The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte KOICHI KAMIJO, NORISHIGE MORIMOTO, AKIO KOIDE
and TOHRU SAKAKURA

Appeal No. 2006-0655
Application 09/459,287

ON BRIEF

Before THOMAS, KRASS, and BLANKENSHIP, Administrative Patent Judges.

THOMAS, Administrative Patent Judge.

DECISION ON APPEAL

Appellants have appealed to the Board from the examiner's final rejection of claims 1 through 5, 8 and 10 through 22. Appellants have canceled claims 6, 7, 9 and 23 through 29, and the examiner has allowed claim 30.

Representative independent claim 1 is reproduced below:

1. A method for authenticating digital data in a system for writing digital data entered from an input device to a memory device and transferring the digital data written in the memory device to a receiving device, said method comprising the steps of:

performing a first device authentication between the input device and the memory device when writing digital data from the input device to the memory device; and

performing a second device authentication between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device.

The following references are relied on by the examiner:

Altschuler et al. (Altschuler)	5,465,300	Nov. 7, 1995
Traw et al. (Traw)	5,949,877	Sep. 7, 1999 (Filed Jan. 30, 1997)
Steinberg	6,510,520	Jan. 21, 2003 (Filed Jun. 26, 1998)
Schneier, Bruce, Applied Cryptography, Second Edition, 1996 John Wiley & Sons, p.455		

Claims 1 through 5, 8 and 10 through 22 stand rejected under 35 U.S.C. § 103. As to claims 1 through 3, 5, 8, 10 through 12, 14 through 19 and 21, the examiner relies upon Steinberg in view of Traw. To this first stated rejection the examiner adds Altschuler as to claim 4, and separately adds Schneier as to claims 13, 20 and 22 in a third stated rejection.

Rather than repeat the positions of the appellants and the examiner, reference is made to the brief (no reply brief has been filed) for appellants' positions, and to the answer for the examiner's positions.

OPINION

For the reasons set forth by the examiner in the answer as embellished upon here, we sustain the rejection of all claims on appeal under 35 U.S.C. § 103.

From our review of appellants' brief, it appears that appellants are arguing only in effect independent claim 1 as representative of the other independent claims 15 and 21 as well as the other claims set forth in the first stated rejection. Separate arguments are presented as to claim 4, which we treat separately below, and no arguments are presented to us as to the third stated rejection of claims 13, 20 and 22.

We turn first to the first stated rejection which encompass each of the independent claims 1, 15 and 21 on appeal with claim 1 as representative of each of them as being obvious over Steinberg in view of Traw. We sustain this rejection for the reasons set forth by the examiner as well as our consideration of Steinberg leads us to conclude that this reference alone would have rendered obvious to the artisan the subject matter of representative claim 1 on appeal.

Initially, we agree with the examiner's reasoning of combinability of the teachings Steinberg and Traw as set forth at pages 3 and 4 of the answer. To the extent Steinberg may be fairly characterized as the examiner does, as not disclosing a first and second device authentication between an input device and a memory device and separately between a memory device and a

receiving device, the examiner has properly relied upon the teachings of Traw relating to authentication between a content source and content sink in an authentication since, as argued, authentication in Traw is noted by the examiner as being independent of the digital data per se. The significant teaching value of Traw, as argued by the examiner at page 4 of the answer, is the motivation such as to prevent copying and/or misuse of the data during transfer, which feature is consistent with the disclosed and broadly claimed features of independent claim 1 on appeal.

Separately, appellants' commentary with respect to Traw at the bottom of page 5 of the brief appears to be an incomplete consideration of the teaching value of this reference. Moreover, the bulk of the arguments actually made against the first stated rejection occur in the paragraph at the middle of page 6 which merely focuses upon Traw as compared to disclosed capabilities. There are no comments here directed to the teaching value of Steinberg. In fact the appellants appear to argue only the disclosed invention which is unpersuasive as to not only combinability but also patentability of the subject matter broadly recited in independent claim 1 on appeal.

As to appellants' comments with respect to Steinberg, they are only made at the middle of page 5. Our review of this indicates as well significant incomplete consideration of the teaching value of Steinberg. Although we have indicated earlier

that we sustain the rejection set forth by the examiner, it appears that Steinberg does in fact teach a pure authentication approach as set forth per se in independent claim 1 on appeal. Among the various teachings in Steinberg, they include the ability to actually encrypt the image data, which appears alone to encompass the broadly defined authentication features of claim 1 on appeal, but as well a separate capability of creation of an authentication file. This is noted by the examiner in the first paragraph at the top of column 2; we note that it is also repeated at this column at lines 40 through 43. Figures 6 and 7 of Steinberg relate to secured data transfers through the creation of authentication data and/or file structures with respect to a storage device itself as well as the host computer. The discussion of Figures 6 and 7 at column 6, line 48 through at least column 7, line 2 appears to be consistent with appellants' disclosed approach for pure authentication without encrypting the image data per se, and its corresponding decryption as well.

Lastly, we turn to the separate rejection of dependent claim 4 which recites that the digital data of independent claim 1 is transferred as authenticated data if the first and second device authentications are successful, whereas this digital data is transferred as ordinary data if the first and second device authentications are not successful. In other words, if the first and second device authentications are not successful, the digital

data of claim 1, such as the disclosed image data, is transferred as ordinary or plaintext data.

As noted by the examiner at page 7 of the answer, the noted disclosed authentication flag which is respectively set or not set as to authenticated or unauthenticated ordinary data is not recited in the disclosed specifics in dependent claim 4. Many of the positions set forth by appellants at pages 7 and 8 go well beyond the actual language of dependent claim 4 to argue disclosed but unclaimed features.

Appellants' apparent most significant argument is at page 8 of the brief where it is urged that Altschuler always transitions from an insecure mode of communication to a secure mode of communication, so that at the end of the secure call setup procedure, the parties are communicating either securely or not at all. This may be one way of interpreting the teaching value of Altschuler, particular the showing in Figure 5 as argued by the examiner. On the other hand, and most significantly, the examiner has noted column 6, lines 20 through 27 in the statement of the rejection as well as the arguments of the examiner at page 8 of the answer. Although the showing in Figure 5 may be construed as appellants have argued, the noted discussion at column 6 clearly indicates that if a secure mode of communication is not perfected, the plaintext mode will be continued in operation, at least until a secure mode may be established.

Thus, the capability of Altschuler is consistent with the transmission of secure data to the extent that the secure mode is operable and the transfer of unsecured or claimed ordinary data if the secure mode is not successful.

In view of the foregoing, the decision of the examiner rejecting all claims on appeal, claims 1 through 5, 8 and 10 through 22, is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 CFR § 1.136(a)(1)(iv).

AFFIRMED

JAMES D. THOMAS Administrative Patent Judge	)	
ERROL A. KRASS Administrative Patent Judge	)	BOARD OF PATENT APPEALS AND INTERFERENCES
HOWARD B. BLANKENSHIP Administrative Patent Judge	)	

JDT:pgc

William A Kinnaman Jr.
Intellectual Property Law
2455 South Road P386
Poughkeepsie, NY 12601