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 22 November 1995

Case Number: T 0162/95 - 3.5.1

Application Number: 85303817.2

Publication Number: 0166541

IPC: H04L 9/00

Language of the proceedings: EN

Title of invention:
Communications network using an enciphering and deciphering device

Patentee:
KABUSHIKI KAISHA TOSHIBA

Opponent:
(01) Siemens AG
(02) GAO Gesellschaft für Automation und Organisation mbH

Headword:
-

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

Keyword:
"Inventive step (yes)"

Decisions cited:
-

Catchword:

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0162/95 - 3.5.1

D E C I S I O N
of the Technical Board of Appeal 3.5.1
of 22 November 1995

Appellant: (Opponent 01)
Siemens AG
Postfach 22 16 34
D-80506 München (DE)

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

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

Representative:
Luckhurst, A. H. W.
MARKS & CLERK
57-60 Lincoln's Inn Fields
London WC2A 3LS (GB)

Decision under appeal: **Interlocutory decision of the Opposition Division of the European Patent Office dated 29 November 1994 concerning maintenance of European patent No. 0 166 541 in amended form.**

Composition of the Board:

Chairman: P. K. J. van den Berg
Members: A. S. Clelland
G. Davies

Summary of Facts and Submissions

I. European patent No. 0 166 541, granted on 20 March 1991, was opposed by two opponents on the ground that the subject-matter of the claims as granted lacked an inventive step (Articles 100(a), 52(1) and 56 EPC).

During the course of the opposition proceedings the following documents, inter alia, were cited:

OI-1: CRYPTOLOGIA, Volume 5 No. 1, January 1981, pages 46 to 50; L.KRUH: "Cipher equipment"

OII-6: US DEPT OF COMMERCE / NATIONAL BUREAU OF STANDARDS, Data encryption standard, 15 January 1977, pages 1 to 10 (submitted by Opponent II) and pages 15 to 18 (submitted by the Proprietor).

II. Oral proceedings were held before the Opposition Division on 28 April 1994. At the end of these proceedings the Division announced its intention to maintain the patent on the basis of claims originally submitted on 7 July 1992 contingent on various further amendments. These having been submitted, an interlocutory decision to maintain the patent as amended was issued on 29 November 1994.

III. The documents constituting the patent as maintained are as follows:

Claims: 1 to 7 received 13 July 1994;
Description: pages 1, 1a, 2, 3, 3a, 3b and 4 to 11 received 13 July 1994; and
Drawings: sheets 1 to 4 of the published patent.

IV. Claim 1 reads as follows:

"A two-way communications network system in which a plurality of transmitting terminals (11, 83) and one receiving terminal (12, 81) are connected by communication lines;
each transmitting terminal (11, 83) comprises an enciphering device (14, 85) for enciphering a communication message (M) to be transmitted by a sender to said receiving terminal (12, 81), and transmitting means (23) for transmitting an output signal of said enciphering device (14, 85) to said receiving terminal via a communication line (13, 82);
said receiving terminal (12, 81) comprises receiving means (25) for receiving the enciphered message (M') from said transmitting terminal (11, 83) and a deciphering device (15) for deciphering the received enciphered message;
said enciphering device comprises key memory means (32, 33, 34, 53) for storing key data (R, I, S) which can specify the sender and the communication message (M) transmitted by the sender to said receiving terminal (12, 81), and enciphering means (31, 35, 36, 51, 52, 54) for enciphering, according to a prescribed enciphering algorithm (f) using the key data (R, I, S) stored in said key memory means (32-34), the message (M) input from the outside to be transmitted to said receiving terminal (12, 81), and for outputting the enciphered message (M') and the key data (I) which can specify the sender,
said deciphering device comprises key memory means (42, 43, 44, 53) for storing key data (R, I, S) which can specify the sender and the communication message (M) transmitted by the sender to said receiving terminal, and deciphering means (41, 45, 46, 51, 52, 54) for deciphering, according to a prescribed deciphering algorithm (f^{-1}) different from the enciphering algorithm

(f) using the key data stored in said key memory means (42-44), the message (M') transmitted from said transmitting terminal (11, 83), and for outputting the deciphered message (M),

characterised in that

said key memory means and enciphering means of each of said enciphering and deciphering devices are sealed inside said enciphering and deciphering devices respectively such that stored key data and the enciphering and deciphering algorithms cannot be accessed from the outside,
said receiving terminal (12, 81) can be used as a transmitting terminal and each of said transmitting terminals (11, 83) can be used as a receiving terminal in such a manner that a message sent from said receiving terminal (12, 81) to one of said transmitting terminals (11, 83) is enciphered using the deciphering algorithm (f^{-1}), and that the enciphered message is deciphered at said one of said transmitting terminals (11, 83) according to the enciphering algorithm (f)."

V. On 26 January 1995 Opponent I filed a notice of appeal and paid the prescribed appeal fee. A statement setting out the grounds of appeal was subsequently filed on 1 February 1995. Oral proceedings, conditionally requested by both Appellant and Respondent, were held on 22 November 1995. Opponent II took no part in the appeal proceedings.

VI. The parties argued essentially as follows.

The Appellant:

The person skilled in the art would find unrealistic the distinction made in the patent between encryption and decryption algorithms; in a system using the Data Encryption Standard (DES), as in the patent, there was in practice no such distinction. This could clearly be seen from document OII-6, page 10: "Consequently to decipher it is only necessary to apply the very same algorithm to an enciphered message block ...". The fact that the order of the blocks of key bits (subkeys) to be applied to the algorithm must be reversed for deciphering was irrelevant, since the subkeys were not part of the algorithm. The skilled person, contemplating the enciphering and deciphering processes in DES, would recognise that the deciphering process itself satisfied the requirements of a DES enciphering process, so that it was unnecessary to provide an additional separate enciphering device in order to encipher messages to be transmitted in the reverse direction. Document OI-1 was silent as to how messages were transmitted in opposite directions between two stations, but did specify that communications might be full duplex; the person skilled in the art could accordingly be expected to adopt precisely the scheme given in the disputed patent.

The order in which the permutations IP and IP^{-1} were applied in the deciphering algorithm was unimportant, since the skilled person would be aware that these permutations could be modified without damaging the effectiveness of the encryption.

Nor was security increased by the claimed arrangement. Anyone in possession of a receiving station had all the required elements for both enciphering and deciphering

messages, namely the algorithm and the subkeys. Indeed, it could be argued that security was decreased in that data was travelling in two directions using closely related encryptions.

The Respondent:

In the DES system the enciphering and deciphering algorithms were always different and gave rise to two different encodings, as discussed in the patent. Document OII-6 could only be interpreted as meaning that the steps in the DES encoding algorithm shown on page 8 must when deciphering be applied in the opposite order and with the order of the permutations IP and IP^{-1} reversed. Furthermore, the Appellant's concentration merely on the subkeys was misleading; the DES algorithm applied to a message and a single key, from which the subkeys were derived by part of the algorithm as shown on pages 15 to 18 of OII-6. The key, with the necessity for its communication from sender to receiver, was also part of the system. In the DES system a given key always gave rise to the same encoding of a given message. It therefore followed that the enciphering in the reverse direction in the patent was not a DES enciphering, since it used the same key but came to a different result. Document OI-1 made quite clear that DES enciphering was used, and therefore either entirely different keys would be used in transmitting data in opposite directions or the same key, and therefore the same encoding. Contrary to the Appellant's view, since the DES deciphering algorithm was not the same as the enciphering algorithm, it would not be apparent to the skilled person that the deciphering algorithm could be used for enciphering data; there was no reason to expect that data encoded using the DES deciphering algorithm would have the security offered by the DES itself.

Security was however increased because the user (customer) could not generate false messages purporting to come from the central receiving station.

Reasons for the Decision

1. The appeal is admissible.

2. *Interpretation of claim 1*

2.1 The Appellant has argued that in the Data Encryption Standard (DES) the enciphering and deciphering algorithms are in fact the same. However, the only specific embodiment given in the patent in suit, although said to use the DES, makes use of algorithms for encryption and decryption which are said to differ. The question which therefore arises is what is to be understood in the context by an "algorithm".

2.2 As pointed out by the Respondent, the DES enciphering process (and equally the deciphering process) starts out with a single key and a text to be enciphered (or deciphered). The production of the subkeys used for enciphering blocks, whilst not carried out anew for every block, is a part of the DES enciphering algorithm as a whole. Sixteen differing subkeys K1 to K16 are produced, these subkeys then being used in that order when enciphering each block. When deciphering each block on the other hand, the same subkeys are used, but in the opposite order.

2.3 Thus, the deciphering algorithm differs from the enciphering algorithm, either in the order attached to the subkeys by the subkey-producing parts of the algorithms, or in the order of addressing the subkeys in

the block-enciphering and block-deciphering parts of the algorithms (see also document OII-6, page 7). This in the Board's view serves to establish that in the DES the two algorithms, when considered as a whole, are indeed different, so that the requirement in claim 1 that f differs from f^{-1} is satisfied by the DES. Using the enciphering algorithm for deciphering is not in accordance with the DES standard. On the other hand, on the Board's understanding of document OII-6 the deciphering of an individual block does not require a reversal of the order of the permutations IP and IP^{-1} applied at the beginning and end of the block algorithm (see page 10: "Deciphering"). The operations on the individual blocks do not therefore constitute a point of difference between the DES enciphering and deciphering algorithms.

3. *Novelty and inventive step*

3.1 It was common ground at the oral proceedings that document OII-6, which defines the Data Encryption Standard, represents the common general knowledge in the art. It was also common ground that document OI-1 is the single most relevant document; it describes a practical system said to use DES encryption/decryption and itself refers to document OII-6 (see page 46, penultimate line). The Board interprets the references to the use of DES as meaning that **all** communications in the system, including two-way (duplex) communications, make use of the DES algorithm. Since, as established above, the DES deciphering algorithm for a given key differs from the enciphering algorithm for that key, applying the deciphering algorithm as an enciphering algorithm is not in accordance with the DES standard as known from document OII-6. The skilled person, implementing the

system of document OI-1, would not use the same algorithms for encryption and decryption. The subject-matter of the independent claim is therefore novel with respect to document OI-1.

3.2 Since document OI-1 clearly indicates that two-way communications may take place but does not give any details of how this is done, the problem facing the person skilled in the art may be considered to be that of implementing such two-way communications in the document OI-1 system.

3.3 In order for a message to be sent in one direction, the sender and receiver must share a key. Thus one party must send a key (or enough information to construct a mutual key) to the other. This key may be sent by some method outside the communication system (e.g. by courier) and entered into the second station by hand, or it may itself be sent in a message. This latter is the primary solution adopted in the system of OI-1, the key-containing message itself being encrypted using a "master key" (page 48, paragraph 2).

3.4 An obvious solution to the implementation of two-way communications would be for the same key and the same encryption to be used in both directions. It was argued by the Appellant that the skilled man would consider such a solution to be unsatisfactory, firstly because it increases the amount of traffic on the communications lines encrypted in a particular way, thus increasing the possibilities for an eavesdropper to break the code, and secondly because it introduces the possibility that the user could construct false messages purporting to come from the central receiving station. Hence it was desirable that the messages in the two directions be encrypted differently. However, in the Board's view, the skilled person faced with this problem would duplicate

the process applied for one-way communication: in other words, a different key would be used depending on the direction of communication. Each station would then use a deciphering algorithm with one key and an enciphering algorithm with the other key.

3.5 Although in the Appellant's view the use of differing processes for enciphering and deciphering would overload a station having full duplex communication, it is clear that this problem exists in any duplex system irrespective of the algorithm and keys used; for full duplex communication separate circuitry and/or software processes are necessary to deal with data to be sent and data received. The skilled person could be expected to respond to any problem of overloading either by increasing the speed of the devices or by reducing the communication rates (it is noted that in OI-1 at page 47, line 5 the data rate is limited to 9600 bits per second).

3.6 Thus the obvious solution to the problem of implementing two-way communications, if the same encryption is not to be used in both directions, is the use of two independent keys. This however requires the transmission of the two keys, which in itself increases the security risks. Thus the master key would be used twice as often, leading to a shorter safe lifetime for that key (see OI-1 page 48, paragraph 2). The communication protocols would clearly be more complex than in a single-key system.

3.7 The patent on the other hand produces two different encryptions from the same key, thus improving security over a one-key system whilst avoiding the complications involved in providing two keys. It is indeed arguable that, as asserted by the Appellant, data communications in such a system are not as secure as in a system using

two completely unrelated keys. However, in any system aiming at confidential communications there are a variety of security threats. Although the customer terminal has available in principle the necessary information in the form of the key or the subkeys for constructing false messages, the claim specifies that the key memory means and enciphering means are sealed. Hence at one level of security they must be considered to be single units, so that an additional layer of security is indeed given by having differing enciphering devices in the sender and receiver.

3.8 None of the prior art available to the Board clearly suggests that two different enciphering algorithms might be used within one system for communications in opposite directions, much less that different algorithms might use the same key. In the absence of any documents pointing in this direction, arguments to the effect that the skilled person would find it obvious to use the deciphering algorithm as an enciphering algorithm, would seem to depend on an ex post facto analysis.

3.9 Hence the Board concludes that the subject-matter of claim 1 satisfies the requirements of the EPC as regards inventive step.

3.10 For the sake of completeness it is observed that the first characterising feature of claim 1, namely that various elements in the devices are sealed, is in the Board's view a self-evident requirement for a secure system. It is noted that the Respondent has not attempted to base any argument for an inventive step on this feature.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

M. Kiehl P. K. J. van den Berg

11.1.96