發明專利說明書

中文說明書替換頁(96年11月)21日

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※ 申請案號：096115119

※ 申請日期：96,4,27 ※IPC 分類：G06F 21/10 (2013.01)

H04L 9/32 (2006.01)

H04N 21/839 (2011.01)

一、發明名稱：(中文/英文)

改良之領域存取

IMPROVED ACCESS TO DOMAIN

二、申 請 人：(共 3 人)

姓名或名稱：(中文/英文)

1. 荷蘭商皇家飛利浦電子股份有限公司
   KONINKLIJKE PHILIPS ELECTRONICS N.V.
2. 荷蘭商沃德方公司
   VODAFONE LIBERTEL BV
3. 荷蘭商史迪其協會
   STICHTING TELEMATICA INSTITUUT

代表人：(中文/英文)

1. J L 凡 德 渥
   VAN DER VEER, J. L.
2. 約翰 沙瑪倫
   SAMARRON, JOHN
   亨利 歐丹賀溫
   ODENHOVEN, HARRY
3. H J 凡 德 魯特
   VAN DER LUQT, H. J.

住居所或營業所地址：(中文/英文)

1. 荷蘭愛因和文市格羅尼渥街1號
   GROENEWOUDSEWEG 1, 5621 BA EINDHOVEN, THE NETHERLANDS

2. 荷蘭瑪斯翠特市賽洛米克街300號
AVENUE CÉRAMIQUE 300, 6221 KX MAASTRICHT, THE NETHERLANDS

3. 荷蘭英奇德市布威傑斯屈特路1號
BROUWERIJSTRAAT 1, 7523 XC ENSCHEDE, THE NETHERLANDS

國　籍：(中文/英文)

1. 荷蘭　THE NETHERLANDS
2. 荷蘭　THE NETHERLANDS
3. 荷蘭　THE NETHERLANDS

三、發明人：(共 4 人)

姓　名：(中文/英文)

1. 羅伯特　保羅　寇斯特
KOSTER, ROBERT PAUL
2. 傑維爾　蒙太奈
MONTANER, JAVIER
3. 索林　馬歇爾　艾科柏
IACOB, SORIN MARCEL
4. 奈吉勃　柯瑞奇
KORAICHI, NAJIB

國　籍：(中文/英文)

1. 荷蘭　THE NETHERLANDS
2. 西班牙　SPAIN
3. 羅馬尼亞　ROMANIA
4. 荷蘭　THE NETHERLANDS

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家(地區)申請專利：

【格式請依：受理國家(地區)、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 歐洲專利機構；2006年05月02日；06113373.2

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

在一包含複數個裝置之領域中，該領域中之該等裝置共用一共同領域密鑰，提供一種使用該共同領域密鑰來使一並非為該領域之一成員的實體能夠建立一可經鑑認及/或解密之物件的方法，該方法包含將一多樣化密鑰提供至並非為該領域之一成員的該實體，該多樣化密鑰係使用一單向函數自用於建立與該物件有關之鑑認資料及/或用於加密該物件之至少該共同領域密鑰得出，該領域中之該等裝置經組態以使用該多樣化密鑰來鑑認及/或解密該物件。

六、英文發明摘要：

In a domain comprising a plurality of devices, the devices in the domain sharing a common domain key, a method of enabling a entity that is not a member of the domain to create an object that can be authenticated and/or decrypted using the common domain key, the method comprising providing to the entity that is not a member of the domain a diversified key that is derived using a one-way function from at least the common domain key for creating authentication data related to said object and/or for encrypting said object, the devices in the domain being configured to authenticate and/or decrypt said object using the diversified key.

七、指定代表圖：

(一)本案指定代表圖為：第(3)圖。

(二)本代表圖之元件符號簡單說明：

101	視訊轉接器/裝置
102	電視顯示器/裝置
103	攜帶型顯示器裝置/裝置
104	行動電話/裝置
105	音訊重放裝置/裝置
201	內容發佈者(CI)
202a、202b	權利發佈者(RI)
210	DRM內容
212a、212b	權利物件(RO)
301	領域發佈者(DI)
S1	儲存媒體

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

九、發明說明：

【發明所屬之技術領域】

本發明係關於改良之領域存取。

【先前技術】

近年來，可用之內容保護系統的數目已迅速增長。一些此等系統僅保護內容免受未授權複製，而其他系統限制使用者之存取或使用內容的能力。此等系統經常被稱作數位權利管理(DRM)系統。

消費者想要享受內容而無麻煩且具有盡可能少之限制。其想要將其裝置聯網以致能所有類型之不同應用且容易地存取任何類型之內容。其亦想要能夠在其本地環境中共用/轉移內容而無限制。

經授權領域(AD)之概念試圖找到一伺服內容所有者之利益(想要對其版權之保護)與內容消費者之利益(想要對內容之無限制使用)的解決方法。基本原則為具有一受控制之網路環境，其中只要內容不越過經授權領域之邊界，其即可被相對自由地使用。通常，經授權領域以亦被稱作本地網路之本地環境為中心。

當然，其他情況亦為可能的。一使用者可(例如)在旅行中帶上一關於具有一有限量之內容之音訊及/或視訊的攜帶型裝置，且在其旅館房間中使用該裝置來存取或下載儲存於家中之其個人音訊及/或視訊系統上的額外內容。即使攜帶型裝置在本地網路外部，但其為使用者之經授權領域的一部分。因此，一經授權領域(AD)為一允許藉由領域

中之裝置而並非藉由任何其他裝置來存取內容的系統。

經授權領域需要解決諸如經授權領域識別、裝置簽入、裝置簽出、權利簽入、權利簽出、內容簽入、內容簽出以及領域管理的問題。對於一對一經授權領域之使用等的更廣泛介紹，參看2002年9月12日至16日在荷蘭舉行的IBC 2002會議公開案，S.A.F.A. van den Heuvel、W. Jonker、F.L.A.J. Kamperman、P.J. Lenoir之Secure Content Management in Authorised Domains, Philips Research的第467頁至第474頁。

在對於經授權領域之某些架構中，領域中之實體(例如，裝置)共用一對稱領域密鑰，該密鑰尤其用以建立、存取及/或鑑認領域中可用之物件(諸如內容或執照(權利物件))。一實例為開放行動聯盟之DRM架構的版本2：核準版本2.0、OMA-AD-DRM-V2_0-20060303-A、03 Mar 2006，此後將其簡稱為OMA DRM v2。此文獻在網際網路上在member.openmobilealliance.org/ftp/public_documents/bac/DLDRM/Permanent_documents/處為可用的且係以引用的方式併入本文獻中。另一實例為WO 2005/088896(代理人案號PHNL040288)。

在此等架構中，不可使領域密鑰對非成員實體可用，因為其將使非成員實體能夠存取受保護物件，即使其並非為領域之成員。更需要使某些非成員實體能夠建立由領域中之實體所使用之物件。當然可將不同密鑰發給此等非成員實體，但其要求每一領域中之每一裝置保留所有此等密鑰

之複本。

【發明內容】

本發明之一目標為使一並非為一經授權領域之一成員的實體能夠建立可由經授權領域之成員使用的物件而不必向實體提供領域密鑰。

在如請求項1之方法中達成此目標。藉由將一使用一單向函數自共同領域密鑰得出的多樣化密鑰提供至並非為領域之一成員的裝置或其他實體，對於此裝置而言，變得可能使用多樣化密鑰來建立與此等物件有關之鑑認資料及/或加密此等物件。領域中之裝置可在需要時建立多樣化密鑰，多樣化密鑰係使用單向函數自可用於裝置之領域密鑰得出。其可接著使用多樣化密鑰來鑑認及/或解密自非成員實體所接收之物件。

根據本發明，非成員實體不能夠存取領域密鑰，然而其能夠建立可藉由領域中之裝置來鑑認及/或解密的物件。此提供較佳控制，實體藉由該控制可將此等物件(諸如OMA DRM權利物件)發佈給領域。

較佳使用單向函數自共同領域密鑰且自並非為領域之一成員之實體的一身份之一表示得出多樣化密鑰。此具有不同實體接收不同多樣化密鑰之優點。

在一較佳實施例中，單向函數包含一鍵控密碼雜湊函數。作為此函數中之輸入，吾人可使用並非為領域之一成員之實體的一身份之一表示(諸如一與裝置相關聯之公用密鑰)。當鑑認或加密演算法要求密鑰具有一特定長度

時，吾人可將單向函數之輸出截斷至所需數目的位元。舉例而言，當用AES加密演算法(使用128個位元密鑰)來使用多樣化密鑰時，應將使用SHA-1單向雜湊函數所產生之密鑰自160個位元截斷至128個位元。

在一較佳實施例中，非成員實體為一經組態用於發佈與內容項相關聯之數位權利的權利發佈者。在此實施例中，使用多樣化密鑰來加密包含數位權利之物件。

在一實施例中，方法進一步包含建立一經數位簽名之驗證符記，該驗證符記包含並非為領域之一成員之實體的一身份之一表示。

在另一實施例中，方法包含使用共同領域密鑰來對於由並非為領域之一成員之實體提供的物件建立一訊息鑑認碼。自另一裝置接收此一物件之裝置現亦要求存在一有效訊息鑑認碼。此防止非成員實體產生一特定領域之有效物件且使得該等物件經由不同通道而可用。

本發明進一步提供一種用於執行該方法之系統及裝置。

在附屬項中闡述其他有利實施例。

【實施方式】

圖1示意展示一包含經由一網路110而互連之裝置101-105的系統100。一典型數位本地網路包括許多裝置，例如，一無線電接收器、一調諧器/解碼器、一CD播放器、一對揚聲器、一電視、一VCR、一數位記錄器、一行動電話、一帶組、一個人電腦、一個人數位助理、一攜帶型顯示單元、一汽車娛樂系統等等。通常將此等裝置互連以允

許一裝置(例如，電視)來控制另一裝置(例如，VCR)。在一些實施例中，一裝置(諸如調諧器/解碼器或一視訊轉接器(STB))作為提供對其他裝置之中央控制的中央裝置操作。

經由不同來源(諸如一寬頻電纜網路、一網際網路連接、一衛星下行鏈路、行動電話網路、如磁碟之儲存媒體或攜帶型裝置)而接收內容(其通常包含如音樂、歌曲、電影、動畫、演講、音樂之視訊片斷、電視節目、圖像、遊戲、鈴聲、說話書及其類似物之事物，但其亦可包括交互服務)。接著可經由網路110而將內容轉移至一用於再現之槽。一槽可為(例如)電視顯示器102、攜帶型顯示器裝置103、行動電話104及/或音訊重放裝置105。

再現一內容項之準確方式取決於裝置之類型及內容之類型。舉例而言，在一無線電接收器中，再現包含產生音訊信號且將其饋送至揚聲器。對於一電視接收器而言，再現通常包含產生音訊信號及視訊信號且將該等信號饋送至一顯示器螢幕及揚聲器。對於其他類型之內容而言，必須採取一類似的適當動作。再現亦可包括諸如解密或解擾一所接收之信號、使音訊信號與視訊信號同步等之操作。

視訊轉接器101或系統100中之任何其他裝置可包含一允許記錄且稍後回放所接收之內容的儲存媒體S1(諸如一適當大的硬碟)。儲存媒體S1可為某種個人數位記錄器(PDR)(例如，一DVD+RW記錄器)，視訊轉接器101連接至其。儲存於一載體120(諸如一緊密碟片(CD)或數位化多功

能碟片(DVD))上之內容亦可進入系統100。

使用一基地台111(例如，使用藍芽或IEEE 802.11b)來將攜帶型顯示器裝置103及行動電話104無線連接至網路110。使用一習知有線連接來連接其他裝置。為了允許裝置101-105進行互動，允許不同裝置交換訊息及資訊且允許其控制彼此之若干可交互運作性標準為可用的。一熟知之標準為通用即插即用標準(http://www.upnp.org)。

設立系統100以藉由作為一較佳根據OMA DRM v2標準或其之一後繼者的經授權領域(AD)操作來管理對內容之存取。圖2展示一根據OMA DRM v2標準之示意架構圖。

在圖2中，一內容發佈者(CI)201使得內容210(在OMA術語中為"DRM內容")對AD中之裝置(此處對裝置101)以受保護形式可用。為了存取內容210，裝置101需要一由一權利發佈者(RI)202提供之權利物件(RO)212。RO 212之提供可與DRM內容210之提供同時發生，但此並非為必要的。舉例而言，吾人可在某一時間時獲得內容且稍後購買一RO來存取該內容。或者，吾人可獲得一RO且僅稍後獲得RO應用於其中的內容。

在OMA DRM中，一RO為一規定與一塊DRM內容相關聯之許可及約束的XML文件。DRM內容在無一相關聯之RO的情況下不可使用，且僅可根據一RO中所規定的許可及約束來使用。RO含有再現實際內容所需要的權利表達及密鑰。藉由被稱作ROAP之一組協定來規定RO獲取、裝置登記及領域管理。

裝置101-105之每一者具有一通常體現為一在所討論的裝置上執行之軟體組件的DRM代理。DRM代理確保遵守一RO中所規定的許可及約束。一權利物件密碼地結合至一特定DRM代理，故僅該DRM代理可使用該權利物件。

DRM內容210可在裝置101-105之間被自由地分配且亦可儲存於(例如)儲存媒體S1上或被分配至其他方。然而，在無一有效RO的情況下，不可存取DRM內容210。若(例如)裝置105將獲取DRM內容210之一複本，則其仍將必須獲得一結合至其DRM代理之RO。RO 212僅可由裝置101之DRM代理使用。

為了建立對內容之基於領域之存取，OMA DRM亦允許結合至一DRM代理之群組而非一單一代理的權利物件之建立及分配。此一群組被稱作一領域，且結合至一領域之權利物件被稱作領域權利物件。為了加入領域，第一裝置101必須詢問權利發佈者202是否允許其來加入一領域。若允許裝置101加入，則RI 202將向裝置101提供一領域情況(DC)。DC含有可用以解密領域權利物件之領域密鑰。關於詳細參看OMA DRM v2說明書之第6.4部分。

OMA DRM說明書進一步界定DRM內容之格式及保護機制、權利物件之格式(表達語言)及保護機制，及用於加密密鑰之管理的安全模型。OMA DRM說明書亦界定可如何使用一系列傳送機制(包括拉動(HTTP拉動、OMA下載)、推動(WAP推動、MMS)及串流)來將DRM內容及權利物件傳送至裝置。RO傳送使用一被稱作權利物件獲取協定

(ROAP)的一次或兩次協定，在一RI與一DRM使用者代理之間執行該協定。或者，可在不在兩個DRM使用者代理或在一RI與一DRM使用者代理之間執行ROAP的情況下執行RO傳送。

注意內容發佈者201與權利發佈者202可為一個且相同實體。在OMA術語中，此實體接著被稱作一內容分配者。

本發明之發明者已認識到在OMA解決方法中需要權利發佈與領域管理之功能分離。上文所描述之架構的一主要缺點為在不同RI之間不可容易地共用或使用領域。

根據本發明，引入一單獨的領域發佈者(DI)。想要加入一領域之裝置現接觸DI而非一RI。因此，現可使用多個RI來向相同領域供給領域RO。此在圖3中示意說明。將兩個RI 202a、202b(發佈領域RO 212a、212b)提供至裝置101。此外，一領域發佈者(DI)301管理哪些裝置加入及離開領域。

領域密鑰(下文簡寫為K_D)現由DI 301而非RI 202提供至裝置101-105。RI 202a、RI 202b不再能夠存取領域密鑰。此將意謂其不再可將領域權利物件發佈至裝置101-105，因為根據OMA DRM v2，必須使用領域密鑰來保護領域權利物件。

根據本發明，發佈給每一RI其自己的多樣化密鑰(下文簡寫為K_{Di})，其中i為多樣化密鑰K_{Di}所發佈給之RI的識別符。較佳結合所討論的權利發佈者之身份而自領域密鑰得出多樣化密鑰。

在一較佳實施例中，藉由使用領域密鑰作為秘密密鑰來計算權利發佈者之身份(較佳為一公用密鑰)之一表示的鍵控雜湊訊息鑑認碼(HMAC)來建立多樣化密鑰。儘管亦可使用許多其他雜湊函數，但較佳使用SHA1密碼雜湊函數。較佳截斷所計算的鍵控雜湊以保留僅開始的128個位元，該128個位元接著充當多樣化密鑰。

或者，一密碼雜湊函數可用以計算領域密鑰之一雜湊，該雜湊接著充當多樣化密鑰。必要時可再次截斷雜湊。較佳地，密碼雜湊函數之輸入不僅為領域密鑰，而且為權利發佈者之身份(較佳為一公用密鑰)之一表示。此較佳實施例向不同RI提供不同密鑰。舉例而言，吾人可雜湊領域密鑰及公用密鑰之序連連接。

在另一實施例中，使用領域密鑰DK作為加密密鑰來獲得密鑰K_{Di}作為RI之身份之一表示的一加密。取決於在DRM系統實施內使用何種類型之名稱、序號等，可以不同方式建立RI之身份的表示。舉例而言，DM可將一長度精確為128個位元(16個位元組)之獨特識別標記Lb_i指定給可與領域進行通信之每一RI。此可為一認證序號。若標記短於16個位元組，則DM應用0個位元、至多16個位元組來預填充每一標記以形成Lb_i。

建立多樣化密鑰之一選擇現為使用領域密鑰DK作為加密密鑰來對此標記Lb_i進行一AES加密。此之一優點為其非常簡單，且保證所得密鑰為獨特的。

若每一RI具有一經任意選擇且獨特的名稱，則該名稱可

經填充來建立一具有正確長度之串。用於填充之標準技術為可用的，參看(例如)ISO/IEC標準9797。下文為一較佳選擇。首先用一區塊預填充名稱，該區塊的長度為128個位元且為名稱之(未填充)長度以位元的二進制表示。接著用值"0"之位元後填充結果直至整個訊息的長度達到128個位元之一倍數。可使用具有作為加密密鑰之領域密鑰DK的AES來加密結果。此具有經任意選擇之名稱可由RI使用的優點。

可考慮許多替代選擇。現將給出若干實例。在大多數情況下，可應用一鍵控MAC函數而非使用領域密鑰DK作為密鑰來加密。

為了獲得其多樣化密鑰K_{Di}，在一較佳實施例中，權利發佈者將一請求發佈給領域發佈者。若將允許權利發佈者將RO發佈至所討論的領域中之裝置，則領域發佈者發佈一包含相關情況之回應。此情況包含權利發佈者之多樣化密鑰且較佳亦包含下文所詳細闡述的領域發佈者之識別符、領域本身、一有效性終止時間(表達為時間點或自一當前時間起的持續時間)及較佳一RI驗證符記。終止時間及驗證符記可採取權利發佈者之一公用密鑰(已使用領域發佈者之一私有密鑰而產生)之一X.509v3認證的形式。

權利發佈者現可產生權利物件且使用多樣化密鑰來加密此等RO。除現使用多樣化密鑰而非領域密鑰以外，此與用標準OMA DRM v2相同。

當領域中之一裝置自一權利發佈者獲取一領域RO時，

其建構此權利發佈者之一多樣化密鑰且使用該多樣化密鑰來解密領域RO。為此，裝置重複如上文對於領域發佈者所概述的過程。

在一實施例中，領域發佈者建立一RI驗證符記，其允許RI證明其被允許對於所討論的領域中之裝置發佈領域RO。驗證符記包含權利發佈者之身份(例如，一公用密鑰)且較佳亦(例如)包含符記將保持有效多久之一指示(例如，藉由指示一終止日期)。驗證符記應由DI數位簽名以使得可驗證其確實性。

在此實施例中，裝置可使用RI驗證符記來獲得權利發佈者之身份(例如，公用密鑰)。當然，若不可成功地驗證數位簽名或若符記不再有效(例如，若當前時間超出所指示的終止日期)，則裝置不應使用RI驗證符記。

根據OMA DRM v2，一權利發佈者及一裝置應在裝置可自權利發佈者接受RO之前執行一RI登記協定。本發明之一益處為此不再為一要求。領域中之一裝置亦可自領域中之另一裝置獲得領域RO，且在該狀況下不需要用最初產生該領域RO之RI登記其本身。

在某些時間間隔處，可用一新領域密鑰替換領域密鑰。在此時刻，領域發佈者亦應對於經發佈給得自先前領域密鑰之多樣化密鑰的所有權利發佈者產生新多樣化密鑰。領域發佈者應接著較佳自動地將此等新多樣化密鑰提供至此等權利發佈者。或者，一旦請求即可供應其。

代替用多樣化密鑰加密RO，多樣化密鑰亦可用以建立

及驗證與權利物件相關聯之鑑認資料。吾人可(例如)將多樣化密鑰用作用於一待應用至權利物件的鍵控雜湊函數或訊息鑑認碼函數的密鑰。此函數之輸出接著用來鑑認權利物件。

需要防止RI在不參與一具有一為領域之一成員的裝置之RO獲取協定(ROAP)的情況下對於一特定領域產生有效的領域RO。為了達成此，在一較佳實施例中，領域中之裝置在ROAP期間接收RO之後使用主要領域密鑰來計算一Device MAC且當其自一RI接收此一領域RO時將Device MAC附加至一領域RO。因此，Device MAC充當已自一經授權RI獲取領域RO之證明。注意此方法亦用於已使用領域密鑰而非一多樣化密鑰所產生之RO。因此，此方法不限於用一多樣化密鑰加密之RO。

可使用領域密鑰K_D作為密鑰來將裝置MAC計算為RO之MAC。此允許領域中之任何裝置建立Device MAC之確實性。Device MAC應伴隨RO，較佳藉由將其添加為領域RO中之一新XML元素。

在此實施例中，需要Device MAC用於隨後之裝置與裝置RO交換及在目標裝置處之安裝。只要一裝置接收一領域RO，此裝置必須在接受領域RO及/或將領域RO安裝於裝置上之前首先驗證Device MAC。

注意一旦領域密鑰K_D改變，Device MAC即不再可使用新領域密鑰來驗證。且一不具有一有效伴隨Device MAC之領域RO應較佳由領域中之裝置拒絕。或者，一已接受

且安裝了一具有一有效Device MAC之領域RO的裝置可使用新領域密鑰來再計算Device MAC。

上文所提議之解決方法的安全性係基於領域密鑰K_D僅由為領域之成員的裝置已知且僅為領域發佈者所已知之假設。然而，若領域密鑰K_D由於某種原因而變得可用於一未授權第三方，則有可能甚至在一RI如此做之授權已終止之後，一RI亦能發佈領域RO。

為了解決此問題，一產生一Device MAC之裝置應使用其對於此Device MAC之私有密鑰來產生一數位簽名。此簽名DeviceSign將與領域RO及Device MAC一起分配。DeviceSign允許領域中之其他裝置識別自RI接收領域RO之裝置。

隨後，如果領域密鑰K_D被破解且發佈未授權RO，則可識別接受此等RO之領域裝置。接著，此裝置可能結合未授權RI來運作。所討論的裝置隨後可(例如)藉由將其裝置識別符添加至一被分配至領域中之所有裝置的裝置撤銷清單(DRL)來撤銷。相容裝置僅接受且安裝包括由一未包括於DRL中之裝置產生的適當DeviceSign之領域RO。

為了支持上文，在一較佳實施例中，領域發佈者產生一經簽名之物件，該物件通知領域中之每一裝置允許一特定裝置(下文為$device_x$)建立DeviceSign簽名。符記含有$device_x$之公用密鑰且由DI來簽名以使得其可藉由領域之任何成員裝置來驗證。較佳使符記可用於$device_x$以使得此裝置可將其分配至其他裝置。

在此實施例中，只要一裝置接收一領域RO，除已討論的其他步驟以外，其需要執行$device_x$之DeviceSign及符記的驗證。

在此實施例中，領域中之其他每一裝置能夠存取一關於領域中之裝置的裝置撤銷清單(DRL)。DRL可儲存於裝置中或(例如)為可經由一網路存取。DRL較佳藉由列出不應接受其DeviceSign之裝置而實現為一黑名單。或者，DRL可藉由僅列出應接受其DeviceSign之裝置而實現為一白名單。

本發明亦可用以保護及/或鑑認除權利物件以外的其他物件。舉例而言，可使用多樣化密鑰來加密內容。

本發明不僅僅可應用於根據OMA DRM之領域。存在在某種程度上實施經授權領域之概念的各種提議。在所謂的基於裝置之AD中，領域係藉由一特定組的硬體裝置或軟體應用程式(在下文中被共同稱作用戶端)及內容而形成。一領域管理者(其可為用戶端之一或多者、一智慧卡或另一裝置)控制哪些用戶端可加入領域。僅允許領域中之特定組的用戶端(成員)利用該領域之內容，例如，打開、複製、播放或輸出內容。同一申請人在國際專利申請案WO 03/098931(代理人案號PHNL020455)、國際專利申請案WO 05/088896(代理人案號PHNL040288)及國際專利申請案WO 04/027588(代理人案號PHNL030283)中提供此等基於裝置之AD的實例，所有申請案茲以引用的方式併入。

一種類型的基於裝置之AD允許結合至一領域之一組用戶端存取結合至該領域之內容。此雙重結合確保所有成員可存取內容。通常藉由經由一共用秘密密鑰而實施結合來建立此結構。此密鑰係由一領域管理者選擇且將其分配至所有成員。當內容結合至領域時，執照藉由用共用密鑰進行之加密而密碼地鏈接至領域。或者，內容可直接結合至一用戶端，且用戶端保持結合至AD。

另一類型之AD為所謂的基於個人之AD，其中領域係基於個人而非裝置。此一系統之一實例由同一申請人描述於國際專利申請案WO 04/038568(代理人案號PHNL021063)中，該申請案係以引用的方式併入本文中，其中內容與個人相聯繫，接著將其集合成一領域。

一所謂的基於混合經授權領域之DRM系統將內容連結至一可含有裝置及個人之群組。此群組通常限於一家庭，以使得：

1.可在屬於家庭之成員的任一者(例如，起居室中之電視、臥室中之電視、PC)上觀看內容。

2.可在由屬於家庭之使用者的任一者在其已在任何用戶端(諸如一旅館房間中之一電視)上鑑認其本身之後觀看內容。此鑑認通常涉及一諸如一智慧卡之使用者鑑認裝置。

可在國際專利申請案WO 2005/010879(代理人案號PHNL030926)及國際專利申請案WO 2005/093544(代理人案號PHNL040315)中找到混合AD系統之實例，該等申請案係以引用的方式併入本文中。

國際專利申請案第PCT/IB2005/053531號(代理人案號PHNL041254)描述一種允許存取一經授權領域之方法，經授權領域係由一領域管理者管理，該方法包含一使用者鑑認裝置(該使用者鑑認裝置鏈接至一外部裝置)對領域管理者宣稱使用者鑑認裝置與外部裝置之間的一局部鏈接在距離上有限的一步驟，及領域管理者允許外部裝置作為經授權領域之一成員操作(若宣稱經接受為正確的)的一步驟。

國際專利申請案第PCT/IB2005/053687號(代理人案號PHNL041329)描述一種經授權領域系統，其包含包括至少一擷取裝置之複數個裝置，其中擷取裝置經組態以對於包含於領域中之兩個或兩個以上裝置擷取撤銷狀態資訊且將所擷取之撤銷狀態資訊分配至擷取裝置與其連接之一或多個裝置。

國際專利申請案WO 2004/077790(代理人案號PHFR030018)描述一種用於將多媒體內容廣播至一用戶端裝置之電信系統。該系統包含一用於在一編碼資料流中編碼多媒體內容之編碼器。該編碼資料流經由一第一網路連接而傳輸至一伺服器。該伺服器能夠自所接收之編碼資料流中所含有之媒體資料產生元資料且建立一進行檔案，其中該媒體資料與元資料交錯。經由一第二網路連接而將該進行檔案下載至一用戶端裝置，該裝置能夠使用該等經交錯之元資料及媒體資料而在下載結束之前開始播放所接收之多媒體內容。

應注意上述實施例說明而非限制本發明，且熟習此項技

術者將能夠在不偏離附加之申請專利範圍之範疇的情況下設計許多替代實施例。

在申請專利範圍中，不應將置於圓括號之間的任何參考正負號理解為限制請求項。詞"包含"不排除存在一請求項中所列出之元件或步驟以外的元件或步驟。在一元件之前的詞"一"不排除存在複數個此等元件。本發明可藉由包含若干不同元件之硬體，且藉由一經適當程式化之電腦來實施。

在一列舉若干構件之裝置項中，此等構件之若干者可藉由硬體之一且相同項體現。僅僅某些量測陳述於相互不同的附屬項中之事實並不指示此等量測之一組合不可用以獲利。

【圖式簡單說明】

圖1示意展示包含經由網路而互連之裝置的系統；

圖2展示根據OMA DRM v2標準之示意架構圖；及

圖3展示根據本發明之包含一單獨領域發佈者及多個權利發佈者的示意架構圖。

貫穿諸圖，相同參考數字指示類似或對應元件。圖式中所指示的一些元件通常實施於軟體中，且因而代表諸如軟體模組或物件之軟體實體。

【主要元件符號說明】

100	系統
101	視訊轉接器/裝置
102	電視顯示器/裝置

103	攜帶型顯示器裝置/裝置
104	行動電話/裝置
105	音訊重放裝置/裝置
110	網路
111	基地台
120	載體
201	內容發佈者(CI)
202、202a、202b	權利發佈者(RI)
210	DRM內容
212、212a、212b	權利物件(RO)
301	領域發佈者(DI)
S1	儲存媒體

P1~4

103年3月7日修正替換頁(本)

十、申請專利範圍：

1. 一種在鑑認(authenticating)一領域(domain)中內容項之權利(right to content itmes)之方法，該領域包含共有一領域密鑰之複數個裝置，該方法包含以下步驟：

至少一內容發佈者(Content issuer)裝置提供一內容項至該領域中的該等裝置，而無一相關聯的權利物件(rights object)；

一或多個非為該領域中成員的權利發佈者裝置，其不能存取該領域密鑰，且不同於該至少一內容發佈者裝置，

對每一內容項加密該相關聯的權利物件，其係利用推得自該領域密鑰且對每一權利發佈者裝置為唯一的一多樣化(diversified)密鑰；及

將該加密的相關聯的權利物件提供至該領域中的該等裝置，

其中當利用該領域密鑰解密該內容項相關聯的權利物件時，該內容項係被鑑認。

2. 如請求項1之方法，其進一步包含利用一鍵控密碼雜湊函數(keyed cryptographic hash function)推得該多樣化密鑰之步驟。

3. 如請求項2之方法，其中該鍵控密碼雜湊函數包含非為該領域之一成員之該權利發佈者裝置的一身份(identify)之一表示及該領域密鑰。

4. 如請求項1之方法，其進一步包含推得該多樣化密鑰之

步驟，其係藉由將一單向函數(one-way functions)之輸出截斷(truncting)至一預定數目的位元而得出。

5. 如請求項1之方法，其進一步包含建立一經數位簽名之驗證符記(validation token)之步驟，該驗證符記包含並非為該領域之一成員之該權利發佈者裝置的一身份之一表示。

6. 如請求項1之方法，其進一步包含建立一訊息鑑認碼(message authentication code)之步驟，其係針對由並非為該領域之一成員之該權利發佈者裝置所提供的該權利物件而建立。

7. 如請求項1之方法，其中該權利物件包含用於存取內容之數位權利。

8. 如請求項1之方法，其進一步包含推得該多樣化密鑰之步驟，其係使用一單向函數自該領域密鑰且自並非為該領域之一成員之該權利發佈者裝置的一身份之一表示而得出。

9. 一種鑑認一領域中內容項之權利的系統，該領域包含共有一領域密鑰之複數個裝置，該系統包含：

至少一內容發佈者裝置，提供一內容項至該領域中的該等裝置，而無一相關聯的權利物件；

至少一非為該領域中的一成員之權利發佈者裝置，其不能存取該領域密鑰，且不同於該至少一內容發佈者裝置，該至少一非為該領域中的一成員之權利發佈者裝置經組態以：

對每一內容項加密該相關聯的權利物件，其係利用推得自該領域密鑰且對該權利發佈者裝置為唯一的一多樣化密鑰；及

將該加密的相關聯的權利物件提供至該領域中的該等裝置，

其中當利用該領域密鑰解密該內容項的相關聯的權利物件時，該內容項係被鑑認。

10. 如請求項9之裝置，其中每一裝置經組態使用該領域密鑰來對於該權利物件計算一訊息鑑認碼，且結合該所計算之訊息鑑認碼將該權利物件分配至該領域中之另一裝置。

11. 如請求項10之裝置，其中每一裝置進一步經組態以接收一新領域密鑰，使用該新領域密鑰來對於該權利物件計算一新訊息鑑認碼，且結合該所計算之訊息鑑認碼將該權利物件分配至該領域中之另一裝置。

12. 一種鑑認一領域中內容項之權利的方法，該領域包含共有一領域密鑰之複數個裝置，該方法包含下列步驟：

一或多個權利發佈者裝置，其非為該領域中的成員且不能存取該領域密鑰：

利用推得自該領域密鑰的一多樣性密鑰針對每一內容項編碼權利物件，當利用該領域密鑰解密該內容項的個別權利物件時該內容項係被鑑認，及

將該權利物件提供至該領域；

推得該多樣性密鑰，其係利用一單向函數自該領

域密鑰且自並非為該領域之一成員之該權利發佈者裝置的一身份之一表示而得出；及

該複數個裝置中至少至一者：

利用該領域密鑰鑑認對應於該權利物件的該等內容項。

十一、圖式：

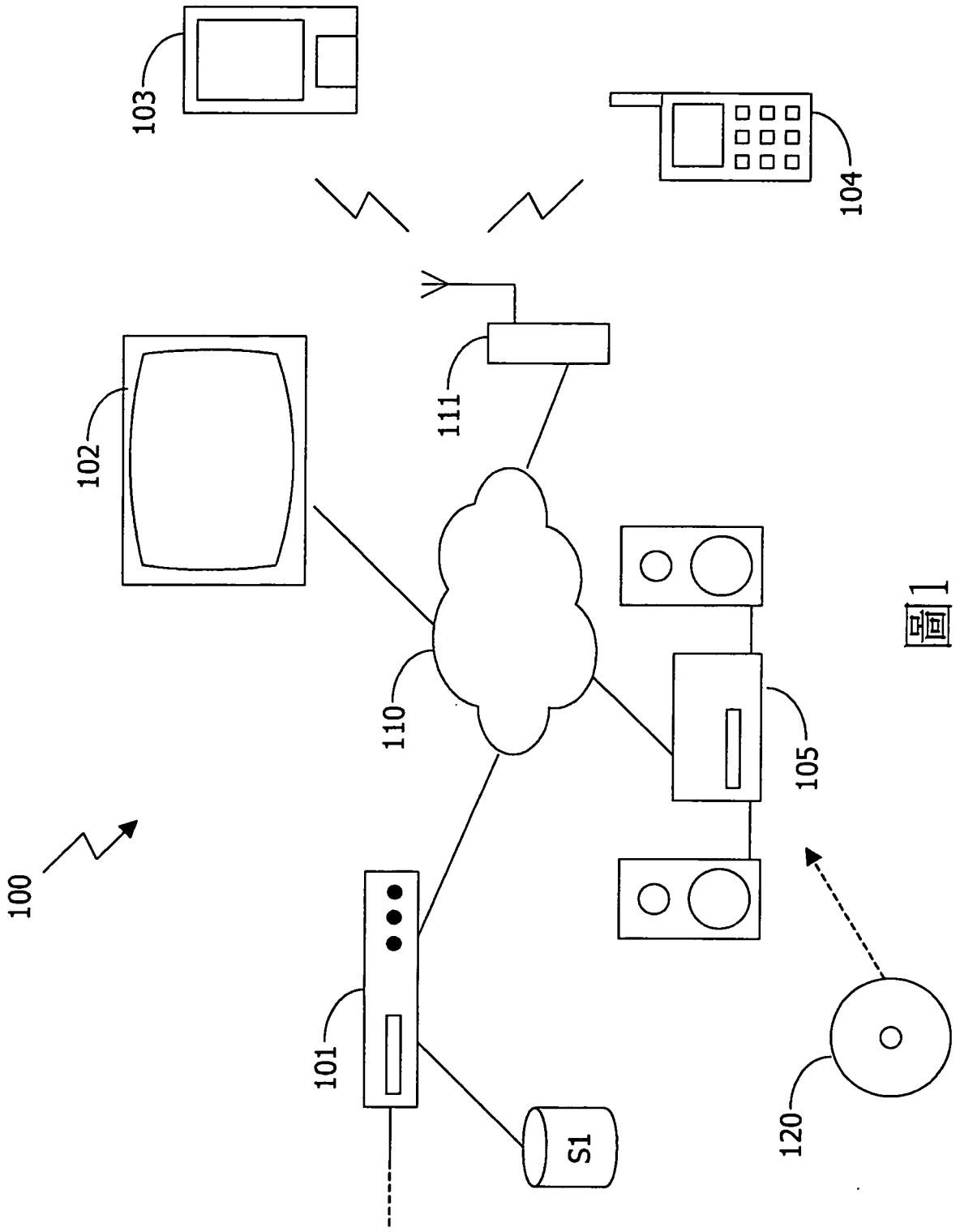

圖1

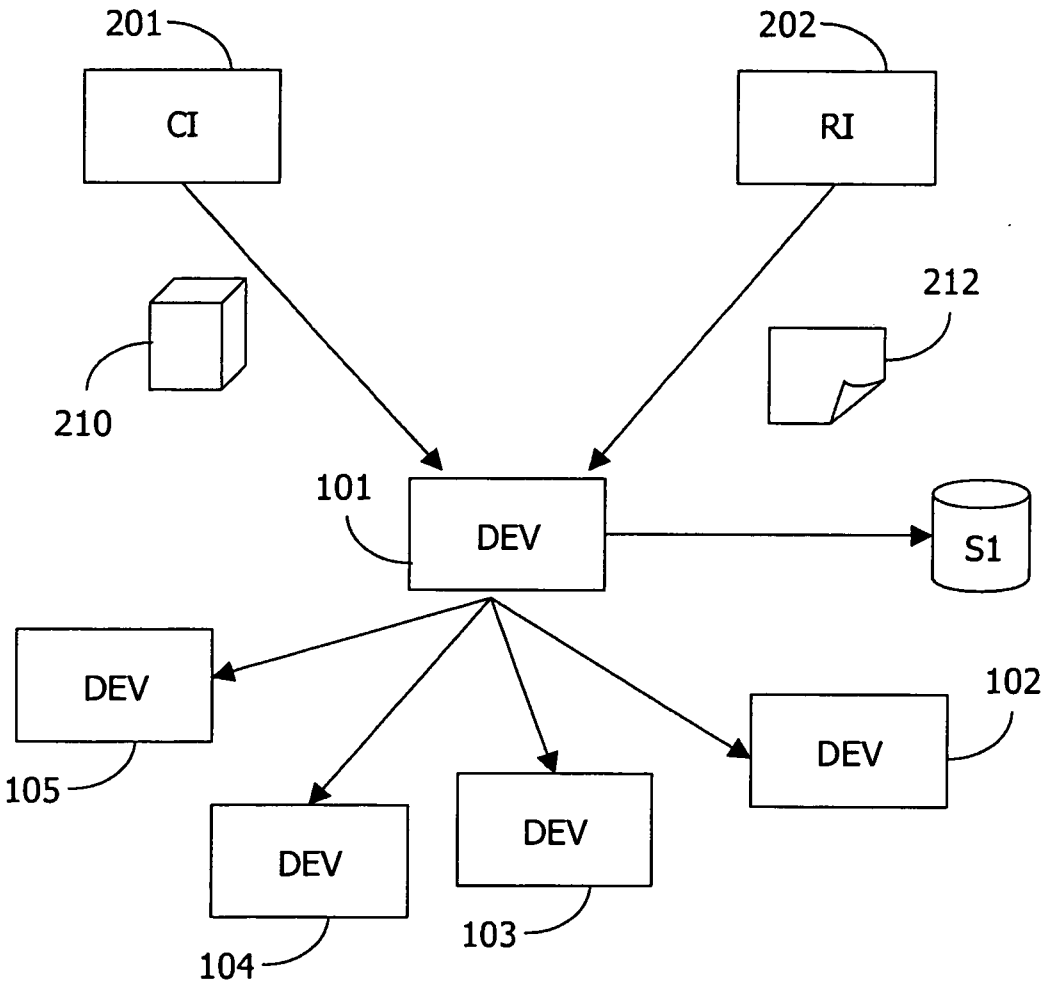

圖2

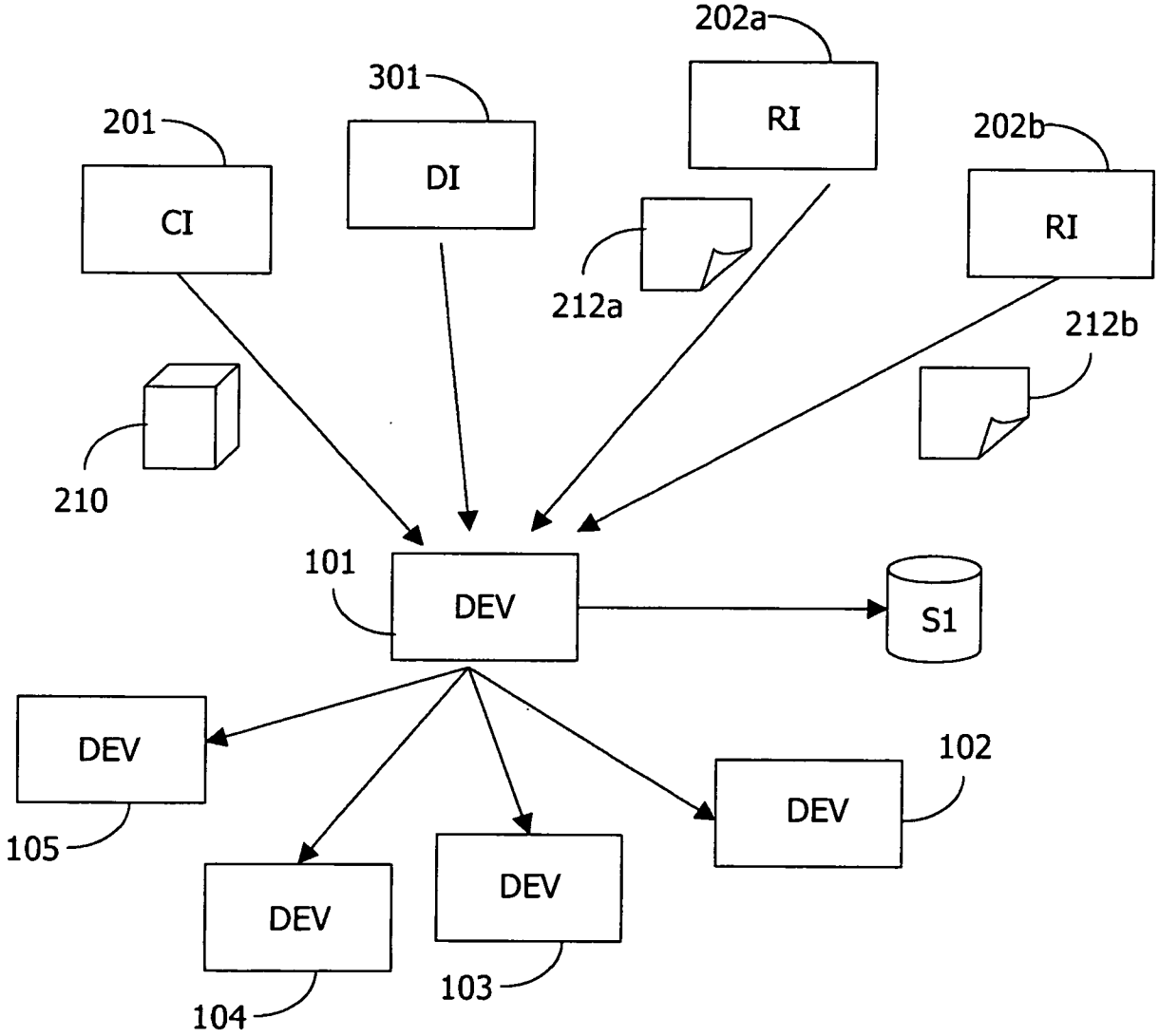
202a
301
RI
201
DI
202b
CI
RI
212a
212b
210
101
DEV
S1
DEV
102
105
DEV
DEV
DEV
104
103

圖3