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

Datasheet for the decision of 18 April 2013

Case Number: T 1820/09 - 3.5.05

Application Number: 02707213.1

Publication Number: 1374476

IPC: H04L9/08, H04N7/167

Language of the proceedings: EN

Title of invention:
Data protection system that protects data by encrypting the data

Applicant:
Panasonic Corporation

Headword:
Data encryption system/PANASONIC

Relevant legal provisions:
EPC 1973 Art. 84, 111(1)

Keyword:
Clarity and conciseness - (yes, after amendment)
Remittal to the first instance for further prosecution - (yes)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 1820/09 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 18 April 2013

Appellant: (Applicant)	Panasonic Corporation 1006, Oaza Kadoma Kadoma-shi Osaka 571-8501 (JP)
Representative:	Grünecker, Kinkeldey, Stockmair & Schwanhäusser Leopoldstrasse 4 80802 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 8 April 2009 refusing European patent application No. 02707213.1 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chair: A. Ritzka
Members: K. Bengi-Akyuerek
P. Schmitz

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division, posted on 8 April 2009, refusing European patent application No. 02707213.1 on the ground of lack of clarity and conciseness (Article 84 EPC 1973) with respect to a sole request.

Moreover, in an *obiter dictum* under the heading "Remarks" of the decision under appeal, the examining division expressed its opinion to the effect that the application lacked an inventive step (Article 56 EPC 1973), having regard to the disclosures of

D3: M. Waldvogel et al.: "The VersaKey Framework: Versatile Group Key Management", IEEE Journal on Selected Areas in Communications, pp. 1614-1631, September 1999;
D4: JP-A-11 187013;
D5: C.K. Wong et al.: "Secure Group Communications Using Key Graphs", IEEE Proceedings of the International Workshop on Community Networking, pp. 1-12, 1998.

II. Notice of appeal was received on 16 June 2009. The appeal fee was paid on the same day. With the statement setting out the grounds of appeal, received on 31 July 2009, new claims were submitted as a sole request (claims 1 and 2). The appellant requested that the decision of the examining division be set aside and that a patent be granted on the basis of the sole request. In addition, oral proceedings were requested as an auxiliary measure.

III. A summons to oral proceedings scheduled for 18 April 2013 was issued on 14 December 2012. In an

annex to this summons, the board expressed its preliminary opinion on the appeal pursuant to Article 15(1) RPBA. In particular, objections were raised under Articles 123(2) EPC and 84 EPC 1973. The appellant was also informed that the case could be remitted to the department of first instance for further prosecution under Article 111(1) EPC 1973 if those objections were overcome.

IV. With a letter of reply dated 18 March 2013, the appellant submitted amended claims 1 and 2 as a sole request together with explanatory comments and requested that the case be remitted to the examining division for further prosecution under Article 111(1) EPC 1973.

V. Oral proceedings were held as scheduled on 18 April 2013, during which amended claims 1 and 2 were submitted as a sole request and were discussed. The appellant finally requested that the decision under appeal be set aside and that the case be remitted to the examining division for further prosecution based on claims 1 and 2 filed during the oral proceedings before the board. At the end of the oral proceedings, the decision of the board was announced.

VI. Claim 1 of the sole request reads as follows:

"A predetermined key assignment method for generating and distributing data encryption and data decryption keys, for use in a data protection system that comprises three or more terminals (103a, ...103n) that obtain encrypted data and decrypt the obtained encrypted data, an encryption key designation device (104) and an encryption device (101) for encrypting distribution data that is to be distributed to the

three or more terminals (103a, ...103n), wherein

each terminal (103a, ...103n) includes:

a decryption key group storage unit (212) for storing the decryption key group that has been individually assigned to the terminal (904) by the predetermined key assignment method;

an encrypted data obtaining unit (211) for obtaining the encrypted data; and

a decryption unit (215) for decrypting the obtained encrypted data using one decryption key included in the stored decryption key group (905),

the encryption device (101) includes:

an encryption unit (205) for encrypting the distribution data successively using all encryption keys designated by the encryption key designation device (104), to generate a plurality of pieces of encrypted distribution data; and

an output unit (206) for outputting the generated plurality of pieces of encrypted distribution data externally,

the encryption key designation device (104) includes:

an invalid terminal designation unit (303) for designating one or more terminals (103a, ...103n) as invalid terminals, an invalid terminal being one whose decryption key has been exposed; and

an encryption key designation unit (306) for

designating encryption keys and decryption keys that are associated with the terminals by the predetermined key assignment method, wherein decryption keys that are not assigned to the one or more invalid terminals are prescribed as valid decryption keys, and supposing that a procedure for selecting a valid decryption key assigned for all terminals among terminals to which a previously selected valid decryption key is not assigned, is repeated until all terminals have been assigned selected valid decryption keys, for designating encryption keys that respectively correspond to all of the valid decryption keys that are selected as a result of the procedure, and

the predetermined key assignment method includes the procedures of:

(a) associating each terminal (103a, ...103n) with a leaf in an N-ary tree structure having a plurality of hierarchies (401, 402, 403), N being a natural number equal to or greater than four;

(b) determining, for each node (401, 402, 403) in the tree structure other than the leaves (404), a plurality of invalidation patterns and deciding an individual decryption key for each determined invalidation pattern,

wherein, each of the plurality of invalidation patterns determined for each node denotes a data value that designates whether any of N nodes that are one level below the node and reachable from the node is invalid or not, and indicates that two or more of the N nodes that are one level below the node and reachable from the node are not invalid,

invalid nodes being nodes that are on the paths from the leaves in the tree structure to the root in the tree structure, and that are associated with the invalid terminals, and

the determined plurality of invalidation patterns include one invalidation pattern that indicates that all of the N nodes that are one level below the node and reachable from the node are not invalid;

(c) associating with each leaf (404) in the tree structure decryption keys that are decided for all the invalidation patterns that each indicate that a node (401, 402, 403) that is on a path from the leaf (404) to a root (405) in the tree structure is not invalid, and further individually assigning to each leaf (404) a decryption key, and

(d) assigning, as decryption key groups (905), to the terminal (904) corresponding to each leaf (404) all the decryption keys that are in correspondence with each leaf (404)."

Reasons for the Decision

1. Admissibility of the appeal

The appeal complies with the provisions of Articles 106 to 108 EPC (cf. point II above) and is therefore admissible.

2. SOLE REQUEST

This request differs from the request underlying the

appealed decision essentially in that claim 1 as amended is directed to a key assignment method comprising *inter alia* features of former claims 1, 5, and 16, with the term "combination pattern" having been replaced by the expression "invalidation pattern", and further specifying that

A. each of the plurality of invalidation patterns determined for each node denotes a data value that designates whether any of N nodes that are one level below the node and reachable from the node is invalid or not, and indicates that two or more of the N nodes that are one level below the node and reachable from the node are not invalid,

B. the determined plurality of invalidation patterns include one invalidation pattern that indicates that all of the N nodes that are one level below the node and reachable from the node are not invalid,

C. associating with each leaf in the tree structure decryption keys that are decided for all the invalidation patterns that each indicate that a node that is on a path from the leaf to a root in the tree structure is not invalid,

while dependent claim 2 as amended incorporates the features of former claim 6 in conjunction with page 47, line 6 to page 48, line 23 and Fig. 13 of the original application.

The added feature A is, in particular, supported by the disclosure of page 36, line 20 to page 37, line 12; page 39, lines 17-25, and Figs. 8 and 9, while the added feature B is based on Figs. 6 and 9 of the application as filed. Added feature C is supported by page 41, line 8 to page 43, line 25 in conjunction with Figs. 10 and 11 of the application as filed.

Hence, the above amendments are admissible under Article 123(2) EPC.

2.1 Article 84 EPC 1973

The examining division held that the former claims 1, 4, 12, 15, 21, and 22 were not clear, while former claims 2, 3, 14, 17, and 18 were not concise (cf. appealed decision, sections 1 to 4).

As a result of the amendments made in response to the clarity objections contained in the decision under appeal and raised in the board's communication under Article 15(1) RPBA (cf. section 3.2.2), the board is satisfied that those objections are overcome. For these reasons, the board concludes that the present claims are clear and concise under Article 84 EPC 1973.

2.2 Article 52(1) EPC: Novelty and inventive step

The board cannot pass final judgment on the questions of novelty and inventive step in the present case, for the following reasons:

2.2.1 The examining division did not decide on the matters of novelty and inventive step in the first-instance proceedings. Instead, in an *obiter dictum*, only a cursory statement was provided as to inventive step, referring to the reasoning set out in its first communication dated 9 October 2006 (cf. point I above).

In that communication, it was merely stated that "no detailed examination as to novelty and inventive step" was performed and that a hierarchical system "wherein the devices are associated to the leaves of the trees, and wherein the keying or rekeying of the devices

during the leave or join of devices is performed using a key block wherein the upper level key in the tree is encrypted using the key of the lower level down to the user" was known from documents D3, D4 or D5 and that therefore a device implementing the known method was generally not considered as meeting the requirements of inventive step (cf. first communication dated 9 October 2006, section 7). In particular, no closest prior art was identified. Nor were any distinguishing features with regard to the subject-matter of claim 1 and the closest prior art whatsoever determined.

2.2.2 The board therefore concludes that, under the present circumstances, it is not appropriate to take a definitive decision on the matters of novelty and inventive step.

3. Remittal to the department of first instance

Following the substantial amendments made to the claims, the sole ground for refusal (i.e. lack of clarity and conciseness under Article 84 EPC 1973) given in the appealed decision no longer applies in the present case (cf. point 2.1 above). However, no complete assessment of novelty and inventive step for the claimed subject-matter was carried out during the first-instance proceedings (cf. section 2.2.1 above).

Since, in addition, the appellant requested that the application be remitted to the department of first instance and since all the outstanding objections raised in the board's communication under Article 15(1) RPBA were resolved at the oral proceedings held on 18 April 2013 (cf. point V above), the board decided to exercise its discretion to remit the case to the department of first instance for further prosecution

under Article 111(1) EPC 1973, on the basis of claims 1 and 2 as filed during the oral proceedings before the board.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the examining division for further prosecution based on claims 1 and 2, filed during the oral proceedings before the board.

The Registrar: The Chair:

K. Götz A. Ritzka

Decision electronically authenticated