

(21)申請案號：100148368

(22)申請日：中華民國 100 (2011) 年 12 月 23 日

(51)Int. Cl. : **G06F21/00 (2006.01)**  
**H04L9/00 (2006.01)**

**H04L29/06 (2006.01)**

(30)優先權：2011/03/11 美國

13/046,037

(71)申請人：英特爾股份有限公司 (美國) INTEL CORPORATION (US)  
美國

(72)發明人：麥拉拉菲 莫塔巴 MIRASHRAFI, MOJTABA (US)；賀茲拉 毛瑟米 HAZRA, MOUSUMI M. (US)；潘達庫 拉梅西 PENDAKUR, RAMESH (US)

(74)代理人：林志剛

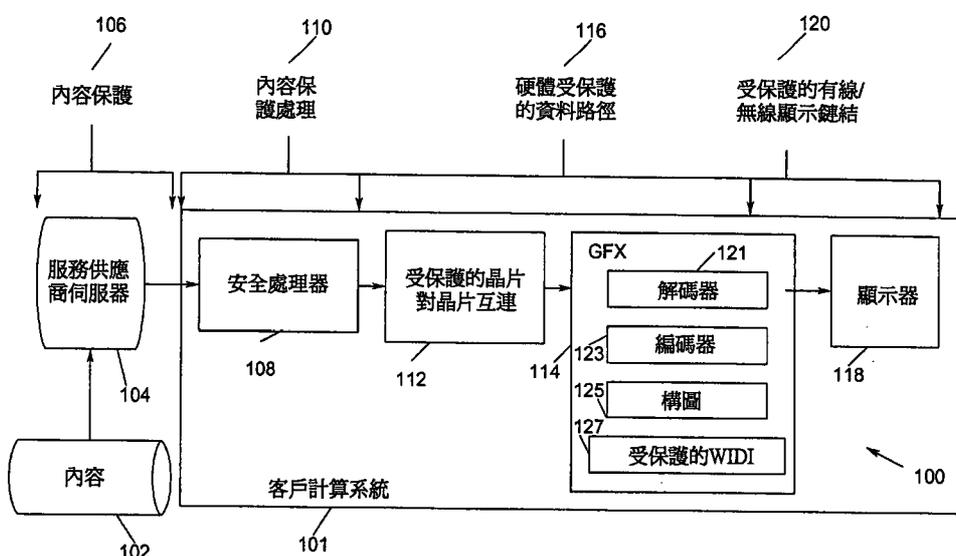
申請實體審查：有 申請專利範圍項數：36 項 圖式數：7 共 52 頁

(54)名稱

用以致能數位內容中之對象物件的採購或對數位內容中之對象物件的資訊請求之方法及設備  
METHOD AND APPARATUS FOR ENABLING PURCHASE OF OR INFORMATION REQUESTS FOR OBJECTS IN DIGITAL CONTENT

(57)摘要

客戶計算系統為使用者顯現數位內容(諸如，例如電影或電視節目)。根據該使用者的興趣，該使用者在所顯現的該數位內容之一序列的視頻圖框之視頻圖框中可選擇對象物件影像。指示該對象物件影像選擇之該使用者輸入資料係可經由安全通訊頻道、透過網路而被發送到耦合至該客戶計算系統的服務供應商伺服器。該伺服器獲得有關對應於該使用者選擇到的對象物件影像之對象物件的資訊。該伺服器發送該對象物件資訊到該客戶計算系統以顯示給該使用者。該對象物件可以是實體世界中的物件，諸如消費者商品等。該對象物件資訊可包括致使該使用者能夠購買該對象物件的資訊。



- 100：安全內容處理管線
- 101：客戶計算系統
- 102：內容
- 104：服務供應商伺服器
- 106：內容保護技術
- 108：安全處理器
- 110：內容保護處理
- 112：受保護的晶片對晶片互連
- 114：整合型圖形引擎
- 116：硬體受保護的資料路徑

118：顯示器

120：受保護的有線/  
無線顯示器鏈結

121：解碼器邏輯

123：編碼器邏輯

125：構圖邏輯

127：受保護的無線顯  
示鏈結

(21)申請案號：100148368

(22)申請日：中華民國 100 (2011) 年 12 月 23 日

(51)Int. Cl. : **G06F21/00 (2006.01)**  
**H04L9/00 (2006.01)**

**H04L29/06 (2006.01)**

(30)優先權：2011/03/11 美國

13/046,037

(71)申請人：英特爾股份有限公司 (美國) INTEL CORPORATION (US)  
美國

(72)發明人：麥拉拉菲 莫塔巴 MIRASHRAFI, MOJTABA (US)；賀茲拉 毛瑟米 HAZRA, MOUSUMI M. (US)；潘達庫 拉梅西 PENDAKUR, RAMESH (US)

(74)代理人：林志剛

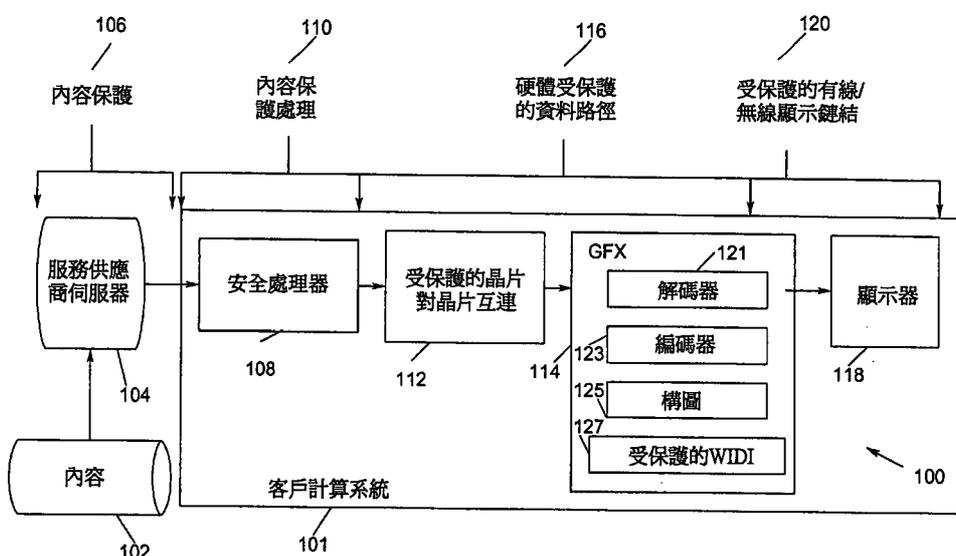
申請實體審查：有 申請專利範圍項數：36 項 圖式數：7 共 52 頁

(54)名稱

用以致能數位內容中之對象物件的採購或對數位內容中之對象物件的資訊請求之方法及設備  
METHOD AND APPARATUS FOR ENABLING PURCHASE OF OR INFORMATION REQUESTS FOR OBJECTS IN DIGITAL CONTENT

(57)摘要

客戶計算系統為使用者顯現數位內容(諸如，例如電影或電視節目)。根據該使用者的興趣，該使用者在所顯現的該數位內容之一序列的視頻圖框之視頻圖框中可選擇對象物件影像。指示該對象物件影像選擇之該使用者輸入資料係可經由安全通訊頻道、透過網路而被發送到耦合至該客戶計算系統的服務供應商伺服器。該伺服器獲得有關對應於該使用者選擇到的對象物件影像之對象物件的資訊。該伺服器發送該對象物件資訊到該客戶計算系統以顯示給該使用者。該對象物件可以是實體世界中的物件，諸如消費者商品等。該對象物件資訊可包括致使該使用者能夠購買該對象物件的資訊。



- 100：安全內容處理管線
- 101：客戶計算系統
- 102：內容
- 104：服務供應商伺服器
- 106：內容保護技術
- 108：安全處理器
- 110：內容保護處理
- 112：受保護的晶片對晶片互連
- 114：整合型圖形引擎
- 116：硬體受保護的資料路徑

## 六、發明說明：

### 【發明所屬之技術領域】

本揭示內容係有關用以安全地處理數位內容之計算系統架構的領域。尤其是，本發明的實施例係有關致能由計算系統所處理之數位內容中的對象物件之採購或對數位內容中的對象物件之資訊請求。

### 【先前技術】

在諸如例如個人電腦（PC）系統等開放式計算平台上，當播放優質內容（諸如，來自DVD、藍光等等）時，典型上藉由媒體播放器應用程式，在軟體中執行數位權利管理（DRM）處理和金鑰管理。這些方案未被妥善保護及已有被駭客侵入的實例，導致內容被剽竊及內容擁有者的收入損失。當內容被播放時，即使在硬體中進行媒體解壓縮（諸如，H.264、MPEG-2等等），內容在系統記憶體中仍是無障礙的，且會被以軟體為基礎及/或以硬體為基礎的攻擊所偷取。由於這些被注意到的安全弱點，所以典型上只有較低的精確（諸如，標準解析度（SD）等）內容或較低價值的高解析度（HD）內容被分佈到開放式計算平台。希望改良藉由開放的計算平台（諸如，例如PC等）之數位內容的安全處理。

### 【發明內容和實施方式】

本發明的實施例包含系統架構，其提供以硬體為基礎

的可信任架構（HW ROT）解決方案來支援優質數位內容的分佈和播放。在實施例中，用於數位內容和服務之 HW ROT 為安全目的用的可信任架構之根源在於客戶計算系統中之硬體和韌體機制，而非軟體之解決方案。從此可信任架構，客戶計算系統建構保護內容認證和播放之整個媒體處理管線。在本發明的實施例中，用於內容處理的客戶計算系統之安全未依賴作業系統（OS）、基本輸入/輸出系統（BIOS）、媒體播放器應用程式、或其他主機軟體。為了與系統妥協，將必須妥協硬體及/或韌體機制，與攻擊在 OS 的頂層上執行之軟體抗衡。

本發明的實施例提供服務給由客戶計算系統所處理之數位內容中的顯示影像所展示之對象物件的採購或對其資訊請求。

在下面的說明中，為了提供對各種實施例的全面瞭解，所以提出許多特定細節。然而，可在沒有特定細節之下實施本發明的各種實施例。在其他實例中，為了不混淆本發明的特別實施例，不詳細說明眾所皆知的方法、程序、組件、及電路。另外，本發明之實施例的各種態樣係可使用各種機制來予以執行，諸如積體半導體電路（“硬體”）、儲存在電腦可讀取儲存媒體上之組織成一或更多個程式的電腦可讀取指令（“軟體”）、或硬體和軟體的一些組合等。為了此揭示目的，提及的“邏輯”應意指硬體、軟體（包括例如控制處理器的操作之微碼）、韌體、或其部分的組合。

本發明的實施例藉由使用客戶計算系統 101 的 CPU、晶片組、及整合型圖形/媒體引擎中之韌體和硬體來執行這些功能，以保護內容保護處理、金鑰管理處理、及內容播放。當內容係由計算系統內的組件來予以處理時，本發明的實施例提供內容的端對端的保護。圖 1 為依據本發明的實施例之安全內容處理管線 100 圖。藉由服務供應商（SP）伺服器 104，可存取內容 102。內容 102 可以是任何數位資訊，諸如音頻、視頻、或音頻/視頻資料、影像、本文、書籍、雜誌、遊戲、或應用程式等。服務供應商伺服器 104 可包括一或更多個伺服器，用以透過任何電信頻道（諸如，網際網路、蜂巢式網路、有線或無線網路等）而提供內容給客戶計算系統。內容在儲存於 SP 伺服器時及在轉移到客戶計算系統 101 期間，可藉由任何已知的內容保護技術 106（例如，數位權管理（DRM）技術、加密技術等等）來予以保護。在一實施例中，內容可藉由此處所討論之增強型隱私權 ID（EPID）簽章驗證協定來予以保護。在一個實施例中，視頻資料係可使用利用 CTR 模式之高等編密標準（AES）加密處理來予以編密。客戶計算系統 101 可以是 PC、膝上型電腦、小筆電、平板電腦、手提式電腦、智慧型電話、個人數位助理（PDA）、機上盒、消費者電子設備、或能夠接收、儲存、及顯現內容之任何其他計算裝置。

在客戶計算系統內，內容保護處理 110 係可藉由安全處理器 108 來執行。在一個實施例中，安全處理器可以在

客戶計算系統的晶片組內。在實施例中，晶片組包含平台控制集線器（PCH）。在另一實施例中，安全處理器可以在客戶計算系統的CPU內。在具有單晶片系統（SOC）組態之另一實施例中，安全處理器可與單一晶片上的其他系統組件被整合在一起。在一個實施例中，安全處理器包含管理引擎（ME）。在其他實施例中，可使用其他類型的安全處理器。安全處理器為與客戶計算系統的其他組件互動之實施在硬體和韌體的子系統。安全處理器係可藉由從受保護的快閃記憶體區載入韌體碼及執行受保護的記憶體中之韌體碼來予以操作。因為在安全處理器內的硬體和韌體中執行內容保護處理，所以內容的保護可被改良而優於以軟體為基礎的系統。

加密金鑰資訊係可透過受保護的晶片對晶片互連 112 而從安全處理器發送到包含中央處理單元（CPU）及整合型圖形（GFX）/媒體引擎之組件。在實施例中，受保護的晶片對晶片互連 112 包含到 CPU/GFX 組件之安全直接媒體介面（DMI）通訊鏈結。DMI 包含具有同時發生資料流量的兩個單向通道之晶片對晶片互連，以及具有提高服務品質的等時轉移。透過 DMI 鏈結所轉移的資料可藉由已知的加密處理技術來加以保護。在實施例中，晶片對晶片安全鏈結可被使用於透過 DMI 傳遞經編密的標題金鑰。安全係根據 PCH 與 CPU 之間的共有祕密。此共有的祕密可被建立在各個電力週期上，及可視需要而在產品家族、世代、及隨機群聚之間改變，以確保共有的祕密之保護和

完整。DMI 機制與在 CPU 上執行之 OS、BIOS、及軟體分開獨立。DMI 機制可被使用而在安全處理器（在 PCH 中）與 CPU 之間建立信任關係。

GFX 引擎 114 可包括內容保護處理以解密內容。GFX 引擎亦包括解碼器邏輯 121，以處理/解碼經解密的音頻/視頻內容，且將做為媒體區塊之音頻/視頻內容傳遞到 GFX 引擎 114 內的圖形處理單元（GPU）。GPU 包括安全技術，其包括使用編碼器邏輯 123，以在記憶體的處理期間保護媒體區塊。GFX 引擎 114 亦包括構圖（composition）邏輯 125，以構圖想要被顯示在顯示器 118 上之影像資料。當在 PCH 中的安全處理器與 CPU/GFX 組件中的 GFX 引擎之間和之內處理內容時，可藉由硬體受保護的資料路徑 116 來保護內容。在實施例中，硬體受保護的資料路徑包含受保護的音頻視頻路徑（PAVP），以維持內容的安全。PAVP 亦支援系統組件之間的經編密的連接狀態。藉由使用 PAVP，系統可在系統組件之間轉移期間與在記憶體內進一步保護內容。

可藉由受保護的有線/無線顯示器鏈結 120 來實施 GFX 引擎、PCH、與顯示器 118 之間的介面。在一個實施例中，透過 PCH 經由記憶體從 GFX 引擎發送到顯示器之顯示資料可藉由高頻寬數位內容保護（HDCP）內容保護方案來予以保護。HDCP 規格提供健全、具有成本效益、及透明的方法，以發送和接收數位娛樂內容到適用的數位顯示器。在實施例中，有線鏈結可依據可從數位內容保護

(LLC) 取得之 HDCP 規格 (版本 2.0) 或者後續版本來予以實施。當資料透過 DisplayPort、數位視訊介面 (DVI)、高解析度多媒體介面 (HDMI)、十億位元視頻介面 (GVIF)、或統一顯示介面 (UDI) 連接而行進時，HDCP 可被使用來阻止顯示資料的複製。HDCP 版本 2.0 規格滿足新興的使用模型，其讓終端使用者能夠方便地透過如 TCP/IP、USB、Wi-Fi、及 WirelessHD 等標準協定和介面來連接顯示器、裝置、及家庭劇院系統。HDCP 版本 2.0 規格使用以標準為基礎的 RSA 公共金鑰和高等編密標準 (AES) 128 位元編密以供健全的內容保護之用。在 HDCP 系統中，兩個或更多個 HDCP 裝置經由受 HDCP 保護的介面來予以互連。由 HDCP 所保護的影音內容從上游內容控制功能流動到在最上游 HDCP 發送器處之 HDCP 系統內。從此處，由 HDCP 系統所編密之 HDCP 內容透過受 HDCP 保護的介面而流經 HDCP 接收器的樹狀拓樸。

HDCP 內容保護機制包括三個元件：1) HDCP 接收器對其緊接的上游連接 (對 HDCP 發送器) 之認證。認證協定為 HDCP 發送器驗證給定的 HDCP 接收器被允許接收 HDCP 之機制。2) 撤銷被 DCP 決定為無效之 HDCP 接收器。3) 透過 HDCP 發送器與其下游 HDCP 接收器之間的 HDCP 保護介面之影音內容的 HDCP 加密。HDCP 接收器可以音頻和視訊的形式來顯現 HDCP 內容給人們消費。HDCP 接收器可以是 HDCP 轉發器 (repeater)，其用作為更往下游發出 HDCP 內容到一或更多個額外的 HDCP 接收

器之下游 HDCP 發送器。在一個實施例中，發送到顯示器 118 之顯示資料可使用 802.11n 無線區域網路 (WLAN) 技術透過受保護的無線顯示 (WiDi) 鏈結 127 來予以發送。

如同從圖 1 所見一般，在本發明的實施例中，從自服務供應商伺服器 104 接收到內容直至內容被顯示在顯示器 118 上為止的時間，沒有加密金鑰或內容可以未編密的形式利用於在計算系統上執行之任何軟體或未授權的硬體。另外，透過橫跨解密、解碼/編碼、構圖、及顯示管線的整個鏈來提供用於視頻資料的記憶體保護。在不妥協總系統性能之下以全記憶體頻寬來提供此能力。

圖 2 為根據本發明的實施例之服務供應商伺服器 104 與安全服務組件 202 圖。在實施例中，安全服務組件 202 可包含一或更多個伺服器及/或組件。在實施例中，安全服務組件可藉由客戶計算系統之一或更多個組件的製造商來予以操作。安全服務組件提供用以控制領域中的客戶計算系統之能力。安全服務組件包含製造組件和部署組件。製造組件包括憑證發行組件 218、金鑰產生 (Key Gen) 組件 220、及保險絲程式設計 (Fuse Prog) 組件 222。憑證發行 218 產生及發行公共金鑰憑證給客戶計算平台的每一個。Key Gen 220 負責視需要產生專用和公共金鑰對，以嵌入到客戶計算平台內。保險絲程式設計 222 負責以健全和安全的方式，利用適當的值來程式設計製造層板上的保險絲。這些值將被客戶計算平台所使用，以便在安全處理器內建立信賴起源 (trust anchor) 和金鑰階梯。

部署組件包括憑證發行組件 204、金鑰產生（Key Gen）組件 206、及撤銷管理器 208。憑證（Cert）發行組件 204 發行數位憑證給 SP 伺服器 and 客戶組件，給予它們與此種客戶系統爲了服務部署而互動之認證。金鑰產生（Key Gen）組件 206 產生加密簽名金鑰對、根金鑰對、數位憑證、及群組公共金鑰，以及爲各個群組簽名群組公共金鑰。撤銷管理器 208 決定想要被添加到撤銷列（RL）之客戶計算系統的識別符和簽章，更新 RL，及分佈經更新的 RL。

SP 伺服器 104 透過網路 201（諸如，網際網路等）而與客戶計算系統通訊。服務供應商包含 SP 伺服器應用程式 212 和 SP 伺服器代理程式 210。SP 伺服器應用程式提供客戶瀏覽能力。SP 伺服器代理程式 210 控制客戶特定訊息的發送，管理加密金鑰和經授權使用者記號，及維持內容傳送服務狀態（關於部署目的，212 及 210 實際上可能是設有防火牆及分開的不同伺服器）。內容編碼器 214 接收內容 102，且爲了安全地傳送到客戶計算系統而編碼。內容伺服器 216 發送經編碼之內容給客戶。金鑰伺服器 226 負責提供標題金鑰給認證期內的客戶計算系統。伺服器憑證 224 被 SP 伺服器代理程式所使用，以參與與客戶計算系統的相互認證及認證期的建立。SP 伺服器代理程式 210、金鑰伺服器 226、與內容伺服器 216 之間的通訊鏈結係由眾所接受的資訊安全慣例來予以保護。金鑰伺服器具有最高的網路和存取保護，以確保只有經授權方能夠

到達它，及由金鑰伺服器所管理的金鑰被隔離且設有防火牆，以防止來自外來網路實體的攻擊者。SP 伺服器代理程式或金鑰伺服器能夠存取與伺服器憑證 224 相關聯的專用金鑰。在實施例中，此專用金鑰和利用此專用金鑰所進行的所有操作係使用伺服器上之硬體安全模組（HSM）（未圖示於圖 2）來保護。

在實施例中，被使用來認證客戶計算系統與 SP 伺服器之加密方案包含依據使用零知識證明來保護使用者的隱私權之加密認證協定。在實施例中，加密認證協定包含加強型隱私權 ID（EPID）方案、具有加強型撤銷能力之直接匿名證明（DAA）方案。EPID 減輕常見的李維斯特、薩莫爾、阿德曼（RSA）的隱私權問題，RSA 為公共金鑰基礎架構（PKI）安全實施，其中，針對每次交易而獨特地識別每一個人。取而代之的是，EPID 提供遠端證明之能力但只識別具有來自特別技術世代的組件（諸如，晶片組等）之客戶計算系統。EPID 為群組簽章方案，其中，一群組的公共金鑰對應於多個專用金鑰，及專用金鑰產生由群組公共金鑰驗證之群組簽章。EPID 提供匿名和無法鏈結的安全特性 --- 給定兩簽章，一個無法決定簽章是否產生自一或更多個專用金鑰。EPID 亦提供無法偽造的安全特性 --- 沒有專用金鑰，一個無法產生有效簽章。

通常，建立具有 EPID 的安全通訊頻道可被完成如下。第一方（諸如，客戶計算系統等）發送 EPID 憑證給第二方（諸如，服務供應商伺服器等）。從不知道第一方的

身分和只知道第一方為具有可信任安全處理器之計算平台，所以第二方認證第一方。第一方然後使用第二方的公共金鑰憑證來認證第二方。因為第二方不需要隱私權，所以第二方的公共金鑰憑證不是 EPID 憑證（但可能是）。幾方然後可進入 Diffie-Hellman (DH) 金鑰交換合約。

在此處併入做為參考的下面共同專利申請案中說明 DAA 及 EPID 之各種適當的實施例：2007 年 7 月 7 日所提出申請的序號 11/778,804 之 Ernest F. Brickell 及 Jingtao Li 的“從雙線映射的直接匿名證明之設備及方法 (“An Apparatus and Method of Direct Anonymous Attestation from Bilinear Maps”)”；2008 年 9 月 11 日所提出申請的序號 12/208,989 之 Ernest F. Brickell 及 Jingtao Li 的“從短群組簽章的直接匿名證明方案之設備及方法 (“An Apparatus and Method for a Direct Anonymous Attestation Scheme from Short-Group Signatures”)”；以及 2008 年 9 月 29 日所提出申請的序號 12/286,303 之 Ernest F. Brickell 及 Jingtao Li 的“具有外來源能力之直接匿名證明方案 (“Direct Anonymous Attestation Scheme with Outsourcing Capability,”)”。在其他實施例中，亦可使用其他認證和證明方案。

客戶計算系統包含至少三個主要組件：主機軟體、晶片組硬體/韌體、及 CPU/GFX/Media 引擎。在本發明的實施例中，假設主機軟體為不可信任的。即使主機軟體被攻擊，也將不會危及任何祕密。主機軟體負責到 SP 伺服器

104 的網路連接及從內容伺服器 216 下載媒體。主機軟體用作為各種 SP 伺服器與晶片組硬體/韌體之間的代理程式。在晶片組硬體/韌體已完成標題金鑰解開和注入到 CPU/GFX 組件之後，主機軟體直接發送經編密之內容到圖形硬體。

晶片組硬體/韌體負責所有受保護的處理，扮演用於內容保護處理的受保護的裝置之角色。在實施例中，晶片組硬體/韌體使用 DMI 機構來發送受保護之標題金鑰到圖形硬體。

CPU/GFX 組件負責最後串流解密、解碼、及顯示。GFX 引擎為被動裝置，不進行政策決定。當要求時，GFX 引擎僅解密內容，然後解碼所呈遞的視頻片段。在實施例中，GFX 引擎（具有受保護之媒體編碼器）為透過 HDMI 及無線（例如，WiDi）顯示之 HDCP 輸出保護來重新編密顯示內容。

在發送高度靈敏資訊之前，必須藉由服務供應商而遠端地識別受保護之客戶計算系統。被使用來識別該平台之機構必須不違反使用者隱私。本發明的實施例提供受保護之機制給服務供應商，以透過網路來驗證服務供應商伺服器正通訊到適當的客戶計算系統並且轉移標題金鑰和其他機密材料給該客戶計算系統。在一個實施例中，被利用以在服務供應商伺服器與客戶計算系統之間建立受保護之交談（session）的協定為 EPID。EPID 允許單一公共金鑰能夠匿名地驗證由被稱作 EPID 群組的 N 個專用金鑰所產生

之簽章。爲了實施 EPID，各個晶片組含有在矽製造期間吹入平台控制集線器（PCH）保險絲中之特有的專用金鑰。在實施例中，晶片組製造商將 1,000,000 個專用金鑰置放在單一群組中，且爲所生產的各個晶片組而產生 400 個群組。爲了用作爲 EPID 驗證器，各個服務供應商將被供應有這些 400 個公共金鑰。

一旦已建立受保護的 EPID 交談，服務供應商伺服器即自由與受保護之客戶計算系統交換受保護的機密資訊。關於內容串流，受保護的標題金鑰可從 SP 伺服器傳遞到晶片組中的安全處理器。安全處理器發送受保護的標題金鑰到圖形和音頻硬體。在此點，經編密之視頻和音頻內容可從內容伺服器 216 被直接發送到解密、解碼、及顯示內容之客戶計算系統圖形和音頻硬體。關於下載內容，安全處理器使用特有的平台儲存金鑰（再次於製造期間被預燒錄到 PCH 保險絲中）將標題金鑰結合（bind）到客戶計算系統，及將已結合之金鑰送回到媒體播放器軟體。當想要播放時，已結合之標題金鑰被重新呈遞至安全處理器，其解開和以受保護的方式而發送它們到圖形和音頻硬體。

圖 3 爲依據本發明的實施例之客戶計算系統 101 圖。服務供應商（SP）播放器/媒體瀏覽器軟體應用程式 302 可被包括在軟體堆疊中，以透過諸如網際網路等網路 201 而與 SP 伺服器 104 接合。SP 播放器/媒體瀏覽器 302 讓使用者能夠瀏覽服務供應商的內容提供，並且能夠選擇欲從 SP 伺服器傳送到客戶計算系統之內容。SP 播放器/媒體瀏

覽器提供使用者介面控制給使用者來管理內容程式庫以及控制內容的選擇、下載、及播放。SP 播放器/媒體瀏覽器與服務代理程式 304 互動。根據本發明的實施例，服務代理程式 304 包含由被授權能夠存取支援端對端內容保護之客戶計算系統的特徵之服務供應商所提供的軟體應用程式。服務代理程式與各種 SP 播放器/媒體瀏覽器應用程式設計介面 (API) (未圖示於圖 2) 接合。服務代理程式 304 包含媒體播放器組件 306。媒體播放器提供內容播放器功能 (例如，控制重放)。

SP 客戶應用程式 308 致使 SP 播放器/媒體瀏覽器 302 及服務代理程式 304 能夠存取客戶計算系統的硬體和韌體上之內容保護特徵並且轉送訊息給服務供應商伺服器 104。在實施例中，SP 客戶應用程式包含包括內容保護 API 之主機代理程式軟體開發套件 (SDK)。在實施例中，SP 客戶應用程式與晶片組的平台控制集線器 (PCH) 312 之安全處理器 314 相通訊。

音頻驅動器 311 提供媒體播放器與音頻解密硬體 316 之間的介面。同樣地，圖形 (GFX) 驅動器 310 提供媒體播放器與 GFX 引擎 320 之間的介面。在實施例中，PCH 312 包含安全處理器 314，其執行韌體以提供內容保護功能以及其他眾所皆知的系統功能。在實施例中，安全處理器係可藉由管理引擎 (ME) 來予以實施。當藉由 PCH 312 及 GFX 引擎 320 來處理內容時，可至少部分分別藉由 PCH 硬體/韌體及 GFX 引擎硬體中之受保護的音頻視頻路

徑 (PAVP) 組件 318、322 來保護內容。

圖 4 為根據本發明的實施例之安全內容處理的流程圖。在方塊 402 中，客戶計算系統的使用者使用 SP 播放器 / 媒體瀏覽器 302 來瀏覽、發現、及購買來自一或更多個服務供應商的內容。在方塊 404 中，執行 SP 伺服器 104 和客戶計算平台 101 的相互認證。建立經認證的交談。提供對給定的一組內容具有使用權之金鑰二進位資料 (key blob)。視需要將金鑰二進位資料結合到客戶計算系統，以確保系統受到機密及完整性的保護。

客戶計算系統然後在方塊 406 中透過網路 201 而從內容伺服器 216 (用於串流操作) 或者從客戶計算系統上的區域儲存器 (用於先前已購買、下載、及儲存之內容) 取得經編密的內容。系統準備在視頻片段上工作 (例如，子圖框)。因此，一旦第一片段的資料被呈遞，硬體就可處理資料。

在方塊 408 中，使用者使用 SP 播放器 / 媒體瀏覽器 302 來開始實施選擇到的內容之播放。金鑰二進位資料被呈遞到安全處理器 314，用以打開和提取標題金鑰。當完成時，標題金鑰藉由安全處理器而被載入到圖形硬體 320 以供解密用。在方塊 410 中，SP 播放器 / 媒體瀏覽器呈遞經編密之內容到 GFX 引擎 320 內之媒體處理引擎。GFX 引擎使用標題金鑰來解密內容，及使用局部受保護的金鑰來重新編密內容。重新編密的資料可被儲存在受保護的位置或系統記憶體。隨後在方塊 414 中獲得、解密、及解壓

縮重新編密的內容。首先執行解密。一旦資料被解密，資料就被解碼/解壓縮。一旦資料被解壓縮，資料被重新編密及透過系統記憶體而被傳遞到構圖引擎。一旦完成構圖，則再次使用系統記憶體來保護和傳遞資料到顯示引擎。在實施例中，沿著此途徑的各個組件視需要而具有解密、處理、及重新編密之功能。

在方塊 416 中，GFX 引擎使用 HDCP 技術（在實施例中）重新編密媒體內容，及將內容傳送到顯示器，以供使用者觀看。在處理的各個步驟中，內容在藉由在客戶計算系統上執行之軟體或未授權的硬體組件而可存取之處從來都不是無障礙的。

圖 5 為依據本發明的實施例之安全內容處理系統圖。SP 伺服器 104 透過網路 201 而互動到客戶計算系統 101。客戶計算系統包含第一組件 500 和第二組件 502。在實施例中，第一組件包含 CPU 及 GFX 組件，而第二組件包含平台控制集線器（PCH）。在另一實施例中，第一和第二組件可被組合成單晶片系統（SOC）實施中的單一組件。第一組件 500 包括複數個處理器核心 504 及 GFX 引擎 320。處理器核心 504 執行主機軟體（SW）506 的各種組件（如圖 3 所說明者），客戶憑證 508、保險絲 521、及共有祕密 519。主機 SW 從硬碟機（HDD）/固態驅動器（SSD）510 讀取資料，包括先前從 SP 伺服器或實體媒體（諸如，DVD、藍光、或其他儲存技術等）所獲得之經編密的內容。在實施例中，主機 SW 包含至少 SP 播放器/媒體瀏

覽器應用程式 302、服務代理程式 304、及 SP 客戶應用程式 308。

GFX 引擎 320 包含複數個組件。媒體編密/解密引擎 520 包含編密和解密內容之邏輯。媒體編碼/解碼引擎 522 包含編碼和解碼內容之邏輯。GFX 構圖 (Comp) 引擎 524 包含構成顯示影像之邏輯。顯示引擎 526 包含傳遞經構圖之顯示影像到顯示器之邏輯。顯示編密/解密引擎 528 包含在透過受保護之鏈結 527 發送顯示資料到顯示器 538 之前編密和解密顯示資料的邏輯。記憶體編密/解密引擎 530 包含編密和解密儲存在記憶體 536 中的受保護的中間表面 534 之資料的邏輯。記憶體 536 亦包括實施機密和完整性受保護的記憶體操作 532 之邏輯。

第二組件 502 包含複數個組件，其中的一些並未圖示以簡化圖 5。第二組件包含安全處理器 314。安全處理器包括韌體及/或硬體邏輯，以提供證明、供應金鑰管理、及輸出控制操作 516 給客戶計算系統。安全處理器亦包括保險絲 517、共有祕密 519、及信賴起源 518，用以支援諸如驗證金鑰和金鑰階層資訊等 PKI。在製造具有金鑰材料用於 EPID 使用之晶片組期間，將保險絲 521、517 程式設計到第一和第二組件的硬體內。當製造客戶計算系統時，從程式設計到製造層板上的保險絲內之資訊建立硬體可信任架構。這確保各個個別客戶計算系統是特有的，但是隱私權受到保護。在製造晶片組及 CPU/GFX 組件期間，將共有祕密 519 硬編碼到第一和第二組件的硬體內。在實施

例中，共有祕密可被使用在建立透過 DMI 鏈結 538 之安全的晶片對晶片通訊頻道。

客戶計算系統亦包括用以供應安全時脈服務之受保護的即時時脈 513、顯示器 538、及非揮發性記憶體（NVM）512。在實施例中，可由第三方播種受保護的即時時脈，且可被虛擬化用於多個服務供應商。NVM 可被使用而為第二組件儲存韌體影像，以及被使用而為安全處理器處理操作儲存臨時資料（諸如，完整性和狀態資訊等）。

在實施例中，處理流程可被說明如下。SP 播放器/媒體瀏覽器 302 呈現使用者介面給使用者。使用者到服務供應商的網站以瀏覽可用的內容。SP 網站具有自動偵測能力，以決定使用者的客戶計算系統是否具有與 SP 伺服器 104 認證之能力的完整性在其內。若能夠，則使用者被允許選擇內容。內容可被購買、租借、或訂閱、或可被串流。使用者為內容付費。SP 播放器/媒體瀏覽器 302 調用安全處理器 316 來認證客戶計算系統 101 與 SP 伺服器 104。在實施例中，認證使用 EPID 技術。至少部分藉由使 SP 伺服器 104 驗證客戶計算系統的憑證 508、執行撤銷核對、及驗證到憑證授權書的證明（在一個實施例中，使用 EPID 協定）來認證客戶計算系統 101。當認證客戶計算系統 101 及 SP 伺服器 104 二者時，在一個實施例中，可依據 EPID 協定來建立安全通訊頻道。在實施例中，一旦安全通訊頻道建立，命令集即可被使用於端對端內容保護能力。

SP 伺服器 104 供應經編密之標題金鑰給客戶計算系統，具有使用內容的限制（例如，時間）。SP 伺服器透過安全頻道來發送經編密之標題金鑰到安全處理器 314。安全處理器 314 使用其自己的金鑰階層來解密經編密之標題金鑰。安全處理器 314 使用儲存金鑰以重新編密新解密的標題金鑰來形成金鑰二進位資料。金鑰二進位資料被結合到客戶計算系統達一特定時間週期。安全處理器 314 發送金鑰二進位資料到 CPU 核心中執行之 SP 播放器/媒體瀏覽器 302。SP 播放器/媒體瀏覽器 302 儲存金鑰二進位資料在 HDD/SSD 510 中。SP 播放器/媒體瀏覽器 302 然後下載使用者選擇到的經編密之內容。在一個實施例中，下載的經編密之內容可被儲存在 HDD/SSD 510 中。

當使用者想要播放內容時，SP 播放器/媒體瀏覽器 302 呈遞金鑰二進位資料回到安全處理器 314。例如安全處理器驗證金鑰二進位資料的簽章，及核對諸如時間等使用限制。安全處理器 314 透過經編密之頻道（例如，DMI 鏈結 538）發送經編密之標題金鑰到 GFX 引擎 320 的媒體編密/解密組件 520。安全處理器通知 SP 播放器/媒體瀏覽器 GFX/媒體引擎已準備好處理經編密之內容。SP 播放器/媒體瀏覽器 302 從 HDD/SDD 510 閱讀經編密之內容，或者透過網路 201 而從 SP 伺服器 104 獲得經編密之內容（用於資料流應用程式），且以逐一片段的方式來發送經編密之內容到 GFX 引擎。

GFX 引擎 320 以逐一片段的方式來處理經編密之內容

。關於各個片段，SP 播放器/媒體瀏覽器無障礙地閱讀片段標頭。片段的剩餘部分被編密，以便 SP 播放器/媒體瀏覽器無法存取內容。SP 播放器/媒體瀏覽器使用初始化向量來記錄播放狀態資訊。在解密接收自安全處理器的經編密之標題金鑰之後，媒體編密/解密引擎 520 使用標題金鑰來解密內容。在一個實施例中，媒體編密/解密引擎的輸出資料仍舊根據眾所皆知的 H.264 編碼方案來壓縮。在其他實施例中，可使用其他編碼方案。媒體編密/解密引擎 522 解碼各個片段，然後使用記憶體編碼/解碼引擎 530 來重新編密片段。已重新編密內容片段被儲存在記憶體 536 中之受保護的中間表面 534。GFX 構圖引擎 524 控制想要被顯示於顯示器上之影像的構圖，包括前景和背景影像、視窗等等。GFX 構圖引擎從記憶體 536 中之受保護的中間表面 534 獲得已重新編密內容片段，以產生經構圖的影像。GFX 構圖引擎 524 發送經構圖的影像資料到顯示引擎 526。

顯示引擎使用顯示編密/解密引擎 528，以從被使用來儲存內容片段在記憶體 536 中之加密來解密經構圖的影像。在一個實施例中，顯示引擎 526 使用顯示編密/解密引擎，以根據 HDCP 技術來重新編密經構圖的影像資料。透過受保護之晶片對晶片介面（例如，DMI 鏈結）538，藉由 GFX 引擎 320 將編密的經構圖之影像資料發送到第二組件 502，用以透過受保護的顯示介面鏈結 527 轉移到顯示器 538。

在實施例中，可具有由客戶計算系統所處理之任何數目的同時、獨立的內容串流。各個內容串流具有其自己的加密內文，以便不與其他串流干擾。此亦使得客戶計算系統能夠確保一個串流上之任何種類的攻擊或危害不影響其他內容串流。

本發明的實施例提供用以購買與由客戶計算系統所顯現之數位內容中所呈現的對象物件相關之商品及/或服務，及/或獲得有關由客戶計算系統所顯現之數位內容中所呈現的對象物件之資訊。圖 6 為依據本發明的實施例之對象物件資訊處理的流程圖。在方塊 602 中，SP 播放器/媒體瀏覽器 302 為使用者顯示數位內容。當使用者聽到或看到內容時，使用者可能對內容中的某些東西有興趣。在實施例中，數位內容包含視頻，例如，諸如電影或電視節目等。例如，使用者可看見正顯示在用於內容的視頻圖框之序列的至少一視頻圖框中之至少一對象物件的影像。通常，至少一對象物件影像可以是呈現由相機所擷取的實體世界物件之任何影像作為視頻圖框的至少一部分。例如，對象物件影像可以是人、植物、或動物、車輛、家用商品、建築物、風景特徵、消費者商品等等的視頻圖框中之影像。在另一例子中，對象物件影像可以是添加到視頻圖框之圖示、符號、或其他代表影像以表示數位內容的音頻部分，諸如正在播放的歌曲等。在另一例子中，對象物件可不實際存在於實體世界，及可已是添加到視頻圖框之電腦產生的、手繪的、或卡通影像。使用者亦可在消費內容的同

時對多項對象物件有興趣。在一個示例性實例中，使用者可在正觀看著演員穿著外套及開著車在特別城市中的有名街道上之電影，及那時的電影配音包含一首歌。在此例中，使用者有興趣得到有關一或更多個下面對象物件之資訊（當適當且可取得時，包括購買資訊）：演員、外套、車子、街道、城市、及歌曲。

在實施例中，當使用者有興趣得到有關相關對象物件的資訊時，或者或許購買對象物件，使用者使用可利用到客戶計算系統之使用者輸入機構來選擇對象物件影像。在本發明的實施例中，可利用的使用者輸入機構可包含現在已知或將發展之任何使用者輸入裝置，諸如電腦滑鼠、鍵盤、遙控裝置、遊戲控制器、觸碰式螢幕、偵測使用者手勢等等。在實施例中，使用者可暫停內容的播放，以便在選擇到的對象物件影像上提供使用者輸入，而後當進行使用者輸入選擇時恢復播放。在其他實施例中，可不執行暫停內容的播放。

在方塊 604 中，SP 播放器/媒體瀏覽器接受來自使用者選擇的輸入選擇，以選擇在顯示器上的視頻圖框之一序列的至少一視頻圖框中所顯現之至少一對象物件影像。在實施例中，使用者輸入資料可包含從內容的顯示開始之經過的時間和視頻圖框之位置的至少其中之一。例如，使用者可選擇顯示於在過去的時間  $t$  之播放期間所出現的視頻圖框中之特別  $(x, y)$  位置中的對象物件影像。在實施例中，時間可被指定成從所顯示的內容開始之小時、分鐘、

秒、及微秒。在另一實施例中，時間可被指定成從顯示內容的開始之計數（例如，圖框計數或其他計數）。在另一實施例中，只有經過的時間可由使用者來指定。在另一實施例中，只有位置可由使用者來指定。

當使用者消費內容及對對象物件影像進行一或更多個選擇時，在方塊 606 中，一個實施例中之 SP 播放器/媒體瀏覽器儲存使用者輸入。在一個實施例中，SP 播放器/媒體瀏覽器使用安全處理器 314 及 DMI 鏈結 538 而將使用者輸入安全地通訊及儲存在 NVM 512 中之安全儲存位置。此有助於提供隱私權給使用者有關消費的內容和相關資訊請求及購買交易。在實施例中，各個個別使用者輸入可被儲存作為分開的操作。在另一實施例中，可在內容消費處理的結束時以單一儲存操作儲存來自消費特別數位內容標題（或其部分）之使用者輸入。即使當客戶計算系統 101 並未連接到網路 201 時仍可出現方塊 602、604、及 606 的處理。

在實施例中，一旦內容被消費且客戶計算系統被連接到網路，SP 播放器/媒體瀏覽器即使用服務代理程式 304、SP 客戶應用程式 308、及安全處理器 314，以從 NVM 512 獲得所儲存的使用者輸入，並且使用上述方法安全地傳輸使用者輸入到 SP 伺服器 104 上之 SP 伺服器應用程式 212。在另一實施例中，若在內容被消費的同時將客戶計算系統連接到網路，及若使用者在資訊請求上已選擇他或她想要立即回饋，則 SP 播放器/媒體瀏覽器可即時發送各

個個別使用者輸入到服務供應商上之 SP 伺服器應用程式作處理。不管使用者輸入是否被整批處理或個別處理，在一個實施例中，在方塊 610 中 SP 伺服器應用程式比較各個使用者輸入與內容對象物件資訊資料庫中之條目。在實施例中，比較可包含試圖將來自使用者輸入的時間及位置資訊與有關內容的音頻及視頻部位之已知的資訊相符。

圖 7 為依據本發明的實施例之服務供應商伺服器上的對象物件資訊處理組件圖。SP 伺服器應用程式 212 透過網路從客戶計算系統安全地接收一或更多個使用者輸入 702。SP 伺服器應用程式可存取到內容 102。在一個實施例中，諸如 SP 伺服器應用程式等 SP 伺服器的一或更多個組件例如可被用於依據內容的靜態分析來產生內容對象物件資訊資料庫 704。也就是說，在分佈內容到任何客戶計算系統之前，可針對對象物件影像分析內容。內容對象物件資訊資料庫包括用以藉由服務供應商所支援的內容中之各個對象物件影像的條目，以依據資訊請求來提供資訊給使用者。在實施例中，內容對象物件資訊資料庫可藉由服務供應商針對各個支援的內容標題來予以建立。

在實施例中，在分佈內容及/或支援對象物件資訊請求之前，服務供應商員工分析內容的音頻及視頻部位，識別對象物件影像，及為支援的已識別對象物件產生資料庫條目。在實施例中，想要被支援之已識別對象物件可依據內容供應商、服務供應商之目前所廣告及/或市場競爭、及/或其他條目來予以選擇。在一個實施例中，與所支援

的對象物件相關聯之相關資訊可被獲得及儲存在內容對象物件資訊資料庫中。在另一實施例中，可儲存到相關資訊的鏈結，及視需要可從任何資訊源（例如，網際網路、其他資料結構、其他資料庫等等）獲得資訊。在又另一實施例中，由於諸如改變市場條件、廣告競爭改變、諸如天氣、運動分數、新聞項目等等目前事件等、每天的時間、年的時間等等諸如此類的事情，服務供應商可針對任何選擇的支援對象物件，在任何時候動態地改變內容對象物件資訊資料庫中之資訊。

獲自內容對象物件資訊資料庫 704 或者獲自與選擇的物件相關聯之其他來源的資訊可被識別作為對象物件資訊 710。例如，當對象物件為消費者商品時，對象物件資訊可包含一或更多個品牌名、製造商、型號、標題、價格、可利用性、特徵等等。例如，當對象物件為諸如男演員或女演員等人時，對象物件資訊可包括一或更多個人的傳記資訊、影片資歷、粉絲俱樂部資訊，到網站的鏈結等等。例如，當對象物件為城市或地標時，對象物件資訊可包括有關參觀城市或地標之資訊。例如，當對象物件影像呈現一首歌時，對象物件資訊可包括一或更多個歌名、藝人、唱片名稱、錄音公司、及購買資訊。通常，對象物件資訊包含與對象物件相關之任何資訊。在一個實施例中，對象物件資訊包括有關購買對象物件或相關商品及/或服務之資訊。

在實施例中，SP 伺服器應用程式可為服務供應商伺

伺服器上之使用者安全地維持使用者特定檔 706。使用者特定檔包含使用者的偏好及興趣的至少其中之一。在實施例中，SP 伺服器應用程式可至少部分根據使用者特定檔來選擇及/或修改對象物件資訊。在一個實施例中，使用者可藉由使用者使用 SP 播放器/媒體瀏覽器之贊同動作來輸入或選擇他的或她的偏好及/或興趣。在另一實施例中，SP 伺服器應用程式可至少部分根據傳送到使用者的客戶計算系統之內容及/或藉由服務供應商伺服器經過一段時間所接收的使用者輸入來發展和維持使用者特定檔。在實施例中，偏好可包括使用者感興趣的資訊類型，與使用者希望如何、何時、及以何種格式接收資訊。在實施例中，偏好可包括購買參數，諸如購買的金額限制、購買通知及認可等等。其他偏好亦可被指定。在實施例中，興趣可包括使用者選擇作為興趣的事情（例如，運動、喜好、電視、影片、及音樂類型等等），與藉由分析過去行為所決定的興趣，諸如所接收的使用者輸入和所傳送及/或所消費的內容等。在實施例中，使用者輸入可被儲存作使用者特定檔的一部分。

回到圖 6，在方塊 612 中，當在比較用於選擇到的對象物件（由對象物件影像來予以表示）之使用者輸入與內容對象物件資訊資料庫中的條目時出現相符時，在一個實施例中，SP 伺服器應用程式獲得和儲存有關對應於選擇到的對象物件影像之對象物件的資訊到使用者特定檔內。在另一實施例中，到相關資訊之鏈結可被儲存在使用者特

定檔中，及視需要可從任何資訊源（例如，網際網路、其他資料結構、其他資料庫等等）獲得資訊。在方塊 614 中，當請求時，服務供應商伺服器上之 SP 伺服器應用程式從使用者特定檔發送對象物件資訊（或者視需要從另一來源獲得對象物件資訊）到客戶計算系統上之 SP 播放器/媒體。在一個實施例中，此發生在使用者登入到由服務供應商所操作之網站以及請求一或更多個對象物件資訊時。在方塊 616 中，SP 播放器/媒體瀏覽器顯示所請求的對象物件資訊給使用者。在實施例中，對象物件資訊可包括讓使用者能夠完成對象物件之購買交易的購買資訊。在實施例中，可即時完成方塊 608、610、612、及 614，而不必等待使用者登入到網站來請求對象物件資訊。在實施例中，使用者可暫停內容的播放，以觀看所請求的對象物件資訊。

回頭參考圖 7，在一個實施例中，可藉由內容上之 SP 伺服器應用程式執行動態分析 708 來取代靜態分析，產生所儲存的內容對象物件資訊資料庫條目。動態分析組件 708 可至少部分依據所接收的使用者輸入 702 來分析內容 102 的音頻部位和視頻圖框。動態分析組件可使用已知的音頻辨識、影像辨識、及/或臉部辨識處理技術來分析由使用者輸入所指示之一或更多個音頻部位和視頻圖框，以當正在客戶計算系統上消費內容時，試圖決定服務供應商伺服器上的內容拷貝中之一或更多個選擇到的對象物件影像或聲音。例如，若內容正被串流到客戶計算系統時，如

透過網路串流內容時，伺服器上的內容可被分析，以決定目前內容部位中的對象物件。SP 伺服器應用程式接受使用者輸入及使它們與目前串流的內容部位相關聯。當藉由此種動態分析識別對象物件時，則 SP 伺服器應用程式獲得相關於所識別的對象物件之對象物件資訊 710，及繼續方塊 612、614、及 616。

以比添加預定的熱點到視頻圖框更加擴充和靈活之方式，本發明的實施例擷取對象物件中之使用者興趣。在本發明的實施例中，服務供應商伺服器可動態地決定是否具有使用者感興趣的任何事情在內容部位中，且在不同時間為同一個使用者輸入獨立採取行動或採取不同的行動。

說明書中參考“一個實施例”或“實施例”意指在至少實施中可包括連同實施例所說明之特別特徵、結構、或特性。說明書中各處之“在一個實施例中”語詞的出現可以或可不必參考同一個實施例。

再者，在說明書和申請專利範圍中，可使用語詞“耦合”及“連接”與其衍生物。在本發明的一些實施例中，“連接”可被用於指示兩或更多個元件彼此直接實體或電接觸。“耦合”可意指兩或更多個元件直接實體或電接觸。然而，“耦合”亦可意指兩或更多個元件未彼此直接接觸，但是仍彼此協作或互動。

因此，雖然已用結構特徵特有的語言及/或方法行為來說明本發明的實施例，但是應明白，所申請的主題並不侷限於所說明的特有特徵或行為。而是，特定特徵和行為

被揭示作為實施所申請的主題之樣本形式。

**【圖式簡單說明】**

參考附圖來提供詳細的說明。在不同圖式中使用同一參考號碼來指示類似或同一項目。

圖 1 為依據本發明的實施例之安全內容處理管線圖。

圖 2 為依據本發明的實施例之服務供應商伺服器和安全服務基礎建設圖。

圖 3 為依據本發明的實施例之客戶計算系統圖。

圖 4 為依據本發明的實施例之安全內容處理的流程圖。

圖 5 為依據本發明的實施例之安全內容處理系統圖。

圖 6 為依據本發明的實施例之對象物件資訊處理的流程圖。

圖 7 為依據本發明的實施例之服務供應商伺服器上的對象物件資訊處理組件圖。

**【主要元件符號說明】**

100：安全內容處理管線

101：客戶計算系統

102：內容

104：服務供應商伺服器

106：內容保護技術

108：安全處理器

- 110：內容保護處理
- 112：受保護的晶片對晶片互連
- 114：圖形引擎
- 116：硬體受保護的資料路徑
- 118：顯示器
- 120：受保護的有線/無線顯示器鏈結
- 121：解碼器邏輯
- 123：編碼器邏輯
- 125：構圖邏輯
- 127：受保護的無線顯示鏈結
- 201：網路
- 202：安全服務組件
- 204：憑證發行組件
- 206：金鑰產生組件
- 208：撤銷管理器
- 212：服務供應商伺服器應用程式
- 210：服務供應商伺服器代理程式
- 214：內容編密器
- 216：內容伺服器
- 218：憑證發行組件
- 220：金鑰產生組件
- 222：保險絲程式設計組件
- 224：伺服器憑證
- 226：金鑰伺服器

- 302：服務供應商播放器/媒體瀏覽器軟體應用程式
- 304：服務代理程式
- 306：媒體播放器組件
- 308：服務供應商客戶應用程式
- 310：圖形驅動器
- 311：音頻驅動器
- 312：平台控制集線器
- 314：安全處理器
- 316：音頻解密硬體
- 318：受保護的音頻視頻路徑組件
- 320：圖形引擎
- 322：受保護的音頻視頻路徑組件
- 500：第一組件
- 502：第二組件
- 504：處理器核心
- 506：主機軟體
- 508：客戶憑證
- 510：固態驅動器
- 512：非揮發性記憶體
- 513：受保護的即時時脈
- 516：證明、供應金鑰管理、及輸出控制操作
- 517：保險絲
- 518：信賴起源
- 519：共有祕密

- 520 : 媒體編密/解密引擎
- 521 : 保險絲
- 522 : 媒體編碼/解碼引擎
- 524 : 圖形構圖引擎
- 526 : 顯示引擎
- 527 : 受保護之鏈結
- 528 : 顯示編密/解密引擎
- 530 : 記憶體編密/解密引擎
- 532 : 機密和完整性受保護的記憶體操作
- 534 : 受保護的中間表面
- 536 : 記憶體
- 538 : 顯示器
- 538 : 直接媒體介面鏈結
- 702 : 使用者輸入
- 704 : 內容對象物件資訊資料庫
- 706 : 使用者特定檔
- 708 : 動態分析組件
- 710 : 對象物件資訊

# 發明專利說明書

(本申請書格式、順序，請勿任意更動，※記號部分請勿填寫)

※申請案號：100148368

※申請日：100年12月23日

※IPC分類：G06F12/00 (2006.01)

H04L29/06 (2006.01)

一、發明名稱：(中文/英文)

H04L9/00 (2006.01)

用以致能數位內容中之對象物件的採購或對數位內容中之對象物件的資訊請求之方法及設備

Method and apparatus for enabling purchase of or information requests for objects in digital content

二、中文發明摘要：

客戶計算系統為使用者顯現數位內容(諸如，例如電影或電視節目)。根據該使用者的興趣，該使用者在所顯現的該數位內容之一序列的視頻圖框之視頻圖框中可選擇對象物件影像。指示該對象物件影像選擇之該使用者輸入資料係可經由安全通訊頻道、透過網路而被發送到耦合至該客戶計算系統的服務供應商伺服器。該伺服器獲得有關對應於該使用者選擇到的對象物件影像之對象物件的資訊。該伺服器發送該對象物件資訊到該客戶計算系統以顯示給該使用者。該對象物件可以是實體世界中的物件，諸如消費者商品等。該對象物件資訊可包括致使該使用者能夠購買該對象物件的資訊。

三、英文發明摘要：

A client computing system renders digital content (such as, for example, a movie or TV program) for a user. Based on the user's interest, the user may select an object image in a video frame of a sequence of video frames of the digital content being rendered. The user input data indicating the object image selection may be sent to a service provider server coupled to the client computing system over a network via a secure communications channel. The server obtains information about an object corresponding to the user-selected object image. The server sends the object information to the client computing system for display to the user. The object may be an object in the physical world, such as a consumer good. The object information may include information enabling the user to purchase the object.

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無

**七、申請專利範圍：**

1. 一種在客戶計算系統上處理數位內容之方法，包含：

藉由該客戶計算系統來顯現數位內容；

接收來自使用者的使用者輸入資料，以在所顯現的該數位內容之一序列的視頻圖框之至少一視頻圖框中選擇至少一對象物件影像；

經由安全通訊頻道，透過網路來發送該使用者輸入資料到耦合至該客戶計算系統之伺服器；

從該伺服器中接收有關對應於該選擇到的對象物件影像之對象物件的資訊；以及

將該對象物件資訊顯示在該客戶計算系統上。

2. 根據申請專利範圍第 1 項之方法，其中，該選擇到的至少一對象物件影像包含由相機所擷取的對象物件之影像作為該等視頻圖框的至少其中之一的至少一部分。

3. 根據申請專利範圍第 1 項之方法，其中，該使用者輸入資料包含展示於該客戶計算系統的顯示器上之該至少一視頻圖框中的該選擇到的至少一對象物件影像之位置以及從該等視頻圖框之顯現的開始之經過時間的至少其中之一。

4. 根據申請專利範圍第 2 項之方法，其中，該擷取的對象物件包含實體世界物件。

5. 根據申請專利範圍第 4 項之方法，其中，該擷取的對象物件包含消費者商品。

6. 根據申請專利範圍第 1 項之方法，其中，該對象物件資訊包含致使該使用者能夠購買該對象物件的資訊。

7. 一種用以處理數位內容之客戶計算系統，包含：

使用者輸入機構，用以輸入使用者輸入資料；

顯示器；以及

處理器，係適用來顯現數位內容、經由該使用者輸入機構而接收來自使用者的使用者輸入資料以在所顯現的該數位內容之一序列的視頻圖框之至少一視頻圖框中選擇至少一對象物件影像、經由安全通訊頻道透過網路來發送該使用者輸入資料到耦合至該客戶計算系統之伺服器、從該伺服器接收有關對應於該選擇到的對象物件影像之對象物件的資訊、以及使該物件資訊顯示在該顯示器上。

8. 根據申請專利範圍第 7 項之客戶計算系統，其中，該選擇到的至少一對象物件影像包含由相機所擷取的對象物件之影像作為該等視頻圖框的至少其中之一的至少一部分。

9. 根據申請專利範圍第 7 項之客戶計算系統，其中，該使用者輸入資料包含展示於該客戶計算系統的顯示器上之該至少一視頻圖框中的該選擇到的至少一對象物件影像之位置以及從該等視頻圖框之顯現的開始之經過時間的至少其中之一。

10. 根據申請專利範圍第 8 項之客戶計算系統，其中，該擷取的對象物件包含實體世界物件。

11. 根據申請專利範圍第 10 項之客戶計算系統，其

中，該擷取的對象物件包含消費者商品。

12. 根據申請專利範圍第 7 項之客戶計算系統，其中，該對象物件資訊包含致使該使用者能夠購買該對象物件的資訊。

13. 一種電腦可讀取媒體，其包含一或更多個指令，當該等指令被執行於客戶計算系統的處理器上時，該等指令組構該處理器藉由下列操作來處理數位內容：

顯現數位內容；

接收來自使用者的使用者輸入資料，以在所顯現的該數位內容之一序列的視頻圖框之至少一視頻圖框中選擇至少一對象物件影像；

經由安全通訊頻道，透過網路來發送該使用者輸入資料到耦合至該客戶計算系統之伺服器；

從該伺服器接收有關對應於該選擇到的對象物件影像之對象物件的資訊；以及

使該對象物件資訊顯示在該客戶計算系統的顯示器上。

14. 根據申請專利範圍第 13 項之電腦可讀取媒體，其中，該選擇到的至少一對象物件影像包含由相機所擷取的對象物件之影像作為該等視頻圖框的至少其中之一的至少一部分。

15. 根據申請專利範圍第 13 項之電腦可讀取媒體，其中，該使用者輸入資料包含展示於該客戶計算系統的顯示器上之該至少一視頻圖框中的該選擇到的至少一對象物

件影像之位置以及從該等視頻圖框之顯現的開始之經過時間的至少其中之一。

16. 根據申請專利範圍第 14 項之電腦可讀取媒體，其中，該擷取的對象物件包含實體世界物件。

17. 根據申請專利範圍第 16 項之電腦可讀取媒體，其中，該擷取的對象物件包含消費者商品。

18. 根據申請專利範圍第 14 項之電腦可讀取媒體，其中，該對象物件資訊包含致使該使用者能夠購買該對象物件的資訊。

19. 一種處理數位內容之方法，包含：

在客戶計算系統上藉由第一應用程式來顯現數位內容；

藉由該第一應用程式，接收來自使用者的使用者輸入資料，以在所顯現的該數位內容之一序列的視頻圖框之至少一視頻圖框中選擇至少一對象物件影像；

將該使用者輸入資料儲存在該客戶計算系統內的安全儲存器中；

經由安全通訊頻道，透過網路來發送該使用者輸入資料到耦合至該客戶計算系統之伺服器上的第二應用程式；

藉由該第二應用程式，比較該使用者輸入資料與該伺服器上之內容對象物件資訊資料庫中的條目；

當該使用者輸入資料與該內容對象物件資訊資料庫中的條目相符時，藉由該第二應用程式而獲得和儲存有關對應於該選擇到的對象物件影像之對象物件的資訊；

經由該安全通訊頻道，藉由第二應用程式而將該對象物件資訊發送到該第一應用程式；以及

藉由該第一應用程式，將該對象物件資訊顯示在該客戶計算系統上。

20. 根據申請專利範圍第 19 項之方法，其中，該選擇到的至少一對象物件影像包含由相機所擷取的對象物件之影像作為該等視頻圖框的至少其中之一的至少一部分。

21. 根據申請專利範圍第 19 項之方法，其中，該使用者輸入資料包含展示於該客戶計算系統的顯示器上之該至少一視頻圖框中的該選擇到的至少一對象物件影像之位置以及從該等視頻圖框之顯現的開始之經過時間的至少其中之一。

22. 根據申請專利範圍第 20 項之方法，其中，該擷取的對象物件包含實體世界物件。

23. 根據申請專利範圍第 22 項之方法，其中，該擷取的對象物件包含消費者商品。

24. 根據申請專利範圍第 22 項之方法，其中，該擷取的對象物件包含人。

25. 根據申請專利範圍第 19 項之方法，其中，該選擇到的對象物件影像表示歌曲。

26. 根據申請專利範圍第 19 項之方法，其中，該對象物件資訊包含致使該使用者能夠購買該對象物件的資訊。

27. 根據申請專利範圍第 19 項之方法，其中，該內

容資訊資料庫包含被支援提供對象物件資訊給該使用者之該內容中的用於各個對象物件影像之條目。

28. 根據申請專利範圍第 27 項之方法，另包含在分佈該內容之前，分析該內容的音頻和視頻部分、識別對象物件影像、及為已識別對象物件影像建立條目在該內容資訊資料庫中。

29. 根據申請專利範圍第 27 項之方法，另包含當該內容正在該客戶計算系統上被消耗時，至少部分根據該使用者輸入資料來分析該內容的音頻和視頻部分、識別對象物件影像、及為已識別對象物件影像建立條目在該內容資訊資料庫中。

30. 根據申請專利範圍第 27 項之方法，另包含動態地改變該內容資訊資料庫中之該對象物件資訊。

31. 根據申請專利範圍第 19 項之方法，其中，藉由該第二應用程式而儲存有關對應於該選擇到的對象物件影像之對象物件的資訊包含：將該對象物件資訊儲存在該伺服器上的使用者特定檔中；以及至少部分根據該使用者特定檔來修改對象物件資訊以發送到該客戶計算裝置。

32. 根據申請專利範圍第 31 項之方法，另包含：至少部分根據遞送到該客戶計算系統的內容和使用者輸入來決定該使用者的興趣；以及將該使用者的興趣儲存在該使用者特定檔中。

33. 一種系統，包含：

客戶計算系統，用以顯現數位內容、接收來自使用者

的使用者輸入資料以便在所顯現的該數位內容之一序列的視頻圖框之至少一視頻圖框中選擇至少一對象物件影像、及將該使用者輸入資料儲存在該客戶計算系統內的安全儲存器中；以及

伺服器，係經由安全通訊頻道透過網路而被耦合至該客戶計算系統、從該客戶計算系統接收該使用者輸入資料、比較該使用者輸入資料與該伺服器上的內容對象物件資訊資料庫中之條目、當該使用者輸入資料與該內容對象物件資訊資料庫中之條目相符時，獲得和儲存有關對應於該選擇到的對象物件影像之對象物件的資訊、以及經由該安全通訊頻道而發送該對象物件資訊到該客戶計算系統；

其中，該客戶計算系統係要顯示該物件資訊給該使用者。

34. 根據申請專利範圍第 33 項之系統，其中，該選擇到的至少一對象物件影像包含由相機所擷取的對象物件之影像作為該等視頻圖框的至少其中之一的至少一部分，以及該使用者輸入資料包含展示於該客戶計算系統的顯示器上之該至少一視頻圖框中的該選擇到的至少一對象物件影像之位置以及從該等視頻圖框之顯現的開始之經過時間的至少其中之一。

35. 根據申請專利範圍第 34 項之系統，其中，該擷取的對象物件包含實體世界物件。

36. 根據申請專利範圍第 33 項之系統，其中，該對象物件資訊包含致使該使用者能夠購買該對象物件的資訊。

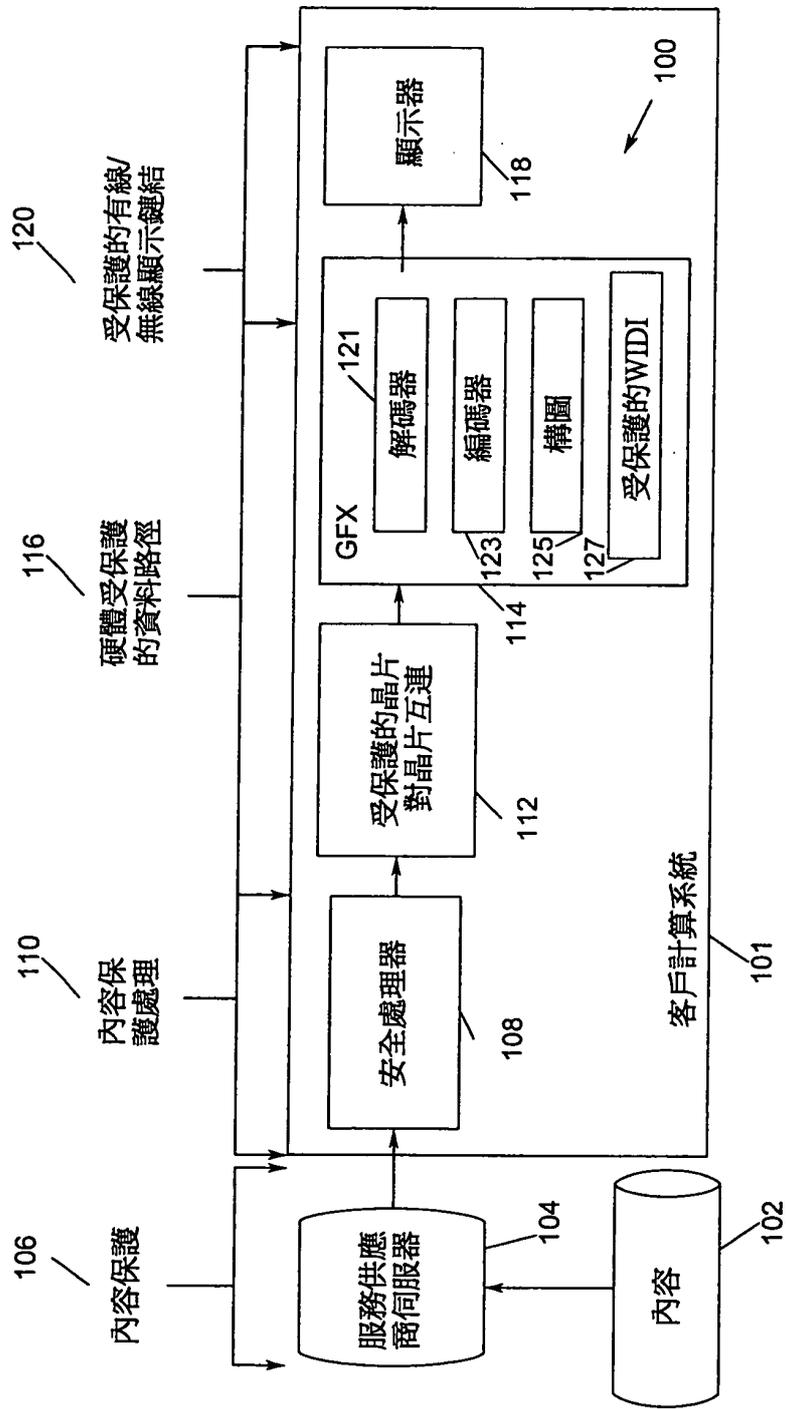


圖1

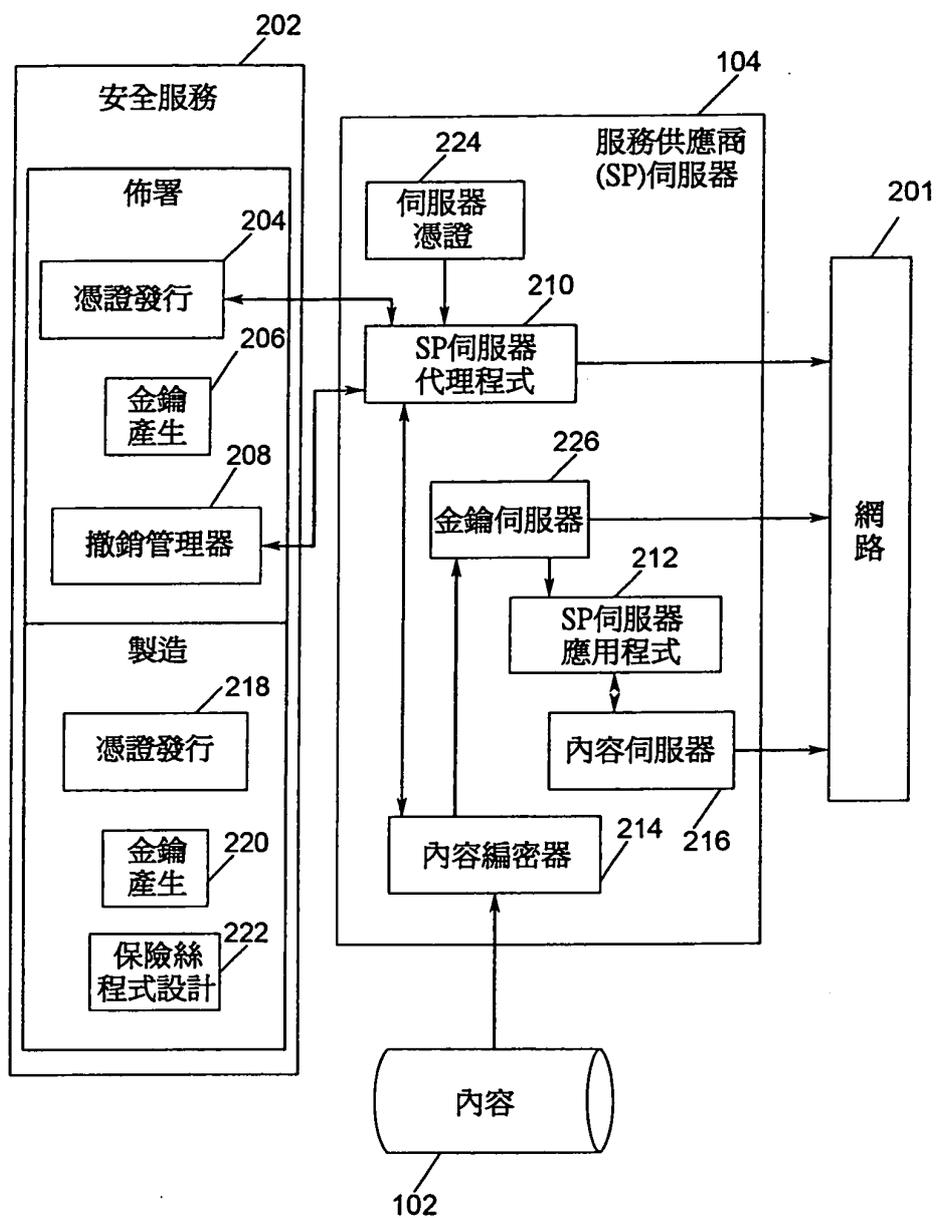


圖 2

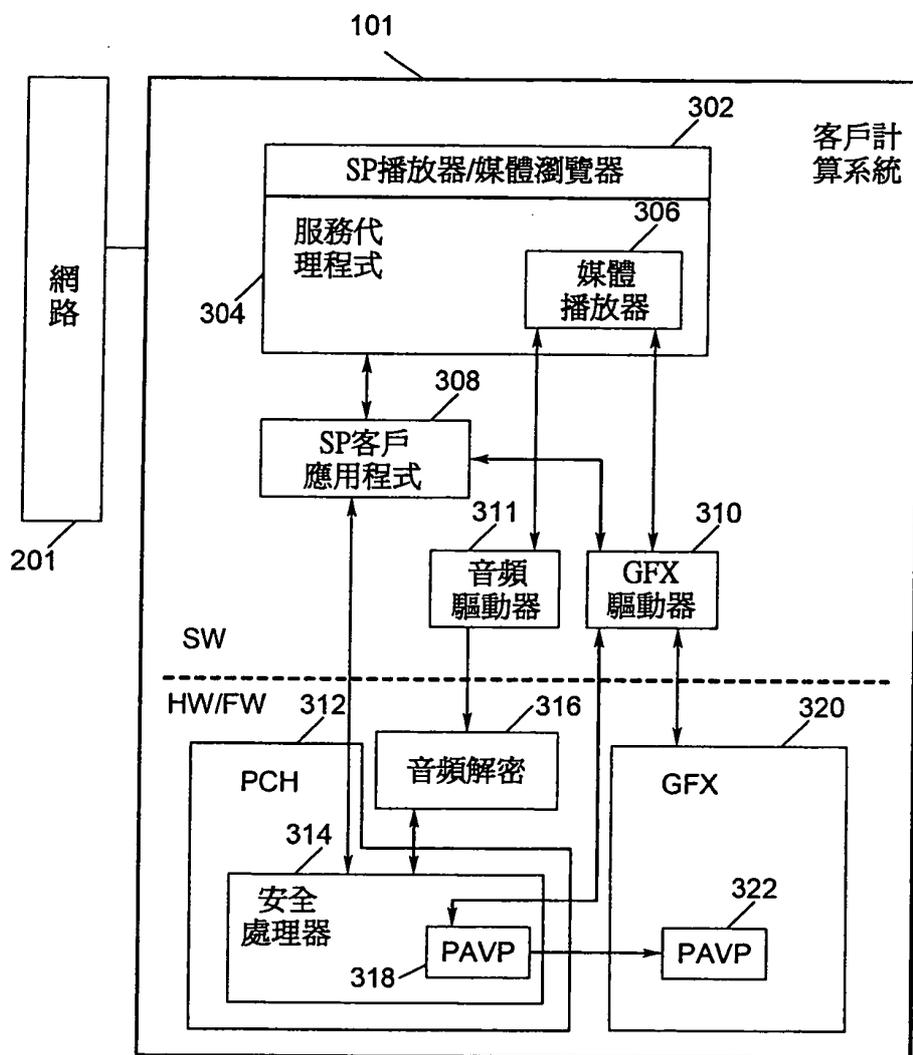


圖3

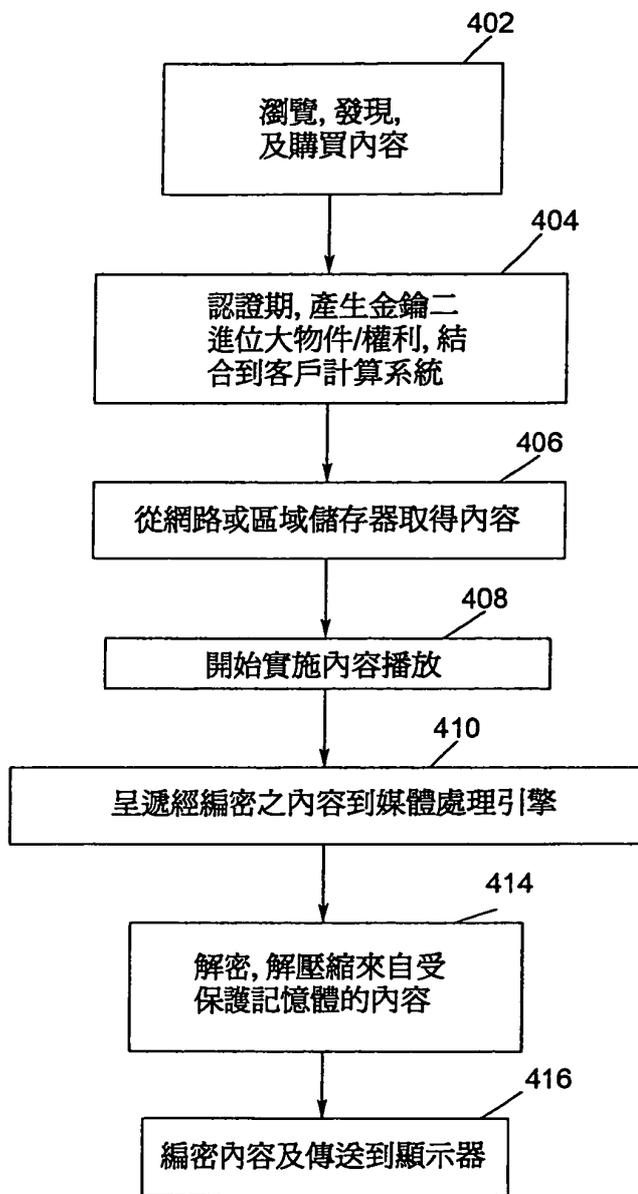
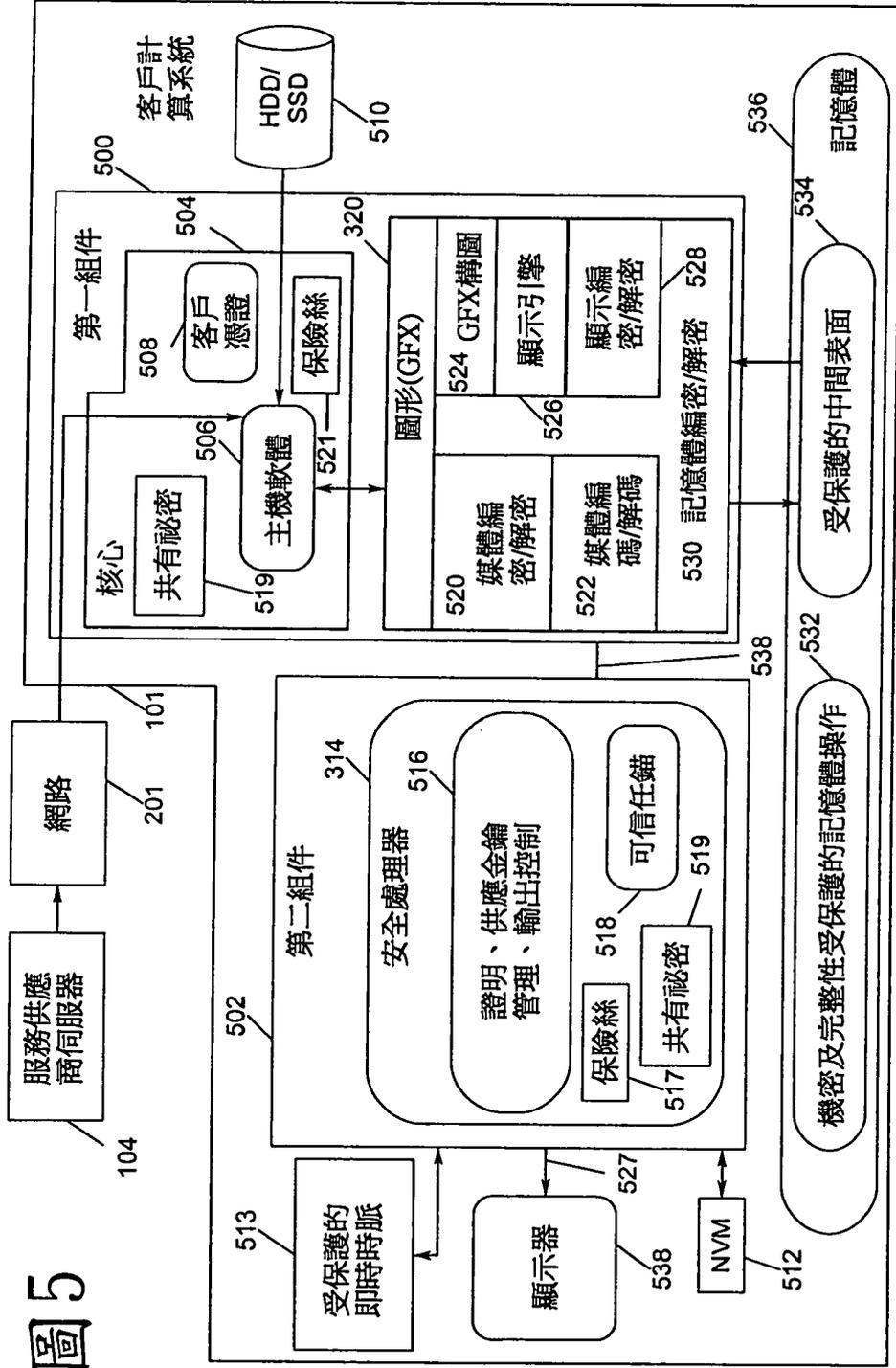


圖 4

圖5



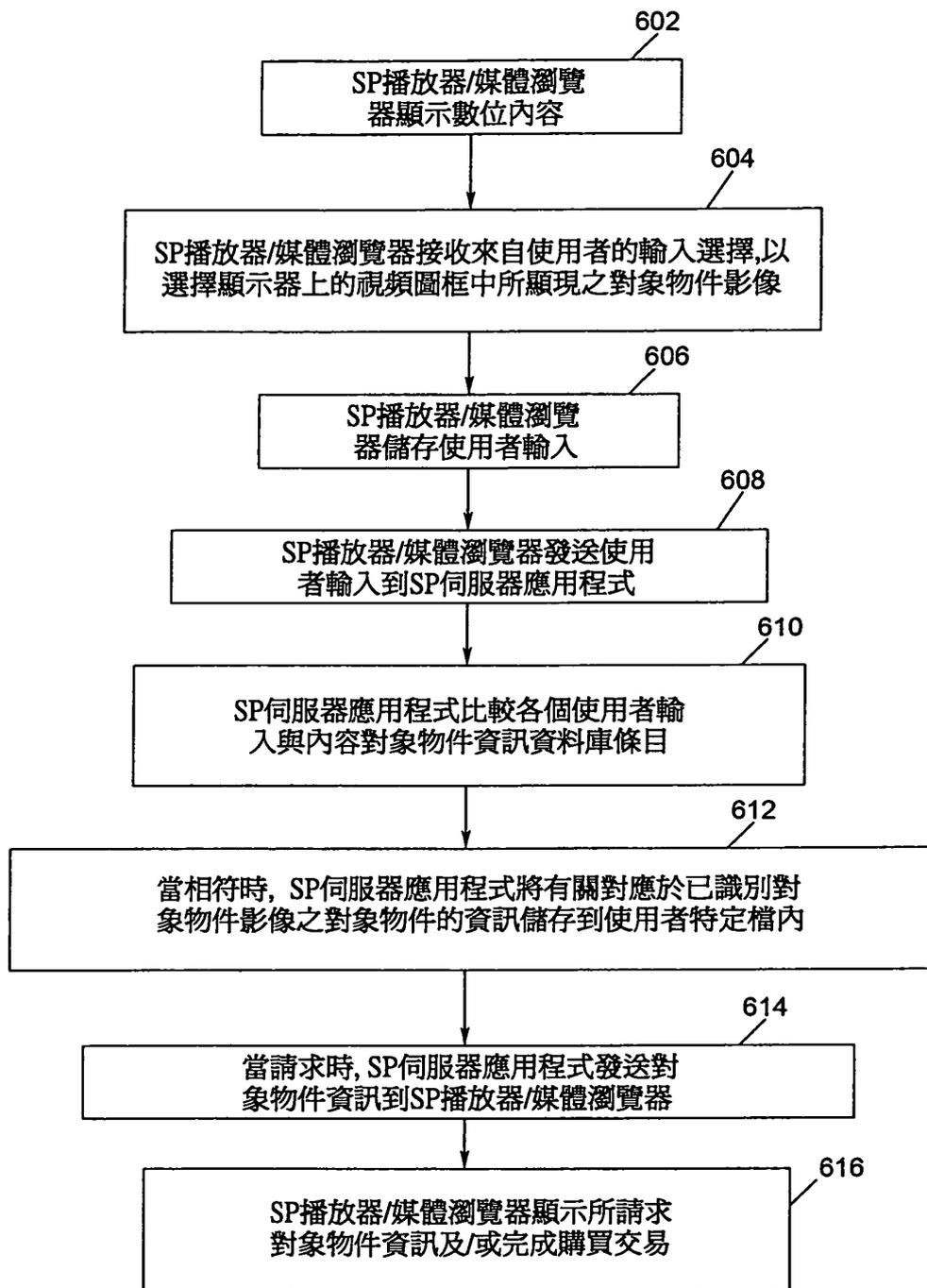


圖6

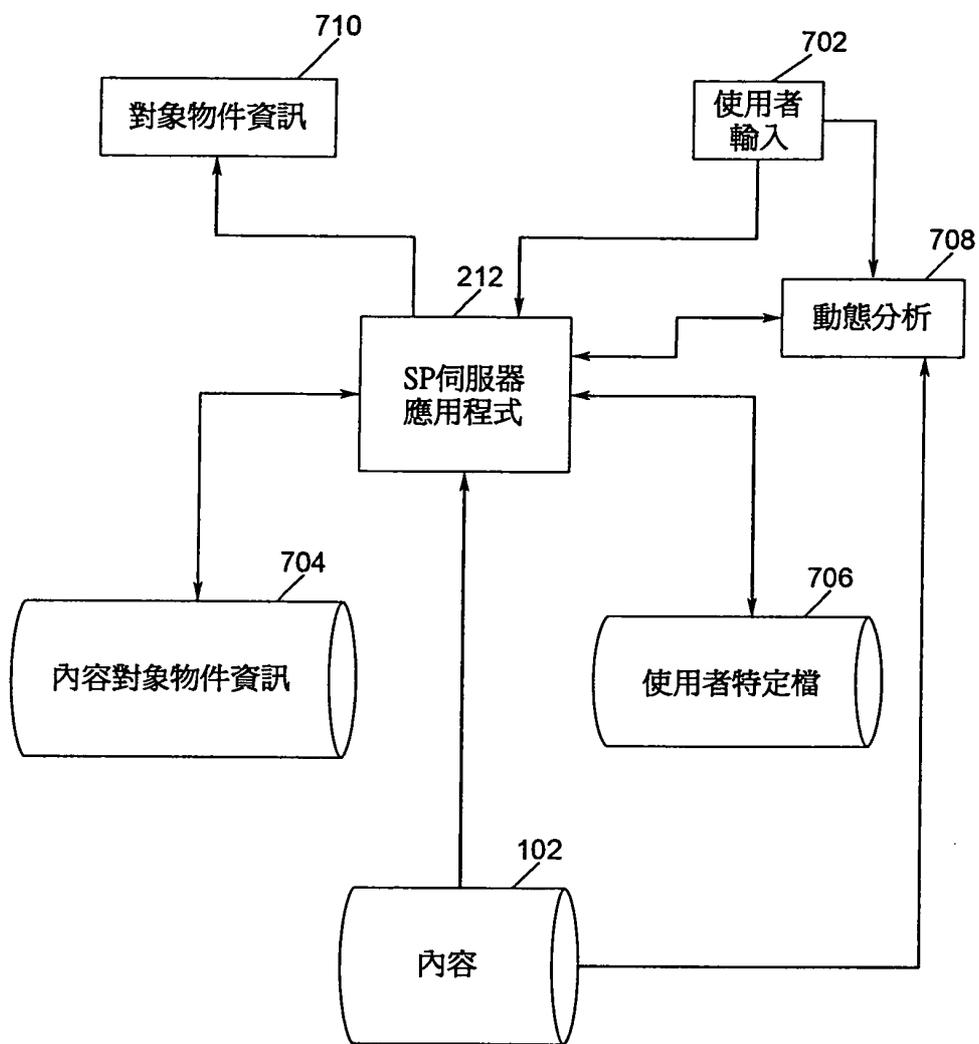


圖7

四、指定代表圖：

(一) 本案指定代表圖為：第(1)圖。

(二) 本代表圖之元件符號簡單說明：

100：安全內容處理管線

101：客戶計算系統

102：內容

104：服務供應商伺服器

106：內容保護技術

108：安全處理器

110：內容保護處理

112：受保護的晶片對晶片互連

114：整合型圖形引擎

116：硬體受保護的資料路徑

118：顯示器

120：受保護的有線/無線顯示器鏈結

121：解碼器邏輯

123：編碼器邏輯

125：構圖邏輯

127：受保護的無線顯示鏈結