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) [X] To Chairmen

D E C I S I O N
of 7 July 1997

Case Number: T 0014/95 - 3.4.1

Application Number: 85101010.8

Publication Number: 0152024

IPC: G07F 7/10

Language of the proceedings: EN

Title of invention:
Portable data storing/processing device

Patentee:
KABUSHIKI KAISHA TOSHIBA

Opponent:
01: Philips Electronics N.V.
02: GAO Gesellschaft für Automation und Organisation mbH

Headword:
-

Relevant legal provisions:
EPC Art. 56

Keyword:
"Independent claims of all requests: 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 0014/95 - 3.4.1

D E C I S I O N
of the Technical Board of Appeal 3.4.1
of 7 July 1997

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

Representative:
Gagel, Roland
Henkel, Feiler, Hänzel & Partner
Möhlstrasse 37
81675 München (DE)

Respondent: (Opponent 01)
Philips Electronics N.V.
Groenewoudseweg 1
NL-5621 BA Eindhoven (NL)

Representative:
Strijland, Wilfred
INTERNATIONAAL OCTROOIBUREAU B.V.
Prof. Holstlaan 6
5656 AA Eindhoven (NL)

Respondent: (Opponent 02)
GAO Gesellschaft für Automation und Organisation mbH
Euckenstrasse 12
D-81369 München (DE)

Representative:
Klunker, Hans-Friedrich, Dr.
Patentanwälte
Klunker . Schmitt-Nilson . Hirsch
Winzererstrasse 106
80797 München (DE)

Decision under appeal: **Decision of the Opposition Division of the European Patent Office posted 3 November 1994 revoking European patent No. 0 152 024 pursuant to Article 102(1) EPC.**

Composition of the Board:

Chairman: G. D. Paterson
Members: H. J. Reich
U. G. O Himmler

Summary of Facts and Submissions

I. The appellant is owner of European patent No. 0 152 024.

II. This patent was revoked by a decision of the Opposition Division on opposition by the respondents "N.V. Philips' Gloeilampenfabrieken" (OI) and "GAO Gesellschaft für Automation und Organisation mbH" (OII). The revocation was based on the grounds that identically worded Claims 1 of the main request, auxiliary request 1 and auxiliary request 2 as filed on 10 October 1994, do not satisfy the requirements of Articles 56 and 52(1) EPC having regard to documents:

D1: US-A-4 211 919,

D2: "Chip Card News", April 1983, No. 5, pages 1 to 8, and

D3: EP-A-0 064 779;

and that independent Claim 2 of the main request as filed on 10 October 1994 is not allowable in view of Article 123(2) EPC.

Claims 1 of the main request, auxiliary request 1 and auxiliary request 2 as filed on 10 October 1994 read:

"1. An IC card which is connectable through a terminal device to a main data processing device and includes a data storing/processing function, said IC card comprising:

a main body (10);

memory means (24) having a memory area which is segmented into a plurality of zones for storing data supplied from said main data processing device to said main body (10); and

access control means (22) for storing an access condition for each zone of said memory means (24) to control the access to each zone;

characterized in that

said access control means (22) further stores an output condition indicating whether or not the data stored in the zones of said memory means (24) is encrypted before being transmitted to the main data processing device, and

encrypting means (26) encrypts the data output from a zone of said memory means (24) when the access condition tor the zone indicates that the data is to be encrypted."

Claims 3 to 6 of the main request, Claims 2 to 6 of auxiliary request 1 and Claims 2 to 5 of auxiliary request 2 are all dependent on a respective Claim 1 with the above wording.

Having regard to above Claims 1, the Opposition Division took the view that their subject-matter differs from the closest prior art disclosed in document D1 in the features defined in their characterising parts. The necessity of encrypting some sensible data stored in the memory of a chip card for security reasons is already known from documents D2 and D3. The solution for protecting access to selective zones of stored data by a password as disclosed in document D1 can be used for solving the encryption criterion problem without any technical modification. The password concept only has to be replaced by the encryption concept. Such substitution does not involve any inventive activity.

Independent Claim 2 of the main request includes features specifying that the access condition data include a (different) password corresponding to each of the zones. These features are not disclosed in the application as filed.

III. The patentee lodged an appeal against this decision, filing with the grounds of appeal on 3 March 1995 new Claims 1 to 6 as his main request, wherein the hitherto existing wording of Claims 1 and 3 to 6 of his former main request (see paragraph II above) was maintained and independent Claim 2 was amended in order to meet the requirements of Article 123(2) EPC.

IV. In a communication annexed to a summons to oral proceedings, the Board expressed its preliminary view that Claim 2 filed on 3 March 1995 may still be regarded as not satisfying Article 123(2) EPC and proposed wording for a possibly allowable amendment in order to overcome this objection.

Having regard to the question of inventive step underlying the subject-matter of Claim 1 the Board took the preliminary view that this item reduces to the question, whether it is obvious to a skilled person to modify the access control means disclosed in document D1 in such a way that it "further stores an output condition indicating whether or not the data stored in the zones of said memory means is (to be) encrypted before being transmitted to the main data proceeding device" and that the encrypting means are activated "when the access condition for the zone indicates that the data is to be encrypted", when integrating the encrypting means disclosed in document D2 or D3 into an IC card such as disclosed in document D1 (i.e. adding a flag for zone-dependent activation of the encrypting means). In view of document

D9: IBM Technical Disclosure Bulletin, vol. 22, No. 5, October 1979, pages 2009 and 2010, cited by respondent OII in its notice of opposition,

and teaching to include into the access condition data "zone data", the question of inventive step underlying Claim 2 depends upon the obviousness of the features defined in paragraph (ii) of Claim 2 (see paragraph V below), concerning the addition of flags for a zone dependent activation of password verification means.

V. For preparing oral proceedings, the appellant filed on 4 June 1997 a new Claim 2 of his main request for overcoming the Board's objection under Article 123(2) EPC.

Claim 2 of the main request as filed on 4 June 1997 reads as follows:

"2. An IC card which is connectable through a terminal device to a main data processing device and includes a data storing/processing function; said IC card comprising:

a main body (10);

memory means (24) having a memory area which is segmented into a plurality of zones in accordance with purposes of use of said IC card for storing data supplied from said main data processing device to said main body (10); and

access control means (22) for storing an access condition for each zone of said memory means (24) to control the access to each zone,

characterized in that

said access control means (22) further stores a plurality of passwords, each of said passwords respectively corresponding to each of a plurality of users and access condition data for each of said plurality of zones, said access condition data including

(i) zone data indicating (a) a name designating the zone, (b) a head address of the zone, and (c) a size of the zone, and

(ii) a plurality of password verification data, each of said password verification data respectively corresponding to one of said zones, each of said password verification data including for each of said passwords one bit which indicates whether verification of the corresponding password is necessary before data is read out or written into the corresponding zone of said memory means; wherein:

said access control means (22) permits data access into a given one of said plurality of zones without verification of a password when the password verification data corresponding to the given zone indicates that verification of the password is unnecessary, and permits data access of a zone after verification of the password when the password verification data corresponding to the given zone indicates that verification of a password is necessary."

VI. Oral proceedings were duly held on 7 July 1997, at the end of which the appellant (patentee) requested that the decision under appeal be set aside and that the patent be maintained on the basis of the following requests:

Main request: Claims 1 and 3 to 6 filed on 3 March 1995, and Claim 2 filed on 4 June 1997;

Auxiliary request 1: filed during oral proceedings on 7 July 1997;

Auxiliary request 2: the set of Claims 1 to 6 filed on 10 October 1994 under the heading "Auxiliary request 1."

Independent Claims 1 and 2 of auxiliary request 1 filed on 7 July 1997 read as follows:

"1. An IC card which is connectable through a terminal device to a main data processing device and includes a data storing/processing function; said IC card comprising:

a main body (10); and

memory means (24) having a memory area which is segmented into a plurality of zones for storing data supplied from said main data processing device to said main body (10);

characterized in by further comprising:

access control means (22) for storing for each zone of said memory means (24) a separate access condition to control the access to each zone,

said access control means (22) further stores an output condition indicating whether or not the data stored in the zones of said memory means (24) is encrypted before being transmitted to the main data processing device, and

encrypting means (26) encrypts the data output from a zone of said memory means (24) when the access condition for the zone indicates that the data is to be encrypted."

"2. An IC card which is connectable through a terminal device to a main data processing device and includes a data storing/processing function; said IC card comprising:

a main body (10);

memory means (24) having a memory area which is segmented into a plurality of zones in accordance with purposes of use of said IC card for storing data supplied from said main data processing device to said main body (10); and

access control means (22) for storing a plurality of passwords, each of said passwords respectively corresponding to each of a plurality of users;

characterized in that

said access control means (22) further stores for each zone of said memory means (24) separate access condition data to control the access to each zone,

said access condition data including

(i) zone data indicating (a) a number designating the zone, (b) a head address of the zone, and (c) a size of the zone, and

(ii) a plurality of password verification data, each of said password verification data respectively corresponding to one of said zones, each of said password verification data including for each of said passwords one bit which indicates whether verification of the corresponding password is necessary before data is read out or written into the corresponding zone of said memory means;

wherein:

said access control means (22) permits data access into a given one of said plurality of zones without verification of a password when the password verification data corresponding to the given zone indicates that verification of the password is unnecessary, and permits data access of a zone after verification of the password when the password verification data corresponding to the given zone indicates that verification of a password is necessary."

Claims 3 to 6 of auxiliary request 1 filed on 7 July 1997 are dependent on Claim 1 or 2.

VII. In support of his requests, the appellant made essentially the following submissions:

(a) Auxiliary request 1 handed over during oral proceedings should be admissible, since the subject-matter defined in independent Claims 1 and 2 of this request is identical with that defined in Claims 1 and 2 of the main request. The amendments introduced do not change the technical content of the claims but only clarify it. In particular, the definition of the access control means has been amended to read: "access control means (22) for storing for each zone of said memory means (24) a **separate** access condition to control the access to each zone". This feature is shifted into the characterising part of Claims 1 and 2 since it is not disclosed in document D1.

(b) Providing selective encryption and selective password verification independent from each other is disclosed in original Claims 1, 3 and 6.

(c) Document D1, column 4, lines 9 to 22 and column 4, lines 64 to column 5, line 3 discloses that in all applications the access conditions to zones 0 and 2 are not changed, "whatever be the applications". Therefore document D1 gives no incentive to provide zone dependent access conditions as claimed in the present invention. As follows from document D1, column 4, lines 49 to 51; column 5, lines 15 to 20 and 31 to 35, when flags EP≠11, Lock≠11 and flag LP changes from = 11 to ≠11, access to zone 0 stays forbidden, a key is needed for readout from zones 1 and 2 and no key is necessary for writing into zones 1 and 2. Hence, the flags are not zone- but function-related and are common for zones 1 and 2 and do not teach to

provide a password dependent access to each zone individually. Moreover, a skilled reader derives from document D1, column 5, lines 7 and 8 that access to the data carrier will require at least two keys. In particular, document D1 discloses no IC card having memory means with a zone to which access is possible without password verification (key). The subject-matter of Claim 2 of the main request and auxiliary request 1 allowing to inactivate password verification for each zone individually, is thus not obvious.

(d) The subject-matter of Claims 1 of the main and all auxiliary requests is directed to a selective encryption for each zone. Though encrypting means are known from documents (D2 and D3, the combination of documents) D1 and D2 or D1 and D3 does not teach to store for each zone a flag indicating on encryption condition, i.e. whether encryption shall be effected or not when data are readout from a respective zone. Document D1, column 1, lines 11 to 13 discloses that from zone 0 no data can be read out at all. A selective, zone-dependent encryption is not obvious, since document D2, page 6, section 3.2, paragraph 5 teaches to provide a **data** dependent encryption. Moreover, in order to save energy a skilled person would store the data in encrypted form rather than provide encrypting means, the activation of which can be selected individually for each zone.

(e) Having regard to the inclusion of zone data - such as name, head address and size - into the access condition data as claimed in Claims 2 of the main request and auxiliary request 1, a skilled person would not consider the teaching of document D9,

since it concerns the problem of organising access to the various fields of a storage system which is shared by plural processors in common. Hence, it is not obvious to use zone-data in order to solve the problem of providing a portable data storing/processing device which is versatile in use and low in cost to manufacture as disclosed in the patent under appeal, page 2, lines 31 and 32.

VIII. Opponent I based its request on lack of inventive step and submitted the following arguments:

(a) IC cards operate as a remote storage means with selective access and therefore belong to the general field of storage. In the introductory part of the description of the patent in suit, the appellant indicates that dividing a memory area in inaccessible and conditionally accessible zones and selective encrypting in accordance with the importance of the data is prior art. The importance can only be marked by the content of the data or by their position within the memory, the latter marking being technically more simple.

(b) Document D1 discloses a distribution of a memory into zones with free or password dependent access and reads in column 1, lines 45 to 47 that it is an object of the invention to provide a card which "may or may not be made specific to an individual". Allowing an unconditioned access to certain zones of a memory and protecting others against access cannot be regarded as implying an inventive step, since no advantage of such measure has been submitted. Selecting the claimed realisation of such separate memories by software with regard to the only other possible realisation by hardware is obvious.

(c) Since a zonewise selective protection of data against access by password verification is disclosed in document D1, a zonewise selective encryption of outgoing data is obvious. In addition to password verification which protects data when resting in one system component (card), encryption protects them - as known from document D2 - during their transport between card and terminal and thus gives full protection. Deciding on the selectivity of such full protection is determined by the nature of the data and thus obvious.

(d) The inclusion of zone data into the access condition data of a memory is not only disclosed in document D9 but general knowledge, in particular the use of address data.

IX. Opponent II contested the submissions of the appellant according to paragraph VIII above essentially by the following arguments:

(a) Claim 2 of the main and auxiliary request 1 contradicts Article 123(2) EPC. Password verification alone without selective encryption is not disclosed in the original description. The separate claiming of password verification and encryption in original Claims 3 and 6 is not supported by the description. Moreover, passwords are disclosed to be not zone-specific but user-specific, so that the corresponding wording of Claim 2 should not read "for each password one bit" but "for each user one bit" which indicates whether verification with the corresponding password is necessary ...".

(b) Document D1 teaches to provide a memory with zones which are accessible at different times and under different conditions; see D1, column 5, lines 7 to 36. Though some access conditions are disclosed to be only globally valid for more than one zone, a reorganisation of the memory into individual access conditions for each of its zones, belongs to a skilled person's routine work in order to satisfy the needs of a given application. In particular, document D1 teaches to arrange different user dependent access conditions to each of the storage zones 0, 1 and 2. After the manufacturer and the editor have written data into zone 0, the flags can be changed to forbid external access. Access conditions for the card user can be programmed independently. By changing flag EP from 11 to ≠11 writing into zone 1 can be made dependent on password verification. Hence, the basic concept of selective access by password verification is already disclosed in document D1. Moreover, document D1, column 4, lines 57 to 60 suggests a variety of uses and column 5, lines 9 and 10 discloses different passwords on the same card identifying different users. On the basis of this background art, a memory reorganisation into the zone dependent selective password verification as claimed in Claim 2 of the main request and auxiliary request 1 is not inventive taking into due account the normal routine activities of a skilled person.

(c) A skilled person would clearly consider the teaching of Document D9 in making the device disclosed in document D9 more versatile in use, since zones of the physical memory of document D1 are shared by various functional parts of the logic memory; see D1, column 4, in particular lines 61 to 64. It is moreover general knowledge

and self-evident to provide names and addresses of storage zones within the access condition data of an IC card in order to guarantee its functioning. In view of the disclosure in document D1, column 4, lines 42 to 44, that the size of the various zones depends on the intended use, an additional inclusion of a size of a zone into the access condition data for increasing the versatility of the card is obvious to a skilled person.

(d) The wording in document D2, page 6, section 2.3, paragraph 5 and document D3, page 1, paragraph 2 underlines the necessity of encrypting critical data for their transmission. It is already suggested in document D1 to store critical data in particular zones and less or not critical ones in others. Following this conventional data organisation, the obvious integration of the encrypting means disclosed in document D2 or D3 into the IC card disclosed in document D1 results automatically into a zone-dependent selective encryption as claimed in Claim 1. A skilled person is able to recognise that flags for selective encryption (flags C in Table 3 of the patent under appeal) can be technically realised in the same way as the obvious organisation of flags for selective zone-dependent password verification (flags D in Table 3 of the patent under appeal); see also paragraph IX-(b) above. Leaving away the password flags and using only flags for selective zone dependent encryption is a matter of discretion and provides no technical difficulties. For the above reasons, the combination of the teachings of documents D1 and D2 (or D3) plus the general knowledge of a skilled person leads to the subject-matter of Claims 1 of all the appellant's requests in an obvious way.

X. At the conclusion of the oral proceedings, the decision was announced that the appeal is dismissed.

Reasons for the Decision

1. *Inventive step - Claim 2 - main request and auxiliary request 1*

1.1 As follows from paragraphs VII to IX above, access conditions to memory means observing password verification are generally known to be a basic element in most conventional uses of IC cards. Therefore, in view of this technical precedence, the Board regards it more logical to first deal with the selective security of data storing as claimed in Claim 2 before considering the selective security of data transmission as claimed in Claim 1.

1.2 From document D1 there is known according to the wording of Claims 2 of the main request and auxiliary request 1:

"An IC card (see D1, Figure 3) which is connectable through a terminal device (i.e. via 6 in Figures 1 and 2) to a main data processing device and includes a data storing/processing function (see PROM 2; column 2, line 60 and microprocessor 1; column 2, line 56); said IC card comprising: a main body (C2 in Figure 3); having a memory area which is segmented into a plurality of zones (0, 1, 2 in Figures 4A and 4B) in accordance with purposes of use of said IC card (column 3, line 64 to column 4, line 6) for storing data supplied from said main data processing device to said main body (column 1, lines 25 to 40 in combination with Figure 9); and"

in the wording of the main request: "access control means (LOCK, LP and EP in Figure 4B) for storing an access condition for each zone to control the access to each zone (column 5, lines 7 to 36)";

or in the wording of auxiliary request 1: "characterized in that said access control means further stores for each zone of said memory means separate access condition data to control the access to each zone (column 5, lines 23 to 27; and lines 31 to 36).

1.3 Document D1, column 4, line 64 to column 5, line 3 teaches that in all kinds of uses a particular type of data is always "located" within the same zone of the memory. From such invariable organisation of the local physical storage of data, in the Board's view, a skilled person will not derive that the access conditions to the data stored are kept constant in all uses. Such an interpretation would moreover contradict the versatility of access conditions disclosed in doucment D1, column 1, lines 46 to 48; see also paragraph VIII-(b) above. In the Board's view, a skilled reader will moreover not interpret the text in document D1, column 5, lines 7 and 8 in that access to the data carrier always requires the presence of at least two user characterising keys at the same time, since document D1, column 5, lines 26 and 35 read that "**a** key is required" and column 8, in particular lines 17 to 19 teach that the key ..." is compared with **one** of the keys" for allowing access to the data. Furthermore, document D1 column 5, in particular lines 35 to 36, discloses that an access condition to only one zone (zone 1) can be set individually (by flag EP). Combining flag EP=11 (unprotected writing in zone 1; column 5, lines 31, 32) with flag LP=11 (unprotected reading from zones 1 and 2; column 5,

lines 23 to 27) results in a freely accessible zone (1) wherein reading and writing is possible without password verification. Hence, changing flag EP from ≠11 to =11 and flag LP from ≠11 to 11 clearly selectively inactivates password verification for the access to zone (1) individually. For the above reasons, the appellant cannot be followed in his submission according to paragraphs VIII-(a) and (c) above.

1.4 In addition to the features stated in paragraph 1.2 above, document D1 discloses furthermore in the wording of Claims 2 of the main and auxiliary request 1:

(a) "said access control means further stores (or in the wording of auxiliary request 1: access control means for storing) a plurality of passwords (see D1, column 5, lines 9 to 19) each of said passwords respectively corresponds to each of a plurality of users (D1, column 5, lines 9 and 10) ... said access condition data including

(ii) a plurality of password verification data (LP, EP) ... corresponding to one of said zones (zone 1), ... said password verification data including for ... a password" two " bits(s) (EP≠11 or LP≠11; see column 5,lines 23 to 36) which indicate(s) whether verification of the corresponding password is necessary before data is read out or written into the corresponding zone of said memory; wherein said access control means permits data access into a given one (zone 1) of said plurality of zones without verification of a password when the password verification data indicate(s) that verification of the password is unnecessary (LP=11 and EP=11; see also paragraph 1.3 above) and permits data access of a zone

after verification of the password when the password verification data corresponding to the given zone indicate(s) that verification of the password is necessary (LP≠11 and EP≠11)";

(b) (i) "zone data indicating ... (b) a head address of the zone (see D1, column 4, lines 9, 10; 14, 15; 19, 20), ...".

1.5 Starting from the closest prior art according to document D1 the objective problem underlying the invention claimed in Claims 2 of the main request and auxiliary request 1 is to provide a portable data storing/processing device which is versatile in use and low in cost to manufacture; see the patent in suit, page 2, lines 31 and 32. Having regard to versatility, the objective problem is known from document D1; see D1, column 1, lines 46 to 48, and column 3, lines 65 to 67 in combination with column 4, lines 57 to 60. Lowering the costs of manufacture represents a technical aim which falls into the routine work of the skilled person. Thus, the formulation of the objective problem underlying Claims 2 does not contribute to an inventive step underlying the subject-matter of these claims.

1.6 The principle of the solution of the above problem consists in providing an IC card wherein for **each** of a plurality of zones at the time of card issuance, **any** access condition can be set. Such versatility allows a mass production which results in a cost reduction; see the patent under appeal, page 4, lines 41 to 43 and page 5, lines 43 to 46. In the wording of Claims 2 of the main request and auxiliary request 1 the objective problem is solved in that:

(ii) ... "each" of said password verification data "respectively" corresponding to one of said zones, "each" of said password verification data including for "each" of said passwords "one" bit for inactivating or activating the password verification means.

In the Board's view, the features defined in paragraph (i) of Claims 2 do not increase versatility. A "head address" is an indispensable element for the functioning of the IC card and moreover disclosed in document D1. No particular effect is disclosed for a"name" and for the "size" of a zone. In view of the appellant's submission in paragraph VII-(e) above, the Board regards the addition of a name and a size to a zone address as redundant for defining the location of the storage and thus falling into a skilled person's discretion. Variable zone sizes are not disclosed in the original description and moreover obvious in view of document D1, column 4, lines 42 to 44. For the above reasons and contrary to the appellant's opinion in paragraph VII-(e) above, the feature defined in paragraph (i) of Claims 1 can be disregarded in the evaluation of an inventive step underlying Claims 2.

1.7 A skilled person arrives at the features distinguishing paragraph (ii) of Claims 2 from the IC card disclosed in document D1, insofar as for **each** zone **any** access condition can be set, by providing on the IC card more than one zone with the selective access-conditions of zone (1) of document D1. In the Board's view, a skilled person can be expected to foresee that providing on the card more zones with the properties of zone (1) of document D1 increases its versatility and allows a larger variety of access conditions to be set for stored data. Since the amount of necessary access variety results from the given practical needs of the

various envisaged customers to which the IC card shall be sold, in the Board's view, it is obvious to a skilled person that increasing the number of customers and thereby reducing the costs of manufacture, needs an increase in the variety of possible combinations of access conditions.

1.8 For the reduction of a password verification flag from two bits in the EC card according to document D1 to "one bit" as claimed, no particular unexpected effect is disclosed. In the Board's view, a skilled person is able to foresee that the use of one bit flags allows to reduce the costs of manufacture. Dispensing with the possibility of separately setting the access condition of the function "reading" (flag LP) and that for the function "writing" (i.e. changing thus a selective functional flag into a selective access flag for both functions), represents a simplification with a foreseeable disadvantage which cannot be regarded as inventive.

1.9 For the reasons indicated in detail in paragraphs 1.2 to 1.8 above, in the Board's judgement Claims 2 of the main and auxiliary request 1 lack an inventive step within the meaning of Article 56 EPC.

2. *Inventive step - Claim 1 - main and auxiliary requests 1 and 2*

2.1 Document D1 discloses the features of identically worded Claims 1 of the main and auxiliary request 2 (see paragraph II above) and those of Claim 1 of auxiliary request 1 (see paragraph VI above) as can be seen from paragraph 1.3 above. Paragraph 1.3 above is restricted to those features which are identically worded in Claims 2 and 1.

2.2 Starting from the closest prior art disclosed in document D1 the objective problem underlying the invention claimed in Claims 1 of the main and auxiliary requests 1 and 2 comprises in addition to the obvious technical aims mentioned in paragraph 1.5 above, to provide an IC card wherein data can be protected when transported from the card; see the patent under appeal, page 3, lines 26 to 31. This problem is known from document D2, in particular page 5, last paragraph. Thus, the formulation of the overall objective problem underlying said Claims 1 does not contribute to an inventive step underlying these claims.

2.3 The above objective problem is solved in the wording of Claims 1 of all requests in that

(a) "said access control means further stores an output condition whether or not the data stored in the zones of said memory means is encrypted before being transmitted to the main data processing device, and"

(b) that "encrypting means encrypts the data output from a zone of said memory means, when the access condition for the zone indicates that the data is to be encrypted".

2.4 An "encrypting means" which encrypts the data output from the memory means of an IC card, is disclosed in document D2, page 5, last paragraph (and as well in document D3; see 44 and 46 in Figure 1 of D3). In view of its known ability to prevent access to the data during data transport from the card, it is obvious to a skilled person to make an analogous use of encrypting means such as disclosed in document D2 in the EC-card disclosed in document D1 and to arrive thereby at the essential technical means claimed in feature (b) of paragraph 2.3 above.

2.5 In the Board's view, it is obvious to a skilled person that only "crucial data" need to be encrypted, as also disclosed in document D2, page 6, section 2.3 paragraph 5. Crucial or secret data with a higher need for protection against access are disclosed in document D1, column 4, line 64 to column 5, line 3 to be located for all uses in the same zones of the memory and less secret data to be stored in the same remaining zones. From the teaching of document D1 that this constant storage organisation requires the institution of zone dependent selective access conditions for password verification, a skilled person, in the Board's view, is able to logically conclude that the same secret data to which access is protected within a particular zone of the memory should also be protected outside this zone. Such obvious local completion of data protection, in the Board's view, leads a skilled person automatically to recognise that the need for encryption is zone dependent and that it would be advantageous to provide means for selectively activating the encrypting means in a zone dependent way such as claimed in feature (a) of paragraph 2.3. above; see also paragraphs VIII-(c) and IX-(d) above. In the Board's view, it belongs to a skilled person's routine work to make the encrypting means (feature (b)) disclosed in document D2, sensitive to selective activation according to the flags defined in feature (a) so that it encrypts "when the access condition of the zone indicates that the data is to be encrypted". For the above reasons, the appellant cannot be followed in his submission according to paragraph VII-(d) above. In particular, the provision of a zone from which read-out can be totally blocked by a flag, in the Board's view, represents a different practical requirement which is functionally independent from the practical need of selective encryption. This separate requirement does not prevent a skilled person

to derive from document D1 that the data-dependent encryption suggested in document D2 gets automatically zone-dependent when realised in the IC card disclosed in document D1.

2.6 For the reasons indicated in detail in paragraphs 2.1 to 2.5 above, in the Board's judgement Claims 1 of all requests lack an inventive step within the meaning of Article 56 EPC.

3. Claims 3 to 6 of the main and auxiliary request 1 fall because of their alternative dependency on the respective Claim 1 of Claim 1. Claims 2 to 6 of auxiliary request 2 fall because of their dependency on Claim 1.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

M. Beer G. D. Paterson