THIS OPINION WAS NOT WRITTEN FOR PUBLICATION

The opinion in support of the decision being entered today (1) was not written for publication in a law journal and (2) is not binding precedent of the Board.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 ADDISON M. FISCHER

Appeal No. 1997-3178
Application 08/464,069[1]

HEARD: January 13, 2000

Before KRASS, BARRETT, and BARRY, Administrative Patent Judges.

BARRETT, Administrative Patent Judge.

[1] Application for patent filed June 6, 1995, entitled "Method For Preventing Inadvertent Betrayal By A Trustee Of Escrowed Digital Secrets," which is a continuation of Application 08/130,126, filed October 4, 1993, now U.S. Patent 5,436,972, issued July 25, 1995.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 from the final rejection of claims 25, 26, and 29-46.

We affirm-in-part.

BACKGROUND

The disclosed invention involves the problem of confirming the identity of a user who is seeking to recover secret information, such as a lost password, using a trustee. The trustee must have some way to positively identify the user so that the secret information will not be revealed to an imposter. A data structure holds both standard information identifying the legitimate user, encrypted private information which only the user knows and which is used by the trustee to verify identity, and encrypted secret information. The trustee decrypts the encrypted portions of the data structure, uses the standard and private information to verify the identity of the user, and transmits the decrypted secret information (such as a password) to the user.

Claim 25 is reproduced below.[2]

25. A computer having a legitimate user of the computer including a processor and a memory device coupled to said processor, a digital data structure corresponding to the legitimate user stored in said memory device including:

identifying information identifying the legitimate computer user, and

secret encrypted digital information other than said identifying information,

wherein the digital data structure is used by a trustee to confirm the identity of the legitimate computer user and to recover the secret encrypted digital information.

The Examiner relies on the following prior art:

Cole et al. (Cole) 5,091,939 February 25, 1992
Hardy et al. (Hardy) 5,222,135 June 22, 1993
Kaufman et al. (Kaufman) 5,418,854 May 23, 1995
(filed April 28, 1992)

Dziewit et al. (Dziewit) WO 92/09161 May 29, 1992
(International application published under the PCT)

---

[2] We question whether the phrase "to recover the secret <u>encrypted</u> digital information" is correct. This suggests that the trustee does nothing since the information is still encrypted. Perhaps it was intended that the trustee recovers "the secret digital information" as recited in claim 32.

Claims 25, 26, and 29-46 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Cole.

Claims 25, 26, 29, 30, 32, 33, 36, 37, 39, and 43-46 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Dziewit (WO 92/09161).

Claims 25, 26, 29, 30, 32, 33, 36, 39, and 43-46 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Kaufman.[3]

Claims 25, 26, 29-33, 35-39, and 43-46 stand rejected under 35 U.S.C. § 102(a) as being anticipated by Hardy.

We refer to the Final Rejection (Paper No. 7) (pages referred to as "FR__") and the Examiner's Answer (Paper No. 14) (pages referred to as "EA__") for a statement of the Examiner's position and to the Appeal Brief (Paper No. 13) (pages referred to as "Br__") and the Reply Brief (Paper No. 16) (pages referred to as "RBr__") for a statement of Appellant's arguments thereagainst.

OPINION

---

[3] Since claim 37 parallels rejected claim 30, it appears that the statement of the rejection should include claim 37. Appellant has assumed that claim 37 is included in the rejection.

Claim interpretation

We begin by interpreting the claims.

First, the claims all recite a "digital data structure" (emphasis added) which distinguishes over serial numbers, warranty information, and other information that may be printed on the computer or on paper in non-digital form and somehow associated with the computer. See RBr2.

Second, claim 25 recites that the digital data structure includes "identifying information identifying the legitimate computer user" and claim 32 recites "storing identifying information identifying the legitimate computer user in an original digital data structure." Neither claim requires that the identifying information is encrypted (for example, with the manufacturer's (trustee's) public key) as an encrypted escrow record. We interpret the "identifying information" to correspond to the standard identifying information in figure 2 which is optionally encrypted as shown at 84 in figure 4. This interpretation is consistent with claims 29 and 36, which enumerate the information shown in figure 2, and with claims 30, 31, 37, and 38 which correspond to the private identifying information and

instructions at 86 in figure 4. Thus, claims 25 and 32 indicate that the identifying information is not encrypted and do not define over the use of non-encrypted data as identifying information. Claims 25 and 32 do not cover the disclosed concept of using encrypted information to confirm the identity of the legitimate user, i.e., an imposter could substitute his own identifying information because it is not encrypted. Similarly, claims 30, 31, 37, and 38 do not require encrypting private information.

Third, claim 25 is directed to a digital data structure stored in a memory. Claim 25 includes a "wherein" clause which expresses that the digital data structure is used by a trustee to confirm the identity of the legitimate computer user and to recover the secret encrypted digital information. We agree with the Examiner's position (argued by Appellant at Br18-19) that the "wherein" clause is merely a statement of intended use of the data structure claim (although we do not find where this position is stated in the rejection), which limitation is met as long as the data structure is capable of such use. We are not persuaded by Appellant's argument (Br19) that the language in the

"wherein" clause is functional language which must be shown in a reference. Claim 25 is directed to the digital data structure, not a system which uses the digital data structure, and the "wherein" clause does not positively recite any structural limitation to the digital data structure. Method claim 32, by comparison, recites a method step using the digital data structure which is a limitation on the method.

Fourth, claims 25 and 32 recite "secret encrypted digital information other than said identifying information," which is not limited to the secret information being a password. The secret information could be anything. Appellant's arguments that references such as Dziewit and Kaufman do not recognize the lost password problem (e.g., Br12, Br18) are not commensurate in scope with the broad claim language.

Fifth, claim 25 recites "wherein the digital data structure is used by a trustee to confirm the identity of the legitimate computer user and to recover the secret encrypted digital information" and claim 32 recites "the trustee using said digital data structure to confirm the

identity of the legitimate computer user, and after positive confirmation of identity, recovering the secret digital information." Claim 25 recites recovering "secret encrypted digital information" instead of recovering "secret digital information" as recited in claim 32. In claims 25 and 32, the trustee uses the "digital data structure" to confirm the user identity, not just the "identifying information" portion of the "digital data structure"; thus, the trustee could use all or part of the digital data structure. Furthermore, claims 25 and 32 do not recite how the trustee recovers the secret (encrypted) digital information from the digital data structure; the secret digital information could be encrypted with a public key (as in Kaufman) and the trustee could just apply its private key (as in Kaufman) to decrypt and recover the information.

Anticipation

"Anticipation is established only when a single prior art reference discloses, expressly or under principles of inherence, each and every element of a claimed invention." RCA Corp. v. Applied Digital Data Systems, Inc., 730 F.2d. 1440, 1444, 221 USPO 385, 388 (Fed. Cir. 1984).

Cole

Cole stores encrypted primary and secondary passwords. The user enters his password, which is then encrypted and compared to the stored encrypted primary password. The computer boots if there is a match. If the user forgets his password, he may call the computer manufacturer to obtain a valid alternate (secondary) password (col. 5, lines 45-49). Alternatively, the secondary password may be generated from external information instead of being stored.

The Examiner states (FR2-3): "The means for storing identifying information identifying the computer user features of claim 25 reads on the storage of the primary password in Cole. The storing of the secret digital information in encrypted format features of claim 25 reads on the storage of the primary password in encrypted format of the last line of the abstract."

Appellant argues (Br7): "Cole's primary password (encrypted or otherwise) cannot be both the claimed identifying information and the secret digital information."

We agree with Appellant. Furthermore, we note that Cole does not store the password in decrypted form because

this would compromise security. Moreover, we do not see how a password can be considered information identifying a user.

Appellant argues (Br6-7): "Cole fails to disclose the claimed digital data structure corresponding to a legitimate user that stores 'identifying information identifying the legitimate computer user' as well as 'secret digital information in an encrypted form other than said identifying information.'"

The Examiner finds the digital data structure limitations in "Cole at col. 2, lines 8-11 and col. 6, lines 18 [sic, 1-8]" (EA5) and "with Cole an alternate password is provided" (EA5). Thus, the Examiner considers the secondary (alternate) password to correspond to the "secret encrypted digital information." Cole, column 2, lines 8-11, states: "Upon verification of the user's identity, the manufacturer or authorized agent supplies an alternate password to the user." Cole, column 6, lines 1-8, states: "Before issuing the alternate password, the computer manufacturer verifies the identity of the user, e.g. via warranty information or from a list of computer serial numbers and associated owners/users. In this

embodiment of the invention, when the caller has adequately identified himself, the computer manufacturer instructs the user to read the date displayed on the screen."

The stored encrypted secondary password in Cole corresponds to "secret encrypted digital information." We do not agree with Appellant's argument, with respect to similar language in claim 32, that "Cole fails to disclose storing 'secret encrypted digital information other than said identifying information in said digital data structure'" (Br8) because we rely on the embodiment where the secondary password is stored, not the embodiment referred to by Appellant where the secondary password is generated from data external to the computer such as the date. The issue is whether Cole discloses a digital data structure including "identifying information identifying the legitimate computer user."

The portions of Cole pointed out by the Examiner do not state that the identifying information was stored in digital form along with the encrypted secondary password in a data structure. The quote from column 2 does not state what information is used to confirm the identity of the user or

where the information is stored. The quote from column 6 indicates that external printed (i.e., non-digital) information is used by the manufacturer to confirm the identity of the user. Column 6 refers to an embodiment where a secondary password is generated, not stored, although the identification procedure could be the same. We agree with Appellant that the Examiner has not identified a digital data structure in Cole including "identifying information identifying the legitimate computer user" and we do not find any such teaching in Cole. The anticipation rejection of claims 25, 26, 29-31, and 39-42 over Cole is reversed.

The arguments with respect to method claim 32 are similar to claim 25. The rejection of claims 32-38, and 44-46 are reversed for the reasons stated in connection with claim 25.

Dziewit (WO 92/09161)

The Examiner states that the limitations of the digital data structure are found in "Dziewit at page 30, 'Third Party Trustee'" (EA5) and "with Dziewit secret encrypted information such as an encrypted contract is provided"

(EA5). The Examiner also relies on the last two lines on page 29 (FR3).

The cited portion of Dziewit on page 30 is concerned with using a third party trustee in the process of authenticating electronically-documented contract transactions. Page 29 of Dziewit discloses that transmissions may be encrypted.

Appellant's argument with respect to claim 25 that Dziewit fails to disclose use of information by a trustee to confirm the identity of the legitimate computer user and to recover the secret encrypted digital information is not persuasive. Claim 25 is directed to a digital data structure stored in a computer memory, not to a system having a trustee which uses the contents of the digital data structure. As discussed in the "Claim interpretation" section, the "wherein" clause is considered a statement of intended use.

Appellant argues (Br12): "The Examiner identifies no specific digital data structure in Dziewit that includes <u>both</u> types of claimed information. An encrypted, digitally signed copy of the electronic contract file stored on disk

is not the same thing as the claimed data structure in claim 25 which includes information identifying a legitimate computer user along with secret digital information in encrypted form other than that identifying information."

We do not understand what the Examiner considers to be the claimed digital data structure. It is true that Dziewit discloses transmitting a contract to the parties using encryption (page 29). The encryption provides security during transmission but is not intended to keep the contract secret from the parties at either end. Thus, the transmitted encrypted contract cannot be considered to be "secret encrypted digital information." However, assuming the encrypted contract is the "secret encrypted digital information," the Examiner does not explain what constitutes the "identifying information identifying the legitimate computer user." Because we find that Dziewit fails to disclose "identifying information identifying the legitimate computer user" and "secret encrypted digital information" in a "digital data structure," the anticipation rejection of claims 25, 26, 29, 30, 39, and 43 over Dziewit is reversed.

The arguments with respect to method claim 32 are similar to claim 25. In addition, claim 32 recites "the trustee using said digital data structure to confirm the identity of the legitimate computer user, and after positive confirmation of identity, recovering the secret digital information." We do not find these limitations in Dziewit even giving the limitations a very broad interpretation. The trustee in Dziewit is merely a third person used for security reasons and the Examiner does not explain how the trustee acts to confirm a legitimate computer user. The rejection of claims 32, 33, 36, 37, and 44-46 is reversed for the reasons stated in connection with claim 25 and because Dziewit does not teach the steps performed by the trustee.

Kaufman

The Examiner states that the limitations of the digital data structure are found in "Kaufman at col. 6, lines 41-49" (EA5) and "with Kaufman public key certificates and encrypted 'long term' credentials are provided" (EA5). Kaufman, column 6, lines 41-49 states:

> In an alternate embodiment of the authentication arrangement, the CSS 24 and the LA 26 may be combined into a single entity. Yet, in accordance with the exemplary embodiment of the invention described below, the CSS and LA are separate nodes. The CSS 24 is accessed at registration to store a user's long-term credential in a database directory and is thereafter accessed at login by the workstation 12 to retrieve that credential for authentication purposes, as described below.

This portion of Kaufman is not very helpful in explaining how the claim limitations are met and we do not understand why the Examiner relies on the embodiment where the CSS and the LA are combined. Nevertheless, we find that Kaufman anticipates claims 25, 29, and 32, and 36.

The CSS (certificate storage server) node 24 shown in figure 3 holds a "digital data structure" including the "username" N, which we find corresponds to the claimed "identifying information identifying the legitimate computer user" in claims 25 and 32. The data structure in CSS 24 also includes a doubly encrypted "credential" $\{\{U\}_{H1}, H2\}_{LA\text{-}PUB}$ which contains an encrypted private key U (col. 4, lines 26-32). For purposes of discussion, we take the encrypted quantity $\{U\}_{H1}$ to be the claimed "secret digital information." $\{U\}_{H1}$ is concatenated with hash total H2 and encrypted with the public key of the login agent (LA),

LA-PUB, to form $\{\{U\}_{H1}, H2\}_{LA\text{-}PUB}$, which corresponds to the claimed "secret encrypted digital information other than said identifying information" stored in the "digital data structure." The CSS 24 is "coupled to said processor" of the legitimate user, i.e., to workstation 12. Although the "wherein" clause of claim 25 is a mere statement of intended use, the LA node 26 acts as a "trustee" and "the digital data structure is used by a trustee to confirm the identity of the legitimate computer user and to recover the secret encrypted digital information." That is, LA 26 recovers the secret digital information $\{U\}_{H1}$ by decrypting using the private key LA-PRIV as shown in figure 5 and stripping H2. The user identity is confirmed for a given user name N if the hash total H2 from the decrypted credential $\{U\}_{H1}$, H2 associated with the name N matches the hash total $H2_A$ received from the workstation (col. 8, lines 11-24). Remember that claim 25 states that the digital data structure is used to confirm the identity, not just the identifying information portion of the data structure. Claim 25 is open ended does not exclude the numerous additional and complicated steps in Kaufman. Neither

claim 25 nor claim 32 recites doing anything with the recovered secret digital information, such as actually sending it to the user; however, the LA in Kaufman encrypts $\{U\}_{H1}$ with key K and send it to the user who can recover U. The method of claim 32 is anticipated for the same reasons as claim 25. The "name" N in Kaufman is one of the enumerated pieces of identifying information recited in claims 29 and 36. The anticipation rejection of claims 25, 29, 32, and 36 over Kaufman is sustained.

Appellant argues (Br18): "In general, there is no recognition in Kaufman that a legitimate user may have forgotten his password. Nor is there any provision in Kaufman to permit a legitimate user to obtain that password from a trustee." However, claims 25 and 32 are not limited to the lost password problem. The "secret digital information" can be the encrypted quantity $\{U\}_{H1}$, the encrypted private key U, in Kaufman. The "secret encrypted digital information" is $\{\{U\}_{H1}, H2\}_{LA\text{-}PUB}$. Thus, the argument is not persuasive.

Appellant argues (Br18): "Kaufman fails to disclose a trustee. Nor does Kaufman disclose a trustee that uses the

information stored in the claimed digital data structure to both 'confirm the identity of the legitimate computer user and to recover the secret digital information.' The log-in agent is not a 'trustee.'" Appellant argues that the login agent (LA) is not trusted with the user's private key and, as a result, the LA cannot impersonate a legitimate user.

Appellant evidently reads a lot into the term "trustee," but does not state exactly what. Since the LA is disclosed to be "semi-trusted" (col. 4, line 11), we find this to meet the "trustee" limitation absent any qualifications on the term in the claim. There can be many levels of "trustee." Claims 25 and 32 do not require the "secret digital information" to be understandable by the trustee. The argument is not persuasive.

With respect to claims 26 and 33, the Examiner states "that the LA identifier includes the public key LA-PUB" (EA7). The LA is not information identifying the trustee stored in the digital data structure in figure 4 of Kaufman. The anticipation rejection of claims 26 and 33, and dependent claims 43 and 44, over Kaufman is reversed.

With respect to claims 30 and 37, the Examiner refers to column 8, lines 8-24. We do not find anything in the cited portion of Kaufman, or in the rest of Kaufman, that constitutes instructions originated by the legitimate computer user to be followed by the trustee in the event an applicant seeks to gain access to secret information in the digital data structure in figure 4 of Kaufman. The anticipation rejection of claims 30 and 37 over Kaufman is reversed.

With respect to claim 39, the Examiner refers to the user's private key at column 8, line 28 (EA7). However, we do not find any question authored by the legitimate computer user to be posed by the trustee attempting to recover a password or encryption key in the digital data structure in figure 4 of Kaufman and the Examiner does not point to anything that would meet this limitation. The anticipation rejection of claim 39 over Kaufman is reversed.

With respect to claim 45, the Examiner points to column 8, lines 20-25 (EA8). We do not find the steps of obtaining and comparing credentials, as claimed, at that location or elsewhere in Kaufman. The anticipation

rejection of claim 45 and dependent claim 46 over Kaufman is reversed.

Hardy

The Examiner states that the limitations of the digital data structure are found in "Hardy at col. 2, lines 34-44" (EA5) and "with Hardy coded release data is provided" (EA5).

Appellant argues that Hardy does not disclose storing information identifying the legitimate computer user (Br21): "Hardy's display screen 30 does not include information that identifies the legitimate computer user. Rather, the displayed information relates to the computer itself, i.e., the computer's serial number, and a random code that does not depend 'on any other parameter which can be controlled by the user.' Column 5, lines 3-4."

We do not find where the Examiner addresses this argument. The random code 32 and the serial number 33 of the workstation involved which are communicated to the authorized service S do not identify the user. Accordingly, the anticipation rejection of claims 25, 26, 29-33, 35-39, and 43-46 over Hardy is reversed.

CONCLUSION

The rejection of claims 25, 26, and 29-46 over Cole is reversed.

The rejection of claims 25, 26, 29, 30, 32, 33, 36, 37, 39, and 43-46 over Dziewit is reversed.

The rejection of claims 25, 29, 32, and 36 over Kaufman is sustained. The rejection of claims 26, 30, 33, 37, 39, and 43-46 over Kaufman is reversed.

The rejection of claims 25, 26, 29-33, 35-39, and 43-46 over Hardy is reversed.

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

AFFIRMED-IN-PART

ERROL A. KRASS Administrative Patent Judge	)	
LEE E. BARRETT Administrative Patent Judge	)	BOARD OF PATENT APPEALS AND INTERFERENCES
LANCE LEONARD BARRY Administrative Patent Judge	)	

NIXON & VANDERHYE
Mark E. Nussbaum
1100 North Glebe Road
Arlington, VA 22201-4714