(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 October 2013 (03.10.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/144134 A1

(51) International Patent Classification:
H04L 12/28 (2006.01)

(21) International Application Number:
PCT/EP2013/056382

(22) International Filing Date:
26 March 2013 (26.03.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
P201230492 30 March 2012 (30.03.2012) ES

(71) Applicant: **TELEFONICA, S.A.** [ES/ES]; Telefonica, S.A., Gran Vía, 28, E-28013 Madrid (ES).

(72) Inventors: **FERNÁNDEZ PÉREZ, Mónica**; Telefonica, S.A., Gran Vía, 28, E-28013 Madrid (ES). **CARNERO FERNANDEZ, Miguel Ángel**; Telefonica, S.A, Gran Vía, 28, E-28013 Madrid (ES).

(74) Agent: **GONZALEZ - ALBERTO, Natalia**; Garrigues IP, S.L.P, Hermosilla, 3, E-28001 Madrid (ES).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: A METHOD AND A SYSTEM FOR ACCESS CONTROL FOR UPNP CONTENT

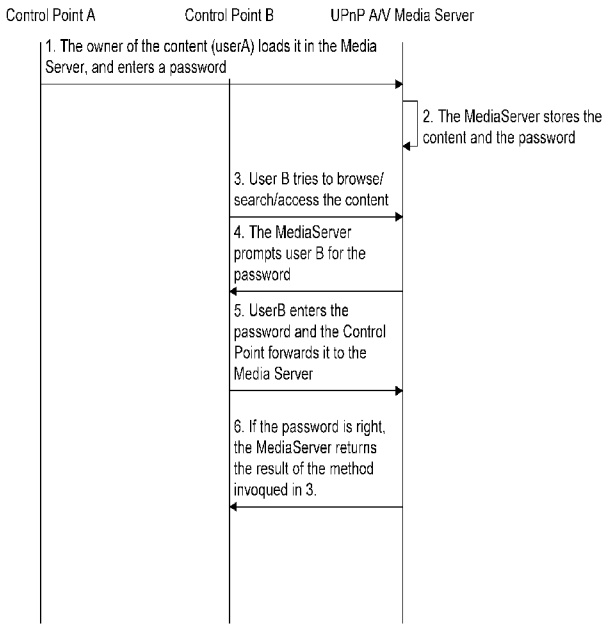

Figure 3

(57) Abstract: The method permitting the protection of an amount of content stored in a UPnP device by a first user, said UPnP device acting as a source of content, comprising: a) loading into said UPnP device, said first user owning said UPnP device, an amount of content and introducing a generated password in said UPnP device; b) requesting, by a control point, for the first user generated password to at least a second user trying to access said amount of content in said UPnP device, c) forwarding said control point to said UPnP device, a password introduced by said second user in response to said request; and d) the access to said amount of content loaded by said first user owning said UPnP device being granted to said at least second user if said password introduced by said second user corresponds to said generated password introduced by said first user. The system of the invention is arranged to implement the method of the invention.

WO 2013/144134 A1

A Method and a System for Access Control for UPnP Content

Field of the art

The present invention generally relates, in a first aspect, to a method for access control for UPnP content, and more particularly to a method enhancing UPnP A/V standard by providing to the end user the tools to provide specific multimedia content protection.

A second aspect of the invention relates to a system arranged to implement the method of the first aspect.

By means of not using the concept of user in UPnP architecture it will be understood that users don't select which devices and control points are allowed to access other devices according to UPnP protocol. UPnP protocol doesn't implement the 'user' concept, nor any mechanism to restrict the access to specific content stored in an UPnP device.

Prior State of the Art

In this digital content era, in which multimedia content is exploding, and there are myriads of devices supporting its storage, distribution and visualization, the Universal Plug and Play Forum (UPnP Forum) has become a de-facto SDO for the definition of a standard enabling easy discovery, configuration and connection of multimedia devices, and easy exchange of content among them.

UPnP Forum has developed a general framework architecture [1] on which the definition of the different devices and the services they support is based. Different classes of devices (Content Media Servers and Renderers, Digital Security Cameras, Printers, etc.) and the standard services they should offer have also been defined, and the standard is being widely adopted by the industry.

Moreover, the Digital Living Network Alliance (DLNA) has used UPnP as the reference standard for multimedia content exchange among devices, and very relevant CE manufacturers (Sony, Samsung, Toshiba, Panasonic…) are already selling their DLNA devices in retail shops.

The UPnP Device Architecture, which is the general framework for the devices definition, consists of a set of protocols for communication between controllers (Control Points) and devices. For device discovery, description, control, eventing and presentation it uses the protocol stack depicted in Figure 1.

As it can be seen, the protocol stack leans on TCP/IP and UDP/IP protocols. It defines UPnP specific protocols like the Simple Service Discovery Protocol (SSDP) for

device discovery, the General Event Notification Architecture (GENA) for eventing, and a specific multicast protocol. Above them stand the UPnP Device Architecture and the UPnP-specific protocols, as defined by UPnP working committees.

Controlled devices function in the role of a server, responding to requests from Control Points. Multiple Media Servers, Control Points or both may be operating in the same physical hardware simultaneously.

The present invention is focused on a specific set of devices, which are the Media Servers. These devices are defined in the UPnP A/V workgroup, and a general overview of their architecture can be seen in [2]. The typical A/V device interaction model can be seen in Figure 2.

An A/V Control Point is able to interact with two or more UPnP devices (acting as source or sink of multimedia content), coordinating and synchronising the behaviour of these devices. Its mission is to discover the devices, configure them as needed, and trigger the content flow. Afterwards, the devices interact directly to exchange the content using an “out-of-band” communication protocol (usually, HTTP).

As shown in the figure, three entities are defined in UPnP A/V: the Control Point, the Media Server (source of content) and the Media Renderer (sink for the content). These entities can be integrated in a single hardware device, or distributed among several hardware devices. For instance, a hardware that integrates a Media Renderer with a Control Point is usually called a Media Player.

UPnP A/V defines [2], a set of services (name, purpose, methods, eventing) that each of these entities must implement, as well as the interaction flow between the entities for content exchange. These services are:

- Media Server
  - Content Directory Service: provides a set of actions that allow the Control Point to enumerate the content that the Server can provide to the home network (browse, list, search…)
  - Connection Manager Service: used to manage the connections associated with a particular device
  - AV Transport Service (optional): used to control the “playback” of the content (play, stop, pause, rewind…)
- Media Renderer
  - Rendering Control Service: provides a set of actions that allow the Control Point to control how the Renderer renders a piece of incoming content (eg. brightness, contrast, etc.)

- Connection Manager Service: as in the former case, it manages the connections associated with a device
- AV Transport Service (optional): used by the Control Point to control the flow of the associated content (play, stop, pause, seek…)

Moreover, UPnP A/V defines the XML schemas for the device, service and content definition.

The latest version of an UPnP A/V Media Server can be found in [3]. Following this specification, a Media Server is able to expose its content via the Content Directory Service, negotiate a common transfer protocol and data format with a Media Renderer, control the content flow, copy content from other devices, and may provide functions to record content using the Scheduled Recording service. It can handle any specific type of media, any data format, and transfer protocol.

Example instances of a Media Server include devices such as CD Players, DVD Players, still-image cameras, hard disks, etc. UPnP offers a certification program, based on a very easy six-step process. This program is offered to Implementer Members only, and grants a certificate assuring that the device fulfils UPnP specifications. There are already lots of devices in the mass-market that own the UPnP certificate. For instance, Motorola, Technicolor, Sony Ericsson, Thomson, Acer, Nokia, Toshiba, Cyberlink, etc. offer certified devices implementing this standard (more products can be found in [4]).

The standard proposed by UPnP Forum for A/V content works pretty well in in-home environments (that is, in the scope of the home LAN) and it really meets its goal of enabling easy discovery, configuration and connection of multimedia devices, and easy exchange of content among them.

Nevertheless, it has one major security flaw that prevents its usage among some advanced users.

UPnP has defined Device Security [5] and Security Console [6]. The main idea of these services is to restrict the access to the Media Servers/Renderers to certain pre-authorized Control Points. There are some patents that refer to this pre-authorized control points security design, US 2009/0103557, US 2010/0312826 and WO 2010/021502. Another proposed solution is the patent WO 2009/131798 consisting on creating User Access Lists to different contents or folders in order to give permissions for accessing Contents or Devices. But this solution, besides needing more complex protocol architecture, would change the current UPnP operation requesting a user authentication to use the UPnP Control Points. In the referenced documents, UPnP

proposes the implementation of a Security Console that offers the users the possibility to select manually which devices and Control Points are allowed to access other devices.

UPnP doesn't implement the "user" concept, nor any mechanism to restrict the access to specific content stored in an UPnP Media Server. All UPnP A/V devices expose the same functionality and content to all the users that obtain access to it through the corresponding Control Point.

For instance, an example where UPnP doesn't provide a solution is in the case where a family with several members owning a single Network Hard Drive that acts like an UPnP A/V Media Server, in which they store all the personal multimedia content (eg. photos, videos, etc) from all the members of the family. Any person obtaining access to any standard Control Point available in the home (for instance, a TV or a PC that implements an UPnP Media Player) could then browse and view the entire content catalogue, with no restrictions. This could be not desirable in certain situations (for instance, the parents would not like their son's friends to view some personal photos). Moreover, even in the case that each member of the family owns it's personal Network Hard Drive, once it is plugged into the home network any standard Control Point could navigate and view all the stored content.

With the current architecture and previously related patents, UPnP allows to limit (or to control) which Control Points can access a specific device. However, it doesn't provide a solution for the above described scenario: once a Control Point is granted access to an UPnP device, any person using this Control Point could access all the content stored in the UPnP device.

Summary of the Invention

It is necessary to offer an alternative to the state of the art which covers the gaps found therein, particularly those related to the lack of proposals which allow the easy access control to the content stored in an UPnP device, without introducing the concept of the user in the UPnP Architecture.

On contrary to the known proposals, the present invention relates, in a first aspect, to a method for access control for Universal Plug and Play (UPnP) content, permitting the protection of an amount of content stored in a UPnP device by a first user, said UPnP device acting as a source of content, said method comprising:

a) loading into said UPnP device, said first user owning said UPnP device, an amount of content and introducing a generated password in said UPnP device;

b) requesting, by a control point, for the first user generated password to at least a second user trying to access said amount of content in said UPnP device,

c) forwarding said control point to said UPnP device, a password introduced by said second user in response to said request; and

d) the access to said amount of content loaded by said first user owning said UPnP device being granted to said at least second user if said password introduced by said second user corresponds to said generated password introduced by said first user.

Other embodiments of the method of the first aspect of the invention are described according to appended claims 2 to 9, and in a subsequent section related to the detailed description of several embodiments.

A second aspect of the present invention concerns to a system adapted to implement the method of the first aspect. The system comprising:

- a media server device, acting as a source of content, wherein an amount of content and a user password are stored;
- a media renderer device, acting as a sink of content; and
- at least a control point, acting as a network element, arranged to enable the connectivity between said source and said sink of content, and allowing a sharing of said content stored in said media server device between said source and said sink by means of a password protection.

Other embodiments of the system of the second aspect of the invention are described according to appended claims 11 to 15, and in a subsequent section related to the detailed description of several embodiments.

Brief Description of the Drawings

The previous and other advantages and features will be more fully understood from the following detailed description of embodiments, with reference to the attached, which must be considered in an illustrative and non-limiting manner, in which:

Figure 1, shows an embodiment of the UPnP Protocol Stack.

Figure 2, shows an embodiment of the typical A/V device interaction model.

Figure 3, shows the general description of the operation flow, according to an embodiment of the present invention.

Figure 4, illustrates the proposed 3-Box model system based in UPnP A/V's general device architecture, according to an embodiment of the present invention.

Figure 5, illustrates an example of the password-protected content creation.

Figure 6, illustrates an example of the browsing through a password-protected element.

Figure 7, Figure 8 and Figure 9 represent several possible embodiments using wide variety of UPnP devices that the present invention can implement.

Detailed Description of Several Embodiments

The present invention enhances UPnP A/V standard to introduce a simple mechanism for access control in order to avoid indiscriminate access to multimedia content.

The simplest mechanism to achieve this without introducing the "user" concept (that has multiple implications and is not compatible with the simplicity that UPnP pursues) is to provide to the end user the tools to protect specific content (either an individual one or a set of contents stored in a folder) by a user-defined password.

This way, the owner of a content stored in an UPnP A/V Media Server has the means to introduce a personal password to his content (or to a set of contents, stored in a folder) that could be distributed to their authorized users.

If any Control Point tries to access the content (or the folder), the Media Server will notify about the fact of the content being password-protected. The Control Point should then prompt the end user for the password. If the user trying to access the content enters the right password, access will be granted. If not, the Control Point will not be able to browse or search through the folder/content. A general description of the operation flow is shown in Figure 3.

1) The owner of the content (user A) loads it in the UPnP A/V Media Server, and enters the access password. The password could affect either individual content (a single multimedia file) or a set of contents (folder). Afterwards, by some off-line methods (out of the scope of this invention), he communicates this password to the people authorized to view/browse/search this content/folder.
2) The UPnP A/V Media Server stores both the content and the password, encrypted by a secure mean.
3) Another user (UserB) tries to view/browse/search (in short, to interact) with the protected content/folder.

4) The UPnP A/V Media Server detects that the content/folder is password protected, and asks the Control Point for the password.
5) The Control Point prompts UserB for the password. Once the user enters the password, the Control Point forwards it to the UPnP A/V Media Server, encrypted by a secure mean.
6) The UPnP A/V Media Server checks if the access password is right. If so, it will return to the Control Point the answer to the method invoked in 3). If not, it will return an “access denied” message and deny the access to the requested content/folder.

As stated in previous sections, the present invention goal is to enable multimedia content protection by a user-generated password. To achieve this, the system on Figure 4is proposed:

The proposed system is based in UPnP A/V’s general device architecture (3-Box model) in which, for content playback, three entities are defined:

- An UPnP A/V Media Server, which is the entity in charge for content storage and publication, as defined in UPnP. This entity will be extended to support the storage, by a secure mean, of the password that protects the contents from undesired access. To this end, the Content Directory Service must be changed as specified in the following paragraphs.
- An UPnP A/V Media Renderer, which is the entity in charge for content viewing. This entity will remain unchanged, as specified in UPnP standards
- An UPnP Control Point, which is the entity that offers the User Interface, allowing the end user to discover the UPnP A/V devices available in the home network, browse or search through the content catalogue of the UPnP A/V Media Servers, and send its content to the UPnP A/V Media Renderer. This entity makes use of standard UPnP services offered by the other entities (i.e. Content Directory Service, Rendering Control Service, Connection Manager Service, A/V Transport Service) to perform its functions, but neither its software architecture nor its technologies are defined by UPnP, nor will be defined in the scope of this invention. However, this entity must be also enhanced to be able to support content protection, as will be seen in the next sections.

The following enhancements must be done in the UPnP A/V Media Server:

The Content Directory Service must be modified to support the introduction of a password to access a content / folder. To this end, the following changes must be done:

- Add to the Browse() method the following action arguments:
  - Password: password to access the specified ObjectID through which the Control Point wants to browse, encrypted by a secure mean (eg. hash code of the original password entered by the end user in the Control Point interface, and communicated through an out-of-band mechanism).
  - Modify the Browse() method so that it returns a new error code:

Error Code	Error Description	Description
721	Password required	The Control Point must enter a password to browse through the specified ObjectID

Password-protected content creation

The message flow for the following use case can be seen in Figure 5.

- The Control Point invokes the CreateObject() method. The container/item elements that describe the content to be loaded into the Media Server include the password that must be entered to browse/search/view the content. The password is communicated to the Media Server through a secure way (e.g. hash key)
- The Media Server stores the content, together with the password, in its hardware, and returns to the Control Point information about the result of this operation.

Browsing through a folder with password-protection

- The Control Point invokes the Browse() method on an ObjectID existing in the Media Server. The password attribute in the container/item object is empty, but the object needs a password to allow browsing.
- The Media Server detects that a Control Point is trying to navigate through an object that is protected, and returns an error indicating this fact.
- The user is prompted by the Control Point to enter the password.
- Once the user has loaded the password, the Control Point invokes again the Browse() method, this time including the password loaded by the user in the password attribute of the container/item. The password is communicated to the Media Server through a secure mean (e.g. hash key)

- The Media Server checks that the password is right, and returns the corresponding result to the Control Point, so that it can be shown to the user.

The present invention can be implemented in a wide variety of UPnP devices. Multiple combinations of UPnP elements can be designed to provide additional security facilities to in-home UPnP devices and services. In the following a list of possible embodiment are provided.

Content stored in standard A/V devices:

This embodiment takes into account the standard A/V devices that could include the proposed invention. The modem-router acts as the network element that enables the connectivity between all the in-home devices. It usually includes a WiFi AP in order to enable wireless connectivity among them (although the WiFi AP could be available in dedicated network equipment)

In this case, a NAS (Network Attached Storage device, i.e. a networked hard disk), a standard PC or a mobile phone could act as source of content (that is, A/V Media Servers). As such, they would be the points where the content and the passwords that protect it are stored. They would also include the UPnP Content Directory Service, with the modifications needed to implement the functionality described by this present invention.

Multiple devices could act as sinks of content (that is, the point where the content is viewed): a TV, a photo frame, a BluRay/DVD player or a set-top-bow. As such, these devices render the desired content once the Media Server / Control Point has checked that the right password has been entered (if the content is password-protected).

The Control Point, in charge of the interaction with the end-user (since it provides the GUI) could be either an application downloaded in the PC and/or the Mobile Phone, or could be embedded in the sinks of content. In this last case, and given the nature of the Media Renderers, the most usual situation is to have a remote control through which the user can interact with a specific menu to navigate through the content, introduce the requested data, and control the content rendering (stop, play, pause…).

Content stored in Game Consoles

An alternative embodiment for this system could lean on the usage of Game Consoles as source of content. In this case, as in the previous one, the modem-router acts as the network element that enables the connectivity between all the in-home devices.

A Game Console acts as the source of content, that is, the point where the multimedia data to be shared in the home network is stored. It will include the UPnP Content Directory Service with the modifications described in this invention to protect specific data from undesired access. In this embodiment, the sinks of content would naturally be the TV and the user's PC. They are in charge of rendering the desired content once the right password is entered.

The Control Point, with the modifications proposed in this invention, would be integrated in the Remote Control and specific software of the Game Console. The Remote Control will enable the navigation through the content stored in the Game Console, and the GUI provided by the Game Console will include a Control Point responsible for user prompting for the password, and its communication to the Content Directory Service.

Content available in Digital Security Cameras

Finally, an embodiment based on the usage of IP Cameras (Digital Security Cameras) is proposed.

The modem-router acts also as the network element that enables the connectivity between all the in-home devices.

A number of IP Cameras act as source of content, offering both still images and video streams. They will include a specific service modified, following the system description of this invention, to grant access to the images/streams only if the right password is provided.

In this embodiment, the sinks of content would be the TV, the user's PC and mobile phones available in the home network. They are in charge of rendering the desired content once the right password is entered.

The Control Point, with the modifications proposed in this invention, would be integrated in the rendering devices (i.e. the sinks of content, TV, PC and mobile phone).

In the case of the PC and the mobile phone, a specific software module will be in charge of offering the GUI, prompt the user for the password (when required) and communicate with the IP cameras following the system description of this invention.

In the case of the TV, the Control Point will be composed of a Remote Control and a specific set of menus that, besides running the standard UPnP actions, is modified to enable user prompting for the password, password introduction, and management of the interactions with the IP Cameras.

Advantages of the Invention

As explained before, one of the main drawbacks of UPnP architecture, which prevents its adoption among advanced users concerned with security, is the lack of mechanisms to avoid undesired access to content stored in UPnP devices. Currently, once a user has gained access to the home LAN, if he owns a standard UPnP Control Point he can browse and access any content available in any UPnP device connected to the home LAN.

The main technical advantage of this invention is to propose a system to enable easy content protection for content exported through UPnP services. This functionality is not available today and is expected to be welcomed by end users.

An additional advantage of the system proposed is its seamless integration into current UPnP architecture, so that it could be incorporated into a wide variety of devices (see the proposed embodiments) with relative ease and no big development effort (for instance, for A/V Media Servers a firmware update could be enough to provide this functionality).

Finally, another advantage is its alignment with UPnP focus and requirements. One of the main ideas of this architecture is its ease of usage (the “plug and play” concept). The invention proposed is easy to understand and to use by the end user, so that it doesn’t contradict UPnP principles and its adoption by end-users is facilitated.

ACRONYMS

ACL	Access Control List
AP	Access Point
CE	Consumer Electronics
DLNA	Digital Living Network Alliance
DVD	Digital Versatile Disc (formerly Digital Video Disc)
GENA	General Event Notification Architecture
GUI	Graphic User Interface
HTTP	Hypertext Transfer Protocol
ID	Identifier
IP	Internet Protocol
LAN	Local Area Network
NAS	Network Attached Storage
PLC	Power Line Communications
SDO	Standard Development Organization
SOAP	Simple Object Access Protocol
SSDP	Simple Service Discovery Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
WiFi	Wireless fidelity

REFERENCES

[1] UPnP Device Architecture, version 1.1, http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf

[2] UPnP AV Architecture:1, http://upnp.org/specs/av/UPnP-av-AVArchitecture-v1.pdf

[3] MediaServer:3, http://upnp.org/specs/av/UPnP-av-MediaServer-v3-Device.pdf

[4] UPnP Forum page for Certified Product Registry, http://upnp.org/sdcps-and-certification/certification/certified-product-registry/

[5] DeviceSecurity:1, http://upnp.org/specs/sec/UPnP-sec-DeviceSecurity-v1-Service.pdf

[6] SecurityConsole:1, http://upnp.org/specs/sec/UPnP-sec-SecurityConsole-v1-Service.pdf

Claims

1.- A method for access control for Universal Plug and Play (UPnP) content, permitting the protection of an amount of content stored in a UPnP device by a first user, said UPnP device acting as a source of content, characterised in that it comprises:

a) loading into said UPnP device, said first user owning said UPnP device, an amount of content and introducing a generated password in said UPnP device;

b) requesting, by a control point, for the first user generated password to at least a second user trying to access said amount of content in said UPnP device,

c) forwarding said control point to said UPnP device, a password introduced by said second user in response to said request; and

d) the access to said amount of content loaded by said first user owning said UPnP device being granted to said at least second user if said password introduced by said second user corresponds to said generated password introduced by said first user.

2.- The method of claim 1, wherein said amount of content stored in said UPnP device is any type of multimedia content.

3.- The method of claim 1, wherein if said password introduced for said at least a second user doesn't corresponds with said first user generated password not allowing a browsing, by said control point used by said at least a second user, through said amount of content.

4.- The method of claim 1, wherein said UPnP device comprises an UPnP A/V Media Server.

5.- The method of claim 6, comprising modifying a content directory service of said UPnP A/V Media Server for supporting said first user generated password introduction.

6.- The method of claim 7, further comprising encrypting said first user generated password by means of security.

7.- The method of claim 6, wherein said first user generated password encrypted comprises a hash code of said first user generated password.

8.- The method of claim 5, comprising returning an error code to said control point regarding the use of said first user generated password.

9.- A system for enabling access control in UPnP devices, comprising:

- a media server device, acting as a source of content, wherein an amount of content and a user password are stored;

- a media renderer device, acting as a sink of content; and
- at least one control point, acting as a network element, arranged to enable the connectivity between said source and said sink of content,

wherein said at least one control point allows a sharing of said content stored in said media server device between said source and said sink by means of a password protection.

10.- The system of claim 9, wherein said system implements a method according to any of the previous claims.

11.- The system of claim 9, wherein said media server comprises a device with multimedia capacity.

12.- The system of claim 9, wherein said control point is arranged for being integrated in said media renderer device.

13.- The system of claim 12, wherein said media renderer device comprises said control point.

14.- The system of claim 9, wherein said control point is arranged for being integrated in said media server device.

15.- The system of claim 14, wherein said media server device comprises said control point.

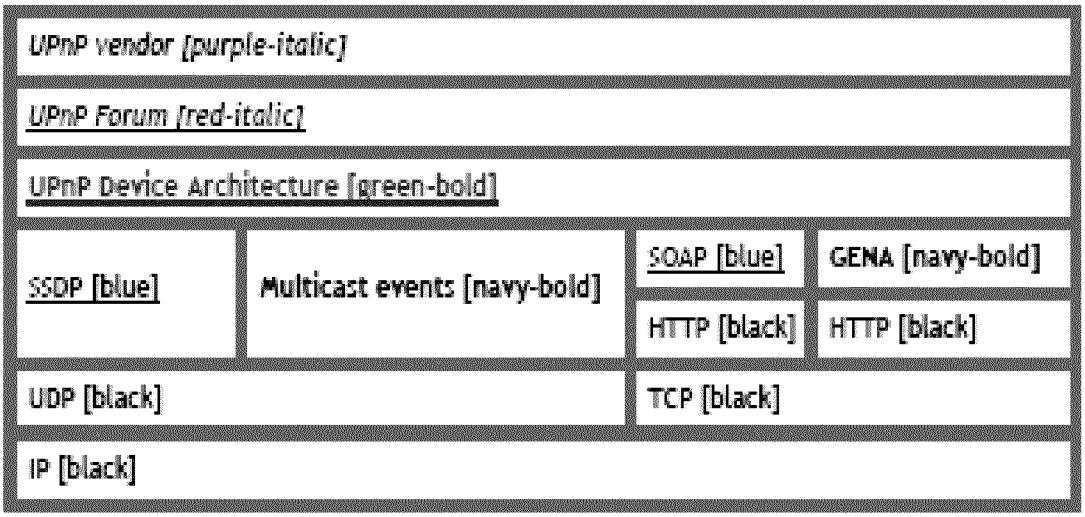

Figure 1

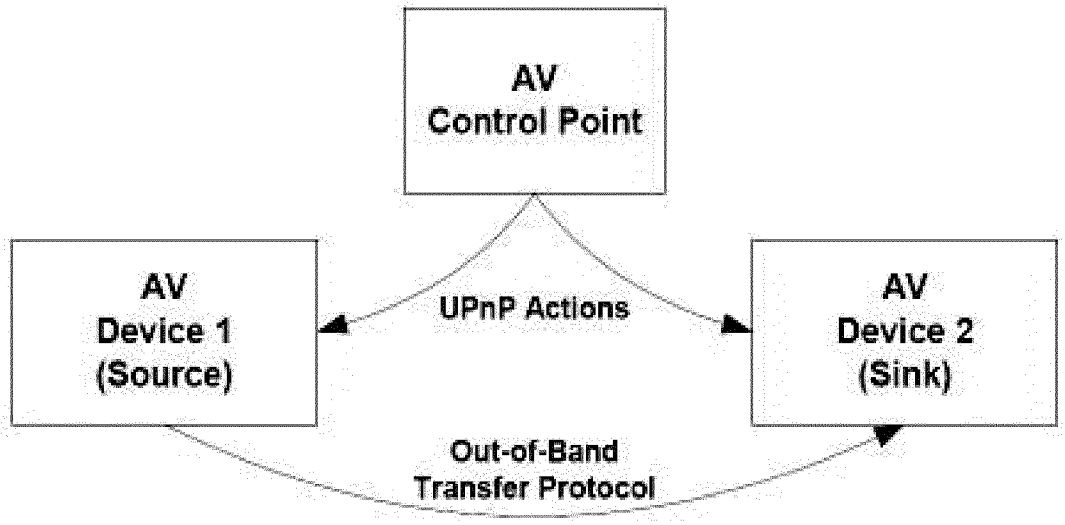

Figure 2

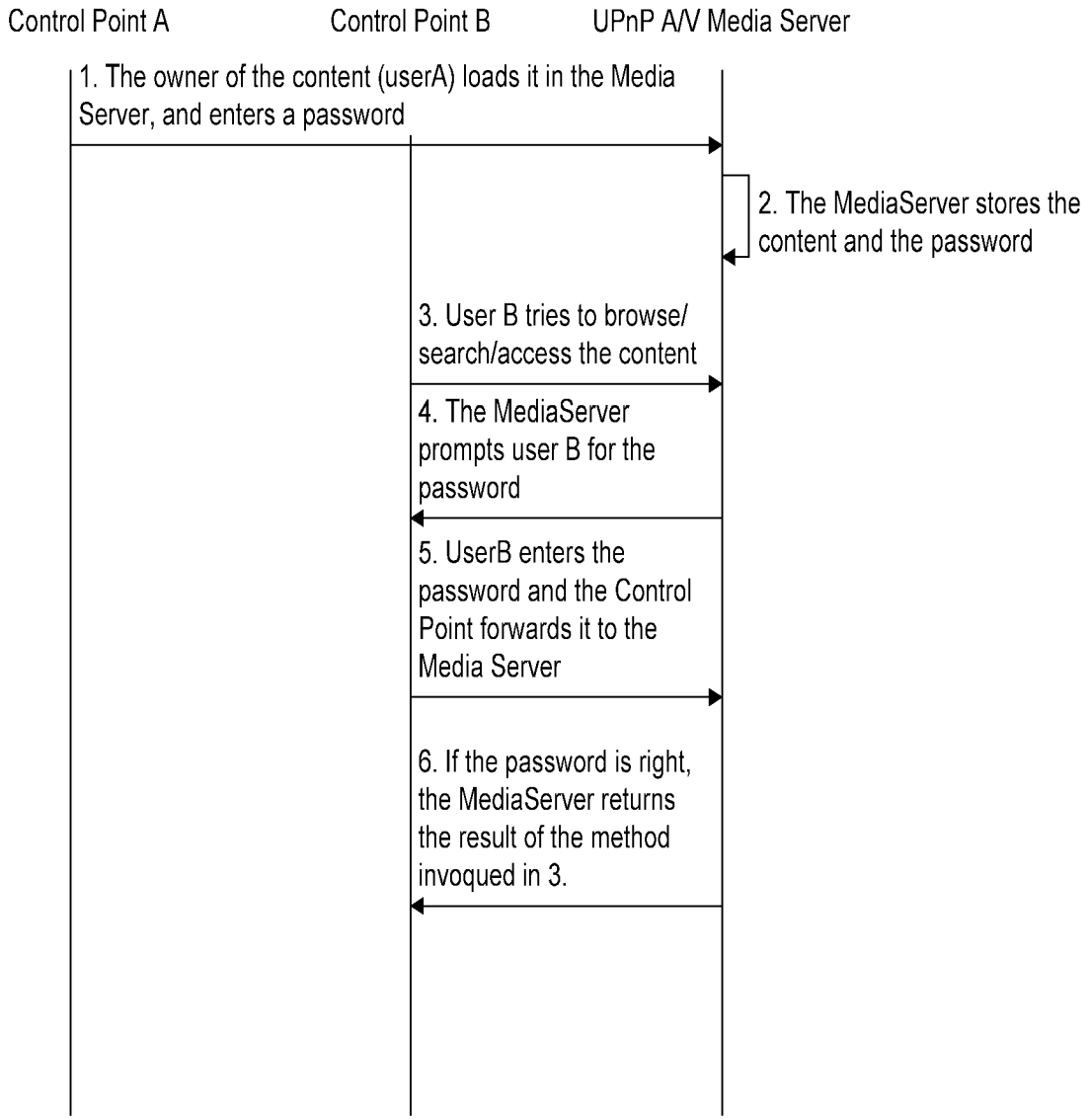
Control Point A
Control Point B
UPnP A/V Media Server
1. The owner of the content (userA) loads it in the Media Server, and enters a password
2. The MediaServer stores the content and the password
3. User B tries to browse/ search/access the content
4. The MediaServer prompts user B for the password
5. UserB enters the password and the Control Point forwards it to the Media Server
6. If the password is right, the MediaServer returns the result of the method invoqued in 3.

Figure 3

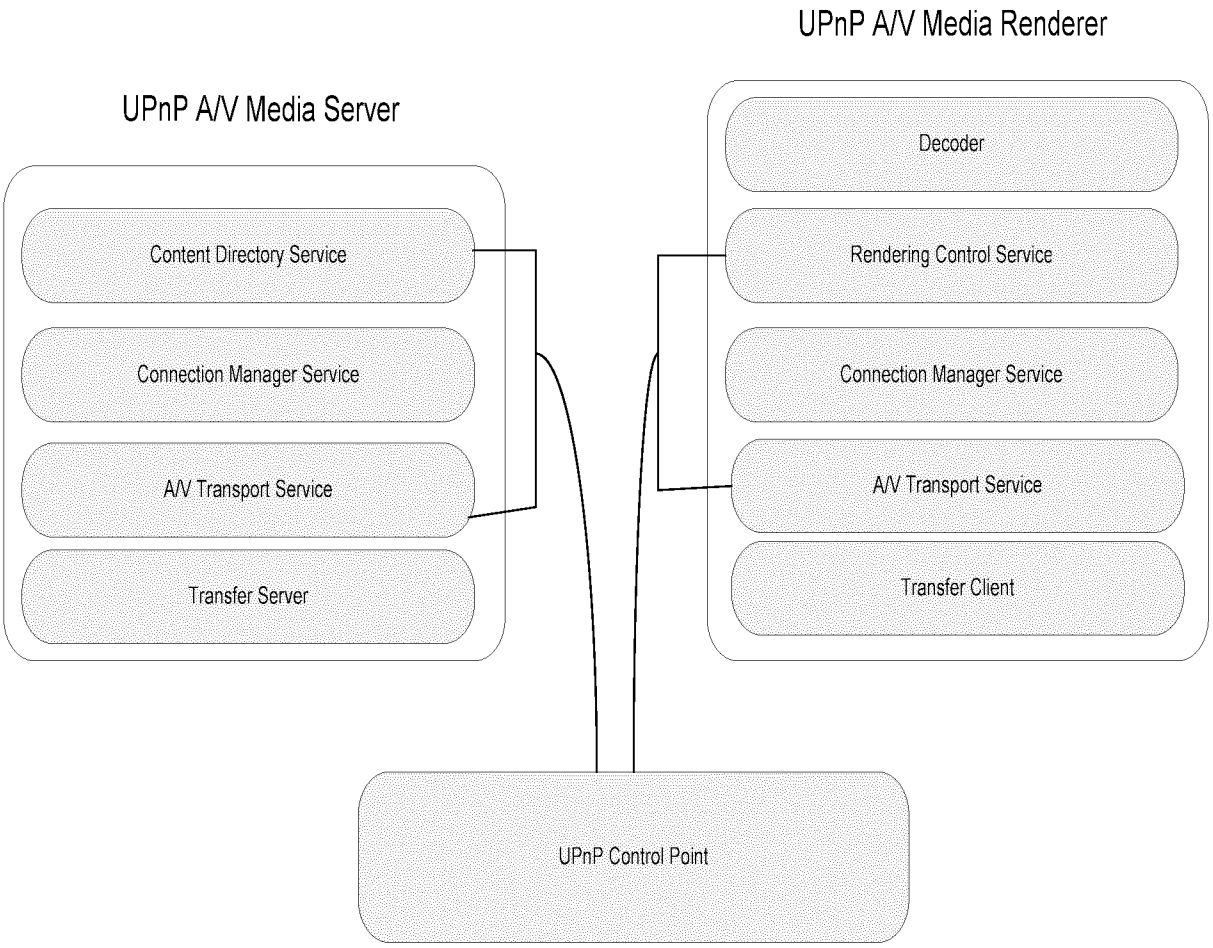

Figure 4

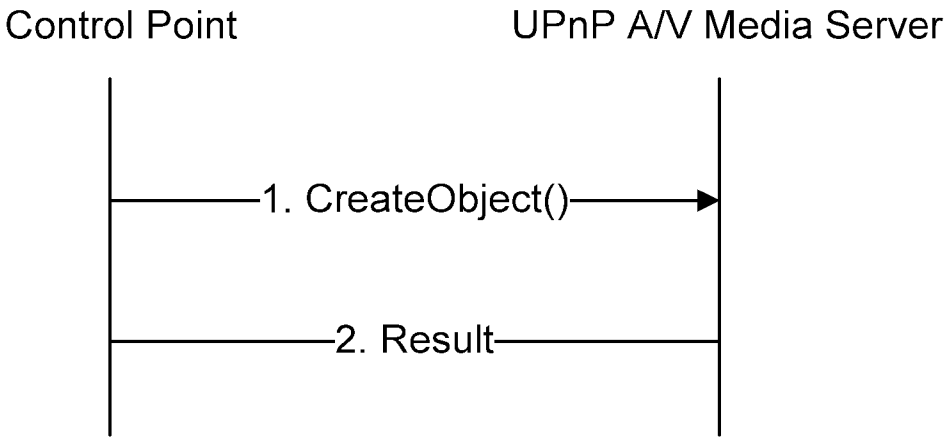

Figure 5

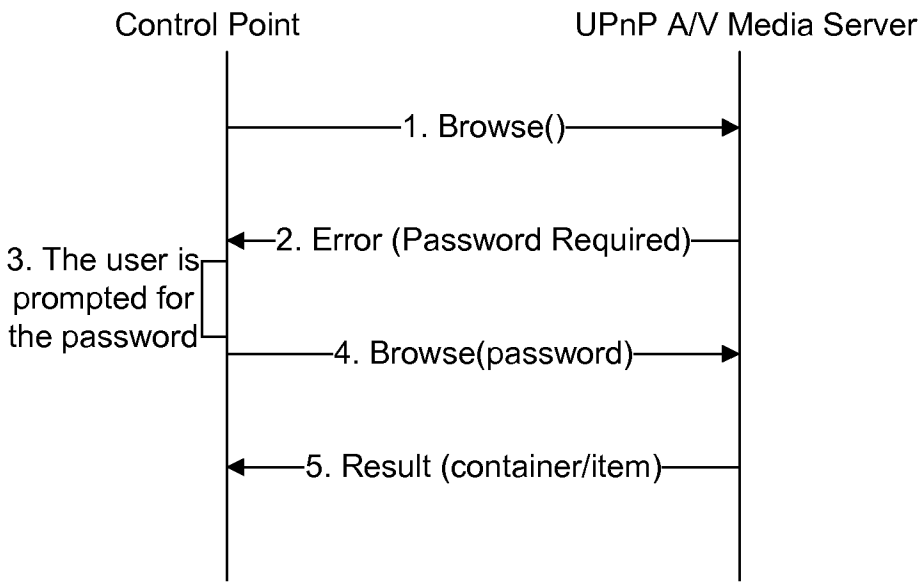

Figure 6

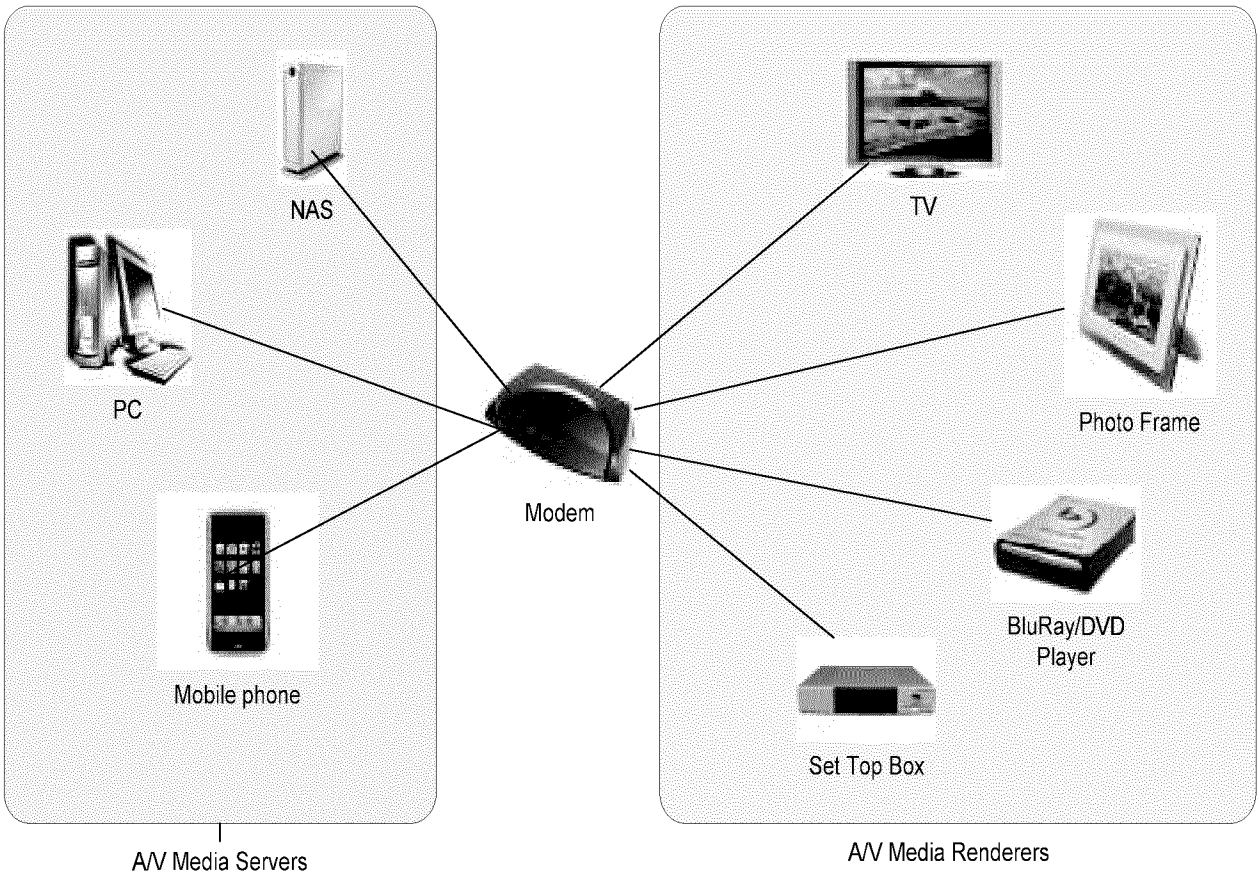

Figure 7

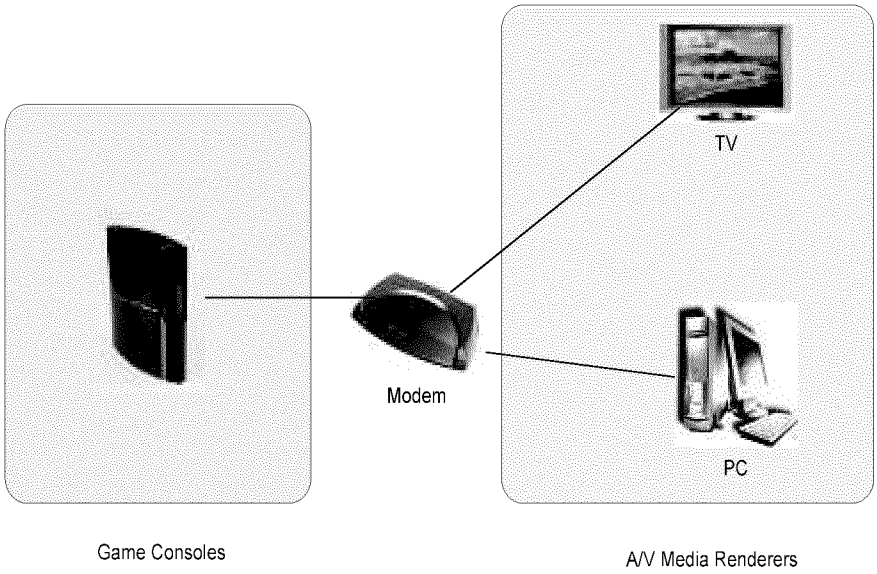

Figure 8

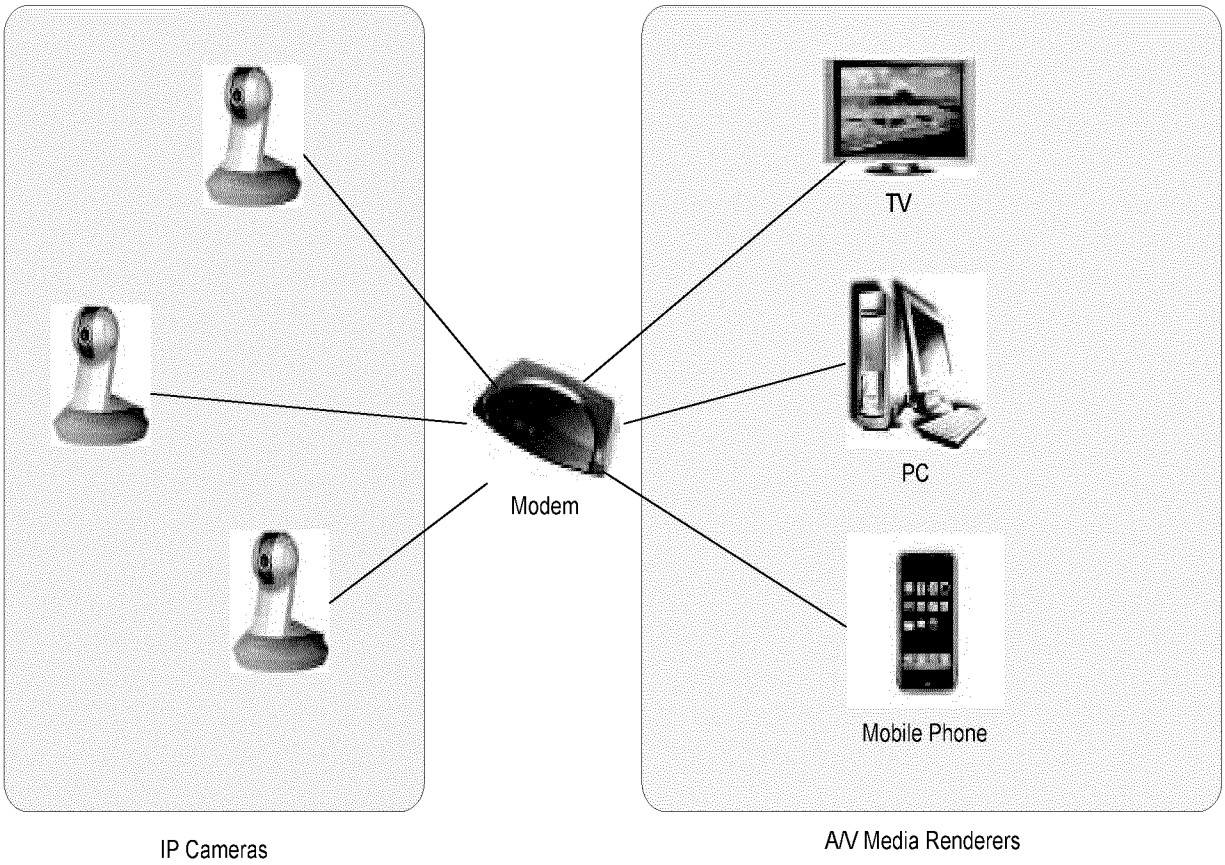

Figure 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/056382

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/28
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/077207 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; BODLAENDER MAARTEN P [NL]) 10 September 2004 (2004-09-10) abstract page 1, line 20 - line 21 page 2, line 1 - line 2 page 2, line 6 - line 7 page 2, line 31 - line 32 page 3, line 1 - line 31 page 4, line 5 - line 7 page 4, line 11 - line 12 page 7, line 1 - line 26 page 8, line 6 - line 27 page 8, line 31 - line 35 page 9, line 4 - page 10, line 4 page 10, line 10 - line 14 page 10, line 19 - line 23 -----	1-15

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 May 2013	03/06/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Martinozzi, A

1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/056382

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2004/114597 A1 (KONINKL PHILIPS ELECTRONICS NV [NL]; VAN GASSEL JOZEF P [NL]; VAN DEN) 29 December 2004 (2004-12-29) abstract page 1, line 2 - line 4 page 1, line 12 - line 15 page 2, line 19 - line 28 page 2, line 33 - page 3, line 5 page 3, line 12 - line 14 page 3, line 24 - line 29 page 4, line 1 - line 3 page 4, line 22 - line 24 page 4, line 33 - page 5, line 11 page 5, line 22 - line 32 page 6, line 8 - line 10 page 6, line 21 - line 31 page 7, line 8 - line 19 -----	1-15
A	WO 2012/010803 A1 (FRANCE TELECOM [FR]; AGRO ROBERTO [FR]; VINCENT YOANN [FR]) 26 January 2012 (2012-01-26) abstract page 2, line 4 - line 15 page 2, line 26 - page 3, line 11 page 3, line 19 - line 23 page 6, line 10 - page 7, line 10 page 7, line 20 - line 28 page 7, line 34 - page 8, line 33 page 10, line 16 - line 24 page 12, line 16 - line 30 page 13, line 22 - line 28 page 15, line 14 - line 33 -----	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/056382

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004077207 A2	10-09-2004	CN 1757033 A	05-04-2006
		EP 1599812 A2	30-11-2005
		JP 2006520496 A	07-09-2006
		KR 20050113626 A	02-12-2005
		US 2006168000 A1	27-07-2006
		WO 2004077207 A2	10-09-2004
WO 2004114597 A1	29-12-2004	CN 1809991 A	26-07-2006
		EP 1642415 A1	05-04-2006
		JP 2007521551 A	02-08-2007
		KR 20060033735 A	19-04-2006
		US 2006179138 A1	10-08-2006
		WO 2004114597 A1	29-12-2004
WO 2012010803 A1	26-01-2012	FR 2964523 A1	09-03-2012
		WO 2012010803 A1	26-01-2012