

Internal distribution code:

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

**Datasheet for the decision
of 23 March 2017**

Case Number: T 2452/11 - 3.5.04

Application Number: 02792388.7

Publication Number: 1486071

IPC: H04N7/167

Language of the proceedings: EN

Title of invention:

Elementary stream partial encryption

Applicant:

Sony Electronics, Inc.

Headword:

Relevant legal provisions:

EPC 1973 Art. 54(1), 54(2), 56

Keyword:

Novelty - main and first auxiliary requests (no)

Inventive step - second and third auxiliary requests (no)

Decisions cited:

Catchword:



Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 2452/11 - 3.5.04

D E C I S I O N
of Technical Board of Appeal 3.5.04
of 23 March 2017

Appellant: Sony Electronics, INC.
(Applicant) One Sony Drive
Park Ridge,
New Jersey 07656 (US)

Representative: D Young & Co LLP
120 Holborn
London EC1N 2DY (GB)

Decision under appeal: Decision of the Examining Division of the
European Patent Office posted on 7 June 2011
refusing European patent application
No. 02792388.7 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman C. Kunzelmann
Members: R. Gerdes
T. Karamanli

Summary of Facts and Submissions

- I. The appeal is directed against the decision to refuse European patent application No. 02 792 388.7, published as international application WO 03/061173 A2.
- II. The patent application was refused by the examining division on the grounds of added subject-matter (Article 123(2) EPC), lack of clarity (Article 84 EPC) and lack of inventive step (Article 56 EPC) in view of documents:
- D1: US 5 796 829 A and
D3: US 5 420 866 A.
- III. The applicant (appellant) appealed against this decision and with the statement of grounds of appeal submitted claims of a main request and first to third auxiliary requests. It also indicated that these claims corresponded to those requests underlying the decision under appeal, save for clarifying amendments.
- IV. The board issued a summons to oral proceedings and sent a communication annexed to the summons, raising objections under Article 123(2) EPC and Article 84 EPC 1973 against the main request. The board also indicated that it considered the device of claim 7 of the main request to lack novelty over a "legacy television receiving device" which was acknowledged as prior art in the application. Moreover, the board expressed its provisional opinion that the subject-matter of claims 1, 6 and 12 lacked inventive step over the "full dual carriage system" referred to in the application. Some of the objections raised against the main request also applied to the auxiliary requests. Moreover, the board referred to documents

D2: WO 98/08341 A1 and

D2e: US 6 307 939 B1, which was a family member of D2 in English.

V. The appellant replied by letter of 22 February 2017 and by letter of 17 March 2017.

VI. Oral proceedings were held before the board on 23 March 2017.

Firstly, it was discussed whether the subject-matter of claim 7 of the main request and claim 6 of the first auxiliary request was novel with respect to the prior art cited in the application itself.

Then a discussion followed on the question of whether the subject-matter of claim 1 of the second auxiliary request was inventive with respect to a full dual carriage system referred to as the closest prior art in the application itself in combination with document D2e or in combination with document D2e and common general knowledge, *inter alia* in view of document D3.

Thereafter, it was discussed whether the subject-matter of claim 1 of the second auxiliary request was inventive with respect to a full dual carriage system referred to as the closest prior art in the application itself in combination with common general knowledge.

Thereafter, it was discussed whether the subject-matter of claim 1 of the third auxiliary request was inventive with respect to the full dual carriage system referred to in the application itself in combination with common general knowledge.

The appellant's final request was that the decision under appeal be set aside and that a patent be granted on the basis of the claims according to the main request or to one of the first to third auxiliary requests, all requests filed with the statement of grounds of appeal.

VII. Claim 7 of the main request reads as follows:

"A television signal receiving device (36) comprising:

a receiver receiving a partially multiple encrypted television signal comprising a first encrypted elementary stream formed by encrypting one of an audio elementary stream, video elementary stream and system information elementary stream under a first encryption algorithm and a second encrypted elementary stream formed by encrypting the one of the audio elementary stream, the video elementary stream and the system information elementary stream under a second encryption algorithm, and an unencrypted elementary stream of the audio elementary stream, the video elementary stream and the system information elementary stream;

a filter configured to remove and discard the second encrypted elementary stream from the partially multiple encrypted television signal;

a decrypter that receives the first encrypted elementary stream from the receiver that are encrypted under the first encryption algorithm and decrypts the first encrypted elementary stream under a first decryption algorithm; and

a decoder that receives and decodes the decrypted elementary stream from the decrypter and the

unencrypted elementary stream to produce a television signal representing a television program suitable for play on a television receiver."

VIII. Claim 6 of the first auxiliary request reads as follows:

"A television signal receiving device (36) comprising:

a receiver receiving a partially multiple encrypted television signal comprising a first encrypted elementary stream formed by encrypting a system information elementary stream under a first encryption algorithm and a second encrypted elementary stream formed by encrypting the system information elementary stream under a second encryption algorithm, an unencrypted audio elementary stream, and an unencrypted video elementary stream;

a filter configured to remove and discard the second elementary stream from the partially multiple encrypted television signal to produce a filtered signal;

a decrypter that receives the first encrypted elementary stream from the receiver that are encrypted under the first encryption algorithm and decrypts the first encrypted elementary stream under a first decryption algorithm; and

a decoder that receives and decodes the decrypted elementary stream from the decrypter, the unencrypted audio elementary stream and the unencrypted video elementary stream to produce a television signal representing a television program suitable for play on a television receiver."

IX. Claim 1 of the second auxiliary request reads as follows:

"A method of multiple encrypting a digital television signal representing a television program, comprising:

encrypting a selected one of an audio elementary stream, a video elementary stream and a system information elementary stream of the digital television signal according to a first encryption method to produce a first encrypted elementary stream;

encrypting the selected elementary stream of the digital television signal according to a second encryption method to produce a second encrypted elementary stream; and

combining the first encrypted elementary stream and the second encrypted elementary stream with at least one unencrypted elementary stream of the audio elementary stream, the video elementary stream and the system information elementary stream of the digital television signal to produce a partially multiple encrypted television signal representing the television program."

X. Claim 1 of the third auxiliary request reads as follows:

"A method of multiple encrypting a digital television signal representing a television program, comprising:

encrypting a system information elementary stream of the digital television signal according to a first encryption method to produce a first encrypted elementary stream;

encrypting the system information elementary stream of the digital television signal according to a second encryption method to produce a second encrypted elementary stream; and

combining the first encrypted elementary stream and the second encrypted elementary stream with an unencrypted audio elementary stream and an unencrypted video elementary stream to produce a partially multiple encrypted television signal representing the television program."

XI. In the decision under appeal the examining division held inter alia that the features of having the same elementary stream duplicated and encrypted according to two encryption algorithms and one stream not encrypted in the transport stream received at the receiver were not limiting features of the receiver. These features did not characterise the receiver itself but the signal actually received by the receiver or how the transport stream might have been generated. This reasoning applied also to the corresponding claim directed to a television signal receiving device of the first auxiliary request (see decision under appeal, Reasons, points 2.1.2.4 and 2.2.3).

XII. The appellant's arguments may be summarised as follows:

The television signal receiving device of claim 7 of the main request was not characterised by the incoming signal but by the way this signal was handled in the receiver. Compared to the "legacy receiver" referred to in the present application, this difference was expressed by the feature of "a filter configured to remove and discard the second encrypted elementary stream from the partially multiple encrypted television

signal". The filtering according to claim 7 could not be equated with the step of ignoring secondary PID packets that was effected by a legacy receiver (see present application, page 23, last paragraph). Instead, as described on page 45, last paragraph, to page 46, first paragraph, the receiver's CPU buffered and processed the filtered packets (corresponding to the selected program) before selected PIDs (corresponding to the inapplicable encryption method) were stripped from the buffered transport stream. The filtering implied that buffered data were "manually" filtered to eliminate packets containing unneeded PIDs.

Concerning novelty of the subject-matter of claim 6 of the first auxiliary request, the appellant referred to the arguments presented in respect of the main request.

Regarding claim 1 of the second auxiliary request the appellant agreed that starting from the full dual carriage system as closest prior art the technical problem could be formulated as how to provide a television signal which was compatible with several conditional access systems and which operated at reduced bandwidth requirements.

D2e disclosed signal components that could be "left in the clear", but it related to a system in which "each component making up the program exists only once, even if it is scrambled" (see D2e, column 4, lines 20 and 21). In addition, D2e was concerned with the marketing of television programs and not with bandwidth reduction (see D2e, column 1, lines 20 to 24 and column 5, lines 5 to 21). Hence, the skilled person would not have resorted to D2e to solve the above technical problem.

The reference in D3, column 3, lines 23 to 27 to the development of the MPEG-2 systems standard was to be understood in the sense that the standard supported encryption on a "stream by stream" basis, not in the sense that some elementary streams could be left unencrypted.

Starting from the full dual carriage system the skilled person would have to implement two steps to arrive at the claimed subject-matter:

- (a) firstly s/he would have to realise that some elementary streams could be sent unencrypted,
- (b) secondly s/he would have to realise that some elementary streams could be used for different groups of consumers.

There was no hint in the documents on file to modify the full dual carriage system in such a way that some elementary streams could be left unencrypted. Also the analogue systems which were discussed in the application (see page 5, second full paragraph) did not lend themselves to sharing signal components.

Claim 1 of the third auxiliary request was limited to an encryption of the system information elementary stream only. Without the possibility to decrypt the system information, the receiver had no knowledge of which stream belonged to which program. There was very low overhead in terms of bandwidth caused by the encryption of the system information according to two different encryption methods.

Reasons for the Decision

1. The appeal is admissible.

The present application

2. The present application relates to the field of encryption systems for digital television signals. Conditional access (CA) systems are used to control availability of television content which is provided in content delivery systems such as cable systems. These systems come as matched sets - one part is integrated into the cable system headend and encrypts content, the other part provides decryption using the corresponding decryption keys and is built into the set-top boxes (STBs) installed in users' homes. Once a cable operator picks an encryption scheme, it is difficult to change or upgrade the scheme without introducing a backward-compatible STB (see present application, pages 2 and 3).

The present application acknowledges that "full dual carriage" systems were known in order to be able to migrate to a new encryption scheme B and maintain compatibility with the "legacy STBs" operating with the old encryption scheme A. "Full dual carriage" means that the transmission of the television signal is duplicated for each encrypted program - once for each type of CA system to be used. Hence, full dual carriage comes at the expense of doubling the bandwidth required to transmit a television program (see present application, page 4).

In order to reduce the required bandwidth for the transmission of television content according to two CA systems, the present application proposes a "virtual dual carriage" system which only selects certain portions of the television signal such as one of its audio, video or system information elementary streams for encryption according to the two CA systems. The other portions are transmitted unencrypted or "in the clear". Bandwidth can be conserved because the same unencrypted portion can be sent to all varieties of STBs.

Main request and first auxiliary request

3. Claim 7 of the main request is directed to a television signal receiving device.
- 3.1 Some of the features of the receiver specify the "partially multiple encrypted television signal" which is received by the receiver. It is established jurisprudence of the boards of appeal that novelty of a claimed device has to exist in the device per se (see, for instance, G 2/88, point 5 of the Reasons). A signal received by a claimed receiver can therefore only lead to novelty of the claimed receiver (over a given prior-art receiver) if the structure or the content of the signal implies a difference between the claimed receiver and the prior-art receiver in question.
- 3.2 In the present case such implications are ruled out by the goal of the invention that "legacy" set-top boxes/receivers should be operational with the new signal; in other words the signal is generated such that legacy STBs can receive the signal and perform their function unaffected by the modification of the signal (see present application, page 19, first paragraph or

page 24, last paragraph). The legacy STBs perform the function of "ignoring 'bad packets'", which implies that packets of the second encrypted elementary stream are ignored by the decoder. This operation corresponds to the claimed filtering function. In addition, the legacy STBs also comprise a decrypter and a decoder as specified in claim 7 (see page 23, last paragraph).

- 3.3 The appellant argued that, as described on page 45, last paragraph, to page 46, first paragraph, the receiver's CPU buffered and processed the packets before selected PIDs were stripped from the incoming transport stream. The filtering implied that buffered data were "manually" filtered to eliminate packets containing unneeded PIDs.
- 3.4 The cited passage relates to a possible implementation of the receiver in terms of its hardware structure (see Figure 14). The sequence of steps carried out in the receiver is not specified in detail, for example the kind of processing effected by the CPU is not indicated except for the vague step of "manually" filtering the buffered data. More importantly, this filtering is not represented by corresponding features in the claim.
- 3.5 In view of the above, claim 7 specifies a legacy television receiving device which is known from the prior art cited in the application itself. Thus, the claimed device is not new (Article 54(1) and (2) EPC 1973).
4. Claim 6 of the first auxiliary request essentially corresponds to claim 7 of the main request. It is limited to a receiver receiving a system information elementary stream encrypted under a first and a second encryption algorithm whereas the audio and video

elementary streams are received unencrypted. In addition, the feature relating to the filter has been modified to read "a filter configured to remove and discard the second ~~encrypted~~ elementary stream from the partially multiple encrypted television signal **to produce a filtered signal**" (deletions marked by the board in strike-through, additions in bold).

4.1 The limitation to the receiving of an encrypted system information elementary stream with the remaining streams being unencrypted relates to properties of the signal which do not have further implications for the structure or functionality of the receiver. The modifications of the feature relating to the filter also do not change the reasoning above (see section 3) and the appellant did not provide arguments to the contrary.

4.2 Hence, the same reasoning as for claim 7 of the main request applies to claim 6 of the first auxiliary request. It follows that the subject-matter of claim 6 is not new (Article 54(1) and (2) EPC 1973).

Second and third auxiliary requests

5. It is common ground that the "full dual carriage" system described in the application (see point 2 above) can be considered as the closest prior art for the subject-matter of claim 1 of the second and third auxiliary requests.

5.1 Claim 1 of the second auxiliary request differs from the encryption method of the full dual carriage system in that the digital television signal is produced from

- (i) a selected elementary stream which has been encrypted according to a first encryption method and
- (ii) the same elementary stream encrypted according to a second encryption method together with
- (iii) at least one unencrypted (other) elementary stream

to produce a partially multiple encrypted television signal representing the television program.

Hence, at least one stream is transmitted as unencrypted information "in the clear". This contrasts with the full dual carriage system, which transmits two encrypted versions of the television program, thereby duplicating the transmission (see application, page 4, first full paragraph).

- 5.2 This distinction has the technical effect that the "bandwidth costs" are reduced (see application, page 8, second paragraph).
- 5.3 It is also common ground that the technical problem can be regarded as how to provide a television signal which is compatible with several conditional access systems and which operates at reduced bandwidth requirements (see application, page 8, first two paragraphs).
- 5.4 The skilled person is considered to be knowledgeable in the field of protection of television content from unauthorised viewing. This person is acquainted with the relevant protection systems for analogue and digital television systems. The skilled person is also familiar with the relevant standards in the field of television.

5.5 Considering this, the skilled person would have been aware that the MPEG-2 standard accommodates encryption on an individual (elementary) stream basis (see, for example D3, column 3, lines 23 to 27 and D2e, section entitled "State of Prior Art", column 2, lines 53 to 57). Furthermore, analogue television systems obscuring only the video or the audio signal component and sending the other signal component in the clear were well known at the effective filing date of the application. Also for digital television systems this knowledge was state of the art (see present application, page 5, second full paragraph and D2e, section entitled "State of Prior Art", column 3, lines 19 to 22).

Hence, in order to solve the technical problem the skilled person would have sent a part of the signal or an elementary stream in the clear, thus obviating the need to send the stream encrypted according to two different encryption methods.

5.6 The appellant argued that starting from the full dual carriage system the skilled person would have to implement two steps to arrive at the claimed subject-matter:

- (a) firstly s/he would have to realise that some elementary streams could be sent unencrypted, and
- (b) secondly s/he would have to realise that some elementary streams could be used for different groups of consumers.

The board does not object to this analysis. However, both of these steps are obvious for the skilled person. As explained above, sending some of the elementary

streams unencrypted was a well-known option for the skilled person. The skilled person would also have been aware that transmitting two identical unencrypted streams was a waste of bandwidth, so that one of these streams could be dispensed with.

With respect to the appellant's argument that the analogue systems which were discussed in the application (see page 5, second full paragraph) did not lend themselves to sharing signal components, the board holds that the underlying bandwidth considerations apply equally to digital and analogue broadcast systems.

- 5.7 Hence, the subject-matter of claim 1 of the second auxiliary request lacks inventive step in view of the "full dual carriage" system disclosed in the application itself and the common general knowledge of the skilled person.

6. Compared with claim 1 of the second auxiliary request, claim 1 of the third auxiliary request is further limited by specifying the encryption of a system information elementary stream under a first and a second encryption algorithm. The encrypted system information elementary streams are combined with unencrypted video and audio elementary streams to produce the partially multiple encrypted television signal.

- 6.1 This limitation amounts to a selection of one of the elementary streams of the television signal for encryption. Together with the video and audio content, the system information belongs to the basic information that makes up the television signal (see present application, page 4, penultimate paragraph and

figure 1). Hence, it would have been an obvious choice for the skilled person to select the system information elementary stream for encryption, whereas the video and audio elementary streams were transmitted unencrypted.

6.2 The appellant correctly argued that this choice implied very low overhead in terms of bandwidth. Nevertheless, the board considers this choice obvious. It is part of the common general knowledge that to protect information against unauthorised access, only key components need be encrypted. Hence, to reduce the required overhead in terms of bandwidth and processing power the skilled person would have considered only encrypting the system information.

6.3 It follows from the above that the subject-matter of claim 1 of the third auxiliary request lacks inventive step (Article 56 EPC 1973).

Conclusion

7. Since none of the appellant's requests is allowable, the appeal has to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar:

The Chairman:



L. Malécot-Grob

C. Kunzelmann

Decision electronically authenticated