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

# Datasheet for the decision of 20 January 2012

**Case Number:** T 1627/07 - 3.5.01

**Application Number:** 00966423.6

**Publication Number:** 1223517

**IPC:** G06F17/30

**Language of the proceedings:** EN

**Title of invention:**
DATA TRANSMISSION SYSTEM AND SALE MANAGING SYSTEM

**Applicant:**
Kabushiki Kaisha Visual Japan

**Headword:**
Database packet commands/KABUSHIKI KAISHA VISUAL

**Relevant legal provisions:**
EPC 1973 Art. 56

**Keyword:**
Inventive step - use of public network and TCP/IP (no - obvious alternative to a dedicated line) - use of VPN (no - obvious measure to increase security) - use of proprietary commands (no - obvious from D3)

**Decisions cited:**

**Catchword:**

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

**Case Number: T 1627/07 - 3.5.01**

# D E C I S I O N
# of the Technical Board of Appeal 3.5.01
# of 20 January 2012

**Appellant:** (Applicant)
Kabushiki Kaisha Visual Japan
3-12-3, Kandajinbocho,
Chiyoda-ku
Tokyo 101-0051 (JP)

**Representative:**
Isarpatent
Patent- und Rechtsanwälte
Postfach 44 01 51
80750 München (DE)

**Decision under appeal:** **Decision of the Examining Division of the European Patent Office posted 13 April 2007 refusing European patent application No. 00966423.6 pursuant to Article 97(1) EPC 1973.**

**Composition of the Board:**

**Chairman:** S. Wibergh
**Members:** W. Chandler
P. Schmitz

## Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse the European patent application No. 00966423.6. It concerns a network for connecting client terminals, such as shop cash registers, with a database on a server, e.g. at company headquarters.

II. The examining division decided that claim 1 of the main request did not involve an inventive step because it would have been obvious (Article 56 EPC 1973) to use the well-known TCP/IP and virtual private network (VPN) in the remote terminal local area network described in WO 99/06925 (D3). Claim 1 or claim 6 of the first to third auxiliary requests were also refused for lack of inventive step as they were considered to add only well-known features. In a section entitled "Obiter dicta", the division referred to the following documents as evidence of common knowledge about encryption in VPNs and database commands, respectively.

D4: A.O. Freier et al.: "The SSL Protocol Version 3.0 <draft-ietf-tls-ssl-version3-00.txt", IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, 18-11-1996, pages 1-65

D5: T. MCAVOY: “Open Database Connectivity (ODBC) and the Human Machine Interface (HMI) Database”, ISA TECH/EXPO Technology Update, Instrument Society of America, Res. Triangle, NC, US, vol 1, NR PART 1, 1997, pages 163-172

III. In the statement of grounds of appeal, the appellant essentially maintained the subject-matter of the refused requests. In response to a communication of the Board summarising the issues to be discussed at the

oral proceedings, the appellant filed claims of a new main and auxiliary request.

IV. At the oral proceedings, the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the above-mentioned main or auxiliary request, both filed by letter received 20 December 2011. At the end of the oral proceedings, the Chairman announced the Board's decision.

V. Claim 1 of the main request reads as follows:

"A network-type data transmission system wherein a server (4) and a plurality of terminal units (2) sharing the server (4) are connected by way of a public network circuit (6), said system comprising:

(A) the terminal unit (2) comprising (A1) a DB-VPN (database-virtual private network) driver (223) for generating, each time each terminal unit (2) brings about a demand for processing a database (428) at the server (4), a packet command for the transmission of a DB operation command complying with a private DB (database) command transmission protocol which is independent of the TCP-IP protocol for the public network circuit (6),

(A2) a communication driver (222) arranged between the DB-VPN driver (223) and public network circuit (6) to carry TCP-IP protocol for the public network circuit (6) into execution, and

(B) the server (4) comprising (B1) a DB-VPN service (423) for converting the received packet

command for the transmission of the DB operation command into a converted DB operation command;

(B2) an ODBC (open database connectivity) driver (424) for compatibly accepting said converted DB operation command with a common interface independent of a variety of interfaces of DBMS (Database Management System)s to invoke a DBMS (425), said DBMS executing said converted DB operation command to reflect an executed result on the DB (database) (428) of the server (4); and

(B3) a communication driver (422) arranged between the DB-VPN service (423) and the public network circuit (6) to carry the TCP-IP protocol for the public network circuit (6) into execution,

characterized in that

said packet command for the transmission of a DB operation command complying with a private DB command transmission protocol which is independent of the TCP-IP protocol for the public network circuit (6) includes the packet command provided with a parameter necessary for each of processings for "DB opening", "DB readout", "DB storage" and "DB closing", and

when data is collected at any one of the terminal units (2), the packet command for the transmission of the DB operation command complying with the private DB command is generated by the DB-VPN driver (223); and said packet command is transmitted through the public network circuit (6) according to TCP-IP protocol to the server (4); and the packet command is received by the communication driver (422) at the server (4); and the received packet command is converted into the converted

DB operation command by the DB-VPN service (423); and said converted DB operation command is executed by the DBMS (425) invoked by the ODBC driver (424); and a result executed by the DBMS (425) is reflected by the ODBC driver (424) on the DB (database) (428) of the server (4) in real time."

Claim 1 of the auxiliary request adds to the end of claim 1 of the main request:

"and when the packet complying with the private DB command transmission protocol independent of the network circuit is generated by the terminal unit, an encryption processing is carried out on the packet at the terminal unit, the packet is transmitted to the server, and the packet is decoded at the server; and

when the server responds to the terminal unit, an encryption processing is carried out on the packet at the server, the packet is transmitted to the terminal unit, and the packet is transmitted to the terminal unit, and the packet is decoded at the terminal unit."

## Reasons for the Decision

1. The Board cannot see any prejudicial error in the examining division's conclusion that the subject-matter of the invention does not involve an inventive step (Article 56 EPC 1973).

2. According to the description, the invention is essentially the connection of terminal units, such as shop cash registers, with a database on a server over a public network using the TCP-IP protocol [13]. The invention uses a proprietary set of twelve database

commands (Figure 7) to request data operations [66]. A "DB-VPN driver" (Figure 4: 223) converts these commands into packets of a protocol (i.e. a virtual private network - VPN - protocol) independent of the network TCP/IP protocol [40]. At the server, a corresponding "DB-VPN service" (Figure 5: 423) converts the packets back into database operations for accessing the database, using the conventional ODBC interface 424 to the DBMS 425 [46].

3. Claim 1 of the main request specifies this subject-matter with some repetition in the characterising part. The claim can be summarised, without the repetition and without the functionality that is implicit from the claimed means, as follows (with the appellant's numbering of the features of the pre-characterising part and the Board's numbering of those of the characterising part):

A network-type data transmission system with a server (4) and a plurality of terminal units (2) connected over a public network circuit (6)

(A) each terminal unit (2) comprising:
(A1) a DB-VPN driver (223) generating packet commands independent of the TCP-IP protocol for the public network circuit (6)
(A2) a communication driver (222)
(B) the server (4) comprising:
(B1) a DB-VPN service (423)
(B2) an ODBC driver to invoke the DBMS of the server (4)
(B3) a communication driver (422)

characterised by:

(C1) packet command with a parameter for "DB opening", "DB readout", "DB storage" and "DB closing"
(C2) the result is reflected on the DB in real time.

4. A number of possible starting points for inventive step were discussed. The appellant was of the view that the invention was totally different from the system of D3, so that its teaching was not applicable. However, the Board cannot agree with this because D3 (Figure 1), like the invention, discloses a plurality of terminal units 12 connected to a database management system (DBMS) 14 on a server 15 via an interface system 10. It is also clear from the opening part that D3 is concerned with the problems of using ODBC drivers.

5. However, a question of interpretation arises as to whether the interface system 10 is to be interpreted as part of the server or part of the terminal units. This determines whether the claimed network connecting the terminal units and the server is to be equated with the remote terminal LAN 18 or the LAN 26, respectively. The examining division took the former approach, but the applicant disputed this (see point 1.2 of the decision). Moreover, in the grounds of appeal the appellant discusses the nature of the remote procedure calls (RPC) in D3 at length, which is only really relevant to the second interpretation because these commands are transmitted over the LAN 26. In the Board's view, the chosen interpretation of D3 only affects the detail of the arguments, but not the outcome and, therefore, this point does not need to be decided.

6. Under both interpretations and despite the position of the characterising clause, the Board agrees that the invention differs from D3 as stated by the division in connection with the then pending requests. These differences are that the network interconnecting the units is a public network using a TCP/IP protocol (A1 - preamble), the use of a VPN with proprietary packet DB commands (C1) and appropriate drivers (A1, B1) and working in "real time" (C2).

7. The examining division considered that these features all solved the problem of providing secure access to various kinds of databases from remote terminals. The Board agrees with this.

8. Again, in general and regardless of the particular interpretation of D3, the Board agrees with the examining division that public networks using the TCP/IP protocol, e.g. the Internet, and their advantages and disadvantages were well known. Thus, it would have been an obvious possibility to use such a network to connect terminals, depending on the circumstances. These circumstances, which the skilled person would also have been aware of, include the facts that public networks were less expensive than dedicated lines and that they effectively enabled a permanent connection. The essentially permanent nature of the connection also implies that the database can be updated in "real time" (feature C2). Thus in the Board's view, it would have been obvious to use a public network for either the remote terminal LAN 18, or the LAN 26 according to the second interpretation of D3.

9. The appellant argued that the terminals 12 in D3 were connected by a LAN, but not a public network and that it would not have been obvious to consider this unsafe

alternative. However, as explained above, the Board considers that the use of a public network would have been an obvious alternative to a LAN depending on the circumstances. If all the communicating devices were geographically distant, the skilled person would have chosen the public network because it was less expensive. The skilled person would have been aware of measures to increase security over a public network. Moreover, as the division stated, D3 discloses at page 9, lines 13 to 14, using Ethernet, which generally also uses TCP/IP, for the remote terminal LAN 18. For the LAN 26, D3 discloses at page 8, lines 29 to 31, using TCP/IP. Furthermore, D3 states in this paragraph that TCP/IP is a commonly used protocol for connecting separate devices and that the two networks are "generally" separate. In the Board's view, all this confirms the above mentioned common knowledge and that the skilled person would choose the network set-up according to circumstances, e.g. the arrangement of the terminals.

10. Similarly and following on from the above, the Board agrees with the division that the skilled person would have been aware that one well-known measure to increase security over a public network was a VPN. As the name suggests, virtual private networks were created precisely to provide secure, reliable transport over such public networks. It would therefore have been obvious to consider using a VPN. The appellant argued that there would have been many possibilities of making the communication in D3 secure, such as using a password or isolating parts of the system. However, the existence of other options does not change the fact that using a VPN is one obvious possibility.

11. Given the two concepts of using TCP/IP and a VPN, the Board judges that the use of VPN drivers (features A1 and B1) follow as matters of routine design in this field. In other words, some new driver (i.e. the DB-VPN driver) is required to convert the database commands into packets suitable for transmission over the VPN and *vice versa*. The appellant emphasised the feature that the private DB command transmission protocol was independent of the TCP-IP protocol on the public network. However, the Board considers that this is generally a feature of the protocol running on the VPN compared with the underlying network protocol.

12. This leaves the feature of the proprietary packet commands (C1). The appellant's main argument, essentially for both interpretations of D3, is that the skilled person would not remove the ODBC driver from the client and replace the SQL commands with the claimed packet DB commands. Alternatively stated, the prior art, already having an ODBC driver, teaches away from replacing this with the claimed "DB-VPN" driver.

13. Firstly, the Board notes that the absence of the ODBC driver at the client is a consequence of using the new commands rather than a feature that stands alone. In any case, it is not explicitly excluded from claim 1. In the Board's view, the use of the new commands is obvious under either interpretation of D3.

14. Using the division's interpretation, the commands are mapped onto the "MSG" commands sent over the remote terminal LAN. The Board agrees with the division's argument that the skilled person would have to decide on some database commands to use and the implicit conclusion that if these commands were converted into a form suitable for being sent over a VPN - a private

network - they would also fall under the claimed "packet command provided with a parameter necessary for [the various database processings]" (feature C1). The appellant discussed the nature of the "MSG" commands at length at point 3.1.1.12 of the grounds of appeal and concluded that they must be SQL commands. However, none of the references to D3 actually state this. In the Board's view, the nearest that D3 comes to this is at page 10, lines 10-13, where it states that the transaction mapper 34 will cause a validation message to "be immediately recognized as such" and will call the ODBC driver object 36. However, it could be that a non-SQL command is recognised. In any case, even if they were SQL commands, this would not appear to change the above argument since the skilled person would still need to convert them to packets for use over the VPN and the resulting commands would then still fall under the claim.

15. The Board judges that this is also obvious under the second interpretation of D3 where the commands are mapped onto the remote procedure call (RPC) commands sent over the LAN 26. In this case, D3 explicitly discloses at column 11, line 18 to column 12, line 1, that an RPC is used instead of an SQL command and an ODBC interface for a database update. This call has the form "RPCxx(AAA,BBB,CCC)", where xx identifies an SQL procedure to be called at the server. When converted to packets to be sent over the VPN, this would also result in the claimed commands. In particular, since such a command is issued for updating the database, it must contain parameters necessary at least for "DB storage", as set out in claim 1.

16. The appellant argued that the system of D3 does not have a packet with a command. However, as mentioned

above, this concept follows once the decision has been taken to use a packet network to send database commands. Even as is stands, the commands in D3 would have to be converted to packets to be transmitted over the networks used there.

17. The appellant also argued that the prior art systems always needed an ODBC "partner" driver at the client. By eliminating this, the invention was more flexible. However, as explained above, under both interpretations D3 provides or suggests a mechanism that does not use an ODBC driver at the client. In both cases, the relevant command uses an SQL procedure at the server, so that the resultant overall situation would be the same as that in the invention, i.e. no "partner" driver at the client. The "flexibility" of such an arrangement depends on the various commands and drivers available. Moreover, there is a strong incentive to arrive at this situation because the overall point of D3 is, as mentioned for example at the end of the opening part of the description, that ODBC drivers have several drawbacks, such as the need to update and expense, and the solution is to not use them for critical tasks.

18. Accordingly the Board judges that claim 1 of the main request does not involve an inventive step (Article 56 EPC 1973).

19. Claim 1 of the auxiliary request essentially adds to claim 1 of the main request the limitation that the VPN packets are encrypted. However, the Board agrees with the examining division's comments in connection with the first auxiliary request that this is a well known aspect of a VPN, which would be obvious if not essential to consider.

20. The appellant requested at point 3.1.3 of the grounds of appeal that the Board substantiate that the encryption features in particular were prior art. However, in the Board's view, the examining division showed this in the obiter dicta on page 14 of the decision (see point II, above). In any case, encryption as such is notoriously well known.

21. Accordingly, claim 1 of both requests does not involve an inventive step (Article 56 EPC 1973), so that the appeal must be dismissed.

## Order

## For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek S. Wibergh

Decision electronically authenticated