

Internal distribution code:

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

D E C I S I O N
of 3 July 2002

Case Number: T 0696/99 - 3.5.1

Application Number: 91108281.6

Publication Number: 0458306

IPC: G06K 19/07, G06K 19/073,
G06K 19/077, G07F 7/10

Language of the proceedings: EN

Title of invention:
Portable information medium

Patentee:
KABUSHIKI KAISHA TOSHIBA

Opponent:
GIESECKE & DEVRIENT GmbH

Headword:
Information medium/TOSHIBA

Relevant legal provisions:
EPC Art. 56, 114(2)

Keyword:
"Inventive step (no)"

Decisions cited:
T 0633/97

Catchword:
-



Case Number: T 0696/99 - 3.5.1

D E C I S I O N
of the Technical Board of Appeal 3.5.1
of 3 July 2002

Appellant: GIESECKE & DEVRIENT GmbH
(Opponent) Prinzregentenstrasse 159
D-81677 München (DE)

Representative: -

Respondent: KABUSHIKI KAISHA TOSHIBA
(Proprietor of the patent) 72, Horikawa-cho
Saiwai-ku
Kawasaki-shi
Kanagawa-ken 210-8572 (JP)

Representative: Blumbach, Kramer & Parner GbR
Radeckestrasse 43
D-81245 München (DE)

Decision under appeal: Decision of the Opposition Division of the
European Patent Office posted 5 May 1999
rejecting the opposition filed against European
patent No. 0 458 306 pursuant to Article 102(2)
EPC.

Composition of the Board:

Chairman: S. V. Steinbrener
Members: A. S. Clelland
E. Lachacinski

Summary of Facts and Submissions

I. This appeal is against the decision of the opposition division to reject an opposition against European patent number 0 458 306, the opposition division having held that the subject-matter of claim 1 as granted, the only independent claim, involved an inventive step.

II. The appellant (opponent) lodged an appeal and paid the prescribed fee; it was requested that the decision under appeal be set aside and the patent revoked. An auxiliary request was made for oral proceedings. In the statement of grounds of appeal the prior art documents referred to in the opposition proceedings were again discussed and a new document was cited:

D10: US-A-4 278 837.

The appellant argued that claim 1 as granted lacked an inventive step having regard to the documents discussed in the opposition proceedings and that an additional objection of lack of inventive step arose with respect to the disclosure of D10, which had only been discovered after the end of the opposition proceedings.

III. The respondent (patentee) requested that the appeal be dismissed (main request) or that the patent be maintained on the basis of sets of claims constituting auxiliary requests I to III. A further auxiliary request was made for oral proceedings. The respondent argued that document D10 was not particularly relevant and should not be admitted to the proceedings because it was late-filed. Arguments were also advanced as to why, should D10 be admitted, claim 1 of each request involved an inventive step having regard to the

disclosure of the document.

Following a summons to oral proceedings, communicating the provisional opinion of the Board, the respondent submitted revised auxiliary requests I to IV to replace the auxiliary requests previously on file.

- IV. Oral proceedings were held on the 3 July 2002. In the course of the oral proceedings the respondent withdrew auxiliary requests III and IV and filed a new auxiliary request III.

- V. Claim 1 of the main request, i.e. claim 1 as granted, reads as follows:

"A portable medium (3; 23) including
an integrated circuit device having individual
circuit means integrally formed in a multi-layered
structure on a single chip,
said multi-layered structure comprising:
first circuit means (14, 34) for storing data to
be kept secret, said first circuit means being located
on an intermediate layer of said multi-layered
structure;
control means (11, 12, 13, 31, 32, 33) connected
to said first circuit means, for processing said data
to be kept secret, and for exchanging information with
an external unit, and
second circuit means (15; 35) located on another
layer of said multi-layered structure above said first
circuit means, effecting a protection of said data to
be kept secret in said first circuit means from an
optical analysis carried out from the top of said
multi-layered structure."

VI. Claim 1 of the first auxiliary request reads as follows:

"A portable medium (3; 23) including an integrated circuit device having individual circuit means integrally formed in a multi-layered circuit structure on a single chip, said multi-layered circuit structure comprising: first circuit means (14, 34) for storing data to be kept secret, said first circuit means being located on an intermediate circuit layer of said multi-layered circuit structure; control means (11, 12, 13; 31, 32, 33) connected to said first circuit means, for processing said data to be kept secret, and for exchanging information with an external unit, and second circuit means (15; 35) located on another circuit layer of said multi-layered circuit structure above said first circuit means, effecting a protection of said data to be kept secret in said first circuit means from an optical analysis carried out from the top of said multi-layered circuit structure."

VII. Claim 1 of the second auxiliary request adds to claim 1 of the first auxiliary request that the second circuit means is an EEPROM for storing input information and the first circuit means is a ROM for storing secret data and a program necessary for a control operation. Claim 1 of the third auxiliary request adds to claim 1 of the first auxiliary request that the multi-layered circuit structure comprises four circuit layers arranged on each other and the following features:

"the second circuit means is an EEPROM (15; 35)

for storing input information, said EEPROM (15; 35) being located on a first circuit layer of said four circuit layers,

the first circuit means is a ROM (14; 34) for storing secret data and a program necessary for a control operation, said ROM (14; 34) being located on a second circuit layer of said four circuit layers of said multi-layered circuit structure;

said control means is a CPU (11, 31) being located on a bottom circuit layer of said four circuit layers, for performing general control of said portable medium (3; 23) and exchanging information with an external unit, and

a special arithmetic operation circuit (12; 32) and a RAM (13; 33) are both located on a third circuit layer of said four circuit layers, for encrypting and decrypting an input signal."

VIII. At the end of the oral proceedings the chairman closed the debate and announced the Board's decision.

Reasons for the Decision

1. The appeal complies with the provisions mentioned in Rule 65(1) EPC and is admissible.
2. *Late-filed document*
 - 2.1 Document D10 is referred to by the appellant for the first time in the statement of grounds of appeal and is therefore late-filed. In accordance with Article 114(2) EPC the Board may disregard facts or evidence which are not submitted in due time; nevertheless, following decision T 633/97 (not published in OJ EPO), the Board

tends to a pragmatic approach to new facts or evidence if filed sufficiently early in the appeal proceedings to permit the Board and the other party to deal with them.

2.2 In the present case, D10 was filed at the commencement of the appeal proceedings and the relevant disclosure is relatively straightforward, so that its consideration in these proceedings has not put any special burden on the Board or the respondent. As will be apparent from the discussion below on inventive step, the Board also considers it to be highly relevant. It is therefore admitted to these proceedings.

3. *Background to the invention*

3.1 Although various documents from the opposition proceedings were cited in the statement of grounds of appeal, in the subsequent course of the proceedings the only document addressed by the parties was D10.

3.2 The patent is concerned with a problem which arises in the use of integrated circuit (IC) cards to encrypt and decrypt information. Such cards incorporate a CPU, memory and various other components, either in the form of a single integrated chip or a plurality of interconnected chips carrying out respective functions. These cards are potentially a security risk since a determined thief can remove the card surface and gain access to the ICs buried in it; by optical analysis of the card memory the encryption/decryption algorithm can be deciphered and the card pirated. The object given in the patent is accordingly to provide a portable medium which has the necessary components

incorporated in an integrated form and can prevent optical analysis of the functions of the IC, thereby ensuring improved security.

3.3 This object is solved by what is in effect a 3D construction of the IC, in which the sensitive, secret, data is hidden under a IC portion which contains less sensitive data. In order to arrive at the sensitive data a thief would accordingly be obliged to destroy the topmost IC layer and would be unlikely to retrieve anything of value.

4. *Interpretation of claim 1 (main request and first and second auxiliary requests)*

4.1 In the discussion below additional wording specific to the first and second auxiliary requests is shown in brackets.

4.2 Claim 1 of these requests gives rise to the issue of how many layers are required; it merely states that the multi-layered (circuit) structure comprises first circuit means for storing data to be kept secret, these means being located on an "intermediate (circuit) layer" of the structure, and second circuit means located on "another layer" of the structure above the first circuit means. It was argued by the respondent that the reference to an "intermediate (circuit) layer" necessarily implied three layers, i.e. the "another layer" on top of the "intermediate (circuit) layer" and a further, unspecified, layer beneath the "intermediate (circuit) layer". The Board has not however found it necessary to decide on this question since the conclusions below on inventive step apply equally to the broader interpretation advanced by the appellant

which requires only the specified two layers, and the narrower interpretation advanced by the respondent.

5. *Inventive step (main request and first auxiliary request)*

5.1 The main and first auxiliary requests are considered together since they differ only in the latter request specifying that the layers are circuit layers and the structure a circuit structure; in the Board's view this is also implicit in the main request, so that the claims of these requests do not differ substantially in scope.

5.2 It was common ground at the oral proceedings that the single most relevant document is D10. D10 discloses a portable medium, see column 4, lines 66 to 68. The most relevant embodiment is that shown in Figure 16 and explained with reference to Figure 15 at column 16, line 36 to column 19, line 16. This passage discloses an integrated circuit in the form of a "crypto-microprocessor" having individual circuit means 54, 56 integrally formed in a multi-layered circuit structure on a single chip. The multi-layered circuit structure comprises first circuit means 56 in the form of processor and deciphering layers which include a deciphering circuit 4 and a key register 5, see Figure 15; these circuits store data which is used to decipher a program, see column 16, lines 38 to 60. From column 7, lines 4 to 24 of D10 it can be seen that the object of the device is to ensure that the cipher key stored in register 5 is inaccessible from the outside, i.e. data to be kept secret is stored. A processor 3 is connected to the deciphering circuit 4 and serves as control means to process data to be kept secret and

exchange information with an external unit by means of an external data bus, see Figures 4 to 9. In Figure 16 second circuit means in the form of a ROM layer 54 are located above the first circuit means and effect protection of the data to be kept secret in the first circuit means from an optical analysis carried out from the top of the multi-layered circuit structure, see column 18, line 62 to column 19, line 16. It is observed that D10 is explicitly concerned with preventing the optical analysis of the circuit, see column 16, lines 38 to 42, column 17, lines 19 and 20 and column 18, lines 12 to 59.

5.3 The subject-matter of claim 1 of the main and first auxiliary requests arguably differs from the disclosure of D10 in requiring that the first circuit means be located on an "intermediate (circuit) layer" of the multi-layered (circuit) structure. In Figure 16 of D10 the first circuit means are formed by layer 56 and constitute the bottom circuit layer of the structure, the only layers beneath it being a glass layer 57 and the chip substrate 58. The Board does not consider this distinction, if it is one, to be of inventive significance. The patent in suit makes clear that the object of the invention is to prevent the optical analysis of the functions of the IC, see column 1, lines 52 to 56, column 4, lines 22 to 24 and 35 to 49 and column 5, lines 49 to 56. Such optical analysis can only be carried out from above, as is indeed stated in claim 1, so that the object of the invention is met by the provision of a circuit layer above the first circuit means. Since the circuit means are located on rather than in the respective layers, see column 4, lines 14 to 22, it is intrinsically difficult to analyse a circuit from below and in this case it makes

no difference whether merely the layer itself has to be removed or a plurality of circuit layers. The lower layers cannot serve to meet this object; the reason for the provision of these layers seems rather to be to increase the packing density of the IC, see column 5, line 57 to column 6, line 5.

5.4 The Board accordingly concludes that it would be obvious for the skilled person, given the disclosure of D10, to provide additional circuit layers and that it is a matter of non-inventive design choice whether these layers are located above or below the secret data. The subject-matter of claim 1 of the main and first auxiliary requests accordingly lacks an inventive step.

5.5 In the course of the oral proceedings the respondent argued that D10 included two separate circuit layers for a very specific purpose. This was given at column 19, lines 9 to 16, as being not to protect secret information on one layer but to make it more difficult for a pirate to recover both the stored information and the cryptographic key necessary to decipher it. The Board accepts that this is the case and observes that the patent in suit does not differ in essence from this, in that in the Figure 5 embodiment information stored in EEPROM is readable from the top layer but the secret data is stored in ROM in the layer beneath it.

6. *Inventive step (second auxiliary request)*

6.1 Claim 1 of this request is further limited with respect to claim 1 of the first auxiliary request by the second circuit means being an EEPROM for storing input

information and the first circuit means a ROM for storing secret data and a program necessary for a control operation. The Board notes that although in D10, Figure 15, the memory 12 is described as a ROM, in accordance with column 6, lines 24 to 30 it may be "any of a variety of conventional storage devices, such as solid-state random-access memory (RAM) or read-only memory (ROM), or buffer memories into which the enciphered program has been read". At column 19, lines 9 to 11 it is stated that the bits of memory 12 and circuit 4 can be stored in "electrically alterable form", which the Board takes to include an EEPROM. The Board concludes from this passage that D10 discloses an EEPROM as a suitable memory for storing input information.

- 6.2 Column 17 refers at lines 18 to 20 to the bits in deciphering circuit 4 (corresponding to part of the first circuit means) being stored in volatile form or "in physically less accessible portions of the chip", implying that they are still stored in ROM. It is noted that in connection with Figure 15 it is stated that key register 5 may be a volatile random-access memory if still more security is desired, see column 18, lines 34 to 36; if this is not considered necessary it is clear to a skilled person that a ROM can be used. Although at column 16, lines 54 to 60, deciphering circuit 4 is said to be "a simple substitution table or a bit transposition matrix" it operates on the data from ROM 12 using the key in register 5; the Board considers that this is in effect running a program necessary for a control operation, ie deciphering the data within the terms of the claim, given that deciphering circuit 4 operates under the control of the processor 3.

6.2 The subject-matter of claim 1 of the second auxiliary request accordingly lacks an inventive step.

7. *Inventive step (third auxiliary request)*

7.1 Claim 1 of this request specifies four circuit layers; it will be clear from the above discussion that the Board does not consider that the number of circuit layers plays any part in solving the problem of keeping data secret. The claim otherwise differs from claim 1 of the second auxiliary request merely in specifying additional circuit components which are either known from D10 or rendered obvious by it. Thus, in D10 the first circuit means are located below a second circuit layer of the multi-layered circuit structure and a processor 3 is provided for performing general control of the portable medium and exchanging information with an external unit. The deciphering circuit 4 and key register 5 are considered to constitute a special arithmetic operation circuit for encrypting and decrypting an input signal; it is self-evident that for arithmetic operations to be carried out some RAM will be necessary. The Board takes the view that the layer on which the processor is located is irrelevant to the protection of sensitive data and accordingly concludes that the subject-matter of the third auxiliary request is obvious in view of the disclosure of D10.

7.2 The respondent argued that although it appeared from column 19, lines 9 to 11 of D10 that the memory 12 could be an EEPROM, the text referring to storage in "electrically alterable form", the same passage indicated that the deciphering circuit 4 was of similar construction whereas the second and third auxiliary requests required that the first circuit means be a

ROM. The use of a ROM was contrary to the teaching of D10 which suggested volatile memory in order to improve security. The Board accepts that D10 does not explicitly state that a ROM can be used for storage of the secret data and the control program but takes the view that the manner in which the data and program are stored is merely a question of uninventive design practice, see point 6.1 above; the respondent was unable to give convincing reasons as to why the specific choice of a ROM contributed to the problem of preventing optical analysis of the functions of the IC as set forth at column 1, lines 52 to 56 of the patent in suit.

8. There being no allowable requests, it follows that the patent must be revoked.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The patent is revoked.

The Registrar:

The Chairman:

M. Kiehl

S. V. Steinbrener