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

Datasheet for the decision of 3 February 2011

Case Number: T 1164/08 - 3.5.01

Application Number: 99967804.8

Publication Number: 1166207

IPC: G06F 12/14, G06F 1/00

Language of the proceedings: EN

Title of invention:
Secure streaming of digital audio/visual content

Applicant:
Audible, Inc.

Opponent:
-

Headword:
Secure streaming/AUDIBLE

Relevant legal provisions:
-

Relevant legal provisions (EPC 1973):
EPC Art. 56, 83

Keyword:
"Inventive step (all requests): no"
"Sufficiency of disclosure: no"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1164/08 - 3.5.01

D E C I S I O N
of the Technical Board of Appeal 3.5.01
of 3 February 2011

Appellant: Audible, Inc.
65 Willowbrook Boulevard
Wayne, NJ 07470 (US)

Representative: Kurig, Thomas
Patentanwälte
Becker, Kurig, Straus
Bavariastrasse 7
80336 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 1 February 2008 refusing European patent application No. 99967804.8 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman: S. Wibergh
Members: R. R. K. Zimmermann
G. Weiss

Summary of Facts and Submissions

I. European patent application no. 99 967 804.8 claims a priority date of 2 March 1999 for a method and apparatus for secure streaming of digital audio and/or visual content.

II. The examining division refused the application in particular for lack of inventive step and insufficient disclosure of the invention. The prior art cited against the application included the following documents:

D4: HITACHI LTD et al., "5C Digital Transmission Content Protection White Paper - Revision 1.0", 14 July 1998, URL: http://www.dtcp.com/wp_spec.pdf; pages 1-13.

D5: "IEEE Standard for a High Performance Serial Bus", IEEE STD 1394 - 1995, The Institute of Electrical and Electronics Engineers, New York, NY, USA, 1996; chapter 6., "Link layer specification"; pages 139-176.

The decision was posted on 1 February 2008.

III. The appellant (applicant) lodged an appeal against the refusal of the application on 27 March 2008 and filed a statement setting out the grounds of appeal including an amended set of claims on 30 May 2008.

IV. By a communication dated 16 April 2010, the Board notified the appellant of its provisional opinion that the examining division was essentially right in its assessment of inventive step. Questioning the appellant's analysis of the differences between the

invention and the prior art of document D4, the Board pointed out that already document D4 required the authentication of both the source and the playback devices on the basis of certificates. Checking content integrity and data validity was a common feature in data transmission. Stopping the replay of data after detecting tampered or invalid data was qualified by the Board as an obvious feature of data security systems.

Referring to the objection of insufficient disclosure the Board indicated that it had not been able to derive any information from the application how to carry out a periodic check of content integrity in a multimedia stream.

V. By letter dated 11 August 2010, the appellant made a number of submissions in response to the Board's communication and filed two new sets of claims as first and second auxiliary requests, maintaining the claims filed on 30 May 2008 as main request. Claim 1 of the main request has the following wording (brackets <...> are added for convenience of reference):

"1. A method comprising:
- receiving, at a playback device, authorization data associated with streamed digital content from a source, wherein said authorization data includes at least source authorization data, playback device authorization data, and content integrity data;
- determining whether said source is an authorized source based on said source authorization data;
- determining whether said playback device is an authorized playback device based on said playback device authorization data;

- if both said playback device and said source are authorized, playing streamed digital content received by said playback device; and
- periodically checking, at said playback device, the validity of said streamed digital content by comparing <content integrity values derived from a portion of said streamed digital content with said content integrity data received with said authorization data, such that the playing of streamed content is stopped when said periodic checking indicates invalid content.>"

The wording of claim 1 of the different requests varies only in the text set above between brackets, which reads in the auxiliary requests as follows:

First auxiliary request:
<a content integrity value derived from a portion of said streamed digital content with content integrity data that corresponds to said portion of said streamed digital content and that is received with said authorization data, such that the playing of streamed content is stopped when said periodic checking indicates invalid content.>

Second auxiliary request:
<a hash value derived from a portion of said streamed digital content with content integrity data that corresponds to said portion of said streamed digital content and that is received with said authorization data, such that the playing of streamed content is stopped when said hash value is not included with said content integrity data.>

VI. The appellant argued that transmitting, streaming or handling of data in blocks of a predetermined size was very common in the art. The skilled person would thus easily understand how to generate a content integrity value and in particular a hash value from a portion of the streamed digital content.

The periodic authorisation and validity checks were carried out in subsequent phases as described in the application in the context of figures 4 and 5. First, before streaming of multimedia data started, the authorisation data including source identifier, user identifiers, and content integrity values, for example hash values, were received by the playback device for authorisation. Only then, after authorisation, the blocks of multimedia data were streamed to the playback device. The playback device generated a hash value based on the blocks at any point in time and compared it to the content integrity values previously received with the authorisation data to check whether the generated value was included in the authorisation data.

By receiving the authorisation data including the integrity values in advance, the integrity and validity check could be done even randomly with any number of data blocks since a valid and authorised block of data would always provide a hash value that was included in the received authorisation data.

While continuing playback of data if the hash value was valid, the playback stopped if the check failed. It was evident therefore that the content integrity check was also a method of authorisation, and not a simple integrity check.

VII. Referring to novelty and inventive step, the appellant submitted that document D4 failed to disclose several features of the claimed invention. The authorisation data for the source, a certificate, included neither authorisation data for the playback device, nor any content integrity data. The authorisation of the playback device was not determined at the playback device, but at the source on the basis of a certificate received from the playback device. All checks were performed before streaming; there was no disclosure in document D4 of any authorisation checks performed by the playback device periodically during the streaming. There was also no suggestion to stop streaming when such checks failed. This synergistic combination of periodic content integrity checks and device authorisation of both content source and playback device resulted in a strong and efficient playback protection scheme.

VIII. In an annex to a summons to oral proceedings, the Board maintained its objections, noting that the application referred in obscure language to authorisation, integrity, and/or validity of data, and suggested that the meaning of these terms should be discussed in the oral proceedings.

IX. In response to the summons, the Board was informed in a letter dated 15 November 2010 that the appellant's representative did not intend to appear at the oral proceedings scheduled for the 3 February 2011.

X. In the oral proceedings held in the absence of the appellant the Board considered the requests filed by

the appellant in writing; after deliberation the Board announced the decision on the appeal.

According to the requests submitted in writing, the appellant has requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 to 12 filed with the statement setting out the grounds of appeal received on 30 May 2008 (main request) or in the alternative on the basis of claims 1 to 12 of auxiliary requests 1 and 2, both requests filed with letter dated 11 August 2010.

Reasons for the Decision

1. The appeal although admissible is not allowable since the requests before the Board do not meet the objections and concerns raised in the communications of the Board (see IV. and VIII. above).

Disclosure of the invention

2. After consideration of the appellant's submissions concerning the disclosure of the invention, the Board maintains the objection under Article 83 EPC 1973. The application does not provide the skilled reader with clear and complete information how to check the validity of the streamed digital content periodically (or even randomly) at the playback device using the content integrity data received with the authorisation data.

This objection does not apply to the whole scope of the claims. Methods for checking the integrity or validity

of multimedia data at the receiver side like a standard CRC error-detecting algorithm (see for example document D5, section 6.2.4.15.3 at p. 164) are part of the common technical knowledge, a fact also invoked by the appellant in its written submissions.

However, the appellant uses the terms integrity and validity in a special sense, namely in the sense of authorisation of the playback (see VII. above). This special usage has full support in the application, which consistently refers to authorisation checks using content integrity values (see for example p. 3, lines 12 to 18; p. 8, lines 13 to 17; p. 9, lines 16 to 21; original claim 2).

Adopting this interpretation for the validity and data integrity, it can not be said any more that a CRC or other standard error-detecting algorithm existed which allows to carry out the claimed periodic validity and integrity checks and to determine intermittently whether playback is authorised.

The appellant explained that such an intermittent authorisation was achieved by including the content integrity values, for example the hash values, into the authorisation data for the entire multimedia stream as allegedly shown in the application, figure 5. Actually, an embodiment transmitting the hash values for all the blocks of the multimedia stream to each single playback device in advance, before starting to transmit the multimedia content itself appears to be rather a surprising solution. While a complete list of hash values would indeed allow to carry out checks at the individual playback devices intermittently in a random

manner, the reason why such checks should prove authorisation of the playback remains obscure.

In any case, the skilled person would not derive such a solution from the application as filed. At p. 9, line 16 ff. the application indicates that "[i]n one embodiment, content integrity values ... are hash values corresponding to one or more portions of the digital content corresponding to authorisation data". "One or more portions " does not mean "all portions" of the multimedia stream. Transmitting the content integrity value for only one portion of the digital content to the playback device makes it impossible to check the hash values for other portions of the multimedia stream and does thus not enable a reliable check for the entire multimedia stream.

Neither does "one or more portions" disclose implicitly the concept of sending all hash values for the entire multimedia stream to the playback devices in advance. Such a solution indeed needs some lateral thinking, considering the extra volume of data traffic generated and the additional security risks caused by sending all such sensitive data in advance over the net. These disadvantages would probably deter the skilled person from taking this "all values solution" into closer consideration, especially since it contradicts the explicitly disclosed alternative "one portion".

Since no other relevant information how to perform the periodic authorisation checks is available from the application the Board concludes that the invention is not disclosed in a manner sufficiently clear and complete for it to be carried out by a person skilled

in the art, contrary to the requirement set out in Article 83 EPC 1973.

Inventive step

3. The submissions of the appellant in support of inventive step are based on interpretations which are neither justified by the wording of the claims nor by the content of the description or the drawings. In particular, there is no clear basis for restricting the scope of the term "authorisation data" in claim 1 to the embodiment shown in figure 5. A wider interpretation of the claims leads to an objection under Article 56 EPC 1973, as will be explained in the following.

Considering the normal technical meaning of the terms used in the application including the claims, the Board holds that the claim wording of all requests covers the data format used in the content protection system disclosed in document D4. In this prior art system, some parts of the authorisation data are transmitted in advance using IEEE 1394 asynchronous packets between source and playback devices while other parts of the authorisation data are transmitted with the multimedia stream using the IEEE 1394 isochronous packet (see the encryption mode indicator EMI in the packet header, Table 2 at p. 9, concerning the authorisation to duplicate content). The Header CRC and Data CRC shown as parts of the IEEE 1394 isochronous packet are cyclic redundancy checksums used for error detection and are thus content integrity values in terms of the present claims. These checksums are generated by using a polynomial algorithm (according to the IEEE 1394

specification, see document D5, section 6.2.4.15 at p. 163). This algorithm is a kind of hash function so that the CRC checksums are hash values in terms of the present application.

Moreover, the claims do neither define any specific time sequence between the method steps, except for some few logical interdependencies, nor any specific distribution of functions concerning the initial authorisation between the source and the playback device. Only the location of the periodic integrity check is clearly defined as "periodically checking, at said playback device, the validity of said streamed digital content" (claim 1 according to all requests). However, also the CRC error-detecting check of the IEEE 1394 isochronous packets in the prior art system is such a periodic check at the receiving side (see document D5, section 6.2.4.15.3 at p. 164).

The Board concurs with the appellant in that document D4 does not disclose what happens when the CRC check indicates an erroneous data packet. The present application claims the stop of replaying the digital content as an essential feature of the invention. The appellant argued that stopping playback was an inventive alternative over the usual methods like dumping or retransmitting the invalid data.

However, simply stopping a technical process that is producing erroneous results is in the absence of exceptional circumstances a trivial measure. What is achieved in the present case by stopping the playback is some protection against tampering of data, but at the price of a needless and annoying interruption when

the invalid data is due to a harmless transmission error, eg caused by noise. Advantages achieved by an invention do not support an inventive step if they are obtained at the price of significant disadvantages which are simply accepted.

Thus, the Board judges that the claimed methods do not meet the requirement of inventive step.

4. In summary, neither the claims filed with the present requests nor the arguments submitted in writing justify a positive assessment of the application. The appeal can thus not be allowed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek S. Wibergh