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 21 October 2008

Case Number: T 1339/04 - 3.5.04

Application Number: 98962647.8

Publication Number: 1040663

IPC: H04N 7/167

Language of the proceedings: EN

Title of invention:
Scrambling unit for a digital transmission system

Applicant:
Nagra Thomson Licensing

Opponent:
-

Headword:
-

Relevant legal provisions:
-

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

Keyword:
"Inventive step (no)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1339/04 **-** 3.5.04

D E C I S I O N
of the Technical Board of Appeal 3.5.04
of 21 October 2008

Appellant: Nagra Thomson Licensing
46, Quai Alphonse Le Gallo
F-92100 Boulogne-Billancourt (FR)

Representative: Wenger, Joel-Théophile
Leman Consulting S.A.
Chemin de Précossy 31
CH-1260 Nyon (CH)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 14 May 2004 refusing European application No. 98962647.8 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: B. Müller
Members: A. Dumont
M. Paci

Summary of Facts and Submissions

I. The appeal is directed against the decision by the examining division to refuse European patent application No. 98962647.8, published as WO 99/33271.

II. The following documents were *inter alia* cited by the examining division:

D1: EP-A-0 762 765 A2

D3: MICHON V et al.: "How to integrate access control mechanisms into digital HDTV systems?", Signal Processing: Image Communication, vol. 4, nos. 4/5, August 1992, pages 421 to 428, Amsterdam, NL.

D4: ETS 300 174, "Network Aspects (NA); Digital coding of component television signals for contribution quality applications in the range 34 - 45 Mbit/s", European Telecommunications Standards Institute, November 1992, pages 1 to 79.

III. The application was refused on the ground that the subject-matter of claim 1 lacked novelty in view of D3. Essentially the examining division held that D3, like claim 1, was concerned with a scrambling unit for a digital audiovisual transmission system (see page 424, left-hand column, line 14 *et seq.*). D3 indicated that scrambling was done after multiplexing. It was therefore safe to assume that two different devices carried out these operations.

The examining division further held in the decision under appeal that the subject-matter of the dependent claims was not novel and inventive over the prior art, referring to the reasons set out in the International

Preliminary Examination Report dated 7 March 2000. It follows from Section V of this report in particular that the subject-matter of dependent claim 11, relating to one or more access control systems being adapted to receive a control word supplied by central control means and to send back to the central control means an encrypted message containing the control word, was considered to lack inventive step, as "access control systems" were disclosed in D1 (column 1, line 24 *et seq.*).

IV. In official communications the board drew the appellant's attention to D3 distinguishing between multiplexer and scrambler as different functional units, so that implementing them as physically separate units might be a matter of normal design choice. The board further noted that the control words and the ECM messages were separately provided to the "multiplex service" according to figure 21 of D4 and appeared to be neither generated, modified nor used by the multiplexer. Providing these pieces of information directly to the scrambling unit would appear obvious to the skilled person. The appellant's attention was further drawn to the prior art acknowledged in the present application (page 2, lines 11 to 18) for features of simulcrypt systems and to the fact that if substantially amended claims were filed the case might have to be remitted to the examining division for further prosecution.

V. Oral proceedings before the board took place on 21 October 2008.

VI. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 to 8 filed with the letter dated 8 October 2008 or, in the alternative, that the case be remitted to the first instance for further prosecution on the basis of claims 1 to 8 filed with the letter dated 8 October 2008.

VII. Claim 1 reads as follows.

"A scrambling system for a digital audiovisual transmission system comprising a central control station and a scrambling unit, the scrambling unit comprising an input for receiving an assembled transport packet stream from a physically separate multiplexer, a scrambling device for scrambling the received transport stream according to a control word and an output for sending the scrambled transport stream to a transmitter means for subsequent transmission, so as to permit the scrambling of the transport packet stream by the scrambling unit independently of the multiplexer operations, characterized in that, the scrambling system comprises a first and at least s *[sic]* second access control systems connected to the central control means and adapted to receive a control word supplied by the central control means and to send back an encrypted message containing the control word, the first access control system having means to generate first encrypted messages and the second access control system having means to generate second encrypted messages, the scrambling unit receiving the control word from the central control unit and comprising insertion means to

insert said first and second messages into the transport stream."

VIII. The appellant essentially argues as follows.

The technical problem of ensuring a high level of security whilst allowing for easy management of various pools of decoders is solved by the combination of the following four features of claim 1:

(a) the multiplexer being placed before the scrambling unit;
(b) the scrambling unit being physically separate from the multiplexer and comprising the means for inserting the encrypted messages into the transport stream;
(c) the central control station providing the control word being a specific device and
(d) the provision of more than one access control system.

The combination cannot be derived from the prior art for the following reasons.

- The prior art conventionally discloses control words generated by the multiplexer and ECM messages inserted into the transport stream at the level of the multiplexer (see the present application, page 1, lines 24 to 27). Section 3.1 of D3 discloses that the ECM message is contained in the "useful data" of the signal multiplex, so that it is not inserted into the assembled transport stream. D3 is also silent about the source of the control word, so that the skilled

reader can deduce that the control word is generated within the scrambler. D3 and D4, which is to be considered as incorporated into D3, disclose no more than what is described in the introduction of the present application, namely that scrambling and multiplexing are closely intertwined (see in particular D3, page 428, lines 5 and 6, setting out that the scrambling function is closely dependent on the coding of the digital signal and the structure of the multiplex). In contrast thereto, the control word and the ECM message being generated by an external specific device relieves the security constraints placed on the multiplexer, whilst allowing for more complex and more secure algorithms for control word generation and scrambling.

- D3 mentions constraints for the timing of ECM messages (see for instance section 3, first paragraph). The scrambling unit and the multiplexer are therefore not physically separate. In contrast thereto, the provision of a specific, external device allows for more time to generate the control words according to more refined algorithms.
- D1 does not disclose a scheme with more than one access control system. It also discloses no authentication by central control means.

Reasons for the Decision

1. The appeal is admissible.

2. *Novelty*

It is not disputed that D3 constitutes the closest prior art and discloses a scrambling system with a multiplexer, a scrambling unit and a transmitter means for transmitting the scrambled transport stream. The means for inserting the ECM messages are not comprised in the scrambling unit. The appellant further accepts that it is known from the prior art that the multiplexer may be placed before the scrambling unit (see D3, page 424, left-hand column, line 14 *et seq.*). As a result, feature (a), mentioned in section VIII above, is known from the prior art.

The board considers that the technical features (b) to (d), mentioned in section VIII above, are neither explicitly nor implicitly disclosed in D3 and that they are the only features distinguishing the subject-matter of claim 1 from the closest prior art.

3. *Inventive step*

3.1 The technical problem

The appellant formulates the technical problem as ensuring a high level of security whilst allowing for easy management of various pools of decoders.

The present application mentions security problems related to encoding systems integrating the scrambling, multiplexing and control word ("CW") generation in the context of a particular implementation, in which an access control means receives the control word from the multiplexer and encrypts it before sending the

encrypted message back to the multiplexer (see the paragraph bridging pages 1 and 2 of the description; page 2, lines 20 to 24; and page 3, lines 10 to 14). The present application further mentions that providing for a number of access control systems in parallel allows a content provider to broadcast the audiovisual data to a mixed pool of decoders, this possibility being commonly known as "simulcrypt" (see page 2, lines 11 to 18 and page 8, lines 20 to 25).

3.2 No synergetic effects

It follows from the above that allowing for easy management of a mixed pool of decoders is related to feature (d), whereas providing a high level of security is related to the other novel features (b) and (c). Thus claim 1 contains specific features relating to the solutions to each of the two parts of the problem. The board cannot see interactions between features (b) and (c) on the one hand and feature (d) on the other producing a synergetic effect. The board is unable to discern, for instance, how increasing the number of access control systems in parallel according to feature (d) would interact with the other features (b) and (c) to improve security or how features (b) or (c) would contribute to managing a mixed pool of decoders, which is related to feature (d). The appellant could also not provide concrete information about any such effects. Features (b) and (c) on the one hand and feature (d) on the other thus are not functionally interdependent for the purpose of solving the two parts of the problem, which are thus two partial problems. As a result, the board considers that claim 1 sets out no more than a mere aggregation of these two sets of features. In

these circumstances the combined effect of the features (b) and (c) on the one hand and feature (d) on the other cannot be said to involve an inventive step. What has to be established instead is whether either features (b) and (c) on the one hand or feature (d) on the other, considered separately, is obvious in the light of the prior art.

3.3 Features (b) and (c)

3.3.1 As pointed out by the appellant, D3 does not disclose a practical implementation of the means generating the control word and of the access control system. D4, to which D3 explicitly refers, shows in figure 21 on page 52 the functional block diagram of an encoder receiving the control words (CWs) for scrambling and the encrypted ECM messages through a conditional access interface, whereas the audiovisual data is provided at the input of a "Multiplex Service". The various functions, in particular multiplexing, scrambling and distributing the encrypted control word, are disclosed as distinct functions. D3 (see page 428, lines 5 and 6) mentions that the scrambling function is closely dependent on the coding of the digital signal and the structure of the multiplex (i.e. the structure of the data stream). This is interpreted by the board as a reminder of general functional requirements given to a designer specifying the access control system as a whole (see D3, page 428, lines 1 to 4) but does not address the practical implementation of the system either as physically integrated or with discrete components. This aspect is mentioned nowhere in the prior art.

3.3.2 As a result, the board sees no reason for the skilled person to envisage an integrated solution and it cannot therefore share the appellant's view that the prior art discloses an encoder in which the units (control word generator, access control system, multiplexer, scrambler), performing the above-mentioned functions, are so intertwined that they must be physically integrated.

3.3.3 Moreover the prior art discloses the ECMs being contained in the multiplex, which is the data supplied to the transmitter means (see D3, section "3.1. Nature of transmitted data" and D4, section 10.1 on page 43). The board cannot therefore concur with the appellant's view that the encrypted messages are necessarily supplied to the multiplexer in the prior art.

3.3.4 As a result, the person skilled in the art, starting from D3 (read together with D4) to design an encoder, would routinely envisage the well-known pros and cons of an integrated unit versus an implementation with physically discrete units and would as a mere matter of design choice opt for an implementation with a central control station, a scrambling unit and a physically separate multiplexer. Furthermore, since the ECM messages containing the encrypted control word are required neither by the multiplexer (which does not use the control word) nor by the scrambler (which does not scramble the ECMs; see D3, page 423, section 3.1, second paragraph), the skilled person would also as a mere matter of design insert the encrypted messages in the signal path at any suitable place before the transmitter means, for instance after the multiplexer. The particular choice made in features (b) and (c)

according to claim 1 is therefore considered by the board to be obvious.

3.3.5 The board is furthermore of the opinion that a fully integrated solution may in theory implement equally powerful algorithms as discrete solutions. The present application does not teach any particular practical technical measure leading to more security or better synchronisation. On the contrary, the solution according to claim 1 requires the transmission of sensitive information (the control word) between the central control station and the scrambling unit over a communication link, which may be a plain TCP/IP link in the present application (see the description, page 8, line 30 to 33). Such a link does not per se improve security or synchronisation. The board is therefore not convinced that features (b) and (c) discussed in the foregoing inherently have the beneficial effects ascribed to them by the appellant.

3.4 Feature (d)

The appellant has not contested that the provision of more than one access control means for easy management of a mixed pool of decoders is known in the prior art as "simulcrypt" (see the description of the present application, page 2, lines 11 to 18). The board is of the opinion that providing in the system according to D3 additional access control means and means for inserting the corresponding additional messages into the transport stream (feature (d)) to solve the same (partial) problem in the context of the present invention was an obvious measure.

3.5 Conclusion

For the above reasons, the subject-matter of claim 1 does not involve an inventive step (Article 56 EPC 1973). Claim 1 is consequently not allowable.

It follows that there is no basis for any further prosecution of the application. Thus the appellant's alternative request that the case be remitted to the first instance for further prosecution on the basis in particular of claim 1 has no purpose.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar The Chairman

D. Sauter B. Müller