，大致上分為兩塊，認證域(Authentication domian)及應用服務域(Secondary domain) ，要達成單點登入，應用服務域必須信任認證域以確保：

1. 正確的確認使用者的身份與驗證資格。

2. 保護用來確認欲訪問應用服務域的用戶端身份不會進行未經授權的使用。

其用作流程為：

1. 用戶端想瀏覽或訪問應用服務域中的某一個應用程式。
2. 被訪問的應用程式會先確認用戶端是否已通過身份驗證；若用戶端是首次訪問，則應用程式會要求用戶端先到認證域進行身份登入。
3. 認證域向用戶端要求身份驗證。
4. 認證域確認用戶端通過身份驗證，為合法使用者，並自動轉回應用服務域，用戶端即可開始使用所需的應用程式。

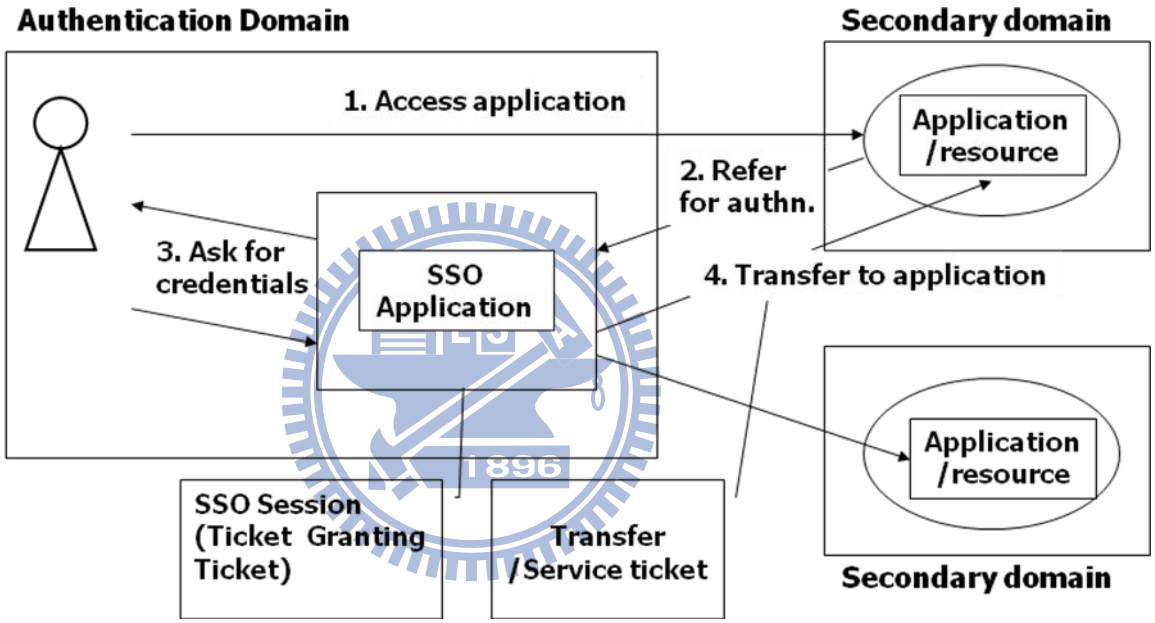


圖6：單點登入示意圖

資料來源：David Orrell, Eduserv Athens Authentication Systems and Single Sign-On (SSO)，EuroCAMP, 7-9 November 2005, Porto, Portugal

2.5 SAML

基於單點登入(SSO)的需求，SAML(Security Assertion Markup Language) 被設計來解決此問題，它允許只有少數經過選擇的團體保留使用者資訊，如果有必要，在經過使

用者確認後，使用者資訊可以被傳送到需要這些資訊的團體。如此，使用者資訊將被信任的團體所保護，使用者也不須每一次訪問被信任的團體時，都必須重新傳遞使用者資訊，徒增資訊外洩的風險。

2.5.1 概述

SAML 是由 OASIS Security Services Technical Committee 提出[12]，一種符合 XML 標準下，用於各安全域(Security Domain)之間，即身份提供者(Identity Provider)和服務提供者(Service Provider)之間，交換認證與授權資訊的 XML 描述。

SAML 版本的沿革如下：

1. 2002年11月，OASIS首次提出SAML 1.0架構。
2. 2003年，SAML1.1成為OASIS的標準。
3. 2005年，SAML 2.0成為OASIS的標準。

其目標為：

1. 提供使用者，實現單點登入(single sign-on)。
2. 通過使用統一的資料交換介面，實現跨安全域的交互操作，便於統一管理分散式應用系統的信任和授權。

SAML 規範定義了 SAML 的組成元件，包含：

1. 宣示 (Assertions)

   定義XML編碼的認證屬性與授權資訊。

2. 協議(Protocols)

   定義封裝宣示的請求與回應協議。

3. 綁定(Bindings)

   定義SAML協議與標準的訊息與通訊協議(如：Http、SOAP)的映射。

4. 配置文件(Profiles)

   定義SAML協議、綁定及宣示如何相互組合支援使用情境。

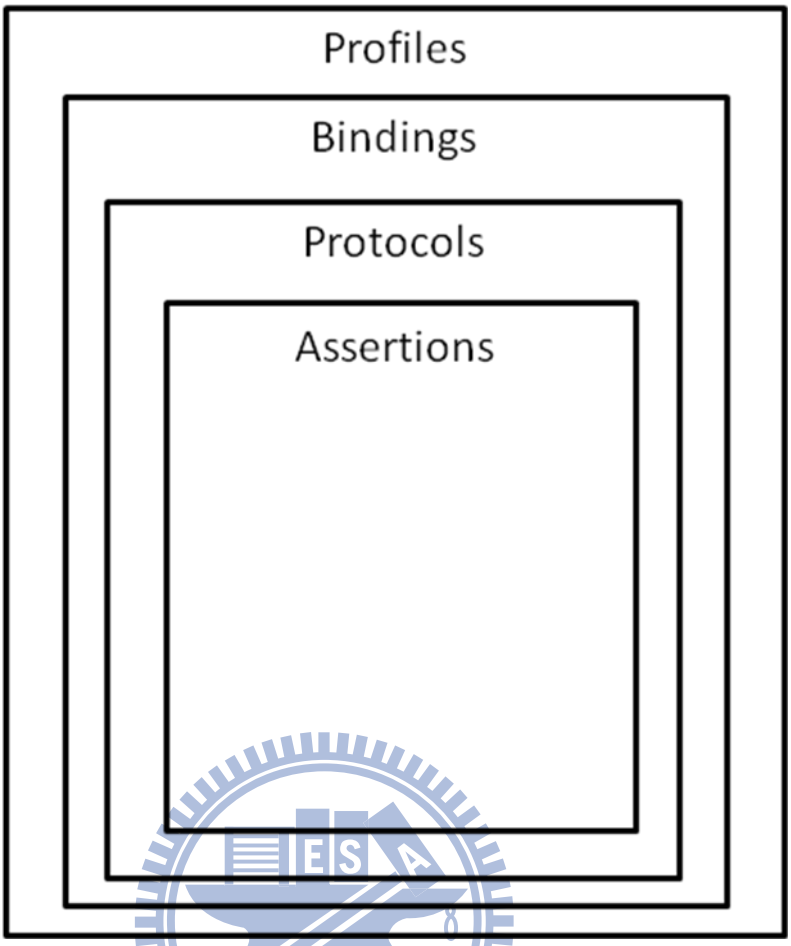


圖7：SAML 組成元件圖

這些認證與授權資訊透過主體(Subject)宣示(Assertion)形式來表達；主體是一個實體(可以是一部電腦、一個人)，在安全域中有一個可供識別的身份，舉個例子來說：在一個公司裡，每個員工的電子郵件地址可以拿來識別其身份。透過宣示各安全域可以傳達多種訊息，包括：

1. 主體所執行的驗證(Authentication Assertion)，以表明使用者是否已經認證。
2. 主體屬性(Attribute Assertion)，表明主體的屬性，如使用者屬於哪個部門。
3. 授權決策(Authorization Decision Assertion)，是否允許主體存取特定資源。

一組宣示組成一個主體的配置檔(Profile)，配置檔中的宣示可以來自不同的組織。宣示是由 SAML 權威（Authority）頒發，身份驗證宣示由身份驗證權威頒發，主體屬性宣示由屬性權威頒發，而授權決策宣示則由策略決策點（Policy Decision Point，PDP）頒發。SAML 還定義了客戶端（Client）請求權威的宣示及權威的應答過程的協議。

2.5.2 SAML 想解決的問題

在單點登入的需求下， SAML 常被拿來解決下列兩個現有網站型應用服務面臨的問題：

1. 大部分的網站型應用服務程式在權限管理資訊的分享上，均各自獨立

   要在既有的網站型應用服務程式間，整合新的資訊安全機制，須要投入大量資源在各系統間，進行程式改寫。

   不同的網站型應用服務程式與生成及使用的安全資訊是緊密結合的。

2. 網站型應用服務程式漸漸須要身份邦聯，以強化使用者服務

   使用者須要更容易在不同應用服務程式中進行交易。

2.5.3 使用情境

SAML 發展出三種使用情境[13]，以解決上述的問題：

1. Single sign-on (SSO)

   Web User須先到Source Web Site進行認證並通過，才能訪問或存取Destination Web Site上受保護的資訊，其use case diagram 如圖7所示

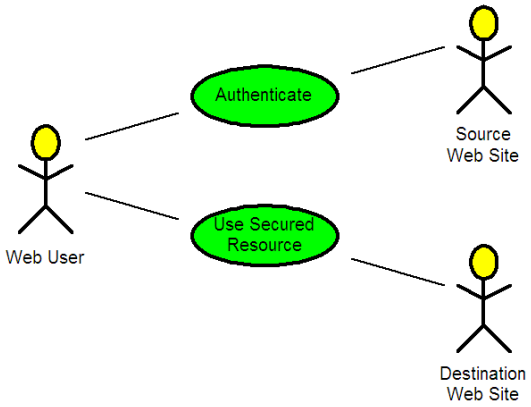


圖8：SAML 單點登入使用情境圖

資料來源： Eve Maler, SAML basics A technical introduction to the Security Assertion Markup Language , XML Technology Center, Sun Microsystems, Inc.

2. Authorization service

   User存取Policy Enforcement Point(PEP,策略實施點)的資源，PEP接著向Policy

Decision Point(PDP,策略決策點)確認User的使用權

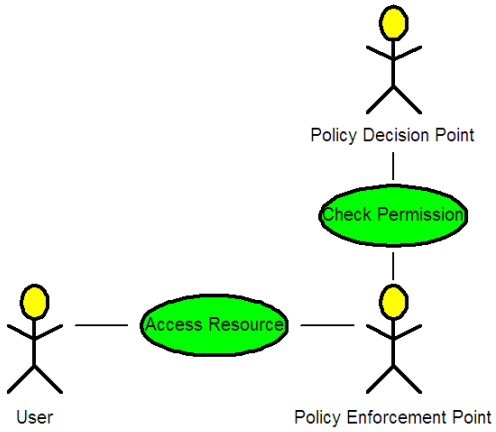


圖9：SAML 授權服務使用情境圖

資料來源： Eve Maler, SAML basics A technical introduction to the Security Assertion Markup Language , XML Technology Center, Sun Microsystems, Inc.

3. Back office transaction

   Buyer向Seller1購買，因Seller1缺貨，Seller1與Seller已互相信任，Buyer可直接轉單至Seller

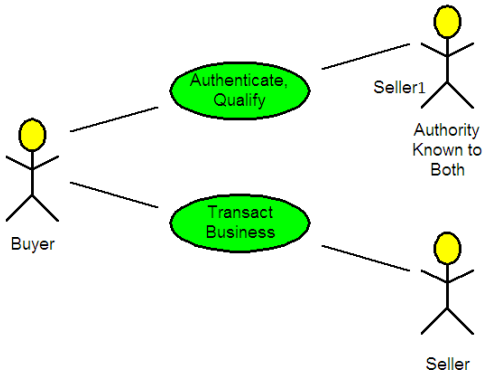


圖10：SAML 後援交易使用情境圖

資料來源： Eve Maler, SAML basics A technical introduction to the Security Assertion Markup Language , XML Technology Center, Sun Microsystems, Inc.

2.5.4 SAML 架構

SAML 架構中，依角色區分為：

1. 身份認證提供者(Identity Provider)：產生宣示、認證及屬性授權及提供單點登入服務。

2. 服務提供者(Service Provider)：消費宣示及提供服務。

3. 使用者(Client) ：向服務提供者要求受保護服務，並向身份認證提供者驗證身份。

其架構圖及流程如下：

1. 使用者向服務提供者要求服務。
2. 服務提供者回應使用者須先至身份驗證提供者進行身份驗證。
3. 使用者至身份驗證提供者進行身份驗證。
4. 身份驗證提供者回應使用者帶有宣示的資訊。
5. 使用者將宣示的認證資料提供給服務提供者。
6. 服務提供者向身份驗證提供者要求宣示。
7. 身份驗證提供者提供服務提供者宣示。
8. 服務提供者告知使用者已通過驗證。
9. 使用者再次向服務提供者提出要求。
10. 服務提供者提供使用者要求之服務。

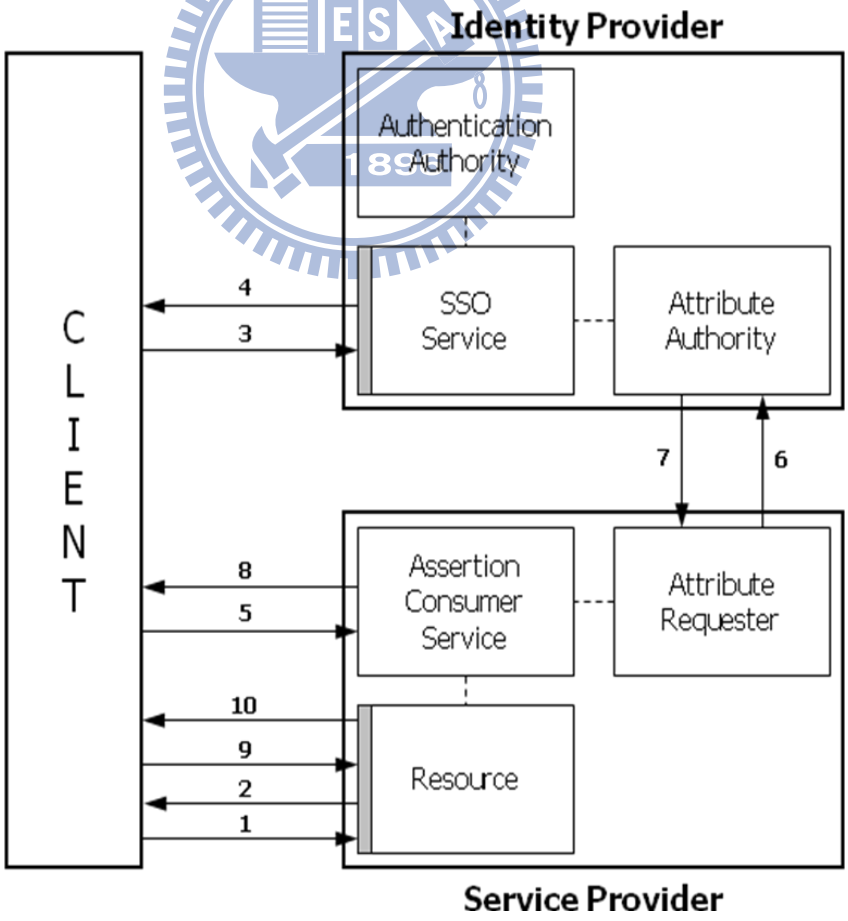


圖11：SAML 架構圖

資料來源： Tom Scavo, Security Assertion Markup Language A Brief Introduction to SAML, NCSA,

2.5.5 SAML 在使用上的案例

接著我們以一個 SAML 在使用上的案例(請參閱圖 12)，說明 SAML 架構下的單點登入：

1. 使用者向來源網站(Web Server 1)驗證，並請求鏈接到目標網站(Web Server 2)受保護的資源。
2. 來源網站使用驗證標誌(artifact)，並重新導向至目標網站，使用者使用該標誌向目標網站請求讀取受保護的資源。
3. 目標網站請求來源網站使用該標誌進行SAML驗證宣示(assertion)，來源網站根據標誌向目標網站提供SAML驗證宣示。
4. 目標網站向使用者提供受保護的資源。

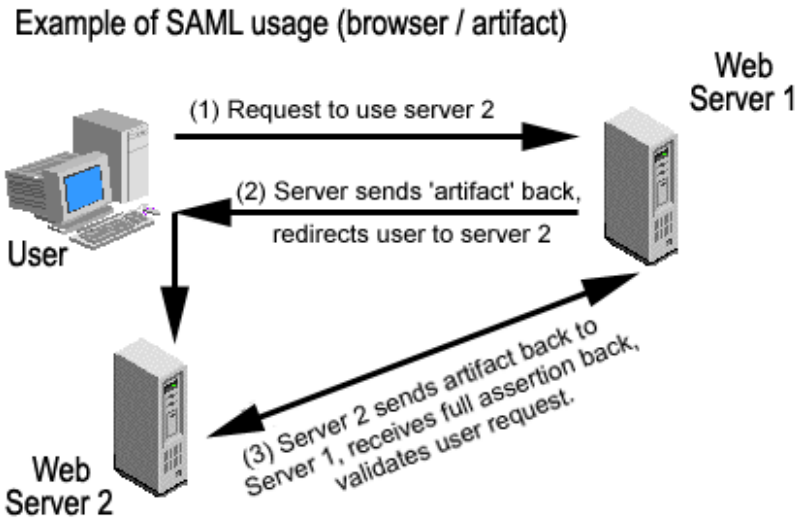


圖12：SAML 的使用案例

資料來源： SAML，http://www.csie.fju.edu.tw/~ie955148/indexXML.html

三、 SAML-based DRM

綜合第二章的文獻探討，我們可歸納出數位版權管理系統具有的特性：

1. 須憑證且憑證取得不易

當使用者要開啟具 DRM 保護的加密數位內容時，須連線到授權伺服器(License Server)發送數位憑證簽章，取得合法使用授權。

2. 認證繁瑣

一個使用者對於一份數位內容(Content)均有一個專用的使用授權(License)；使用授權是依照數位內容(Content)、電腦及使用者而異，如前述之任何一項改變了，就必須重新連線授權伺服器(License Server)取得授權，造成使用者在頻繁使用一個或多個數位內容時，必須隨時與授權伺服器進行取得授權的行為。

3. 高價值交易

DRM 原來設計是用來保護企業內部高價值的數位內容或保護數位內容擁有者權益，並非設計用來保護電子報、試閱性電子小說、電子雜誌等這類小額且頻繁交易之數位內容。

同時，我們也發現，在申請憑證或註冊各家數位版權管理系統時，須填具個人隱私資料(圖 13 以 iTunes 為例)，如：信用卡持有人電話、住址、卡號、授權碼、身份證等，對小額且頻繁交易市場的消費者而言，若只是試閱幾個章節的電子小說、買一份電子報或電子雜誌，不需要也不願意將個人隱私[17]暴露於低安全性的網際網路上。當消費者在多個數位版權管理系統中挑選數位內容時，如：在時代雜誌網站中挑選某一期電子雜誌或在 iTunes 網站中購買幾首最新發表的 mp3 等，由於各家數位版權管理系統均有自己獨特的授權伺服器，並無一開放標準，使用者必須保存多組對應不同消費需求的憑證與授權帳密。

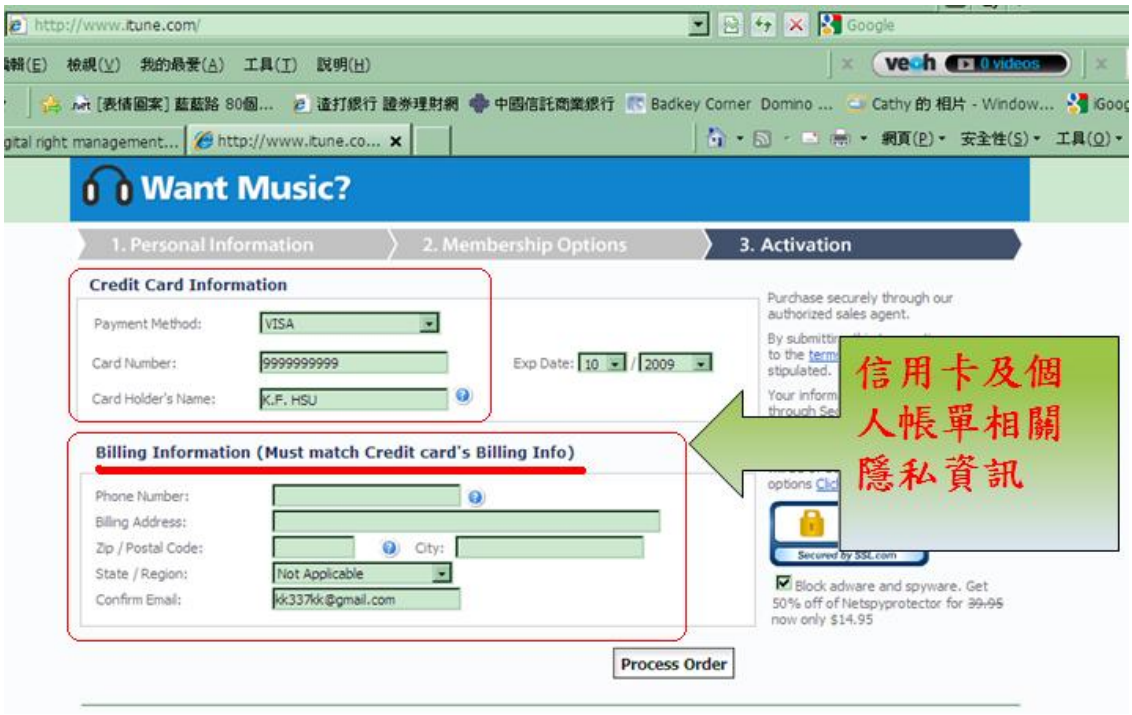


圖13：iTunes 註冊及購買流程

資料來源 http://www.itune.com

本章將提出一個基於數位版權管理系統架構且更能適用於小額頻繁交易市場的數位版權管理模型。

3.1 悠遊卡機制

悠遊卡[15]（英語譯名：EasyCard）是由悠遊卡股份有限公司發行，通用於大台北地區、宜蘭縣、連江縣和部份臺灣北部及中部地區國道客運的非接觸式電子票證系統智慧卡，可於交通用途或用於全國陸續增加的小額消費商店中使用。現實生活裡，消費者可經由很輕鬆、簡便的方式，申購悠遊卡，即可使用悠遊卡進行各種食、衣、住、行…等生活必需消費或娛樂，當大家在使用悠遊卡時，不須經過嚴密的身份認證，僅須出示悠遊卡，將悠遊卡輕觸扣款器的感應區，當交易完成時，費用將自動從卡片中扣除，交易時間不到一秒。即可完成交易。

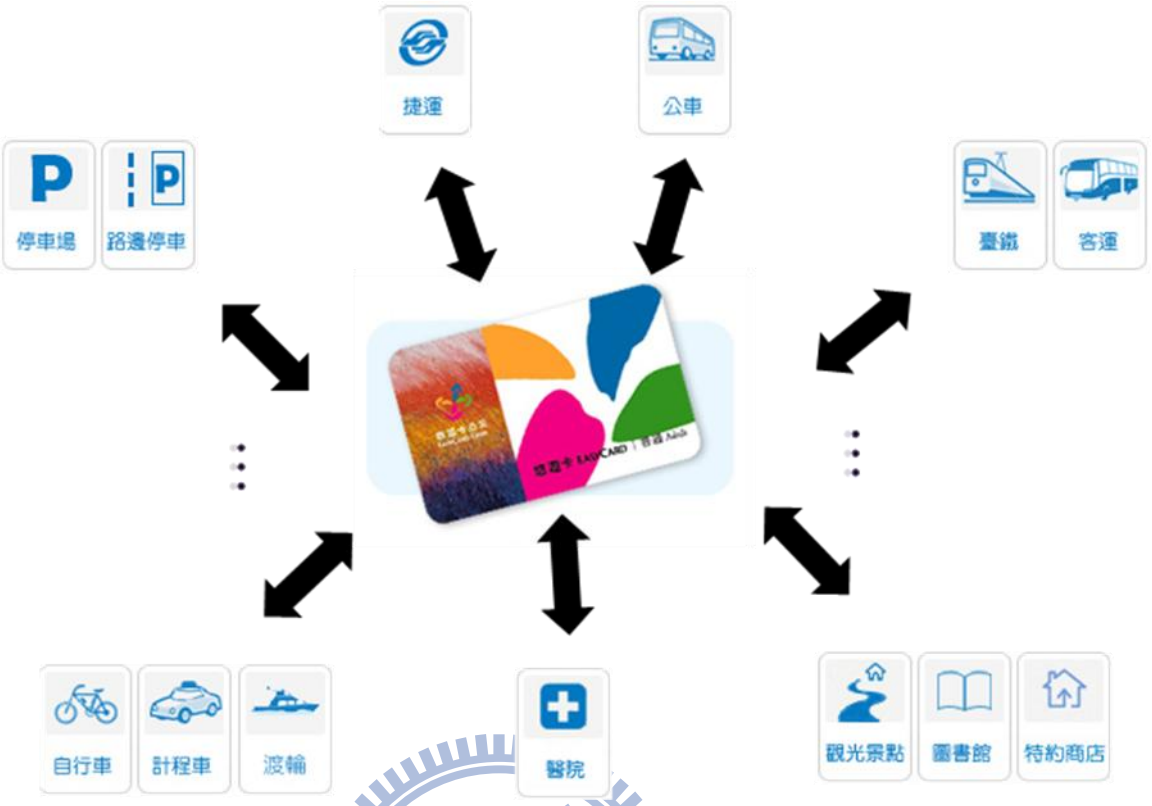


圖14：悠遊卡的世界

資料來源:http://www.easycard.com.tw/ ，悠遊卡公司

本研究發現悠遊卡的特性，包括：

1. 匿名

消費者在購買悠遊卡時，不需要提供個人隱私資料，只需要支付固定金額即可取得悠遊卡，當悠遊卡金額用完後，只需要再至儲值中心(悠遊卡客服中心 、便利商店、各交通車站 、捷運各車站服務處及自動售票機…)進行儲值即可持續使用。

2. 認證簡單

只需輕觸感應區，即可迅速完成交易，免除準備零錢、重複購票等困擾，並可不斷加值，一卡使用多年。

3. 適用於小額消費(頻繁交易)且適用不同商家

悠遊卡推行的主要用意即在交通與小額消費市場領域(悠遊卡小額消費特約商店，已超過一萬家)。

這些特性剛好與數位版權管理系統在小額頻繁交易市場上遇到的阻礙相反。

3.2 SAML-based DRM 運作原理

圖15為傳統DRM的運作模式[14]，其步驟如下：

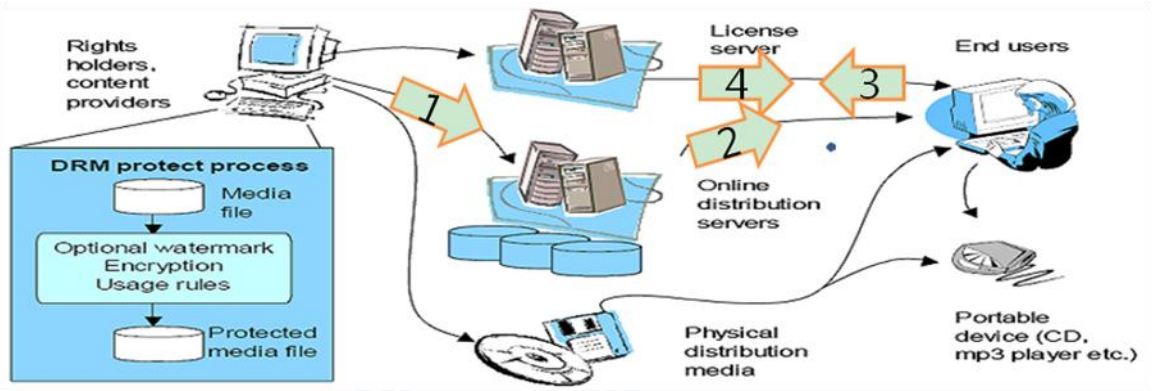


圖14：傳統DRM運作模式

1. 數位內容提供者(Rights holders,content providers)先將數位內容加密打包後，在線上發佈主機(Online distribution servers)發佈。
2. 消費者(End users)向線上發佈主機要求下載受保護的數位內容。
3. 消費者在播放時，向許可權管理中心(Licesnse server)要求使用權。
4. 消費者獲取使用權，並撥放受保護的數位內容。

由於單點登入(SSO)機制的效益(簡化身份驗證流程、易於使用、易於管理、增加安全性等)，若藉由導入悠遊卡及單點登入機制的好處與數位版權管理系統結合，將可解決數位版權管理系統在小金額頻繁交易市場上遇到的阻礙，因此本研究提出了 SAML-based DRM 的構想，藉由悠遊卡及單點登入(SSO)的概念，本研究試著在 User 與 License server 間，加上一個身份認證伺服器(Identity Provider, IDP)，消費者在向 IDP 購買一定點數之使用授權後，利用 IDP 進行單點登入，由 IDP 與消費者進行身份驗證(消費者只需要輸入一特定的帳號及密碼)，簡化使用者的身份驗證與授權工作，當消費者完成身份驗證後，即可取用應用服務伺服器上已購買擁有使用授權的數位內容。其運作機制如圖 16：

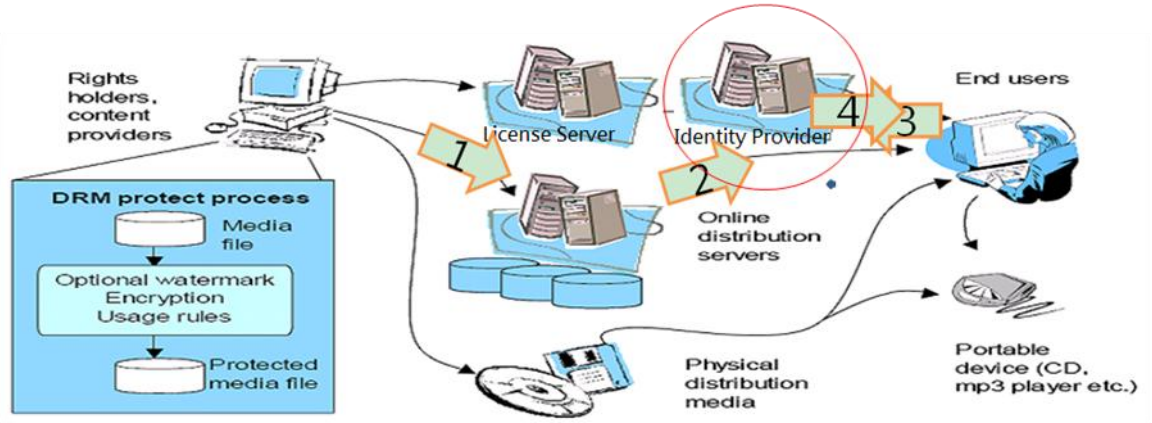


圖16：SAML-based DRM運作模式

1. 數位內容提供者(Rights holders,content providers)先將數位內容加密打包後，在線上發佈主機(Online distribution servers)發佈。
2. 消費者(End users)向線上發佈主機要求下載受保護的數位內容。
3. 消費者在播放時，向身份認證伺服器，進行認證與受權。
4. 消費者獲取使用權，並撥放受保護的數位內容。

3.3 SAML-based DRM 特色

SAML-based DRM 的特色包含了：

1. 簡化流程：

類似 iCash、悠遊卡甚至是 Online Game 點數卡方式，簡化使用端消費在進行身分認證的程序(以使用者而言，在消費時，只須使用一組帳密登入 IDP 一次即可)。

應用 OASIS Security Services Technical Committee 提出之 SAML 規範，建立標準並簡化 DRM 系統上繁瑣的憑證取得與驗證及使用授權取得流程。

一個使用授權可取得多個數位化內容，使用者存取多個數位化內容時，不需重覆跟許可權管理中心(Right Issuer)取得授權(傳統數位版權管理系統，每取得每個數位化內容，皆必須經由一個完整憑證驗證及取得流程)。

DRM 系統應用在頻繁交易與短期租賃上，最繁瑣的部分莫過於每進行一個數位內容的存取，便需要對授權伺服器進行一次以上的 License 資訊交換與驗證，以

確保數位內容的安全性，本系統透過 SAML 單點登入的機制，簡化了存取第二個數位內容以後的 License 驗證動作(如圖 17 所示)，以達到簡化流程的目的。

2. 隱私保護(間接命名機制進行交易)：

以代號取代消費者資訊，以代號點數使用記錄取待消費者購買記錄，保護消費者。

3.4 系統架構

圖 17 為本研究所提出的架構圖，依角色可分為用戶端(Client)、身份認證伺服器(Identity Provider)及數位版權管理系統(在本研究提出的架構中，數位版權管理系統，被視為提供服務的 Service Provider，它包含了 Content Server 及 License Server)。

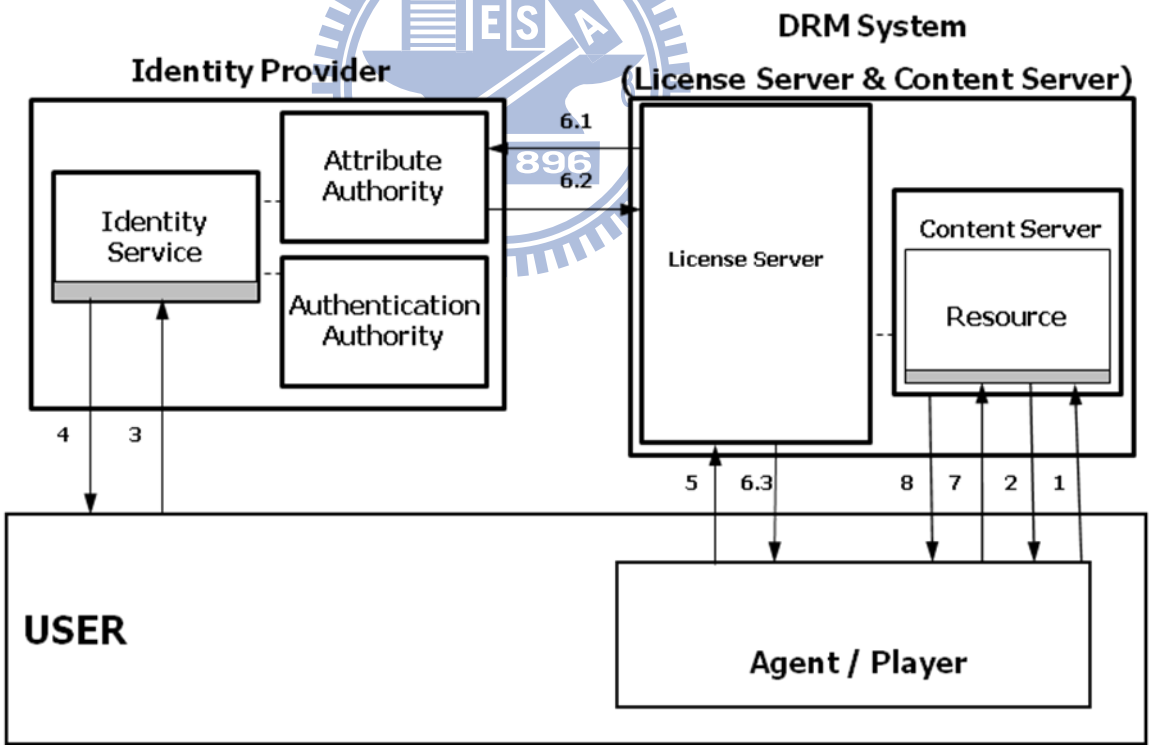


圖17：SAML-based DRM架構

本架構的循序圖如圖 18，其流程如下：

1. 使用端向 Content Server 要求播放受保護的 Content。
2. Content Server 要求使用端進行身份認證。

3. 使用端至 Identity Provider 登入。
4. 帶有 Assertion 的資訊回傳給使用端。
5. 使用端將帶有Assertion的認證資料提供給 License Service。
6. Content Service 向 Identity Provider 進行使用者身份驗證，並回傳是否已通過驗證。
7. 使用端再次向 Content Server 要求 播放Content。
8. Content Service 將已驗證解密的 Content 回傳給使用端。

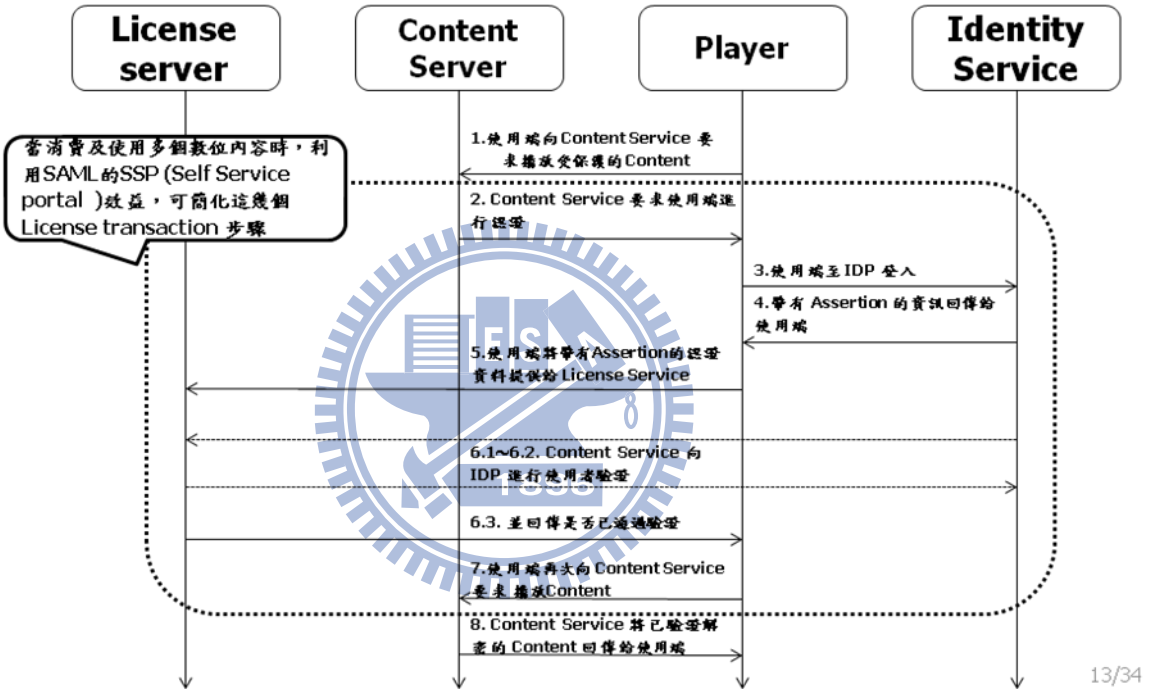


圖18：SAML-based DRM 循序圖

3.5 系統原理

由於本研究中的數位版權管理系統為我們為了驗證 SAML-based DRM 架構的可行性與實用性，而自製的一僅透過帳密及簡單之數位內容保護的系統，當 SAML-based DRM 架構在與業界或學術界現有的數位版權管理系統結合時，數位版權管理系統中的授權伺服器(License Server)必須依據 SAML 的規範修改，以接收來自 SAML-based DRM

架構中身份認證伺服器帶有使用者認證資訊的 XML 文件，並針對此 XML 文件進行解譯，才可從現有的數位版權管理系統架構轉換為 SAML-based DRM 架構。

本研究的目的在簡化傳統 DRM 系統上，進行短期租任及頻繁交易產生繁瑣的 License 認證問題，因此在 SAML-based DRM 架構下，我們將原本 DRM 系統上身份驗證的工作移轉至身份驗證伺服器(License Provider)，我們將利用 SAML 規範的宣示(Authentication Assertion、Attribute Assertion、Authorization Decision Assertion)儲存與傳遞驗證資訊並透過 SOAP 與數位版權管理系統進行溝通。

3.5.1 宣示(SAML Assertion)

以一個被作者(issuer)R 定義某個主體(Subject)S 在某個時間點(Time)T 及某個條件(Condition)C 下可以對系統進行使用的宣示(Assertion)A 為例：

我們利用驗證宣示(Authentication Assertion) 告知數位版權管理系統，某個主體或使用者(Subject，本例中為 9679531)在某個時間點(Time，本例中為 2010-07-03~2011-07-03)T 內能透過某種身份驗證方式(Method，本例中為 password)M 通過驗證，其宣示如下：

```
<saml:Assertion
  MajorVersion="1" MinorVersion="0"
  AssertionID="128.9.167.32.12345678"
  Issuer="NCTU SELab"
  IssueInstant="2010-07-03T10:02:00Z">
  <saml:Conditions
    NotBefore="2010-07-03T12:00:00Z"
    NotAfter="2011-07-03T12:00:00Z" />
  <saml:AuthenticationStatement
    AuthenticationMethod="password"
    AuthenticationInstant="2001-12-03T10:02:00Z">
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="estore.nctu.edu.tw"
        Name="9679531" />
    </saml:Subject>
  </saml:AuthenticationStatement>
</saml:Assertion>
```

其中，<saml:AuthenticationStatement>…</saml:AuthenticationStatement>即是身份驗證宣示。

另外由於主體或使用者有某些特性或屬性，我們可利用 SAML 規範的主體屬性宣示(Attribute Assertion)達到將此資訊傳遞給數位版權管理系統的目的，比方說，我們必須告知數位版權管理系統上例主體(9679531)對系統的角色是系統管理員，其宣示如下：

```
<saml:Assertion …>
  <saml:Conditions …/>
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="estore.nctu.edu.tw"
        Name= "9679531" />
    </saml:Subject>
    <saml:Attribute
      AttributeName="Role"
      AttributeNamespace="http://nctu.edu.tw">
      <saml:AttributeValue>
        Admin
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

<saml:Attribute>…</saml:Attribute>即是屬性宣示。

當主體或使用者通過身份驗證後，最終目的是賦予主體或使用者適當的權限，我們將透過 SAML 規範的認證決策宣示(Authorization Decision Assertion)，告知數位版權管理系統，某主體或使用者是否有權使用此數位內容，其宣示如下：

```
<saml:Assertion …>
  <saml:Conditions …/>
  <saml:AuthorizationStatement
    Decision="Permit"
    Resource="http://estore.nctu.edu.tw/UserCart.aspx">
   <saml:Actions Namespace ="nctu.edu.tw" >
      <saml:Action>Execute</saml:Action>
   </saml:Actions>
```

```
    <saml:Subject>
        <saml:NameIdentifier
            SecurityDomain="nctu.edu.tw"
            Name="9679531" />
      </saml:Subject>
  </saml:AuthorizationStatement>
</saml:Assertion>
```

宣示中，指出主體(Subject)9679531 在通過身份驗證(Authentication Assertion)後，可(Permit)針對資源(Resource) http://estore.nctu.edu.tw/UserCart.aspx，進行執行(Execute)的動作。

3.5.2 運作模型

上一節我們說明了一些以 XML 文件描述的宣示(Assertion)後，接下來我們利用下圖說明整個運作模型：

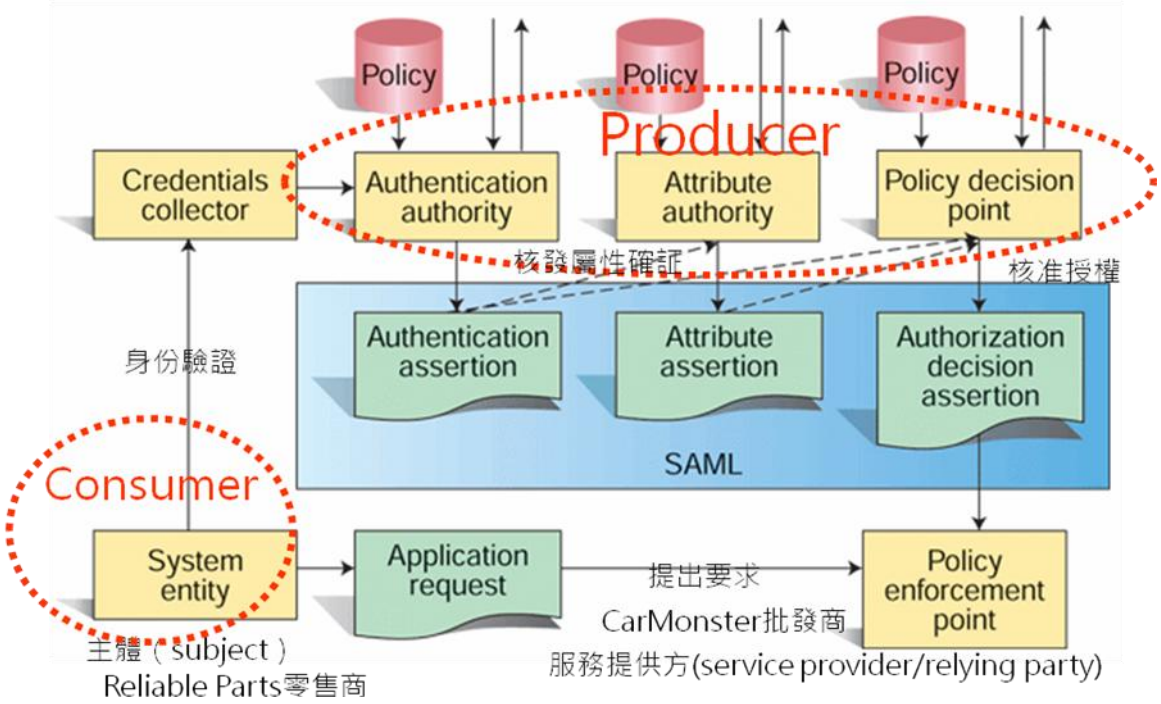


圖19：SAML-based DRM 運作模型圖

資料來源： Eve Maler, SAML basics A technical introduction to the Security Assertion Markup Language , XML Technology Center, Sun Microsystems, Inc.

1. 整個系統的運作，均從Consumer主體(Subject)想要對CarMonstor(Service

Provider)進行某項動作提出要求開始。

2. 在Consumer主體向CarMonstor提出要求後，系統會要求Consumer進行身份驗證。
3. 當局(authorities)產生宣示(Assertion)，系統提供三種不同的當局，以因應三種不同的宣示；Authentication authority產生Authentication Assertion，Attribute authority產生Attribute assertion，Policy decision point或稱為PDP則產生Authorization decision assertion。
4. 這些當局除了產生宣示外，也會接收外部的資料，這些資料將被儲存在一個政策資料庫中(Policy store)，舉例來說，PDP有可能要去政策資料庫中查詢，今天9679531這個使用者，是否仍被授權觀看某份數位資料。

3.5.3 資料交換協定

對儲存身份認證及授權資訊的宣示(Assertion)有了明確定義之後，接著我們繼續說明身份認證伺服器與數位版權管理系統間的資料交換協定，我們使用在網路上廣泛使用的 http request /response 協定來傳輸宣示(Assertion)及相關資訊，如下圖：

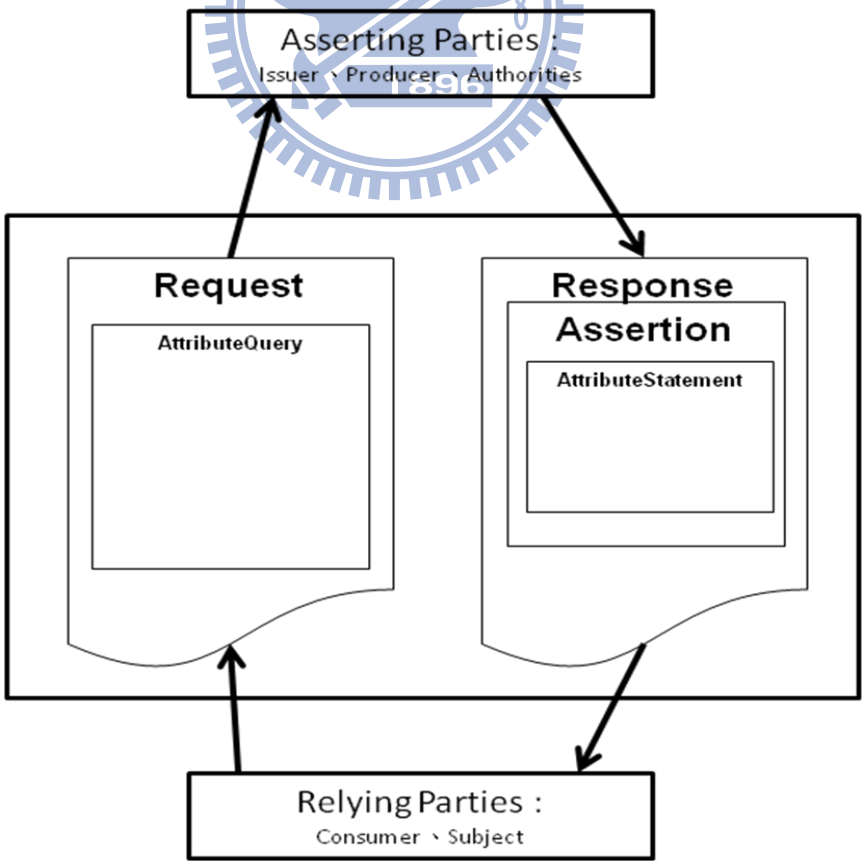


圖20：SAML-based DRM 資料交換協定

1. Consumer或Subject透過數位版權管理系統產生HTTP Request(我們提供了Authentication Assertion request、Attribute Assertion request、Authorization Decision Assertion request等3種查詢)

(1) 請身份認證伺服器確認這個Subject或Consumer是否有相關資訊在系統中，如果有請提供這個Subject或Consumer的身份認證資訊)，Request片段如下：

```
<samlp:Request
 MajorVersion="1" MinorVersion="0"
  RequestID="128.14.234.20.12345678" >
  <samlp:AuthenticationQuery>
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="nctu.edu.tw"
        Name="9679531" />
    </saml:Subject>
  </samlp:AuthenticationQuery>
</samlp:Request>
```

(2) 請身份認證伺服器確認這個Subject或Consumer是否有相關資訊在系統中，如果有請提供這個Subject或Consumer的屬性資訊)，Request片段如下：

```
<samlp:Request … >
  <samlp:AttributeQuery
    CompletenessSpecifier="Partial">
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="smithco.com"
        Name="9679531" />
    </saml:Subject>
    <saml:AttributeDesignator
      AttributeName="Role"
      AttributeNamespace="http://nctu.edu.tw">
    </saml:AttributeDesignator>
  </samlp:AttributeQuery>
</samlp:Request>
```

(3) 請身份認證伺服器確認這個Subject或Consumer是否有相關資訊在系統中，如果有請提供這個Subject或Consumer針對某項資源是否有權限存取的資訊)，Request片段如下：

```
<samlp:Request …>
```

```
    <samlp:AuthorizationQuery
      Resource="http://estore.nctu.edu.tw/UserCart.aspx">
      <saml:Subject>
        <saml:NameIdentifier
          SecurityDomain="nctu.edu.tw"
          Name="9679531" />
      </saml:Subject>
      <saml:Actions Namespace="http://…">
        <saml:Action>Read</saml:Action>
      </saml:Actions>
      <saml:Evidence>
        <saml:Assertion>
          …some assertion…
        </saml:Assertion>
      </saml:Evidence>
    </samlp:AuthorizationQuery>
</samlp:Request>
```

2. 由身份認證伺服器回應此Request，Response片段如下：

```
<samlp:Response
  MajorVersion="1" MinorVersion="0"
    RequestID="128.14.234.20.90123456"
    InResponseTo="128.14.234.20.12345678"
    StatusCode="Success">
    <saml:Assertion
      MajorVersion="1" MinorVersion="0"
      AssertionID="128.9.167.32.12345678"
      Issuer="NCTU SELab">
      <saml:Conditions
        NotBefore="2010-07-03T10:00:00Z"
        NotAfter="2010-07-03T10:05:00Z" />
      <saml:AuthenticationStatement …>
      </saml:AuthenticationStatement>
    </saml:Assertion>
</samlp:Request>
```

3.5.4 資料綁定

SOAP 是為了簡化網頁伺服器（Web Server）在從 XML 資料庫中提取資料時，無需

花時間去格式化頁面，並能夠讓不同應用程式之間透過 HTTP 通訊協定，以 XML 格式互相交換彼此的資料，使其與程式語言、平台和硬體無關。

因此我們使用了 SOAP 的方式傳小節 3.5.3 定義之 Request 及 Response。下方分別為 Request 及 Response 經過綁定後的片段：

SOAP Binding Authentication Request：
POST /SamlService HTTP/1.1 Host: estore.nctu.edu.tw
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security
<SOAP-ENV:Envelope
xmlns:SOAP-ENV=”http://schemas.xmlsoap.org/soap/envelope/”>
<SOAP-ENV:Body>
<samlp:Request xmlns:samlp:=”…” xmlns:saml=”…” xmlns:ds=”…”>
<ds:Signature> … </ds:Signature>
<samlp:AuthenticationQuery>
…
</samlp:AuthenticationQuery>
</samlp:Request>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
SOAP Binding Authentication Response：
HTTP/1.1 200 OK Content-Type: text/xml
Content-Length: nnnn
<SOAP-ENV:Envelope
xmlns:SOAP-ENV=“http://schemas.xmlsoap.org/soap/envelope/”>
<SOAP-ENV:Body>
<samlp:Response xmlns:samlp=”…” xmlns:saml=”…” xmlns:ds=”…”>
<Status>
<StatusCodevalue=”samlp:Success”/>
</Status>
<ds:Signature> … </ds:Signature>
<saml:Assertion>
<saml:AuthenticationStatement>
...
</saml:AuthenticationStatement>
</saml:Assertion>
</samlp:Response>

</SOAP-Env:Body>
</SOAP-ENV:Envelope>

四、 系統實作與成果

本章節將分別以兩個情境(短期租賃、頻繁交易)展示系統實作之成果。

4.1 系統環境

本系統因屬雛形展示，我們將使用個人電腦實作，並將身分驗證伺服器(Service Provider)、數位內容伺服器(Content Provider)即 DRM 系統於同一部機器上。

以下為實作 SAML-based DRM 系統的硬體環境：

CPU：Intel Core Duo 1.66 Ghz

記憶體：3072 MB

作業系統：Windows XP

軟體及資料庫部分，我們使用 Windows 的網站伺服器 IIS，為系統平台，網頁部分，我們使用 Microsoft 的 asp.net 進行撰寫，並使用 Oracle 的資料庫系統儲存數位內容及使用者的訂閱與購買資訊。軟體相關版本詳述如下：

網站服務器 : Microsoft IIS 5.1

身份認證伺服器 : 使用 Simple SAML 實作

數位內容伺服器 : 製作一具簡單功能的 DRM 系統

資料庫 : Oracle 9i

開發環境 : 微軟 Visual Studio 2008, VB.net

4.2 情境展示-短期租賃

虛擬商店中有一些借閱性質(有時效性，通常為數天)的新出版電子小說或電子雜誌，消費者發現後想直接借閱

步驟:

進入虛擬商店 (如使用者是第一次登入，系統會要求使用者先登入 Identity Server)

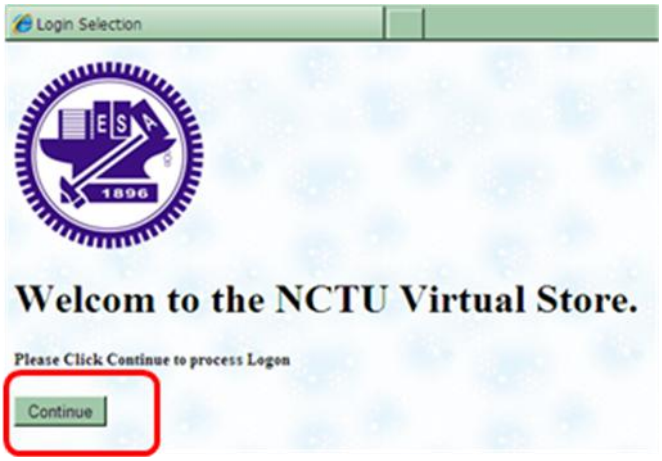


圖21：虛擬商店登入畫面

虛擬商店要求先至 Identity Server 登入，進行身份驗證

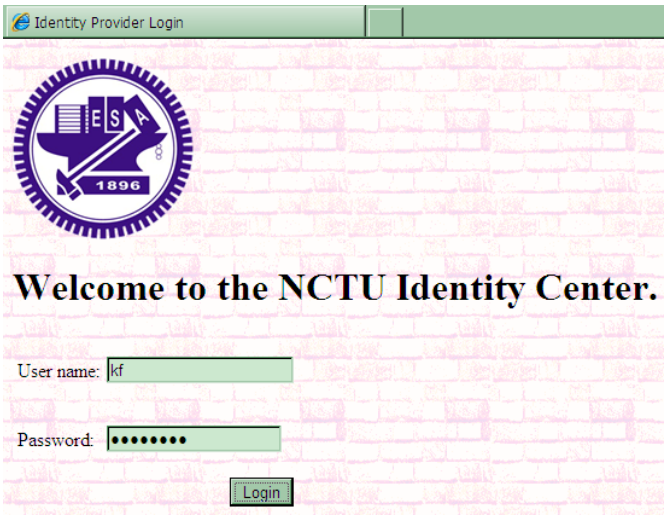


圖22：身份認證伺服器登入畫面

經過身份驗證後，登入虛擬商店後，消費者可直接查看到自己購買過的數位內容、剩餘點數資料(本例剩餘為 19635 點)及新上架之數位內容(本例中無已購買過的數位內容)，並可直接利用剩餘點數購買或借閱有興趣的電子雜誌

圖23：數位版權管理系統使用者主畫面

消費者選取想購買或租賃的數位內容(購買租期只有 5 天的旅遊雜誌)，在選取該雜誌後按下 Purchase 購買

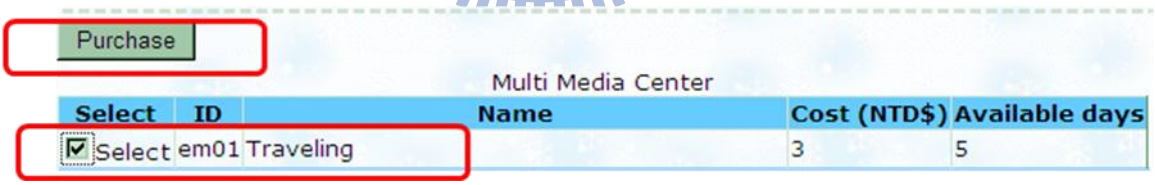


圖22：購買數位內容畫面

系統自動扣除點數(扣除 3 點)，並將消費者選購之內容提供給消費者閱讀

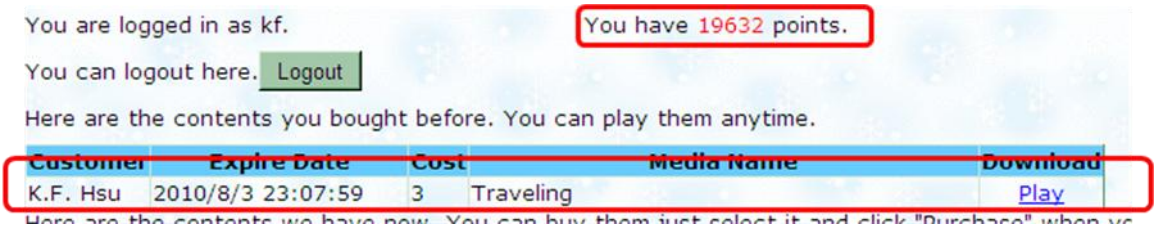


圖24：使用者已購買的數位內容清單畫面

在有效期限內(2010/8/3)，消費者將可隨時閱讀此電子雜誌，消費者可直接點選

Play 播放

圖25：使用者點選Play進行數位內容播放

4.3 情境展示-頻繁交易

虛擬商店中有當日各種類型的電子報紙(財經、生活、政治)，消費者想一次購買多種及多份電子報

步驟:

進入虛擬商店 (如果使用者是第一次登入，系統會要求使用者先登入 Identity Server)

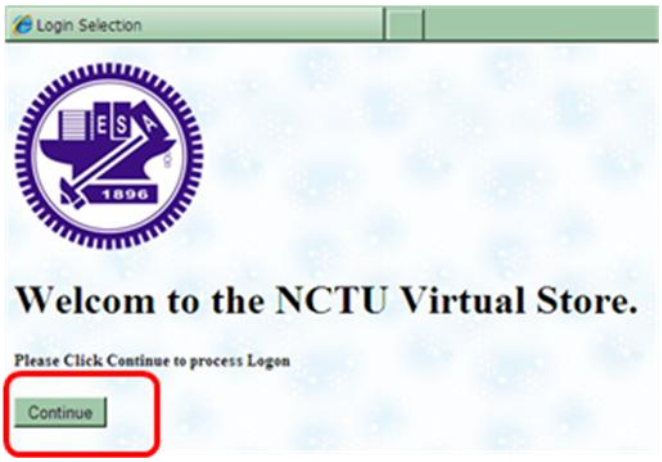


圖26：虛擬商店登入畫面

虛擬商店要求先至 Identity Server 登入，進行身份驗證

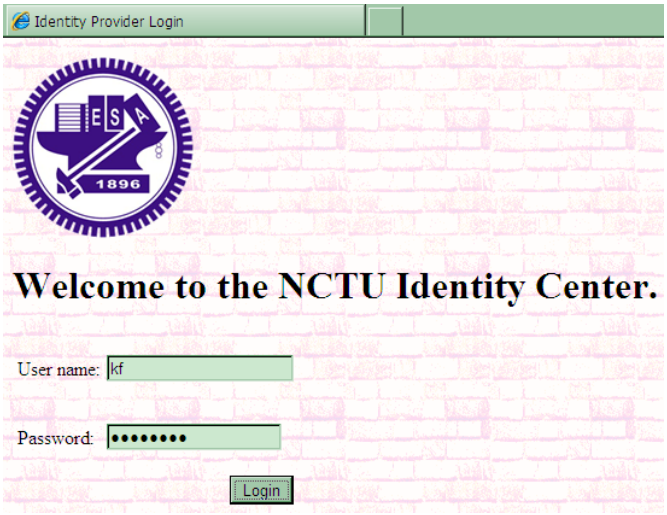


圖27：身份認證伺服器登入畫面

登入虛擬商店後，消費者可直接利用點數購買第一份電子報，消費者在看完第一份電子報後，馬上想購買第二份不同的電子報(這個動作如果是頻繁發生，消費者在每一次觀看時，即必須與 DRM 系統進行認證與授權)

圖28：數位版權管理系統使用者主畫面

消費者選取想購買的其它電子報，挑選後按下 Purchase 購買

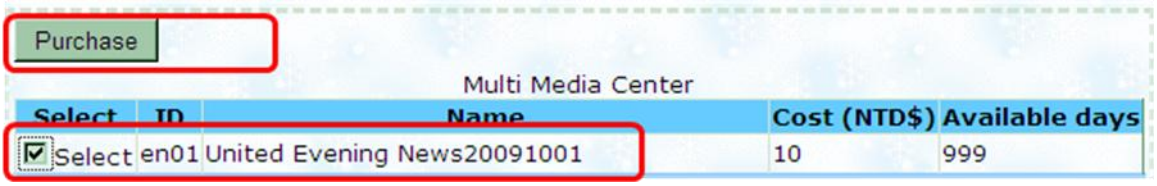


圖29：購買數位內容畫面

系統自動扣除點數(本例中為 10 點)，並將消費者選購之內容提供給消費者

圖30：使用者已購買的數位內容清單畫面

在有效期限內(2013/4/23)，消費者將可隨時閱讀此電子小說，消費者可直接點選 Play 播放

圖31：使用者點選Play進行數位內容播放

五、 結論

5.1 總結

在本論文的開始及第二章，我們探討了目前的 DRM 系統應用在小金額頻繁交易的市場上所遭遇的問題，並在第二章介紹了 DRM 的基本架構，並深入說明此問題，介紹了目前在企業中廣為使用的單點登入機制。藉由這些研究，我們得以提出一個應用在小金額頻繁交易模式的 DRM 架構。

接著，我們探討了悠遊卡普及的原因，並將其與單點登入機制應用於 DRM 系統上，我們也提出了 SAML-based DRM 架構，並於系統實作時設計出一個 SAML-based DRM 的雛型。

隨著著作權及個人隱私權的抬頭，DRM 系統仍擁有絕大的商機與市場，但如果在小金額頻繁交易上使用目前的 DRM 架構，對消費者而言，在購買階段，必須先將個人隱私資料提供給電子商務廠商，接著在進行撥放數位內容時，如每天觀看 2 份以上的電子日報，消費者必須進行繁瑣的憑證取得與認證程序，這些行為與位數位化之前的消費行為相比，將對消費者的消費行為造成巨大的衝擊。「科技來自於人性」，這句廣告詞點出了科技的發展與推廣必須由人性出發，本論文以簡便且保護消費者隱私的角度，提出了一個類似悠遊卡消費與單點登入機制的 DRM 系統，期使 DRM 系統在小金額消費市場上能更具彈性與合理性，進而更加普及。

單點登入機制的最大優點在於其可跨越多個應用服務系統，只要身份認證伺服器與其他應用服務系統互相信任即可，我們選擇 SAML 的原因也在於 SAML 是一種規範，只要所有的應用服務系統與身份認證系統進行身份確認之間的資料交換，符合 SAML 的規範即可，在未來的發展上，我們也將繼續提出 Advanced SAML-based DRM 系統架構，如圖 32 所示，藉由 SAML 用來解決單點登入問題的特性，達到只要完成單一身份認證，卻能在各家的 DRM 系統(如圖 32 中 DRM System A 及 DRM System B)消費，就

如實體世界的 VISA 卡一樣，成為虛擬商店中的 VISA 卡。

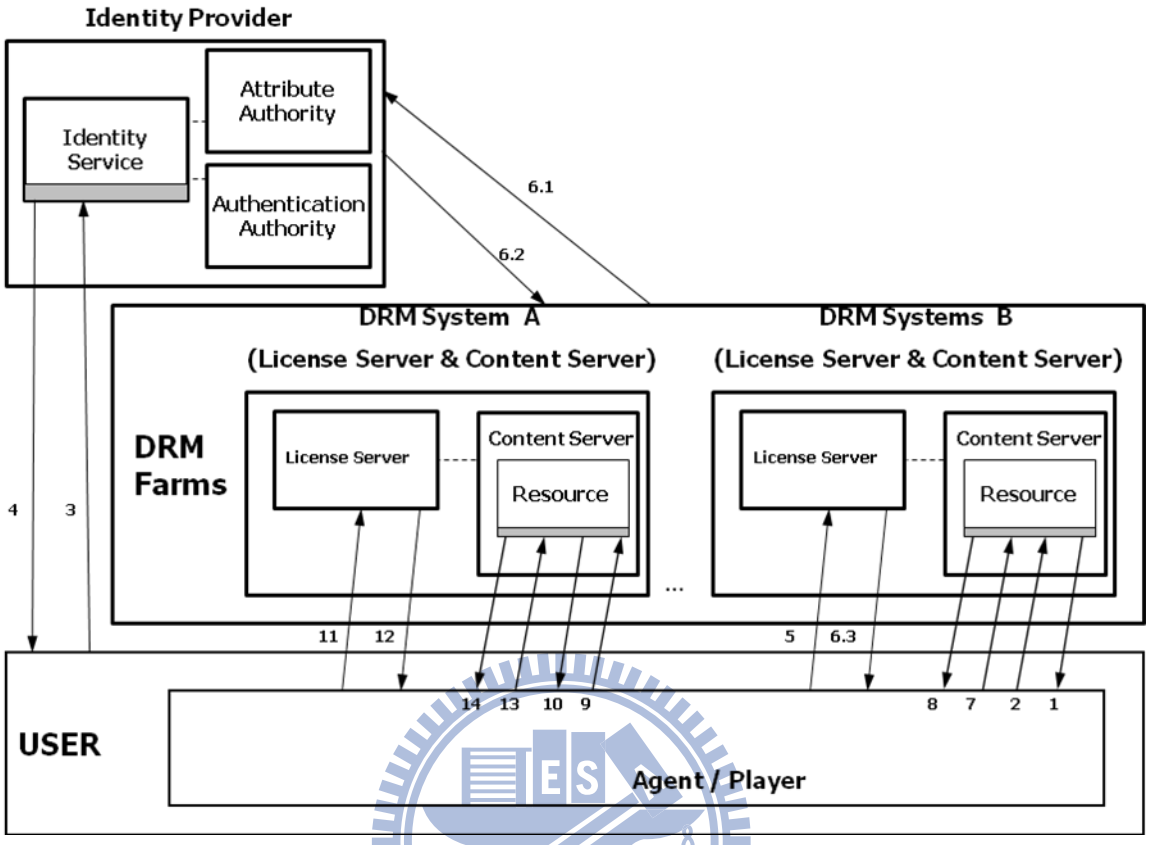


圖32：Advanced SAML-based DRM架構

六、 參考文獻

[1] Piyali Mandal, Ashish Thakral, Shekhar Verma, “Watermark Based Digital Rights Management.” IEEE Information Technology Coding and Computing, 2005. ITCC 2005, vol 1.pp.74-78,2005.

[2] Microsoft, “Windows Media-Digital Right Management”, [On-line].Available: http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx

[3] Apple, “Thoughts on Music” , [On-line].Available: http://www.apple.com/hotnews/thoughtsonmusic/

[4] 智勝國際,”DRM 數位版權保護全方位解決方案”, http://www.caidiy.com/drm/ 。

[5] 優碩科技, http://www.trustview.com.tw/tw/qa.aspx。

[6] OASIS “SAML 2.0”, [On-line].Available: http://www.oasis-open.org/specs/#samlv2.0。

[7] 楊佳泰,「以 Xrml 為基礎之多媒體數位版權管理機制之研究」, 國立中正大學, 碩士論文, 民國九十四年。

[8] Microsoft, “Digital Right management”, [On-line].Available: http://www.microsoft.com/windows/windowsmedia/tw/drm/

[9] C. Conrado, F.Kamperman, C.J. Schrijen, and W. Jonker, “Privacy in an Identity-based DRM system,” IEEE Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA’ 03), Prgue, September w2003, pp. 385-395.

[10] 洪啟富,「基於身份與隱私為主體的數位版權管理系統之研究」, 國立清華大學, 碩士論文, 民國九十四年。

[11] David Orrell, Eduserv Athens Authentication Systems and Single Sign-On (SSO), EuroCAMP, 7-9 November 2005, Porto, Portugal .

[12] Eve Maler, “SAML basics A technical introduction to the Security Assertion Markup Language” , XML Technology Center, Sun Microsystems, Inc.

[13] Wikipedia, “SAML” , [On-line].Available: http://en.wikipedia.org/wiki/SAML

[14] 陳俊廷,「可權限轉移之數位版權管理系統的研究與實現」, 國立交通大學, 碩士論文, 民國九十八年。

[15] 悠遊卡, http://www.easycard.com.tw/

[16] Tom Scavo, Security Assertion Markup Language A Brief Introduction to SAML, NCSA,

[17] Bok-Nyong Park, Jae-Won Kim and Wonjun Lee, “Precetp: A Privacy- Enhancing Licenese Management Protocol For Digital Rights Management”, Proceeding of the 18th International Conference on Advanced Information Networking and Application, Vol. 1, pp.574 - 579, 2004.