The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.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. 28

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte BARBARA L. FOX, BRIAN A. LAMACCHIA
and BRIAN C. BECKMAN

Appeal No. 2003-0072
Application No. 09/032,407

ON BRIEF

Before THOMAS, HAIRSTON and KRASS, Administrative Patent Judges.

KRASS, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appal from the final rejection of claims 1, 13-17 and 19-30. Claims 2-12 and 18 have been indicated by the examiner as being directed to allowable subject matter and are not on appeal herein.

The invention is directed to an electronic method of doing business. In particular, a user is enabled to perform an

electronic commerce transaction over an unsecured network without requiring encryption. The user obtains a commercial relationship certificate from a second party, e.g., a bank, and the commercial relationship certificate is provided to a third party seller over an unsecure network. The seller presents the commercial relationship certificate, digitally signed by the user, to the second party over an unsecure network in exchange for payment.

Representative independent claim 1 is reproduced as follows:

1. A method for performing an electronic commerce transaction over an unsecure network without requiring encryption, comprising the steps of:

(a) enabling a first party to apply for registration with a second party in order to receive a commercial relationship certificate, the first party having access to financial resources through the second party;

(b) presenting a certified identifier of the first party to the second party, said certified identifier enabling the second party to confirm a true identify of the first party;

(c) transferring the commercial relationship certificate to the first party from the second party over the unsecure network, the commercial relationship certificate being digitally signed by the second party and including the certified identifier and an index to the financial resources accessible to the first party through the second party, neither said commercial relationship certificate nor said index being encrypted or secret;

(d) providing the commercial relationship certificate to a seller over the unsecure network, the commercial relationship certificate being digitally signed by the first party to indicate that the first party agrees to make a payment for goods provided

by the seller in an amount indicated in the certificate as digitally signed; and

(e) said seller presenting the commercial relationship certificate that was digitally signed by the first party to the second party over the unsecure network in exchange for the payment, the second party referencing the amount indicated in said commercial relationship certificate in making the payment to the seller from the financial resources accessible by the first party.

The examiner relies on the following references:

Matyas et al. (Matyas)	4,941,176	Jul. 10, 1990
Rosen (407)	5,455,407	Oct. 3, 1995
Rosen (518)	5,557,518	Sep. 17, 1996
Tozzoli et al. (Tozzoli)	5,717,989	Feb. 10, 1998 (filed Oct. 13, 1994)
Pare Jr. et al. (Pare)	5,764,789	Jun. 9, 1998 (filed Sep. 27, 1996)
Ginter et al. (Ginter)	5,892,900	Apr. 6, 1999 (filed Aug. 30, 1996)

Schneier, "Applied Cryptography", Second Edition, Protocols, Algorithms, and Source Code In C, John Wiley & Sons, Inc. (1996), pp. 37-39, 58-59 and 483-502.

Claims 1, 13-17 and 19-30 stand rejected under 35 U.S.C. § 103. As evidence of obviousness, the examiner offers Ginter, Schneier, Pare and Rosen(518) with regard to claims 1, 13-17 and 19. The examiner offers Ginter, Schneier and Rosen (518) with regard to claims 20 and 21 and the examiner offers Ginter, Schneier, Matyas, Rosen (407) and Tozzoli with regard to claims 22-30.

Reference is made to the briefs and answer for the respective positions of appellants and the examiner.

OPINION

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the examiner to establish a factual basis to support the legal conclusion of obviousness. See In re Fine, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In so doing, the examiner is expected to make the factual determinations set forth in Graham v. John 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).

We reverse.

It is the examiner's position that Ginter suggests the performance of electronic commerce transactions over an unsecure network without requiring encryption, at column 224, lines 14-25, but lacks an explicit recitation of "performing an electronic commerce transaction over an unsecure network without requiring encryption" (answer-page 6). So the examiner turns to Schneier, at pages 37, 483-502 and vii, for a suggestion of "performing an electronic commerce transaction over an unsecure network without requiring encryption." The examiner then concludes that it would have been obvious to add the modifications of Schneier to the

method disclosed by Ginter "because such modifications would have provided '*a separate algorithm for digital signatures that cannot be used for encryption*.'" (Answer-page 6, quoting Schneier at page 37).

Then, at page 7 of the answer, the examiner indicates that Ginter shows elements suggesting "enabling a first party to apply for registration with a second party, the first party having access to financial resources through the second party..." (identifying column 42, lines 4-16, column 210, lines 49-52, and column 223, lines 14-16 of Ginter) and elements suggesting "transferring <u>the commercial relationship</u> certificate to the first party from the second party over the unsecure network, the <u>commercial relationship</u> certificate being digitally signed by the second party and including the certified identifier..." (identifying column 261, lines 10-47 of Ginter).

Because Gitner lacks an explicit recitation of "a commercial relationship certificate...," the examiner interprets Ginter's certificate as a commercial relationship certificate and also refers to the Rosen (518) disclosure of a "certificate" at column 5, lines 38-40.

Since Ginter fails to explicitly show "an index to the

financial resources accessible to the first party through the second party...," the examiner cites various figures and column 4, lines 30-45, column 23, lines 45-52, column 24, lines 13-19, column 31, lines 13-21, and column 32, lines 19-21, of Pare.

The examiner concludes that it would have been obvious to add the modifications of Pare to the method of Ginter "because such modifications would have provided a system that would have provided '*financial services system that is highly resistant to fraudulent account accesses by unauthorized people*'" (answer-page 8, referring to Pare's column 6, lines 37-39).

We have carefully reviewed the examiner's rejection and rationale therefor and conclude that the examiner has not established a prima facie case of obviousness with regard to the instant claimed subject matter.

From the portions of the references to which the examiner alludes, it appears that the examiner has merely referenced words which sound similar to certain terms within the instant claims but which have no bearing on the instant claimed invention. For example, instant claim 1 calls for a "commercial relationship certificate." Claim 20 calls it a "certificate...assuring an authenticity of the first party" and produced by "the combination of the public key and the unique reference being digitally signed

by the second party." Claim 22 describes it as a "certificate that is digitally signed by the opening bank and which includes an identifier and a reference to the LOC..." To find a teaching of this claimed certificate, the examiner refers to Rosen 518, at column 5, lines 40-41, wherein an "Issuer Certificate 16" is mentioned. However, the examiner does not adequately explain how this is equivalent to a "commercial relationship certificate," as defined by instant claim 1 or to the certificates defined by instant claims 20 and 22.

Moreover, while the examiner contends that various portions of the various references teach the various claimed elements, pointing to various portions of the references, the examiner does not specifically identify how these recitations in the references specifically relate to the claimed elements nor does the examiner adequately explain what would have led an artisan to combine the various references.

This is especially important since the instant claimed invention is directed to performing electronic commerce transactions over an unsecure network without requiring encryption. Yet, the portion of Ginter relied upon, in column 224, is under the heading of "Cryptographic Sealing. Moreover, while the examiner appears to admit that Ginter does not

specifically disclose the performance of electronic commerce transactions over an unsecure network, and turns to Schneier for such a teaching, specifically citing pages 37, and 483-502, for performance of such transactions and for the teaching of a "Digital Signature Algorithm without encryption" (page 37), it is clear from even the title of Schneier ("Applied Cryptography") that Schneier is concerned with encryption.

But, even assuming, arguendo, that the cited portion of Schneier, at page 37, is suggesting that a digital signature can be employed over an unsecure network where there is no encryption employed, there would appear to be no reason for the artisan to combine any such teaching with Ginter since Ginter is not interested in performing transactions over a network unless there is encryption, i.e., Ginter is not interested in using unsecure networks.

Furthermore, the examiner's rationale for combining the various references is suspect. It is proposed to "add the modifications of Schneier to the method disclosed by Ginter because such modifications would have provided 'a separate algorithm for digital signatures that cannot be used for encryption'" (answer-page 6, without the underlining of the examiner). But, why provide this separate algorithm in Ginter?

Since Ginter is interested in only secure networks, why would the artisan believe it necessary to provide an algorithm for digital signatures that cannot be used for encryption in Gitner?

The examiner combines Pare with Ginter "because such modifications would have provided a system that would have provided '*financial services system that is highly resistant to fraudulent account accesses by unauthorized people*'" (answer-page 8). Other than hindsight, it is not clear what would have led the artisan to look to Pare for an index to financial resources accessible to the first party through the second party so as to add this feature to Ginter.

Further, while Rosen 518 may contain a disclosure of an "Issuer Certificate," it is not at all clear that such a certificate is equivalent to the claimed "commercial relationship certificate" that is digitally signed by a second party and includes a certified identifier. Moreover, it is this commercial relationship certificate which must include the "index to the financial resources accessible to the first party through the second party." Still further, as claimed, neither the commercial relationship certificate nor said index is encrypted or secret. The examiner has not made out a convincing case, in our view, as

to why the skilled artisan would have combined the applied references nor, if these references were combined, that it would result in a "commercial relationship certificate" that is digitally signed by a second party and includes a certified identifier as well as an "index to the financial resources accessible to the first party through the second party," and wherein neither the commercial relationship certificate nor said index is encrypted or secret.

With regard to claims 22-30, the examiner applied Ginter and Schneier as above, adding Matyas for letter of credit (LOC) modifications (because they would have been highly useful in defining a "process for authentication of messages from originator to recipient" (answer-pages 19-20)), and Rosen 407 for the opening bank being associated with the accessing of the financial resources of the buyer (because the modifications would have been highly useful in providing "some form of 'electronic money' that can be used in cashless payment transactions as alternatives to the traditional currency and check types of payment systems")(answer-page 21)). The examiner adds Tozzoli for a showing of elements to suggest "said seller sending the certificate to an advising bank, the advising bank being associated with a beneficiary of the electronic commerce

transaction...” (answer-page 21).

The examiner’s rationale for combining the references in rejecting claims 22-30 also appears to be based more on hindsight than on what the skilled artisan would have gleaned from these references. But, in any event, since the initial combination of Ginter and Schneier was flawed, for the reasons supra, and Matyas, Rosen 407 and Tozzoli do not provide for the deficiencies thereof, we also will not sustain the rejection of claims 22-30 under 35 U.S.C. § 103

The examiner’s entire rationale appears to us to be a patch quilt of bits and pieces of the applied references, and disparate recitations in those references. We remain unconvinced that an artisan, on his/her own, without the guidance of appellants’ disclosure, would have combined the applied references in a manner as to result in the instant claimed invention.

Accordingly, the examiner's decision rejecting claims 1, 13-17 and 19-30 under 35 U.S.C. § 103 is reversed.

REVERSED

JAMES D. THOMAS Administrative Patent Judge	)	
KENNETH W. HAIRSTON Administrative Patent Judge	)	BOARD OF PATENT APPEALS AND INTERFERENCES
ERROL A. KRASS Administrative Patent Judge	)	

EK/RWK

MICROSOFT CORPORATION
LAW OFFICES OF RONALD M. ANDERSON
600 108TH AVENUE N.W., SUITE 507
BELLEVUE, WA 98004