BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Internal distribution code:
(A) [ ] Publication in OJ
(B) [ ] To Chairmen and Members
(C) [ ] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 27 July 2012

Case Number: T 1372/08 - 3.5.06

Application Number: 04744585.3

Publication Number: 1652025

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
Hybrid device and person based authorized domain architecture

Applicant:
Koninklijke Philips Electronics N.V.

Opponent:
-

Headword:
Authorized domain/PHILIPS

Relevant legal provisions:
EPC Art. 123(2)

Relevant legal provisions (EPC 1973):
EPC Art. 56, 84

Keyword:
"Original disclosure - main and first auxiliary request (no)"
"Clarity - second auxiliary request (yes)"
"Inventive step - second auxiliary request (yes)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1372/08 **-** 3.5.06

D E C I S I O N
of the Technical Board of Appeal 3.5.06
of 27 July 2012

Appellant: (Applicant)
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
NL-5621 BA Eindhoven (NL)

Representative:
Niessen, Arnoldus Jeroen
Philips International B.V.
Intellectual Property & Standards
High Tech Campus 44
NL-5656 AE Eindhoven (NL)

Decision under appeal:
Decision of the Examining Division of the European Patent Office posted 26 February 2008 refusing European patent application No. 04744585.3 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman: D. H. Rees
Members: S. Krischer
C. Heath

Summary of Facts and Submissions

I. The appeal is directed against the decision of the examining division, posted on 26 February 2008, to refuse the application 04744585.
The reason for the refusal was lack of inventive step over document:

D2 S. A. F. A. van den Heuvel et al.: "Secure Content Management in Authorised Domains"; in International Broadcasting Convention (IBC), Amsterdam, The Netherlands; 15 September 2002; pages 467-474; XP2273504.

II. A notice of appeal was received on 17 April 2008. The fee was received the same day. A statement of the grounds of appeal was received on 19 June 2008. A claim set for a main request was filed.
Oral proceedings were conditionally requested.

III. The board issued a summons to oral proceedings, raising objections with respect to Articles 123(2), 52(2), (3) and 56 EPC.

IV. With a letter dated and received 25 June 2012, the appellant re-filed the main request and filed a first, second and third auxiliary request.

V. Oral proceedings were held on 27 July 2012. A new second auxiliary request was filed, replacing the previous one. The third auxiliary request and another newly filed request were withdrawn. At the end, the chairman announced the board's decision.

VI. The appellant requests to set the decision aside and to grant a patent on the basis of a main request filed with the grounds and re-filed on 25 June 2012 (claims 1-10), a first auxiliary request (claims 1-5) filed on 25 June 2012, or a second auxiliary request (claims 1-5) filed during oral proceedings.
The further text on file is: description pages 1, 6, 8-18 as published; pages 2-5, 7 filed with letter dated 6 April 2007; drawing sheets 1-3 as published.

VII. Claim 1 of the main request reads as follows:

"1. A method of generating an Authorized Domain, the method comprising the steps of

- selecting a domain identifier uniquely identifying the Authorized Domain (100),
- binding at least one user and at least one device to the Authorized Domain identified by the domain identifier by obtaining or generating a single domain list or certificate comprising the domain identifier, a unique identifier for at least one user and a unique identifier for at least one device thereby defining that the user and the device both are bound to the Authorized Domain (100), and
- binding at least one content item to the Authorized Domain given by the domain identifier by

a) binding said content item to a User Right Certificate, where said User Right Certificate identifies the content item and a user bound to the Authorized Domain, and/or

b) binding said content item to a Device Right Certificate, where said Device Right Certificate identifies the content item and a device bound to the Authorized Domain, and/or

c) binding said content item to a Domain Right Certificate, where said Domain Right Certificate identifies the content item and the Authorized Domain,

thereby obtaining a number of devices and a number of users that is authorized to access a content item bound to said Authorized Domain (100), the method further comprising the step of controlling access to a given content item bound to the Authorized Domain (100) by a given device being operated by a given user, the step comprising:

- checking, using the User Right Certificate and/or the single domain list or certificate if the given user is bound to the same Authorized Domain (100) as the given content item, or
- checking, using the Device Right Certificate and/or the single domain list or certificate if the given device is bound to the same Authorized Domain (100) as the given content item,

and allowing access for the given user via the given device to the content item if the given user is bound to the same Authorized Domain (100) but the given device is not,

or if the given device is part of the same Authorized Domain (100), but the given user is not."

Claim 6 of the main request is a corresponding system claim (see the first auxiliary request).

VIII. The first auxiliary request is obtained from the main request by deleting claims 1 to 5 (method claims) and renumbering the remaining (system) claims. Thus claim 1 of the first auxiliary request reads as follows:

"1. A system for generating an Authorized Domain (AD), the system comprising:

- means for obtaining a domain identifier uniquely identifying the Authorized Domain (100),
- means for binding at least one user and at least one device to the Authorized Domain identified by the domain identifier by obtaining or generating a single list or certificate comprising the domain identifier, a unique identifier for at least one user and a unique identifier for at least one device thereby defining that the user and the device both are bound to the Authorized Domain (100), and
- means for binding at least one content item to the Authorized Domain identified by the domain identifier by

a) binding a content item to a User Right Certificate, where said User Right Certificate identifies the content item and a user bound to the Authorized Domain, and/or

b) binding a content item to a Device Right Certificate, where said Device Right Certificate identifies the content item and a device bound to the Authorized Domain,

and/or

c) binding a content item to a Domain Right Certificate, where said Domain Right Certificate identifies the content item and the Authorized Domain,

thereby obtaining a number of devices and a number of users that is authorized to access a content item of said Authorized Domain (100), the system further comprising means for controlling access to a given content item bound to the Authorized Domain (100) by a

given device being operated by a given user, where the means is adapted to:

- check, using the User Right Certificate and/or the single domain list or certificate if the given user is bound to the same Authorized Domain (100) as the given content item, or
- check, using the Device Right Certificate and/or the single domain list or certificate if the given device is bound to the same Authorized Domain (100) as the given content item,

and to allow access for the given user via the given device and/or other devices to the content item if the given user is bound to the same Authorized Domain (100) but the given device is not,

or if the given device is part of the same Authorized Domain (100) but the given user is not."

IX. Claim 1 of the second auxiliary request differs from the first auxiliary request in that "and/or other devices" and "but the given device is not" is deleted in the phrase starting with "and to allow access", in that "or to allow access for the given user via the given device to the content item if the given device" replaces "or if the given device", and in that "but the given user is not" is deleted at the end. That is, the final features now read as follows:

"and to allow access for the given user via the given device to the content item if the given user is bound to the same Authorized Domain (100),

or to allow access for the given user via the given device to the content item if the given device is part of the same Authorized Domain (100)."

Reasons for the Decision

1. *Original disclosure*

1.1 Main request

1.1.1 The last two steps of claim 1 of the appealed decision read as follows:

> "and allowing access for the given user via the given device and/or other devices ... if the given user is bound to the same Authorized Domain (100), or allowing access for the given user and/or other users via the given device ... if the given device is part of the same Authorized Domain (100)."

In claim 1 of the main request in appeal, this passage reads as:

> "and allowing access for the given user via the given device ... if the given user is bound to the same Authorized Domain (100) ...,
> or if the given device is part of the same Authorized Domain (100), ..."

This means that in the present claim the result of the second part of the step of allowing access ("if the given device is part of ...") is combined by a logical or-operator with the result of the first condition ("if the given user is bound ..."). This results in a different behaviour: In the refused claim 1 and in original claim 7, there were two alternative steps of checking (either the user's or the device's binding to the AD was checked) and two *corresponding* steps of allowing access (either according to the user's or to

the device's binding to the AD). This is also confirmed by the use of the different formulations

> "for the given user via the given device and/or other devices"

in the last but one step, and

> "for the given user and/or other users via the given device"

in the last step.
In the present claim, there is still *either* the user's *or* the device's binding checked, but the two following if-conditions both need to be checked and the results of both are needed to satisfy the claim although only one of them is evaluated in the preceding checking step. Furthermore, the result of the two if-condition checks is combined by a logical or-operator which implies that the allowance is given more often in principle than with the execution of either the user's check and corresponding allowing step or the device's check and corresponding allowing step.

1.1.2 Further compared to the original claims (and the claims in the appealed decision) the following expression has been added:

> "[if the given user is bound to the same Authorized Domain (100)] but the given device is not"

This means that a second check is performed (Is the given device not bound to the AD?) and combined with the result of the first test (Is the given user bound to the AD?) with a logical and-operator ("but"). Thus,

the access is allowed if the two tests are answered in the positive. There are only two passages in the description dealing with such a situation, namely page 15, lines 14-16 and page 17, lines 23-25. In both passages, there is no need to check the device's adherence to the AD. In the first passage, the person's adherence is sufficient. In the second passage, it is known that the device does not belong to the same AD. Thus, it appears that there is no original disclosure that both checks are performed under these conditions.

1.1.3 Similarly, applying to the user, the following expression has been added:

> "[or if the given device is part of the same Authorized Domain (100),] but the given user is not"

Again, this means that a second check is performed (Is the given user not part of the AD?) and combined with the result of the first test (Is the given device part of the AD?) with a logical and-operator. Thus, the access is allowed if the two tests are answered in the positive. There are again only two passages in the description dealing with such a situation, namely page 15, lines 17-19 and page 18, lines 3-5. In the first passage, there is no *need* to check the *user's* adherence to the AD. In the second passage, it is *known* that the user does not belong to the same AD. Thus, again there seems to be no original disclosure that a second check is performed.

1.1.4 During oral proceedings, the appellant argued that the expressions "but the given device is not" and "but the given user is not" are not meant to be steps, but are

merely indicating the positive effect which the claimed invention has in certain situations. This was not convincing to the board, since it follows from the description that the claimed method is computer-implemented, and a conditional method step (starting with "if") can only be implemented by testing the condition, including the part starting with "but".

1.1.5 Thus, claim 1 of this request violates Article 123(2) EPC.

1.2 First auxiliary request

1.2.1 The same objection holds for system claim 1 of the first auxiliary request which contains corresponding amendments to those of method claim 1 of the main request.

1.2.2 Thus, claim 1 of this request also violates Article 123(2) EPC.

1.3 Second auxiliary request

1.3.1 The sole independent claim 1 of this request does not contain the objectionable formulations used in the main and the first auxiliary request; instead it uses the same formulations as in the refused claim 6 (i.e. those of original claim 18), with the exception of the (clarifying) deletion of "and/or other devices" and "and/or other users" in the allowing steps (see below).

1.3.2 The decision did not raise any objection with respect to Article 123(2) EPC for the refused claims. The board also does not see any reason to do so.

1.3.3 As to the amendments in the claims of this request in comparison with the refused claims, the board finds that they satisfy the requirements of Article 123(2) EPC:

- "check, *using the User Right Certificate and/or the single domain list or certificate* ..." (claim 1, page 19 submitted at oral proceedings, line 22): See figure 1; page 14, lines 4-14; page 11, lines 19-22.
- "check, *using the Device Right Certificate and/or the single domain list or certificate* ..." (claim 1, page 19, line 25): See page 11, lines 14-18; page 13, lines 26-28; page 11, lines 19-22.

1.3.4 Thus, the second auxiliary request fulfils the requirements of Article 123(2) EPC.

2. *Clarity of claim 1 of the second auxiliary request*

2.1 As to the objection raised in the summons, section 6.4, point b) with respect to the User Right Certificate being unable to be used to check the adherence of a content item to a domain, the appellant explained during oral proceedings that figure 1 and page 14, lines 4-14 are to be understood that a content item is bound to any domain any user who has a User Right Certificate for this item is bound to. Every user who is also bound to this domain has the right to access that item. The board was satisfied with these explanations and did not maintain this objection.

2.2 During oral proceedings the board also objected to a lack of clarity arising from "and/or other devices" and "and/or other users" in the allowing steps of claim 1 of the then second auxiliary request filed with the

letter dated 25 June 2012. Lines 20 and 21 of the claim define the context and purpose of the checks, namely to control access to a given content item by a given device being operated by a given user. It follows that the allowing step concerns exactly this given user and this given device and not other devices or other users. In response the appellant filed the new second auxiliary request deleting the phrases objected to. The board has not found any further cause to doubt the clarity of the claimed subject-matter.

2.3 Thus, claim 1 of the second auxiliary request is clear in the sense of Article 84 EPC.

3. *Inventiveness of claim 1 of the second auxiliary request*

3.1 In the appealed decision, claim 1 was refused for lack of inventive step over document D2. All differences of the claim to D2 relate to the inclusion of users in ADs. The technical problem was regarded as how to bind rights to devices *and persons* instead of devices only. It was argued that the passage in D2 on page 5, paragraph 2 pointed the skilled person in the direction that the user could also be considered in the concept.

3.2 In the grounds, it is stated that it is not disputed that D2 is the closest prior art. The technical problem is formulated as "how to add user management to an AD system which is not complicated, i.e. which is efficient and simple for people to use" (page 2, paragraph 4). As a solution to that problem, three features a)-c) are given.

3.3 The board agrees with the appealed decision that the desire to include the user as a determinant of access is a business decision, to be included in the formulation of the objective technical problem to be solved, rather than the solution. This merely represents a change in the access rights policy, namely from the device-based management to a combination of the latter with a user-based management. This change in the policy alone does not contribute to an inventive step. Moreover this amended policy is at least implicitly suggested in D2. In addition to the passage cited in the appealed decision, the board notes that D2 clearly defines an AD as including users (page 3, section "FUNCTIONAL SPECIFICATION", paragraph 2):

> "An Authorised Domain is an environment of (networked) devices, media, rights and users; in which users and devices handle content according to the rights."

This does not mean that the implementation described in D2 actually *uses* the adherence of users to ADs for allowing access, but it makes it obvious to do so, since in an AD "the consumer is free to access and distribute content" (D2, abstract, line 4), therefore the name "Authorised Domain" (AD).

3.4 However, the claimed invention does not only consist of the mere idea to integrate the users in the access right policy, but gives implementation details *how* to do this. The binding of users to domains necessitates a new data structure for representing the bindings. In D2 the binding of devices to a domain is represented by a secret key or identifier for this domain stored in each device of the domain (page 6, "AD device management",

points 1. and 2.): All devices possessing the same secret domain key/ID belong to the same domain. Thus there is no need for a central list of members of the domain in order to check whether a device can access a certain content, nor is there any suggestion that such a list should be created for any other reason. It is specifically stated (page 5, final paragraph) that Rights Management (as opposed to Device Management) should not be handled centrally. Thus the skilled person would understand that content access would be simply a bilateral issue between members, based on holding the same key. It is noted that one of the conditions for a device to be allowed to register as a member of an AD is stated to be that the AD should not exceed a certain size, but this does not mean that the device which handles registration and deregistration necessarily keeps a list of members. It could equally, and in fact more efficiently, simply keep a counter containing the current number of members, as pointed out by the appellant (submission of 25 June 2012, page 5, paragraph 4).

3.5 Generalising this method to users would necessitate storing a secret domain key/ID with the user. A user could memorise the secret domain key/ID and input it by hand from his memory, or he could use a smart card containing it. The invention however avoids the clear inconveniences of these two approaches: by using a centralised single list of the devices and users belonging to the same domain, it facilitates the integration of users to the domain concept. No secret domain key/ID has to be stored with the user. No learning of a long key/ID by heart and no smart card is necessary.

3.6 The invention furthermore proposes User Right Certificates as a data structure to represent the binding of content items to users in addition to the system implemented in D2 (which does not handle users at all). It is not clear in D2 if the access rights are stored as Device or Domain Right Certificates, or as a mixture of both (see D2, figure 2; page 5, fourth paragraph; and page 7, points 1. and 2.). The invention clearly uses both, Device and Domain Right Certificates, in addition to the User Right Certificates.

3.7 Thus, the objective technical problem with respect to the closest prior art D2 can be formulated as how to implement the addition of users to the authorised domain concept of D2.

3.8 As shown above, the claimed invention solves this problem by replacing distributed secret domain keys/IDs by a central list of members, in addition to the use of User and Device Right Certificates. Neither D2 nor any of the other documents in the procedure would lead the skilled person to introduce centralised lists for use in access control. However centralised lists of members were specified at least in original dependent claims 8 and 14, so that the search must be taken to have extended to this matter. Therefore, the board concludes that claim 1 of the second auxiliary request is inventive in the sense of Article 56 EPC.

4. *Adaptations*

The board notes that the description needs to be adapted before a patent can be granted, e.g. on page 3 filed with letter dated 6 April 2007, the word "method" should be replaced by "system" in line 24.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The application is remitted to the department of first instance with the order to grant a patent on the basis of claims 1-5 of the second auxiliary request filed during oral proceedings, and a description adapted hereto.

The Registrar: The Chairman:

L. Fernández Gómez D. H. Rees