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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 December 2006 (07.12.2006)

PCT

(10) International Publication Number
WO 2006/129251 A2

(51) International Patent Classification:
G06F 21/00 (2006.01) *G06F 21/20* (2006.01)

(21) International Application Number:
PCT/IB2006/051669

(22) International Filing Date: 25 May 2006 (25.05.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
200510074256.8 3 June 2005 (03.06.2005) CN

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **QU, Jin** [CN/CN]; Philips Electronics China, 21/f Kerry Office Building 218 Tian Mu, Xi Road, Shanghai 200070 (CN). **MA, Fulong** [CN/CN]; Philips Electronics China, 21/f Kerry Office Building 218 Tian Mu, Xi Road, Shanghai 200070 (CN).

(74) Common Representative: **KONINKLIJKE PHILIPS ELECTRONICS N.V.**; c/o HAQUE, Azir, Philips Electronics China, 21/f Kerry, Office Building, 218 Tian Mu Xi Lu Road, Shanghai 200070 (CN).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

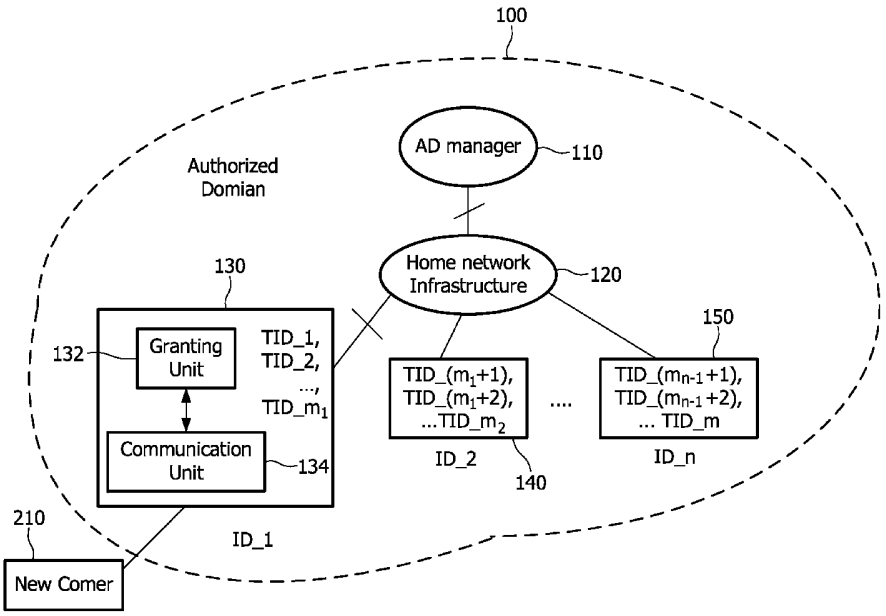
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** METHOD AND APPARATUS FOR ENROLLING A TEMPORARY MEMBER OF AN AUTHORIZED DOMAIN



(57) **Abstract:** The present invention provides a method / an apparatus for enrolling a member of an authorized domain. The method comprises receiving a request form a device for joining the AD, and granting a temporary certificate to the device according to a predetermined rule, whereby the device becomes the member of the AD, wherein the temporary certificate is issued by a manager of the AD beforehand. In this way, a new comer still could be enrolled as a member of the AD even if the AD manager is not available.

WO 2006/129251 A2

METHOD AND APPARATUS FOR ENROLLING A TEMPORARY MEMBER OF AN AUTHORIZED DOMAIN

FIELD OF THE INVENTION

This invention relates generally to an authorized domain, and more particularly to enrolling a temporary member of an authorized domain.

BACKGROUND OF THE INVENTION

The concept of Authorized Domains (ADs) tries to find a solution to both serve the interests of the content owners (that want protection of their copyrights) and the content consumers (that want unrestricted use of the content). The basic principle is to have a controlled network environment in which content can be used relatively freely as long as it does not cross the border of the authorized domain. Typically, authorized domains are centered around the home environment, also referred to as home networks.

Of course, other contexts are also possible. A user could fox example take a portable device for audio and/or video with a limited amount of content with him on a trip, and use it in his hotel room and to access or download additional content stored on his personal audio and/or video system at home. Even though the portable device is outside the home network, it is a part of the user's authorized domain. In this way, an Authorized domain (AD) is a system that allows access to content by devices in the domain, but not by any others.

Various proposals exist that implement the concept of authorized domains to some extent. In so-called device based ADs, the domain is formed by a specific set of devices and content. A domain manager (one or more of the devices) controls which devices may join the domain. Only the specific set of devices of the domain is allowed to make use of the content of that domain, e.g. to open, copy, play or export it. Example of such device – based ADs are given in international patent applications WO 03/098931 and WO 04/027588 by the same applicant.

Another type of AD is the so-called person based Authorized Domains, where the domain is based on persons instead of devices. An example of such a system is described in international patent application WO 04/038568 by the same applicant, in which content is coupled to persons, which then are grouped into a domain.

A so-called Hybrid Athorized Domain-based DRM system ties content to a group that may contain devices and persons. This group is typically limited to a household, such that:

1. content can be watched on any of the devices that belongs to the household (e.g. TV in Living, TV in Bedroom, PC),
2. content can be watched by any of the users that belong to the household after they have authenticated themselves on any device (such as a television in a hotel room). Such authentication normally involves a user authentication device such as a smart card. Examples of hybrid AD systems can be found in international patent application serial number PCT/IB2004/051226 and in European patent application serial number 04101256.8 by the same applicant.

Since an Authorized Domain must be limited, this now means that the domain manager must be involved in authenticating a new member (a device or a person), even though this new member is a temporary member, such as a TV set in a hotel. An example of this authentication is a challenge response protocol provided in European patent application serial number EP04105441.2 by the same applicant. This challenge response protocol between a domain manager and a user authentication device such as a smart card, which device is linked to a foreign device, comprises an assertion that the link between the user authentication device and the foreign device is limited in distance.

But, in some circumstances the AD manager of an Authorized Domain is not available, for instance, the AD manager is down. Therefore, there is a need to provide a more flexible mechanism for enrolling a temporary member of an authorized domain that still keeps the domain limited.

SUMMARY OF THE INVENTION

It is an object of the invention to provide a more flexible mechanism for enrolling a temporary member of an authorized domain that still keeps the domain limited.

The object is achieved in a method for enrolling a member of an authorized domain. The method comprises the steps of receiving a request form a device for joining the authorized domain, and granting a temporary certificate to the device according to a predetermined rule, whereby the device becomes the member of the authorized domain, wherein the temporary certificate is issued by a manager of the authorized domain beforehand.

The object is also achieved in an apparatus for enrolling a member of an authorized domain. The apparatus comprises communication means for receiving a request form a device for joining the authorized domain, and granting means for granting a temporary certificate to the device according to a predetermined rule, whereby the device becomes the member of the authorized domain, wherein the temporary certificate is issued by a manager of the authorized domain beforehand.

According to an embodiment of the invention, a manager of an Authorized Domain (AD) issues a number of temporary certificates in advance, and distributes the temporary certificates to the fixed members of the AD. The AD manager could periodically update a list of effective temporary certificates. When a new comer (device or person) requests to join the AD, one of the fixed members could grant one of the temporary certificates to the new comer without any involvement of the AD manager.

By using such a mechanism of issuing some temporary certificates in advance, there is no need to keep the AD manager be available all the times. This invention also reduces the involved parties of the authentication process from 3 to 2, which could further reduce the computer complexity and time/bandwidth consumption of the authentication process.

Other objects and attainments together with a fuller understanding of the invention will become apparent and appreciated by referring to the following description and claims in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

FIG 1 is a schematic diagram of an authorized domain with a number of temporary certificates according to one embodiment of the invention;

FIG 2 is a schematic diagram of an authorized domain enrolling a new comer by using a temporary certificate according to one embodiment of the invention; and

FIG 3 is a schematic diagram of an authorized domain with a temporary member using a temporary certificate according to one embodiment of the invention.

Throughout the drawings, the same reference numerals indicate similar or corresponding features or functions.

DETAILED DESCRIPTION OF THE INVENTION

FIG 1 is a schematic diagram of an authorized domain with a number of temporary certificates according to one embodiment of the invention.

Authorized Domain (AD) 100 includes n members 130, 140, 150 (ID_1, ID_2, … ID_n), a home network infrastructure 120 and an AD manager 110. The members 130, 140, 150 and the AD manager 110 are connected to the home network infrastructure 120 that includes a number of wired/wireless connectors.

The members include devices and users. The devices includes home appliance, such as TV set and audio box, and personal portable electronics product, such as PC, mobile phone and PDA. The users could be represented in the form of a smart card. The members could also only include devices. Likewise the members could only include users.

The AD manager 110 is a home network server. It could also be one of the AD members that are capable of managing the AD.

The AD manager generates m temporary certificates that include:

AD_ID (identification number for AD 100)

TID (identification number for this temporary certificate)

Valid period (period when this temporary certificate is valid)

Signature (signature by the AD manger 110).

The valid period of the temporary certificate could just last for a short time period, for example, a fewer hours or a few days, far shorter than that of a general certificate issued by AD manager 100 to the general member (for example, ID_1), for example, a few years.

The temporary certificate may also include a specific content ID and its corresponding rights, thus by using the temporary certificate only this specific content could be proceeded in the specific way (such as play only, not duplicate) defined in the rights.

The rights could also be included in the user rights issued by the content provider. The user rights may include:

AD_ID (identification number of the AD)

Content_ID (identification number of the content)

Rights for the general members (for example, 1 years, play, edit, duplicate)

Rights for the temporary member (for example, 3 days, maximum 6 times play, no duplication)

Signature (signature by the content provider)

The m temporary certificates are evenly distributed to the n members 130, 140, 150 via the home network infrastructure, for example, TID_1 to TID_m_1 (m_1=m/n) for member 130 (ID_1), TID_(m_1+1) to TID m_2 for ID_2 (m_2=2*m/n), and TID_(m_{n-1}+1) to TID_m for ID_n (m_{n-1}=(n-1)*m/n). It is also understandable that the portable members may obtain more temporary certificates than the non-portable members.

The AD manger could keep a list of issued temporary certificates and its status. When a temporary certificate expires, it will be marked as "expired" or be deleted. The AD manager could also periodically update the list of issued temporary certificates based on the reports coming from the members, for example, change the status of the granted temporary certificate from "available" to "granted" and record the identification of the granted temporary member.

Under some specific situations, The AD manager could revoke the temporary certificates. For example, the member being allocated with some temporary certificates is hackered, or the temporary member is hackered.

FIG 2 is a schematic diagram of an authorized domain enrolling a new comer by using a temporary certificate according to one embodiment of the invention.

The new member 120 is a device that needs to temporary join the AD, such as a TV set in a hotel, an audio player belonging to a friend of the user of the AD.

Authorized Domain (AD) 100 includes n members 130, 140, 150 (ID_1, ID_2, … ID_n), a home network infrastructure 120 and an AD manager 110. The members 140, 150 are connected to the home network infrastructure 120 that includes a number of wired/wireless connectors.

The AD manager 110 is not available for all AD members since it is not connected to the home network infrastructure 120. For instance, the AD manager 110 is down.

The member 130 (ID_1), such as a mobile phone, storing with m_1 temporary certificates (TID_1 to TID_m_1), is not connected with the home network infrastructure 120. For example, there is no wired / wireless connection available for member 130.

The member 130 includes a communication unit 134 and a granting unit 132. The communication unit 134 receives a request form the new comer 210 for joining the authorized domain, and the granting unit 132 grants a temporary certificate, for instance, TID_1, to the new comer 120 based on the request, then the new comer 120 becomes a temporary member of the authorized domain.

The communication unit 134 is a NFC (near field communication) device. It also could be any other wired /wireless transceiver that could communicate with the new comer 210. The request received by the communication unit 134 includes the identification of the new comer 120 (TM_ID), and the request applies for a temporary membership of the AD.

The communication unit 134 also could communication with the AD manager via the home network infrastructure 120 to get the temporary certificates when the AD manager is available.

The granting unit 132 is an agent of the AD 100. to grant a temporary certificate to the new comer 210, whereby the new comer becomes a temporary member of the AD. The granting units 132 adds the identification of the new comer 120 (TM_ID) to the temporary certificate TID_1, thus the temporary TID_1 includes:

AD_ID (identification number for AD 100)

TID_1 (identification number for this temporary certificate)

TM_ID (identification number for this temporary member)

Valid period (period when this temporary certificate is valid)

Signature (signature by the member ID_1).

The granting unit 132 sends the temporary certificate TID_1 to the new comer 210, whereby the new comer becomes a temporary member of the AD.

The granting units 132 also could carry out some other functions, such as authenticating the new comer 120, encrypting the temporary certificate TID_1 by using the public key of the new comer 120, and etc. Since the temporary certificates only last for a short time, the algorithm of authentication, encryption and other security process could be much simpler compared to granting a general certificate to a general member.

There may be several kinds of temporary certificates available for the member 130 to grant, and the granting unit 132 could just randomly select one to grant, or the granting unit 132 could select a temporary certificate to grant for a certain class based on the rules predetermined by the AD manger, for instance, a temporary certificate having 1 valid day for any temporary member in Asia (It is understandable to have a product sold in a specific area carrying a specific prefix of its ID).

The member 130 could also be a smart card that represents a person member of the AD 100. Under this circumstance, the new comer 210 needs to include a card reader (not shown) to communicate with the member 130.

It is understandable that the member 130 could be connected to the home network infrastructure 120. Under this circumstance, the temporary certificates (TID_1 to TID_m_1) do not need to be stored in the member 130, for example, could be stored in the member 150 (ID_n). The member 130 could get the temporary certificate TID_1 that it will grant to the new comer 120 from the member 150 (ID_n).

It is also understandable that the AD manager 110 could be connected to the home network as long as the AD manager 110 issues the temporary certificates in advance and are not involved in the process of granting a temporary certificate from the member 130 to the new comer 210.

The invention can also be implemented by means of a suitably programmed computer provided with a computer program for enrolling a member of an authorized domain. The computer program product for enrolling a member of an authorized domain comprises code for receiving a request form a device for joining the authorized domain, and code for granting a temporary certificate to the device according to a predetermined

rule, whereby the device becomes the member of the authorized domain, wherein the temporary certificate is issued by a manager of the authorized domain beforehand.

These portions of program code may be provided to a processor to produce a machine, such that the code that executes on the processor create means for implementing the functions specified as above.

FIG 3 is a schematic diagram of an authorized domain with a temporary member using a temporary certificate according to one embodiment of the invention.

Authorized Domain (AD) 100 includes n members 130, 140, 150 (ID_1, ID_2, ... ID_n), a home network infrastructure 120, an AD manager 110 and a temporary member 210. The members 130, 140, 150 and the temporary member 210 are connected to the home network infrastructure 120 that includes a number of wired/wireless connectors.

The AD manager 110 is not available for all AD members since it is not connected to the home network infrastructure 120. For instance, the AD manager 110 is down.

The temporary member 210 sends a request of sharing a content of the AD 100 to member 140 (ID_2) of the AD 100. The request includes the identification number of the temporary member 210 (TM_ID) and the temporary certificate (TID_1).

The member 140 verifies the temporary certificate (TID_1) to prove that the temporary member 210 is a legitimate member of the AD 100. To achieve this verification, the member 140 may check the identification number of the temporary member, the identification number of the AD, the temporary certificate number and the signature included the temporary certificate.

After the verification if the temporary member 210 is a legitimate member, the member 140 sends the content encrypted by the content key and the content key encrypted by the public key of the temporary member 120.

After receiving the encrypted content and encrypted content key, The temporary member decrypts the encrypted content key by using its private key, then decrypts the encrypted content by using the content key, finally the temporary member could enjoy the content.

It is understandable that the request form the temporary member 210 could be sent to any members of the AD 100 that are connected to the home network infrastructure 120. The request could also be sent to a server of a content provider that is capable of verifying the temporary certificate.

It is also understandable that the AD manager 110 could be connected to the home network infrastructure 120 when the above process of using a temporary certificate is implemented.

While the invention has been described in conjunction with specific embodiments, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended to embrace all such alternatives, modifications and variations as fall within the spirit and scope of the appended claims.

CLAIMS:

1. A method for enrolling a member of an authorized domain, comprising the steps of:
receiving a request form a device for joining the authorized domain, and
granting a temporary certificate to the device according to a predetermined rule, whereby the device becomes the member of the authorized domain,
wherein the temporary certificate is issued by a manager of the authorized domain beforehand.

2. The method of claim 1, wherein the device represents a person of the authorized domain.

3. The method of claim 2, wherein the device is a smart card.

4. The method of claim 1, wherein the temporary certificate enjoys less right than an ordinary certificate issued by the manager of the authorized domain.

5. An apparatus for enrolling a member of an authorized domain, comprising:
communication means for receiving a request form a device for joining the authorized domain, and
granting means for granting a temporary certificate to the device according to a predetermined rule, whereby the device becomes the member of the authorized domain,
wherein the temporary certificate is issued by a manager of the authorized domain beforehand.

6. The apparatus of claim 5, wherein the communication means further for obtaining the temporary certificate from the manager of the authorized domain.

7. An authorized domain, comprising:
a manager for issuing a temporary certificate, and
an apparatus for enrolling a member of the authorized domain, comprising:
communication means for receiving a request form a device for joining the authorized domain,

granting means for granting a temporary certificate to the device according to a predetermined rule, whereby the device becomes the member of the authorized domain, wherein the temporary certificate is issued by the manager beforehand.

8. The authorized domain of claim 7, further comprising at least one more apparatus for enrolling a member of the authorized domain, wherein the manager issues at least one more temporary certificate and allocates the at least two temporary certificates among the at least two apparatuses according to a predetermined rule.

9. A computer program product for enrolling a member of an authorized domain, the computer program product comprising:
code for receiving a request form a device for joining the authorized domain, and
code for granting a temporary certificate to the device according to a predetermined rule, whereby the device becomes the member of the authorized domain,
wherein the temporary certificate is issued by a manager of the authorized domain beforehand.

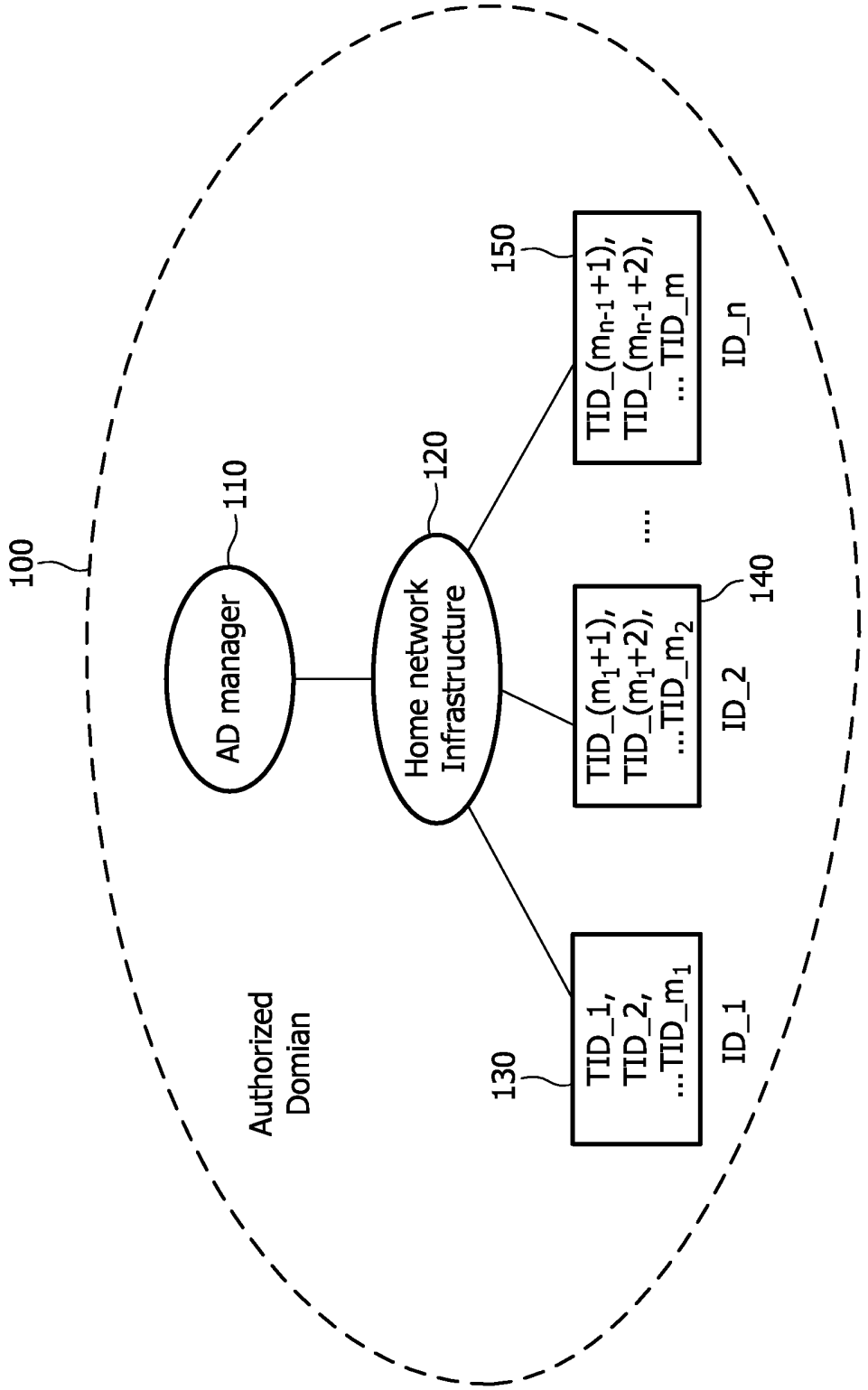

100
AD manager
110
Home network Infrastructure
120
Authorized Domian
TID_1, TID_2, ...TID_m1
ID_1
130
TID_(m1+1), TID_(m1+2), ...TID_m2
ID_2
140
....
TID_(mn-1+1), TID_(mn-1+2), ... TID_m
ID_n
150

FIG. 1

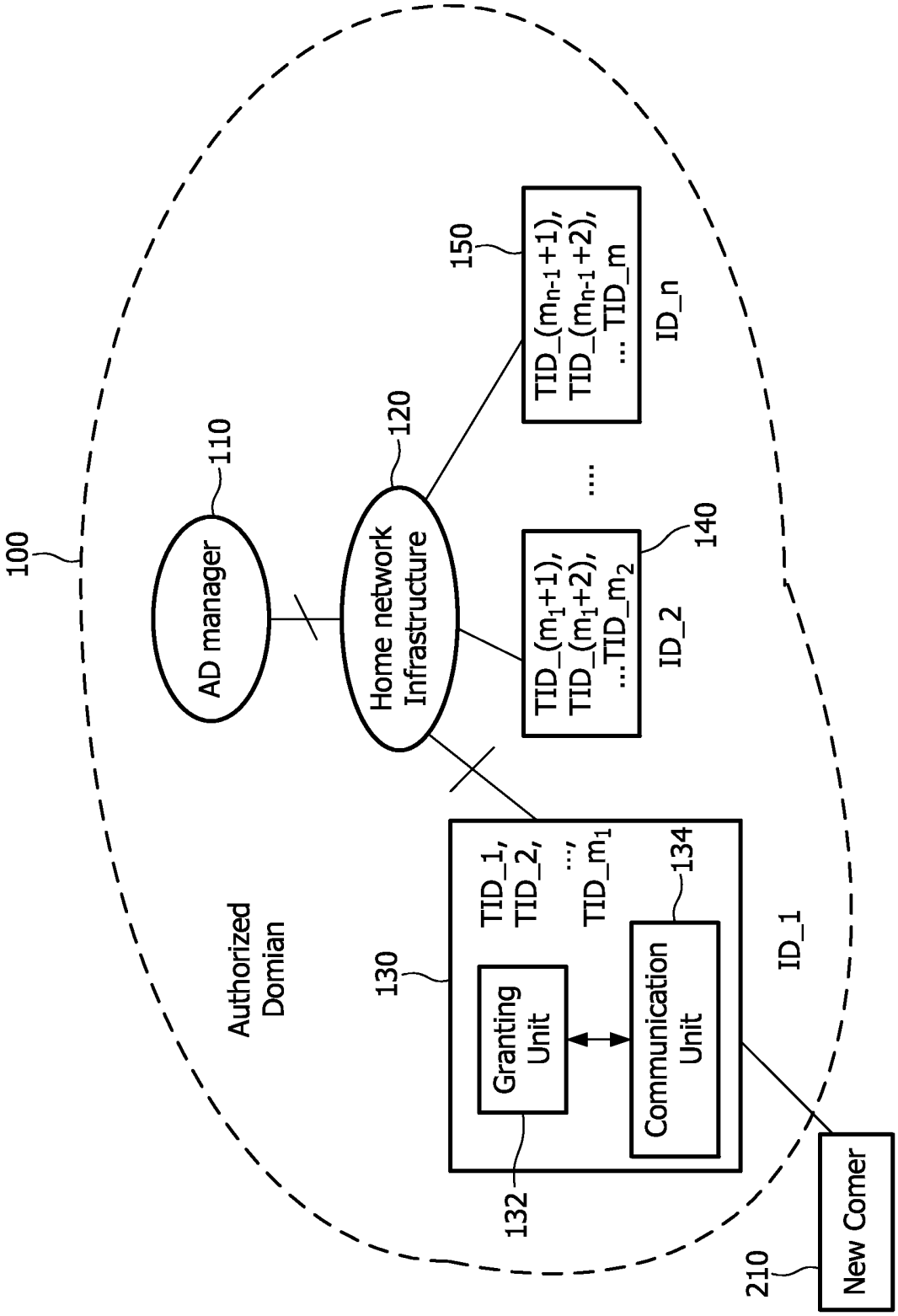

100
AD manager
110
Home network Infrastructure
120
150
TID_(m_{n-1}+1), TID_(m_{n-1}+2), ... TID_m
ID_n
....
140
TID_(m_1+1), TID_(m_1+2), ...TID_m_2
ID_2
Authorized Domian
130
TID_1, TID_2, ..., TID_m_1
Granting Unit
132
Communication Unit
134
ID_1
210
New Comer

FIG. 2

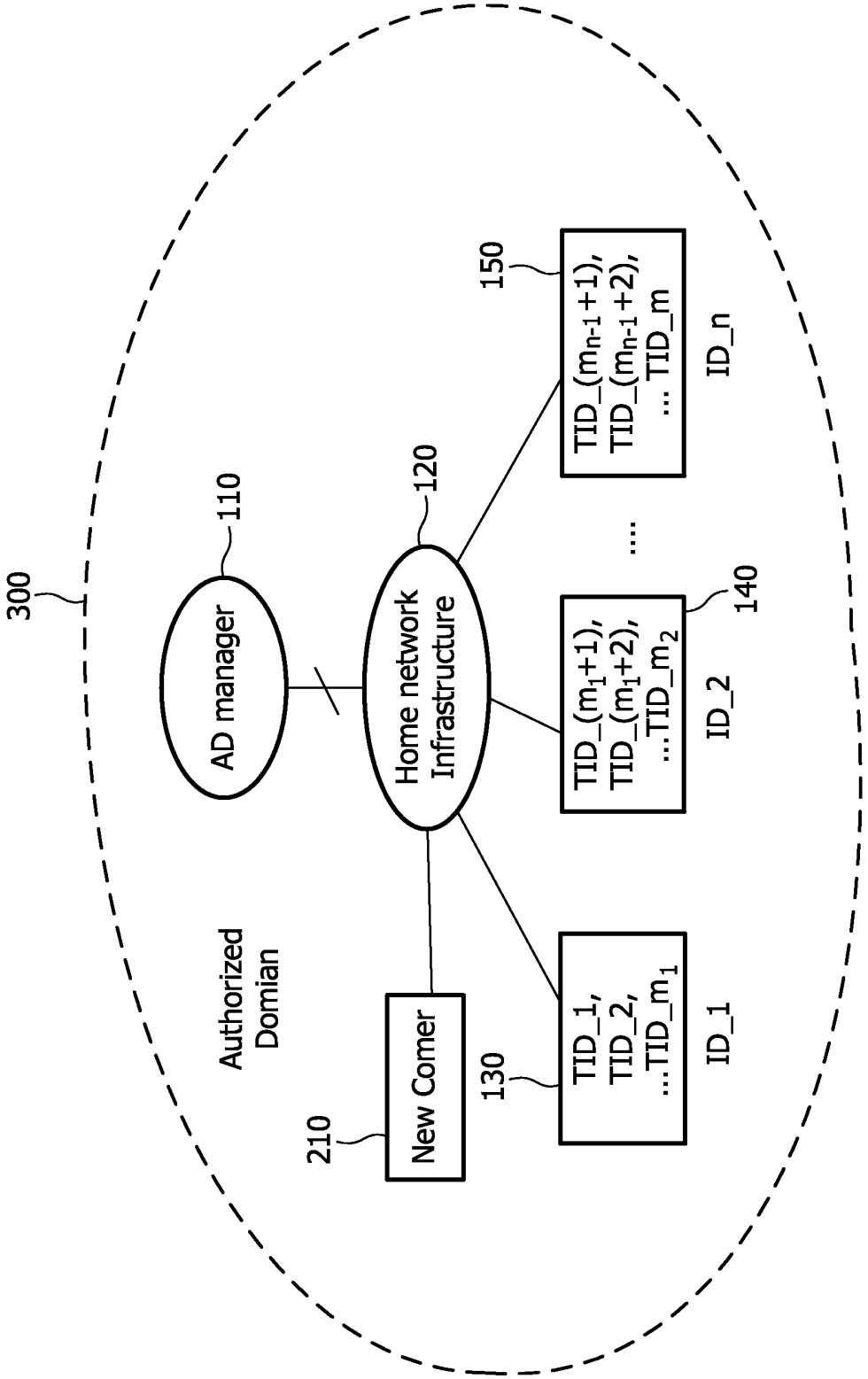

300
AD manager
110
Home network Infrastructure
120
150
TID_(m_{n-1}+1), TID_(m_{n-1}+2), ... TID_m
ID_n
....
140
TID_(m_1+1), TID_(m_1+2), ...TID_m_2
ID_2
TID_1, TID_2, ...TID_m_1
ID_1
130
New Comer
210
Authorized Domian

FIG. 3