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 17 June 2004

Case Number: T 1054/00 - 3.5.3

Application Number: 91106678.5

Publication Number: 0455135

IPC: H04Q 7/20

Language of the proceedings: EN

Title of invention:
Security module for radio telephone

Patentee:
NEC CORPORATION

Opponent:
GIESECKE & DEVRIENT GmbH

Headword:
Security module/NEC

Relevant legal provisions:
EPC Art. 84, 123(3), 56
EPC R. 57a

Keyword:
"Inventive step - (yes) after amendment"

Decisions cited:
T 0396/01, T 1018/02

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1054/00 - 3.5.3

D E C I S I O N
of the Technical Board of Appeal 3.5.3
of 17 June 2004

Appellant: (Proprietor of the patent)
NEC CORPORATION
7-1, Shiba 5-chome
Minato-ku
Tokyo (JP)

Representative:
D. Heunemann
VOSSIUS & PARTNER
Postfach 86 07 67
D-81634 München (DE)

Respondent: (Opponent)
P. Niedermeier
GIESECKE & DEVRIENT GmbH
Prinzregentenstrasse 159
D-81677 München (DE)

Representative:
-

Decision under appeal: **Decision of the Opposition Division of the European Patent Office posted 11 August 2000 revoking European patent No. 0455135 pursuant to Article 102(1) EPC.**

Composition of the Board:

Chairman: A. S. Clelland
Members: D. H. Rees
R. T. Menapace

Summary of Facts and Submissions

I. This is an appeal by the proprietor of European Patent No. 0 455 135 against the decision of the opposition division to revoke the patent.

II. The opponent (respondent) had requested the revocation of the patent on the grounds that the invention lacked an inventive step with respect to the disclosure of *inter alia* the following documents

E1: WO-A-89/07375 and

E2: DE-A-3 736 190

III. In the decision under appeal, dispatched on 11 August 2000, the opposition division held that the subject-matter of granted independent claims 1 and 12 did not involve an inventive step having regard to a combination of documents E1 and E2. Claim 1 of a first auxiliary request (maintained in appeal) was found not to satisfy the requirements of Articles 123(2) and (3) EPC, and a second auxiliary request (also maintained in appeal) whose only claim corresponded to claim 12 as granted was also found not to involve an inventive step.

IV. Notice of appeal was filed, in a letter dated 18 October 2000 and received, together with the appropriate fee, on 20 October 2000. A statement of grounds of appeal, reiterating the previous requests and adding a third auxiliary request, was submitted on 21 December 2000.

V. In a response submitted on 17 May 2004 to a summons to attend oral proceedings, the appellant submitted independent claims for new auxiliary requests 3 to 9, and during the oral proceedings held on 17 June 2004 a new modified main request (referred to as "main request 2") and further auxiliary requests 10, 10a, 11 and 12 were made.

VI. The independent claims as granted read as follows:

"1. A security module (30) for use with a radio telephone and preventing a KEY code from being read out from the outside, comprising:
an electrically rewritable non-volatile memory (302) to which the key code is written;
encrypting means (303) for encrypting data entered from the outside on the basis of the key code stored in said non-volatile memory (302), and outputting said encrypted data;
interface means (301) for receiving data from the outside and outputting said encrypted data; and
control means (304) for enabling said non-volatile memory (302) to be accessed via an internal bus (306) and an external bus (307) and, when said non-volatile memory (302) is accessed, deleting the KEY code.

12. A method of preventing a key code in a memory from being stolen, comprising the steps of:
storing said key code in said memory;
incorporating said memory in a module;
encrypting in said module data with said key code; and
erasing said key code from said memory when said memory is accessed from the outside of said module."

VII. At the oral proceedings the appellant requested maintenance of the patent according to the following requests (insertions with respect to the claims as granted in italics, deletions in parentheses):

Main request 1: claims 1 to 12 as granted.

Main request 2: claims 1 to 11 as granted, i.e. without claim 12.

Auxiliary request 1 (filed in the opposition proceedings): claim 1 amended to read "... when said non-volatile memory (302) is accessed *from the outside of said module*, deleting the KEY code." Claims 2 to 12 as granted.

Auxiliary request 2 (filed in the opposition proceedings): claim 12 as granted only, i.e. without claims 1 to 11.

In auxiliary requests 3 to 9, claims 2 to 11 as granted are maintained, and amendments introduced to the independent claims as follows.

Auxiliary request 3:

"1. ...
control means (304, *304a*) for enabling said non-volatile memory (302) to be accessed via an internal bus (306) and an external bus (307) and, when said non-volatile memory (302) is accessed, *electrically* deleting the KEY code.

12. ...
electrically erasing said key code from said memory when said memory is accessed from the outside of said module."

Auxiliary request 4:

"1. A security module (30) for use with a radio telephone and preventing a KEY code from being read out from the outside, comprising:
an electrically rewritable non-volatile memory (302) to which the key code is written *and which is connectable to an internal bus (306) and an external bus (307)*;
encrypting means (303) for encrypting data entered from the outside on the basis of the key code stored in said non-volatile memory (302), and outputting said encrypted data;
interface means (301) for receiving data from the outside and outputting said encrypted data; and
control means (304, *304a*) for enabling said non-volatile memory (302) to be accessed via an internal bus (306) and an external bus (307) and *when said non-volatile memory (302) is electrically connected via the internal and external bus to the outside*, [when said non-volatile memory (302) is accessed,] *electrically* deleting the KEY code.

12. A method of preventing a key code in a memory from being stolen, comprising the steps of:
storing said key code in said memory;
incorporating said memory in a module;
encrypting in said module data with said key code; and
electrically erasing said key code from said memory *when said non-volatile memory (302) is electrically*

connected via the internal and external bus to the outside [when said memory is accessed from the outside of said module]."

Auxiliary request 5:

"1. A security module (30) for use with a radio telephone and preventing a KEY code from being read out from the outside, comprising:
an electrically rewritable non-volatile memory (302) to which the key code is written *and which is connectable to an internal bus (306) and an external bus (307)*;
encrypting means (303) for encrypting data entered from the outside on the basis of the key code stored in said non-volatile memory (302), and outputting said encrypted data;
interface means (301) for receiving data from the outside and outputting said encrypted data; and
control means (304, *304a*) for enabling said non-volatile memory (302) to be accessed via an internal bus (306) and an external bus (307) and *when said non-volatile memory (302) is electrically connected via the internal and external bus to the outside*, *and* when said non-volatile memory (302) is accessed, *electrically* deleting the KEY code.

12. A method of preventing a key code in a memory from being stolen, comprising the steps of:
storing said key code in said memory;
incorporating said memory in a module;
encrypting in said module data with said key code; and
electrically erasing said key code from said memory *when said non-volatile memory (302) is electrically connected via the internal and external bus to the*

outside and when said memory is accessed from the outside of said module."

Auxiliary request 6:

Claim 1 as in auxiliary request 5, with the final feature amended to read, "when said non-volatile memory (302) is accessed *by the control means (304, 304a), electrically* deleting the KEY code."
Claim 12 as in auxiliary request 5.

Auxiliary request 7:

"1. ... (as granted)
control means (304, *304a*) for enabling said non-volatile memory (302) to be accessed via an internal bus (306) and an external bus (307) *and for deleting the KEY code when connecting the internal bus (306) and the external bus (307)* [and, when said non-volatile memory (302) is accessed, deleting the KEY code].

12. A method of preventing a key code in a memory from being stolen, comprising the steps of:
storing said key code in said memory;
incorporating said memory in a module;
encrypting in said module data with said key code; and
erasing said key code from said memory when *an internal bus connected to the memory is connected to an external bus* [said memory is accessed from the outside of said module]."

Auxiliary request 8:

"1. ... (as granted)
control means (304, *304a*) for enabling said non-volatile memory (302) to be accessed via an internal bus (306) and an external bus (307) *and for deleting the KEY code when connecting the internal bus (306) and the external bus (307)* and, when said non-volatile memory (302) is accessed[, deleting the KEY code].

12. A method of preventing a key code in a memory from being stolen, comprising the steps of:
storing said key code in said memory;
incorporating said memory in a module;
encrypting in said module data with said key code; and
erasing said key code from said memory when *an internal bus connected to the memory is connected to an external bus and* said memory is accessed from the outside of said module."

Auxiliary request 9:

"1. ... (as granted)
control means (304, *304a*) for enabling said non-volatile memory (302) to be accessed via an internal bus (306) and an external bus (307) *and for deleting the KEY code when connecting the internal bus (306) and the external bus (307)* and, when said non-volatile memory (302) is accessed[, deleting the KEY code] *by the control means (304, 304a)*.

12. A method of preventing a key code in a memory from being stolen, comprising the steps of:
storing said key code in said memory;

incorporating said memory in a module;
encrypting in said module data with said key code; and
erasing said key code from said memory when *an internal bus connected to the memory is connected to an external bus and* said memory is accessed from the outside of said module."

Auxiliary request 10 is based on a combination of granted claims 1 and 6, with the other claims appropriately renumbered. Claim 6 reads:

"A security module as claimed in any one of claims 1 to 5, wherein said control means (304) comprises a test terminal which isolates said internal bus (306) from said external bus (307) when inactive or connects said internal bus (306) and said external bus to allow access to occur when active, and a differentiating circuit (304a) for outputting a clear pulse for deleting said KEY code."

Auxiliary request 10a is as auxiliary request 10 without the independent method claim (claim 12 as granted).

Auxiliary request 11 is as auxiliary request 10 with the addition of the final feature, " ... when access via the external bus to the non-volatile memory (302) is enabled," to claim 1.

Auxiliary request 12 is as auxiliary request 11 without the independent method claim.

VIII. The respondent requested that the appeal be dismissed.

IX. The decision of the board was announced at the end of the oral proceedings.

Reasons for the Decision

1. The appeal complies with Articles 106 to 108 and Rule 64 EPC and is therefore admissible.

2. *Admissibility of the requests filed in the appeal proceedings.*

2.1 Main request 2 is for maintenance of the patent on the basis of claims 1 to 11 as granted. There are no new objections introduced by this amendment, which was put forward in response to the discussion at the oral proceedings. The respondent has not objected to the admission of this request. The board therefore exercises its discretion to admit it.

2.2 The only additional features introduced into the claims of auxiliary request 3 are (1) the insertion of reference sign "304a" into the control means (in claim 1), and (2) that the deletion of the key code is accomplished "electrically" (in both claims 1 and 12). The first of these amendments has a minor clarifying effect. The second does not aid in overcoming an objection of lack of an inventive step with respect to the documents E1 and E2 (see points 3 and 4 below), since it would be evident to the skilled person that memory deletions in the systems disclosed in those documents would also be carried out electrically. No other reason for making this request was put forward. As it is patently clear that this request does not

bring anything to the debate, the board exercises its discretion not to admit it.

2.3 According to claim 1 of auxiliary requests 5, 8 and 9, the key code is deleted when the internal bus is connected to the external bus "and" when the non-volatile memory is accessed. It is not clear whether both conditions have to occur simultaneously or sequentially for deletion to take place, or whether the occurrence of one condition is sufficient. Therefore the claims of these requests do not satisfy Article 84 EPC; the requests are therefore not admitted.

2.4 Claim 1 as granted specifies that the key code is deleted when the non-volatile memory is accessed. The board considers that the skilled person would understand "access" to refer to read or write operations. Further, the skilled person would understand the claim to mean that the key would be deleted when**ever** an access occurs, for example when the memory is accessed internally (see also points 4.1 to 4.6 below). Thus any amendment of claim 1 which allows a read or write operation on the non-volatile memory to take place without the key being deleted is necessarily a violation of Article 123(3) EPC. For this reason requests 4, 6 and 7, in all of which claim 1 is amended to define that the deletion takes place in response to other events than a read or write access, are also not admissible.

2.5 The combination of granted claims 1 and 6 on the other hand clearly restricts the subject-matter of granted claim 1 and does not raise any new formal objections. The amendment made in auxiliary request 10 was put

forward in order to overcome similar objections to those made above, and the respondent has not raised any arguments against the request's admission. The same considerations apply to auxiliary request 10a, in which the independent method claim is deleted. The board therefore exercises its discretion to admit these requests.

2.6 Auxiliary requests 11 and 12 correspond to requests 10 and 10a respectively, but further restrict the independent apparatus claim to specify that the clear pulse already specified in the claim deletes the key code "when access via the external bus to the non-volatile memory (302) is enabled." This amendment reflects the disclosure of the application as filed - see column 5, lines 37 to 49, of the published application, and was said by the appellant to have been introduced in case the board considered that the simple combination of claims 1 and 6 did not restrict deletion to when access was enabled.

The respondent argued that claim 1 of these requests violated Article 123(3) EPC in that it redefined the deletion of the key code to take place when access is enabled rather than when the memory is accessed. However this argument is not convincing; the new claim defines two separate conditions for deletion, the first when a memory access takes place and the second when access via an external bus is enabled. Any apparatus satisfying the claim must carry out deletion in both these circumstances, so that the subject-matter of granted claim 1 has been further restricted and there is no violation of Article 123(3) EPC.

The board therefore exercises its discretion to admit these requests.

2.7 In summary, the requests admitted into the proceedings and therefore remaining to be dealt with substantively are main requests 1 and 2, and auxiliary requests 1, 2, 10, 10a, 11 and 12.

3. *Claim 12 as granted - inventive step*

3.1 Since main request 1, and auxiliary requests 1, 2, 10 and 11 all include claim 12 as granted (renumbered in requests 10 and 11), the board will consider this claim first.

3.2 In the board's view the single most relevant document is E2, which concerns a chip card (column 1, line 66, to column 2, line 4) for storing sensitive data in a memory and which constitutes a module in the sense of claim 12. The memory has a protected area only accessible by a system controller ("einem nur der Systemverwaltung zugeteilten Bereich", column 3, lines 15 and 16). In the board's view the protected area, rather than the chip card's memory as a whole, corresponds to the memory defined in claim 12. The chip card's memory can be accessed internally by the system or externally by a user. By definition, any access of the protected area other than by the system controller is unauthorised. If access of the protected memory area is attempted by a user ("wenn ein Benutzer unberechtigt Information ... auslesen will", column 3, lines 14 to 16) E2 proposes that counter-measures be taken, for example the deletion of information (column 3, lines 13 to 18). E2 does not specify which information, but in

the context the skilled person could be expected to delete the sensitive data itself. Equally, E2 does not specify in detail what the sensitive data represents and does not discuss the encryption of data, mentioning only a user ID as an example ("Kennummer", column 2, lines 61 to 65), but the board considers that it would be obvious to the skilled person to apply the teaching of E2 to a module carrying out encryption and containing cryptographic keys, given the common general knowledge in the art that cryptographic keys are sensitive data (cf. E1). Although the appellant argued that E2 was concerned with a chip card rather than a radiotelephone, the board notes that claim 12 is not limited to a radiotelephone and indeed embraces a chip card. The board further considers a user ID to be equivalent to a key code.

3.3 Thus the subject-matter of granted claim 12 lacks an inventive step. It follows that none of main request 1 and auxiliary requests 1, 2, 10 and 11, each of which includes a claim corresponding to granted claim 12, are allowable.

4. *The remaining requests - inventive step*

4.1 The interpretation of granted claim 1 was disputed by the parties. The claim relates to a security module for storing a key code in a non-volatile memory. The arguments centred around the interpretation of the last clause of the claim, specifying that the module has "control means for enabling said non-volatile memory to be accessed via an internal bus and an external bus and, when said non-volatile memory is accessed, deleting the KEY code."

4.2 The appellant argued that the phrase "when said non-volatile memory (302) is accessed" must be interpreted to mean when said non-volatile memory (302) is accessed via the combination of the external and internal bus; thus the access is from the outside, as specified in claim 12. Further, the external bus must be interpreted as including the test terminal 305 (Figure 6) and the internal bus as including the line marked "CPLS" in Figure 6, over which a clear pulse is fed to the memory. Finally, "accessed" must be interpreted to mean, or at least include, the activation of the test terminal. Reference was made to a passage in the description (column 5, lines 8 to 20 of the published patent) in support of this interpretation. This passage discloses that when the test terminal is activated, a clear pulse is sent to the memory which causes it to be erased.

4.3 However, the board considers the plain meaning of "when said non-volatile memory (302) is accessed" to be that deletion of the key code takes place whenever any access to the memory takes place, whether over the external bus or the internal bus, or from elsewhere in the module. Moreover, the skilled person would understand the term "access" to relate only to read and write operations. The "clear pulse" fed by the differentiating circuit 304a to the non-volatile memory to effect the deletion, as disclosed in the cited passage of the description, is therefore not an "access". The appellant's argument to the contrary is also not in accordance with the plain meaning of the claim that the control means causes the key to be deleted **as a response to** an access; the clear pulse, according to the description, is the action taken by

the control means to carry this out. It therefore follows as the result of an access, rather than being itself an access. Thus the passage from the description cited by the appellant does not concern an "access" and is therefore irrelevant to the interpretation of the term in the claim.

4.4 As regards the appellant's argument that the test terminal 305 and the line marked "CPLS" in Figure 6 should be considered part of the respective buses specified in claim 1, the board considers that a person skilled in the art would not regard the test terminal or the memory clearing line as disclosed in the description and figures as a whole to be part of a "bus" in the conventional sense - see e.g. Figure 6 and the use of only reference numbers 307 and 306 for the external and internal buses in claim 1.

4.5 Finally, to the extent that the passage in the description referred to by the appellant relates to a read or write access at all, it does not discuss what happens when an access takes place, but rather what happens when access to the memory is enabled, which is a different event.

4.6 For all these reasons the board cannot accept the appellant's proposed interpretation of claim 1.

4.7 The plain wording of claim 1 as granted admittedly does not correspond to the description. However it is technically credible. Indeed, the respondent has put forward a possible, if speculative, circumstance in which such key deletion on every access might take place, namely in the context of a "one-time-pad" type

cryptographic system. It is noted that in this case, and considering a read access, the deletion would take place as the operation immediately **after** the access. This is not excluded by the claim.

4.8 Since claim 1 is clear the question whether the claimed subject-matter involves an inventive step must be determined on the basis of the wording of the claim itself, and not on the basis of a different disclosure in the description (cf. T 1018/02 reasons 3.8, "[T]he description cannot be used to give a different meaning to a claim feature which in itself imparts a clear, credible technical teaching to the skilled reader" and T 396/01 reasons 2.3, "It is not possible, by way of construction, to attribute to a claim another meaning than the one which is clearly deducible from the claim itself" both decisions not published in the OJ EPO).

4.9 It appears to the board that the disputed patent does not disclose or imply any technical problem overcome by the combination of features according to claim 1 as granted. The respondent has, as noted above, indicated that this combination of features might be technically credible in the context of one-time-pad cryptography, but even if the skilled person were to assume (without any indication in the patent that this was intended) that this is the correct field for the invention as claimed, the claimed features do not present a concrete solution to any specific problem with respect to the disclosure of the nearest prior art (see the discussion of E2 at point 3.2 above). It appears to the board that the skilled person, aware from the teaching of E2 that the contents of the memory can be deleted upon unauthorised access, would appreciate that deletion

could in fact be effected as and when desired. Thus the claimed subject-matter does not involve an inventive step.

4.10 Hence main request 2 is not allowable. Auxiliary requests 10a and 12 remain to be considered.

4.11 The only independent claim of auxiliary request 10a is a combination of claims 1 and 6 as granted. Claim 6 adds two features to the subject-matter of claim 1: (1) a test terminal which when activated connects the internal and external buses to allow an access (implicitly using the combination of these buses, since the act of connection is "to allow an access"); and (2) a differentiating circuit for outputting a clear pulse for deleting the key code. These two features are not necessarily interrelated, since there is no indication of what event causes the differentiating circuit to output a clear pulse. Without any other further features specified, the skilled person would interpret the differentiating circuit as being the agent for carrying out the only claimed feature relating to deletion of the key code, namely deletion when any access takes place. As in the case of granted claim 1 discussed above, this claimed subject-matter does not correspond to the description and no problem solved by the specified combination of features, compared to the nearest prior art E2, has been identified. Hence for the reasons given at point 4.9 above, this claimed subject-matter also lacks an inventive step and auxiliary request 10a is not allowable.

4.12 Finally, the only independent claim of auxiliary request 12 further specifies that the deletion effected

by the differentiating circuit occurs when the access via the external bus to the non-volatile memory is enabled. This is a solution to the problem that access may be needed via an external bus in order to test that the memory functions properly, but that such access via an external bus, not being under control of e.g. a microprocessor in the module, presents a security weakness. It ensures that the key code can never simply be read out over the external bus, by deleting it before access over this bus is even attempted.

4.13 There is no indication in any of the prior art available to the board that a key code or any other sensitive data should be deleted whenever access to the data using a particular route is enabled. The board considers the corresponding combination of claimed features to involve an inventive step. The claimed subject-matter is further restricted by features which do not apparently contribute to the inventive concept, namely that the key code is also deleted (using unspecified means) whenever an actual access takes place. However, this further restriction has no effect on the inventive combination of features.

4.14 The respondent argued that the combination of features claimed, considered as a whole, was self-contradictory. The claim specifies an apparatus which stores a key value and deletes this value on either of two events occurring: (1) on any access, which, as the respondent pointed out, could make sense in the context of one-time-pad cryptography, especially if it is taken that the deletion takes place **after** the access; or (2) when (uncontrolled) access via an external bus is **enabled**, in order to avoid loss of confidentiality. These

features may not have any apparent relation to one another, but they are not contradictory, and the claimed subject-matter as a whole is clear.

4.15 Auxiliary request 12 is therefore allowable.

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 10 submitted as auxiliary request 12, description and drawings as granted.

The Registrar: The Chairman:

D. Magliano A. S. Clelland