UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Ex parte DARRELL KRULCE

Appeal 2007-003513
Application 10/137,042
Technology Center 2400

Decided: 1 July 8, 2009


THOMAS, Administrative Patent Judge.

1 The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the Decided Date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).
STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner’s final rejection of claims 1 through 17. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Invention

The present invention is directed to a method and apparatus for providing password security to an electronic device. In one embodiment, password security is provided by an apparatus, the apparatus comprising an input device for allowing entry of an encrypted password, a memory for storing a decryption function and a decoding function, and a processor. The processor receives the encrypted password from a user wanting access to the electronic device and applies the decryption function to the encrypted password to produce a decrypted password. The processor then applies the decoding function to the decrypted password to determine access rights to the electronic device. (Spec. 2, [0008].)

Representative Claim

1. An electronic device having password security to the electronic device, comprising:
   an input device being operable to input entry of a variable length encrypted password into the electronic device;
   a memory for storing a decryption function and a decoding function, the variable length encrypted password being a function of the decoding function and access rights granted to a user of the electronic device; and

2 The above-noted panel only recently received this appeal for decision.
a processor for receiving the encrypted password, for applying the decryption function to the encrypted password to produce a decrypted password, and for applying said decoding function to said decrypted password to determine the access rights to the electronic device.

**Prior Art and Examiner’s Rejections**

The Examiner relies on the following references as evidence of unpatentability:

<table>
<thead>
<tr>
<th>Reference</th>
<th>Patent No.</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gullman</td>
<td>US 5,280,527</td>
<td>Jan. 18, 1994</td>
</tr>
<tr>
<td>Ulch</td>
<td>US 4,216,375</td>
<td>Aug. 5, 1980</td>
</tr>
</tbody>
</table>

Independent claims 1, 9, and 10 stand rejected under the written description portion of the first paragraph of 35 U.S.C. § 112. All claims on appeal claims, 1 through 17, stand rejected under the second paragraph of the 35 U.S.C. § 112, as being indefinite. Similarly, all claims on appeal stand rejected under 35 U.S.C. § 103. In a first stated rejection of claims 1, 8 through 10, and 17, the Examiner relies upon Gullman alone. In a second stated rejection of claims 2 through 4, and 11 through 13, the Examiner relies upon Gullman in view of Garg. Lastly, in a third stated rejection involving claims 5 through 7, and 14 through 16, the Examiner relies upon Gullman in view of Ulch.

**Claim Groupings**

Within the rejections under 35 U.S.C. § 103 and based upon the Appellant’s arguments in the Appeal Brief (no Reply Brief has been filed), we will decide the appeal based on independent claim 1 as representative of all claims on appeal.
ISSUE

For purposes of both rejections under 35 U.S.C. § 112 and all rejections under 35 U.S.C. § 103, has Appellant shown that the Examiner erred in finding that the feature of representative independent claim 1 on appeal of an “encrypted password being a function of the decoding function and access rights granted to a user” lacks written description support, renders all claims indefinite, and is taught by Gullman?

FINDINGS OF FACT (“FF”)

1. The heading “invention” in this opinion reflects the disclosed invention as does the Examiner’s statement at page 3 of the Answer: “[T]he encrypted password as described in the specification is a result of the access rights being transformed by the encoding function then further encrypted.” Page 7 of the Brief indicates that this is a correct statement of the disclosed invention while recognizing that the relationship may not be explicitly stated in the Specification.

2. With respect to the background discussion at column 1 of Gullman, it was known in the art that personal identification numbers (PINs) were known to control or permit access rights to banking environments. Additionally, Gullman states:

   Common security mechanisms include use of a personal identification number (PIN) and use of a security token. A PIN is used to identify an individual and authorize access to a host system (e.g., banking transaction system). A security token is a non-predictable code derived from a private key, e.g. a unique fixed value, and a public key, e.g. a time varying value. For example, a password (fixed key) is encoded based upon time- variant information. Such token then is forwarded to the host which decodes the token back to a password. (Col. 1, ll. 28-37.)
Upon entry of the cardholder’s biometric information, the processor executes the verification algorithm. The verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number) and time-varying self-generated information to derive a token output. (Col. 2, ll. 53-59.)

According to the invention, the biometric security mechanism 14 generates a security token which the user inputs to the access device 12[.] Such security token is formed from biometric information, a fixed code and, in one embodiment, a time-varying code or, in a second embodiment, a host-generated challenge code. (Col. 3, ll. 36-42.)

To properly decode the token, the security apparatus 14 is synchronized with the host system 10 so that the time varying code is identical at both the security mechanism 14 and the host system 10. In the challenging code embodiment, the host system, having generated the challenge code, retains the challenge code in memory to decode the token. The host 10 identifies the user with the fixed code and verifies the identification based on the correlation factor. The host system 10 permits full or limited entry based upon the level of authorization assigned to a given user (as identified by the fixed code). For example, a given user may be allowed to perform an electronic funds transfer only from a prescribed account. (Col. 4, ll. 23-36.)

Each security apparatus includes a unique embedded code (e.g., fixed code) as previously described. The correlation factor, fixed code and a time-varying code from the time code generator 26 together are used to derive a security token. The derived token is then displayed. The user then reads the token from the display 20 and enters the token at the access device 12. The access device 12 transmits the token to the host 10 which decrypts or decodes the token to derive the fixed code and correlation factor. If the fixed code identifies a valid user and the correlation factor is above the threshold level, then access is permitted. If not, then access is denied. With a fixed code to
identify a particular person or group of persons, the host can be programmed to control the type of access or transactions allowed for such fixed code. (Col. 6, ll. 30-45.)

PRINCIPLES OF LAW
WRITTEN DESCRIPTION

The manner in which the specification as filed meets the written description requirement is not material. The requirement may be met by either an express or an implicit disclosure. In re Wertheim, 541 F.2d 257, 262 (CCPA 1976). It is permissible to add inherent properties or characteristics of the invention to the disclosure and claims. Kennecott Corp. v. Kyocera Int’l, Inc., 835 F.2d 1419, 1422 (Fed. Cir. 1987), cert. denied, 486 U.S. 1008 (1988). An invention claimed need not be described in ipsis verbis in order to satisfy the written description requirement of 35 U.S.C. § 112, first paragraph. In re Lukach, 442 F.2d 967, 969 (CCPA 1971). The question is not whether an added word was the word used in the specification as filed, but whether there is support in a specification for the employment of the word in the claims, that is, whether the concept is present in the original disclosure. See In re Anderson, 471 F.2d 1237, 1244 (CCPA 1973).

ANALYSIS

Independent claims 1, 9, and 10 on appeal were amended by the amendment submitted on February 3, 2006 to include the feature of “encrypted password being the function of decoding function and access
rights granted to a user.” We agree with the basic views set forth by the Examiner that the written description as filed does not support Appellant’s possession of the presently claimed invention as to this quoted feature. Of particular note is that the claimed invention in each independent claim starts with an encrypted password. There is no positive statement of encryption being performed in the claim. An encrypted password is first decrypted, and then decoded to yield access rights to the associated device. Conversely, what is not claimed and what is not clearly disclosed or depicted in any figure within the written description of this disclosed invention, are features that the artisan would clearly understand must necessarily occur. These include the initial *encoding* in some manner of access rights that subsequently yield a password, which is then in turn encrypted, and is then recited in the claims as an already encrypted password.

Appellant asserts at the bottom of the page 5 of the Brief that his sketch appearing at page 6 of the Brief was culled from the disclosed invention. That the arrows indicate a certain measure of bi-directionality is not consistent with the disclosed invention. Even as depicted in the sketch, the access rights are first encoded to yield the password, which is then encrypted to yield an encrypted password, which is subsequently assigned to or used by a user and decrypted by the claimed process into a password that has been decrypted and labeled as such, which in turn is decoded to yield the access rights to the given device. Rather than the claimed encrypted password being a function of the decoding function, the encrypted password is disclosed to be a function of the encoded password. This is the crux of the Examiner’s issue with respect to the written description rejection and is
consistent with the Examiner’s observation we quoted in FF 1, to which Appellant agrees at page 7 of the Brief as noted in this FF as well.

Appellant’s reference to Paragraph [00018] at the bottom of page 6 does not persuade us otherwise. The fact that in another environment “the decrypting function and the decoding function are integrated into a single function” is not what is claimed before us, since the memory of representative independent claim 1 on appeal is required to store a decryption function and a decoding function rather than a single function having two functionalities. In any event, the basic thrust of Appellant’s disclosed invention does not appear, from an artisan’s perspective, to yield an encrypted password that is capable of being a function of a decoding function.

Therefore, the Examiner’s rejection of independent claims 1, 9 and 10 under the written description portion of 35 U.S.C. § 112, first paragraph, is affirmed.


The Examiner rejects claims 1 through 17, all claims on appeal under this statutory provision. This rejection appears at pages 3 and 4 of the final rejection. Appellant’s Brief does not present any arguments with respect to this rejection, and since no Reply Brief has been filed contesting otherwise, we summarily sustain the rejection.


Appellant’s remarks at pages 8 and 9 of the Brief do not contest the Examiner’s correlation for representative independent claim 1 of the security
token in Gullman as being the claimed encrypted password. Nor does the Appellant contest the Examiner’s rationale of a variable length feature of the password being an obvious variation of teachings of Gullman as set forth at page 5 of the Answer, for example. In fact, numerous portions of Gullman, which were isolated and reproduced in FF 2, clearly justify the artisan’s understanding that the various codes, including the so-called “fixed code,” may be variable length based codes according to Gullman.

Page 11 of the Answer properly contests Appellant’s assertions at the bottom of page 8 of the Brief that access rights cannot be derived from the security token of Gullman. Appellant appears to contradict himself here where it is indicated additionally that Gullman’s security token is derived from sources, such as biometric data, a fixed code and a challenge code. Nevertheless, it is asserted that the token is not a function of access rights but that “access rights are merely assigned to a particular user as identified by the fixed code.” The argument does not follow from what Appellant has already described as the basis for the derivation or generation of the security token in Gullman. We have provided in FF 2 numerous instances in Gullman in which access rights have been effectively encoded and/or encrypted according to the Examiner’s reasoning.

Appellant’s additional remarks at page 9 of the Brief relating to the disclosed invention are not reflective of any claimed feature. As such, the disclosed invention cannot properly be used to distinguish the presently claimed invention over the teachings and suggestions of Gullman, as relied upon by Examiner within 35 U.S.C. § 103.

Lastly, Appellant makes brief mention of the disputed feature of each of independent claims 1, 9, and 10 at the middle of the page 9 of the Brief.
Appeal 2007-003513  
Application 10/137,042

Appellant does not challenge the Examiner’s correlation of the disputed feature to the disclosed features noted at page 4 of the Answer that include column 4, lines 26 through 29 and column 5, lines 15 through 27 of Gullman.

It is noted that independent claim 10 is the only claim on appeal that recites features utilizing 35 U.S.C. § 112, 6th paragraph. Appellant has not contested the Examiner’s implied correlation of the features of Gullman to the claimed “means” based upon the analysis made with respect to independent claim 1 as a model for corresponding features recited in the other independent claims on appeal. Additionally, Appellant has not provided any indication from the disclosed invention what corresponds to the claimed means.

With respect to the second and third stated rejections under 35 U.S.C. § 103 further relying upon Garg and Ulch respectively, Appellant has not argued that the references are not properly, respectively combinable within 35 U.S.C. § 103. Therefore, no governing case law is cited in this Opinion to that effect.

What is argued for these rejections is the same feature as argued with respect to first stated rejection in representative independent claim 1 on appeal, namely, the functional recitation of the encrypted password being a function of the decoding function. In apparently criticizing the Examiner’s correlation of features of dependent claims 11 through 13 as corresponding to features recited in claims 2 through 4, Appellant has not contested the Examiner’s correlation for the features of dependent claims 2 through 4 to the combination of Gullman and Garg. Correspondingly, Appellant’s complaint with respect to the features of dependent claims 14 through 16
and the Examiner’s reliance upon the correspondingly recited features in dependent claims 5 through 7 are equally unpersuasive, since Appellant has not directly challenged the Examiner’s correlation of claims 5 through 7 to the combination of Gullman and Ulch.

CONCLUSIONS AND DECISION

We have affirmed Examiner’s rejection of independent claims 1, 9, and 10 under the written description portion of the first paragraph of 35 U.S.C. § 112. Likewise, we have affirmed the Examiner’s rejection of all claims on appeal, claims 1 through 17, as being indefinite under the second paragraph of 35 U.S.C. § 112. Lastly, we have sustained the Examiner’s three separately stated rejections, encompassing all claims on appeal, under 35 U.S.C. § 103. All claims on appeal claims, 1 through 17, are unpatentable.

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

AFFIRMED