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

D E C I S I O N
of 29 September 2004

Case Number: T 0090/02 - 3.5.3

Application Number: 92307041.1

Publication Number: 0528572

IPC: H04L 29/06

Language of the proceedings: EN

Title of invention:
Device for encrypting and decrypting of signals

Patentee:
CONTROL LOGIC (PROPRIETARY) LIMITED

Opponent:
Giesecke & Devrient GmbH

Headword:
Selectively encrypting or decrypting/CONTROL LOGIC

Relevant legal provisions:
EPC Art. 100(a), (b), (c), 52, 56

Keyword:
"Inventive step - yes"

Decisions cited:
G 0010/91

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0090/02 - 3.5.3

D E C I S I O N
of the Technical Board of Appeal 3.5.3
of 29 September 2004

Appellant: (Proprietor of the patent)	CONTROL LOGIC (PROPRIETARY) LIMITED 270 Brickfield Road Durban, Natal Province (ZA)
Representative:	Nicholls, Michael John J.A. KEMP & CO. 14, South Square Gray's Inn London WC1R 5JJ (GB)
Respondent: (Opponent)	Giesecke & Devrient GmbH Prinzregentenstrasse 159 D-81677 München (DE)
Representative:	-

Decision under appeal: **Decision of the Opposition Division of the European Patent Office posted 26 October 2001 revoking European patent No. 0528572 pursuant to Article 102(1) EPC.**

Composition of the Board:

Chairman: A. S. Clelland
Members: D. H. Rees
R. Moufang

Summary of Facts and Submissions

I. European Patent No. 0 528 572 was revoked in a decision given at oral proceedings held on 18 September 2001, with written reasons despatched on 26 October 2001.

II. The patent had been opposed on the grounds that the subject-matter of the claims as granted did not involve an inventive step (Articles 100(a), 52 and 56 EPC) and that the subject-matter of the patent extended beyond the content of the application as filed (Article 100(c) EPC). The following documents were cited:

D1: EP 0 209 811 A

D2: EP 0 282 992 A

III. The independent claims of the request on which the opposition division's decision was based read as follows:

"1. An electronic coding device (21) for selectively encrypting or decrypting data signals, comprising:
a processor (24) to code digital data in accordance with a selectable one of a predetermined encryption and a predetermined decryption algorithm (33, 40), the processor (24) having an input for receiving a digital input signal and an output for generating a coded digital output signal; and
a configuration storage memory (27) connected to the processor (24),
characterised in that
the configuration storage memory (24) [sic] is instructable to select one of the predetermined

encryption algorithm and predetermined decryption algorithm and to convert the coded digital output signal produced by the processor (24) after encryption and after decryption to conform to any one of a number of predetermined protocols."

"5. A method of configuring an electronic coding device for selectively encrypting or decrypting data signals, comprising the step of:
interfacing a programming means (50) to a configuration storage memory (27) connected to a processor (24) for coding digital data in accordance with a selected one of a predetermined encryption and a predetermined decryption algorithm (33, 40), the processor (24) having an input for receiving a digital input signal and an output for generating a coded digital output signal; and
characterised in that it includes the further steps of instructing the configuration storage memory (27) to select one of the predetermined encryption algorithm and predetermined decryption algorithm, and
instructing the configuration storage memory (27) to selectively convert the coded digital output signal produced by the processor (24) after encryption and after decryption to conform to any one of a number of predetermined protocols."

IV. The opposition division found that the application as amended in this request satisfied the requirements of Articles 123(2) and (3) EPC and that the subject-matter of the independent claims was new, but did not involve an inventive step, having regard to the combination of D1 and common general knowledge.

V. Notice of appeal was filed with the appropriate fee on 24 December 2001 and a statement of grounds of appeal was submitted in a letter dated 25 February and received 26 February 2002. The appellant (patentee) requested that the decision of the opposition division be set aside and that the patent be maintained according to a main or one of six auxiliary requests submitted with the statement of grounds. The independent claims of the main request were the same as those of the main request on which the decision of the opposition division was based. In a letter dated 13 August and received 19 August 2002 the respondent (opponent) argued that the subject-matter of all the requests did not involve an inventive step. Both parties made conditional requests for oral proceedings.

VI. In a communication accompanying an invitation to oral proceedings the board noted that the reference sign "24" for the configuration storage memory at one point in claim 1 of the patent as granted should read "27", which error extended to all the appellant's requests for the appeal. In response, the appellant submitted versions of the requests with the reference numeral corrected but otherwise unchanged, received 23 August 2004.

VII. At the oral proceedings the appellant requested that the decision under appeal be set aside and that the patent be maintained on the basis of claims 1 to 22 (part) of the main request filed 23 August 2004 and claim 22 (part, formerly 23) as granted, columns 1 to 4 of the description as filed on 23 August 2004 with inserts 1 and 2 as filed on 29 September 2004 and 23 August 2004 respectively, columns 5 to 9 of the

description as granted and Figures 1 to 6 as granted, or on the basis of corresponding auxiliary requests 1 to 6 as filed on 23 August 2004. The respondent requested that the appeal be dismissed. At the end of the oral proceedings the chairman closed the debate and announced the board's decision.

Reasons for the Decision

1. With respect to the main request, the respondent raised objections of lack of clarity, added subject-matter, insufficient disclosure, and lack of an inventive step. The first three of these objections all arose from the formulation of the subject-matter of claim 1 that "the configuration storage memory (27) is instructable to ... convert the coded digital output signal produced by the processor (24) ... to conform to any one of a number of predetermined protocols", and the equivalent in claim 15. Understood literally, this meant that the configuration storage memory must itself carry out some kind of processing *after* the encoding or decoding processing performed by the processor. In consequence a clarity objection arose because it was not clear how this processing could take place. Further, the processing was not disclosed in the application as filed, leading to the further objections of added subject-matter and, since the skilled person would not know how to carry it out, insufficiency of disclosure. A similar point arose with respect to claim 15, the independent method claim.

2. The feature objected to was included in the independent claims as granted. According to the established case-

law of the Boards of Appeal an alleged lack of clarity in a claim, where that lack of clarity does not arise from amendments to that claim in the proceedings after grant, does not constitute grounds for rejecting the claim, since lack of clarity is not a ground of opposition. This objection therefore fails.

3. Equally, since this feature was present in the independent claims as granted, the objection 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 must be seen as an objection under Article 100(b) EPC. However, this ground for opposition was not considered in the opposition proceedings. As decided in decision G 10/91 (OJ 1993, 420, see point 3 of the Opinion), a board may consider fresh grounds for opposition in appeal proceedings only with the approval of the patentee. In the present case, the appellant (patentee) did not approve the introduction of the new ground.

4. Article 100(c) EPC was considered in the opposition proceedings and the objection of added subject-matter in the patent as granted is therefore not a new ground of opposition. Hence it must be considered on its merits. The board considers that the skilled person would reject a literal reading of the claim as not technically credible, since the usual function of a memory is to store data, not to process it. The skilled person would therefore seek to interpret the claims in the light of the description, from which it would be clear that the feature as claimed is an abbreviated formulation of the memory containing an indicator of the protocol to be used, and the processor responding

to this indicator by carrying out, or causing the I/O port to carry out, the appropriate conversion. The skilled person would also deduce this feature from the application as filed. Thus the feature as claimed does not extend beyond the content of the application as filed.

5. With regard to the question of whether the subject-matter of claim 1 involves an inventive step, it was common ground between the parties that of the cited documents D1 represented the closest prior art. D1 discloses an electronic coding device in the form of an (e.g. bank) terminal, which maintains contact with a central host system including a database, and into which a user's chip card is inserted. Communications with the host system are encrypted using the DES system, and data sent to the chip card is also encrypted using RSA (DES and RSA being two well known encryption methods). Figures 4A and 4B together show a structural diagram of the terminal including DES encryption, DES decryption and RSA encryption units (84, 85 and 82 respectively). Further, in order to deal with a variety of standards of user's cards, the terminal has a "main controller" or processor 77 which obtains a collection of data from the inserted card, the so-called "answer-to-reset" data, which then determines the parameters of the communication between terminal and card (e.g. the maximum voltage used by the terminal). It is thus arguable that the terminal converts its coded digital output signals to the card to conform to any one of a number of predetermined protocols, in the terms of the patent in suit. Moreover, as a step in the protocol adaptation of the terminal to the card, the obtained data are stored in a memory, the "initial parameter

RAM" 76. Thus it is also arguable that this is a configuration storage memory as specified in claim 1 of the patent in suit.

6. However, D1 does not disclose the use of a configuration memory to select one of an encryption and a decryption algorithm. The respondent argued firstly that the skilled person would appreciate that Figure 4 of D1 in fact merely laid out the functions carried out by the terminal, and that in reality these functions would be implemented in a microprocessor. Alternatively, even if the various "arithmetic units" were actual hardware modules in the terminal, they were clearly under the control of "main controller" 77. In either case, the controller or processor would necessarily or at least obviously store data, in the form of a flag or similar, to indicate which of the operations of encryption and decryption should currently be carried out. It would further be obvious to store this data in the RAM with the output protocol data.

7. The board does not find these arguments convincing. In contrast to the invention in the patent in suit, in D1 there is no need to instruct the processor whether to encrypt or decrypt arriving data since the function to be performed is determined simply by its origin. For example, referring to Figure 4, all data received at I/O controller 86 comes from the host. All data received from the host system must be decrypted using the DES algorithm in unit 85. Even if the system were implemented as software running in a general-purpose microprocessor, the system would typically respond to incoming data simply by invoking a software module to decrypt the data (and carry out any other standard

processing for incoming data). There would be no need to set "configuration" data to tell the microprocessor what to do. That would be determined simply by the fact that the software module was running. Indeed there seems to be nothing in D1 excluding both encryption and decryption taking place concurrently, whether this be realised by separate hardware units or by multi-tasking in a processor. A "configuration" of the system to carry out just one of these tasks at a time would seem to be undesirable.

8. Thus the respondent has not identified anything in the disclosure of D1 which would lead the skilled person in the implementation of the system disclosed therein to use a configuration storage memory to store data instructing the selection of one of a predetermined encryption and a predetermined decryption algorithm.

9. The respondent also suggested that the combination of selectable features in a system was in itself commonplace, and that if the skilled person wanted to provide a selection of one of encryption and decryption in D1, it would be obvious to do so by adding to the data in the initial parameter RAM 76 an indication of which was to be selected. However, the respondent has not identified any motivation for the skilled person to provide such an option and in any case the skilled person would in fact be actively discouraged from doing so. Each of the encryption and decryption functions in D1 has a specific purpose; selecting one of them would mean disabling the other, so that the system would be unable to function properly.

10. Document D2 also discloses a system having a memory used for storing data which determines the appropriate protocols to use in communicating with (in this case) a plurality of external devices. However, it does not discuss data encryption or decryption at all, and therefore cannot supply the missing motivation to provide a selected one of these processes.

11. The board accordingly concludes that the subject-matter of claim 1 involves an inventive step having regard to the disclosure of D1 and D2.

12. Claim 15 concerns a method used to enter the configuration data, including the encryption / decryption selection data, in the configuration storage memory. Since no motivation for the skilled person to provide such a configuration has been identified, there is equally no motivation to supply a method of carrying out the configuration and the above conclusion with regard to claim 1 also applies to this claim.

13. Thus none of the objections raised by the respondent against the subject-matter of the claims of the main request are convincing. No objection was raised against the description as amended finally in the oral proceedings.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the first instance with the order to maintain the patent on the basis of claims 1 to 22 (part) of the main request filed 23 August 2004 and claim 22 (part, formerly 23) as granted, columns 1 to 4 of the description as filed on 23 August 2004 with inserts 1 and 2 as filed on 29 September 2004 and 23 August 2004 respectively, columns 5 to 9 of the description as granted and Figures 1 to 6 as granted.

The Registrar: The Chairman:

D. Magliano A. S. Clelland