

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 21

**UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

---

Ex parte ERAN GABBER, and ABRAHAM SILBERSCHATZ

---

Appeal No. 2000-1999  
Application 08/748,314

---

ON BRIEF

---

Before KRASS, JERRY SMITH, and BLANKENSHIP, Administrative Patent Judges.

KRASS, Administrative Patent Judge.

This is a decision on appeal from the final rejection of claims 1-44.

The invention pertains to a protocol for secure communication of electronic commercial transactions.

The nature of the invention is easily understood from reference to representative independent claim 1 reproduced as follows:

1. A protocol for securely communicating a financial transaction between a customer and a merchant, a central authority having a central authority private



Appeal No. 2000-1999  
Application 08/748,314

Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teachings, suggestions or implications in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed. Cir.), cert. denied, 488 U.S. 825 (1988); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 293, 227 USPQ 657, 664 (Fed. Cir. 1985), cert. denied, 475 U.S. 1017 (1986); ACS Hosp. Sys., Inc. v. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). These showings by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). If that burden is met, the burden then shifts to the applicant to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. See Id.; In re Hedges, 783 F.2d 1038, 1039, 228 USPQ 685, 686 (Fed. Cir. 1986); In re Piasecki, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984); and In re Rinehart, 531 F.2d 1048, 1052, 189 USPQ 143, 147 (CCPA 1976).

In the instant case, the examiner admits that the primary reference to Sirbu lacks any teaching of a quotation from the merchant containing the public key of the merchant, a signature of the central authority which is a function of the account, and a

Appeal No. 2000-1999  
Application 08/748,314

signature of the merchant which is a function of the account and the price. The examiner also admits that Sirbu does not disclose an order from the customer containing the public key of the customer, a signature of the central authority which is a function of the account, and a signature of the customer which is a function of the account and the price.

The examiner relies on Schneier for a disclosure that information sent between parties is signed using the private key of the sending party, referring to page 37, paragraphs 3-6. Schneier is also relied on for a teaching of a public key sent with a message in a digital certificate which contains a signature of the certification authority which is a function of the sender's information, referring to page 185, paragraph 6, and page 186.

The examiner concludes therefrom that it would have been obvious "to use a digital signature and certificate in the invention of Sirbu...motivated by the need to verify the person sending the information and the information sent" (answer-page 4).

We will not sustain the rejection because, while the examiner has provided a reference, in Schneier, that mentions public and private keys and certification authority, the examiner has not established Schneier as teaching what is specifically claimed. That is, claim 1, for example, requires the quotation to include the merchant public key, a central authority private key-signed signature that is a function of the merchant account, an unsigned copy of a price and a merchant private key-signed signature that is a function of the merchant account and the price. The claim further requires that the

Appeal No. 2000-1999  
Application 08/748,314

received order include the customer public key, the central authority private key-signed signature that is a function of the customer account, an unsigned copy of the price and a customer private key-signed signature that is a function of the customer account, the merchant account and the price.

The examiner has not specifically identified where, in Schneier, such claimed limitations are taught and we do not find, in Schneier, the particular claimed combinations of elements for the quotation and the order.

The examiner has identified, in Schneier, that the reference discloses “digital signing the message data with the private key of the sender” (answer-pages 8 and 10). The examiner further points to page 185, paragraph 6 and page 186 of Schneier for a teaching of “sending the public key with the message that is digitally signed” (answer-page 10). However, even assuming that all the examiner contends is true, this still does not offer a reference, or a combination of references, which suggests the specific combination of elements, i.e., a quotation that includes the merchant public key, a central authority private key-signed signature that is a function of the merchant account, an unsigned copy of a price and a merchant private key-signed signature that is a function of the merchant account and the price; and an order that includes the customer public key, the central authority private key-signed signature that is a function of the customer account, an unsigned copy of the price and a customer private key-signed signature that is a function of the customer account, the merchant account and the price.

Appeal No. 2000-1999  
Application 08/748,314

The examiner identifies bits and pieces of the claim, i.e., that public and private digital keys and key-signed signatures, per se, were known but does not, or cannot, identify, where in the prior art, the claimed combinations of various private, public and key-signed signatures are suggested. Appellants have pointed out that the claimed central authority private key-signed signature is concatenated in the distributed protocol so that the commercial transaction between the customer and the merchant can be carried out independent of any certification, or central, authority, a significant advantage if the central authority becomes unavailable (see reply brief-page 3). In the absence of any contrary evidence from the examiner, such an argued advantage shows even more strongly the nonobviousness of the claimed subject matter and that the examiner cannot reasonably conclude that merely because private, public, and key-signed signatures were well known, it would have been obvious to provide for the specifically claimed combination and to modify Sirbu with such a combination in order to arrive at appellants' claimed invention.

Since the examiner has not convinced us that the specific combinations of elements set forth in the instant claims have been taught or would have been

Appeal No. 2000-1999  
Application 08/748,314

suggested by the applied references, we will not sustain the rejection of claims 1-44  
under 35 U.S.C. §103.

The examiner's decision is reversed.

REVERSED

ERROL A. KRASS	)	
Administrative Patent Judge	)	
	)	
	)	
	)	BOARD OF PATENT
JERRY SMITH	)	
Administrative Patent Judge	)	APPEALS AND
	)	
	)	INTERFERENCES
	)	
HOWARD B. BLANKENSHIP	)	
Administrative Patent Judge	)	

Appeal No. 2000-1999  
Application 08/748,314

Glenn W. Boisbrun  
Hitt Chwang and Gaines, P.C.  
225 University Plaza  
275 West Campbell Road  
Richardson, TX 75080

EAK/jlb