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 6 May 2011

Case Number: T 1773/07 - 3.5.04

Application Number: 01117553.6

Publication Number: 1175095

IPC: H04N 5/913

Language of the proceedings: EN

Title of invention:
Video on demand pay per view services with unmodified conditional access functionality

Applicant:
Hughes Electronics Corporation

Headword:
-

Relevant legal provisions:
-

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

Keyword:
"Inventive step (no) - all requests"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1773/07 - 3.5.04

D E C I S I O N
of the Technical Board of Appeal 3.5.04
of 6 May 2011

Appellant: Hughes Electronics Corporation
200 N. Sepulveda Boulevard
El Segundo
California 90245-0956 (US)

Representative: Grünecker, Kinkeldey
Stockmair & Schwanhäusser
Anwaltssozietät
Leopoldstraße 4
D-80802 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 8 March 2007 refusing European patent application No. 01117553.6 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: F. Edlinger
Members: M. Paci
C. Vallet

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse European patent application No. 01 117 553.6, published as EP 1 175 095 A2.

II. The decision under appeal was based on the ground that the subject-matter of claims 1 and 10 did not involve an inventive step (Article 56 EPC 1973) in view of the following prior-art documents:

D1: US 5,912,969 A and
D2: EP 0 989 557 A1.

III. With the statement of grounds of appeal, the appellant submitted a set of amended claims according to an auxiliary request and amended description pages.

IV. In a communication accompanying the summons to oral proceedings the board expressed doubts as to whether the amended claims according to both requests met the requirements of Article 84 EPC 1973 (clarity) and Article 123(2) EPC (added subject-matter).

V. With a letter dated 5 April 2011 the appellant filed respective sets of amended claims according to a main request and an auxiliary request, replacing all previous claims.

VI. Oral proceedings were held before the board on 6 May 2011 during which *inter alia* inventive step was discussed. At the end of the oral proceedings, the board's decision was announced.

VII. The appellants' final requests are that the decision under appeal be set aside and that a patent be granted on the basis of the set of claims 1 to 16 according to the main request filed with the letter of 5 April 2011, or in the alternative, on the basis of the set of claims 1 to 13 of the auxiliary request filed with the letter of 5 April 2011.

VIII. Independent claim 1 according to the **main request** reads as follows:

"A method of storing program material for subsequent replay, comprising the steps of:

receiving encrypted program material (506) and encrypted access control information (504), the access control information including a first encryption key (546), the program material being encrypted according to the first encryption key (546);

further encrypting the encrypted program material (506) and the encrypted access control information (504) according to a second encryption key (516) to obtain doubly encrypted program material (514) and doubly encrypted access control information (518);

encrypting the second encryption key (516) according to a third encryption key (520); and

storing the doubly encrypted program material (514), the doubly encrypted access control information (518), and the encrypted second encryption key (524)."

Claims 2 to 16 according to the main request have no bearing on the present decision.

IX. Independent claim 1 according to the **auxiliary request** reads as follows:

"A method of storing program material for subsequent replay, comprising the steps of:

receiving encrypted program material (506) and encrypted access control information (504), the access control information including a first encryption key (546), the program material being encrypted according to the first encryption key (546);

further encrypting the encrypted program material (506) and the encrypted access control information (504) according to a second encryption key (516) to obtain doubly encrypted program material (514) and doubly encrypted access control information (518);

encrypting the second encryption key (516) according to a third encryption key (520);

storing the doubly encrypted program material (514), the doubly encrypted access control information (518), and the encrypted second encryption key (524);

reading the doubly encrypted access control information (518), the doubly encrypted program material (514), and the encrypted second encryption key (524);

decrypting the encrypted second encryption key (524) using the third encryption key (520) to produce the second encryption key (516);

decrypting the doubly encrypted access control information (518) using the second encryption key (516) to produce the encrypted access control information (504);

decrypting the doubly encrypted program material (514) using the second encryption key (516) to obtain the encrypted program material (506);

decrypting the encrypted access control information (504) to produce the first encryption key (546); and

decrypting the encrypted program material (506) using the first encryption key (546), wherein

the access control information further comprises data describing a right associated with the program material;

the step of decrypting the encrypted access control information (504) to produce the first encryption key (546) further produces the data describing the right associated with the program material; and

the step of decrypting the encrypted program material (506) using the first encryption key (546) is performed according to the data describing the right associated with the program material."

Claims 2 to 13 according to the auxiliary request have no bearing on the present decision.

X. The examining division's reasoning in the decision under appeal regarding claim 1 then on file (the subject-matter of which was essentially the same as that of claim 1 of the present main request) can be summarised as follows:

D1, which is considered to represent the closest state of the art, discloses (column 3, line 16) a method of storing program material for subsequent replay, comprising the steps of:
receiving encrypted program material (column 7, line 6);
further encrypting the encrypted program material according to a second encryption key (column 4, lines 1 to 4);
encrypting the second encryption key according to a third encryption key to produce a fourth encryption key (column 4, lines 8 to 11); and
storing the further encrypted program material and the fourth encryption key (column 4, lines 13 to 16).

The subject-matter of claim 1 differs from the method of D1 in that encrypted access control information including a first encryption key is also received with the encrypted program material, further encrypted and stored.

The term "access control information" is very broad. It covers information such as EMM and ECM (see D2), or merely an encryption key (encrypted or not).

The objective problem may be regarded as being how to provide encrypted access control information including the encryption key together with the program material.

The skilled person confronted with this problem would use prior-art documents which deal with recording devices recording encrypted broadcasted information, such as D2.

D2 provides a solution to this problem. It discloses a data recording/reproducing system (column 5, line 53) having means for receiving digital video data, audio data, EMM (individual information), ECM (program information) and encrypted broadcasting scrambling key (column 7, lines 22 to 25). In the ninth embodiment (see figures 29 and 31 and paragraphs [0195] to [0197]), D2 discloses the possibility of storing the broadcasting scrambling key in encrypted form together with the encrypted program material.

D2 therefore discloses receiving and storing "access control information" including a first encryption key.

Starting from D1, it is considered to be obvious that the skilled person would clearly appreciate the possibility that the first encryption key could also be transmitted by the broadcaster and subsequently stored together with the encrypted program material.

For the above reason, it is considered that the skilled person would use the teaching of D2 to provide an encryption key (either the "access control information" itself or included in the "access control information") in a system known from D1 without the need for any inventive activity.

XI. The appellant's arguments regarding inventive step can be summarised as follows:

Main request

Although both D1 and D2 are relevant prior art, D2 should be regarded as the closest prior art because it relates to digital rights management, like the problem of the present invention, whereas D1 only addresses the problem of copy protection. The examining division thus erred in selecting D1 as to the closest prior art.

In contrast to the method of claim 1, no **double** level of encryption is used in D2, neither for the program material to be stored nor for the access control information. Hence the method of claim 1 involves an inventive step when starting from D2.

Even if D1 were regarded as the closest prior art, the method of claim 1 would still involve an inventive step for the reasons set out below.

D1 describes the storage of program material transmitted in encrypted form. After reception, but before storage, the program material is subjected to a further encryption. The program material is therefore doubly encrypted before storage.

The method of claim 1 differs from that of D1 in that the first encryption key, i.e. the key that has been used at the broadcast station for encrypting the program material transmitted in encrypted form, is transmitted in encrypted form together with the encrypted program material, is further encrypted (i.e.

doubly encrypted) and is stored together with the doubly encrypted program material.

The objective technical problem solved by the present invention is not only to provide the encryption key together with the program material, as alleged by the examining division, but also to enable the shifting of the billing procedure to the time of reproduction.

Contrary to what the examining division set out in the reasons for the appealed decision, these distinguishing features are not taught by D2 for the following reasons:

- D2 teaches decrypting the encrypted program material before re-encrypting it, and then storing it. Hence there is no double level of encryption of the program material, even in the ninth embodiment of D2 highlighted by the examining division.
- D2 teaches separating the key encryption data from the program material, not storing both together. D2 also teaches away from further encrypting the program material and the first encryption according to the **same** second encryption key.
- D2 does not enable the shifting of the billing procedure until **after** storage of the program material.

The decision under appeal was based on hindsight because there are no features in the apparatus of D1 for extracting an encryption key from the data stream. D1 provides no details regarding the key employed by decryptor 2023. As any information regarding the first encryption key is not transmitted with the video data, the decryptor can only employ a locally pre-stored decryption key. In contrast, the present invention assigns individual encryption key data with the

associated program data. In this manner, a billing procedure employed during the decryption and reproduction procedure is individually performed for each video data.

Even if transmission of an encryption key together with encrypted program material had been contemplated, the skilled person would not have tried to adapt the apparatus of D1 but, instead, would have turned to D2 which offered a better solution for this type of transmission.

Hence, the method of claim 1 according to the main request involves an inventive step in view of D1 and D2, taken alone or in combination.

Auxiliary request

The method of claim 1 according to the auxiliary request corresponds to claim 1 according to the main request with the additional features of dependent claims 2 and 3. In particular, claim 1 specifies that the access control information further comprises data describing a right associated with the program material and that the step of decrypting the encrypted program material using the first encryption key is performed according to the data describing the right associated with the program material. Since the reproduction is restricted based on a particular right which is provided together with the key information of the encrypted program data, an improved management of a restricted reproduction is achieved.

D1 neither discloses nor suggests providing any supplemental information indicating a right for limiting the processing of the program material.

D2 does not disclose recording a reproduction right together with the program material and restricting the reproduction of the program material accordingly. In contrast, D2 always decrypts the program material based on ECM/EMM without considering reproduction rights and does not store any information regarding a reproduction right on the storage medium.

Hence, the method of claim 1 according to the auxiliary request involves an inventive step in view of D1 and D2, taken alone or in combination.

Reasons for the Decision

1. The appeal is admissible.

Main request

Closest prior art

2. According to the established jurisprudence of the boards of appeal, the closest prior art for assessing inventive step is normally a piece of prior-art disclosing subject-matter conceived for the same purpose or aiming at the same objective as the claimed invention and having the most relevant technical features in common, thus requiring the minimum of structural modifications. A further criterion for the selection of the most promising starting point is the

similarity of technical problem. (See Case Law of the Boards of Appeal of the European Patent Office, 6th edition 2010, I.D.3.1).

3. According to the present application (see page 2, first paragraph) the invention relates to "systems and methods for providing video program material to subscribers, and in particular to a method and system for securely storing and replaying media programs". According to page 3, lines 13 to 15, the main purpose or objective of the claimed invention is to address the following need: "What is needed is a system and method for securely recording broadcast media programs (including impulse purchase pay-per-view programs) for limited use playback at a later time."

The board notes that both D1 and D2 disclose methods and systems for securely storing copyright-protected broadcast media programs and for limiting the reproduction of the stored programs only to those who are entitled to do so (see D1, column 1, lines 14 to 19 and 37 to 42, and D2, paragraph [0001]). Therefore, both D1 and D2 disclose subject-matter conceived for the same purpose or aiming at the same objective as the invention of claim 1 according to the main request. By contrast to D2, D1 also discloses double encryption of program material, as will be shown below.

The appellant has not disputed that more of the technical features of the method of claim 1 are disclosed by D1 than by D2.

For the above reasons, in accordance with the established jurisprudence of the boards of appeal, D1

may be regarded as the closest prior for the method of claim 1.

4. The appellant argued that D2 should be regarded as the closest prior art because it relates to digital rights management, like the problem of the present invention, whereas D1 only addresses the problem of copy protection.

The board agrees with the appellant that the application describes embodiments of the invention which comprise features addressing the problem of digital rights management. However, the method of claim 1 according to the main request comprises no such feature. Indeed, the only expression in claim 1 which might refer to digital rights management is "access control information". However, claim 1 merely states that the access control information includes a first encryption key. It is not implicit in the expression "access control information" that it contains digital right management data in addition to a first encryption key.

For these reasons, the appellant's argument that the method of claim 1 solves not merely a problem of copy protection, but also a problem of digital rights management, fails to convince the board.

5. The board therefore concludes that D1 should be regarded as being the closest prior art.

Disclosure of D1

6. D1 discloses an apparatus (200 and 300 shown in figure 11 and described in particular from column 6, line 42, to column 7, line 12) for receiving encrypted digital audiovisual program material (encrypted MPEG signal input to demodulator 201), storing it (on data storage 304) and replaying it at a later time. The received program material has been previously encrypted in the transmitter (100) by an encryptor circuit (1012) using a **first encryption key** (this is implicit from the terms used and the given context; see D1, column 6, lines 57 to 60). If the received encrypted program material is to be recorded, a specific identification information processing circuit (400 consisting of 411, 403 and 412) which, as is clear from column 1, lines 51 to 53 and 60 to 62, and column 6, lines 52 to 56, may take the form shown in figure 3, carries out the following steps prior to recording:
- the encrypted program material is further encrypted by a pseudo-random signal, acting as **a second encryption key**, generated in a pseudo-random circuit generator (4001 in figure 3) (see column 4, lines 1 to 8);
- the pseudo-random signal, i.e. the second encryption key, is encrypted by a key encryption circuit (4013) using specific information identification acting as **a third encryption key** (see column 3, lines 44 to 50, and column 4, lines 4 to 11); and
- both the doubly encrypted program material and the encrypted second encryption key are recorded on a data storage medium (see column 4, lines 11 to 18).
During reproduction, reading and decrypting steps corresponding to the reverse of the above three steps

are performed, as shown in figure 3, in order to remove the additional level of encryption and to restore the program material to the state in which it was before being processed for recording, i.e. encrypted by the first encryption key only. The encrypted program material is then passed to a decryptor circuit (2023 in figure 11) which outputs an unencrypted MPEG signal.

Distinguishing features

7. It is undisputed that the method of claim 1 differs from that of D1 in that the access control information, including the first encryption key, is transmitted in encrypted form together with the encrypted program material, is further encrypted (i.e. doubly encrypted) using the second encryption key and is stored together with the doubly encrypted program material and the encrypted second encryption key.

Objective technical problem

8. The appellant has submitted that, starting from D1, the objective technical problem was not only to provide the encryption key together with the program material, but also to enable the shifting of the billing procedure to the time of reproduction.

The board has no objection to this formulation of the objective problem.

Obviousness

9. Before the priority date of the present application, it was well-known from conditional access systems to

broadcast encrypted (or scrambled) digital audiovisual (AV) data and to also broadcast the encryption (or scrambling) key, itself in encrypted form, which is required for decrypting the encrypted digital AV data. It was further well-known in this context before the priority date of the application (see, for instance, the well-known Digital Video Broadcast (DVB) standards) to transmit Entitlement Control Messages (ECM) carrying a Control Word (CW) and Entitlement Management Messages (EMM) specifying individual (subscriber) information together with the encrypted AV data and to decrypt the ECM and EMM in a subscriber's receiver, for instance by using a smart card containing an individual key. This was discussed in the oral proceedings before the board and not disputed by the appellant. This type of broadcasting of encrypted (or scrambled) AV data is also disclosed, for instance, in D2 in which EMM (individual information) and ECM (program information) are broadcast in addition to the encrypted AV data (see paragraph [0023]), the ECM containing, in encrypted form, the encryption (scrambling) key (Ks) required for decrypting the encrypted AV data by the use of a user ID key (Km) stored on an IC card (see paragraphs [0024] to [0027] and figure 1).

10. It is further undisputed that, before the priority date of the application, digital AV data was commonly transmitted as packets, in particular according to the well-known MPEG-1 or MPEG-2 standards, as is the case in D1 (see MPEG encoder 1011 in figure 11), in D2 (see column 12, lines 12 to 17) or in accordance with the commonly known DVB standard.

11. According to D1, at the broadcasting end, the digital AV data is packetised by MPEG encoder 1011 (in figure 11) and encrypted by encryptor 1012. At the receiving end, the reverse operations are performed by decryptor 2023 and MPEG decoder 2024. D1 provides no information as to how the decryptor obtains the encryption key required for decrypting the encrypted AV data. Since D1 does not disclose that the encryption key is broadcast to the receiving end, it cannot be assumed to be implicitly the case in D1 because there are other possibilities such as the encryption key being pre-stored in the decryptor. However since, as explained under point 9 *supra*, it was commonly known to broadcast ECM and EMM messages from which the encryption key could be recovered by receivers entitled to do so, the board considers it would have only been standard practice for the skilled person to try to adapt the apparatus shown in figure 11 of D1 to this type of broadcast.

In the board's view, such an adaptation would have posed little difficulty to the skilled person. Since all the AV data in D1 is broadcast as packets (MPEG), the ECM and EMM messages would also have had to be transmitted in packets, for instance in packets inserted between packets of encrypted AV data. In this regard, it should be noted, as was well-known in the art before the priority date and has not been disputed by the appellant, that when encrypted data is transmitted as packets, only the payload of the packets is encrypted, not the header of the packets. The packets containing EMM and ECM would thus have been packets among packets, and all packets would have been processed in the same manner before being recorded on

the data storage medium. Recording the packets containing ECM and EMM on the data storage medium would have been necessary because the decryptor (2023) would have needed them for decrypting the encrypted AV data reproduced from the data storage medium. Indeed, the decryptor would have needed the ECM and EMM messages transmitted with the encrypted program material for decrypting the reproduced program material because, as was well-known in the art, the content of the ECM and EMM was often changed for security reasons. Since the encrypted program material is not decrypted before it is stored in D1, there is no need to carry out the billing at the time of reception. Technically speaking, the billing procedure can be done when the stored packets are decrypted in the same manner as it would be done when the arriving packets are directly decrypted (see the different switch positions in figure 11). Shifting the billing procedure to the time of reproduction would thus only have required a possible change in managing the billing procedure at the service provider side.

Hence the skilled person would have arrived in an obvious manner at the method of claim 1 according to the main request.

The appellant's arguments

12. The appellant argued that the skilled person would not have tried to adapt the apparatus of D1 but, instead, would have turned to D2 which offered a better solution for the type of transmission in which the encryption key is broadcast together with the encrypted AV data.

The board is not convinced that the skilled person, starting from D1, would have regarded D2 as a better solution and thus abandoned any attempt at adapting the apparatus of D1. Instead, the skilled person would have considered that D2 was proposing a different, rather complicated solution, which was not particularly compatible with the apparatus of D1 because in D1 the decrypting of the AV data occurs **after** the recording/reproducing stage (see decryptor 2023), whereas in D2 it occurs **before** the recording/reproducing stage (in the broadcasting descrambling means 20) and thus requires a billing procedure before recording.

Conclusion

13. For the above reasons, claim 1 according to the main request does not fulfil the requirements of Article 56 EPC 1973 (inventive step).

14. Hence the appellant's main request is not allowable.

Auxiliary request

15. The method of claim 1 according to the auxiliary request corresponds to the method of claim 1 of the main request with the additional features of dependent claims 2 and 3 of the main request. These additional features consist essentially of:
- a reading step and several decrypting steps (of the reproducing process), which essentially mirror in reverse order the encrypting steps and the storing step (of the recording process); and

- the access control information comprising data describing a right associated with the program material, this data being recovered when the encrypted access control information is decrypted, and the decryption of the encrypted program material being performed according to this data.

16. As is clear from the well-known conditional access systems using ECM and EMM (see point 9 *supra*), these messages contain not only an encryption key (the Control Word (CW)) but also data describing a right associated with the program material, such as information about how many times the material may be viewed and whether it may be recorded.

As explained under point 11 *supra*, it would have been obvious for the skilled person to adapt the apparatus/method of D1 to receive and record both program material encrypted with an encryption key and ECM/EMM messages, containing the encryption key and transmitted in packets inserted between packets of encrypted AV data. As is clear from figures 3 and 11 and column 5, lines 3 to 26, of D1, the reproduction steps, like the method of claim 1 according to the auxiliary request, comprised a reading step and decrypting steps (of the reproducing process) which essentially mirrored in reverse order the encrypting steps and the storing step (of the recording process). The recorded packets containing the ECM and EMM messages would also have been reproduced. Since the ECM and EMM messages contained, in addition to the encryption key, data describing a right associated with the program material, the skilled person would have necessarily adapted the apparatus shown in figure 11 of

D1 so that it took account of this right for deciding whether and when (or how many times) to allow the decryption of the encrypted program material by decryptor 2023 or recording of the material as the case may be.

For the above reasons, claim 1 according to the auxiliary request does not fulfil the requirements of Article 56 EPC 1973 (inventive step).

17. Accordingly, the appellant's auxiliary request is not allowable.

Conclusions

18. Since none of the appellant's main and auxiliary requests is allowable, the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

K. Boelicke F. Edlinger