UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 12/597,877 | 11/18/2009 | Aline Gouget | 1032326-000501 | 3449 |

21839 7590 06/14/2016
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

| EXAMINER |  |
|---|---|
| KIM, STEVEN S |  |

| ART UNIT | PAPER NUMBER |
|---|---|
| 3685 |  |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 06/14/2016 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPDOC1@BIPC.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

*Ex parte* ALINE GOUGET and PASCAL PAILLIER

Appeal 2013-010435
Application 12/597,877[1]
Technology Center 3600

Before HUBERT C. LORIN, CYNTHIA L. MURPHY, and
SHEILA F. McSHANE, *Administrative Patent Judges*.

McSHANE, *Administrative Patent Judge*.

## DECISION ON APPEAL

The Appellants seek our review under 35 U.S.C. § 134(a) of the Examiner's decision to reject claims 2–9. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

[1] According to the Appellants, the real party in interest is Gemalto SA. Appeal Brief filed April 1, 2013, hereafter "App. Br.," 2.

## BACKGROUND

The invention relates to a divisible electronic cash scheme where a user can withdraw a divisible coin of a monetary value that can be spent anonymously. Abstract, Specification, hereafter "Spec.," 3:22–24, 3:29–32. Anonymity can be revoked, however, if there appears to be cheating occurring such as by double spending of electronic cash. Abstract, Spec. 1:15–17, 3:26–28.

Representative claim 9 is reproduced from page 3 of the Claims Appendix of the Appeal Brief (Claims App'x) as follows, with emphasis added to relevant claim limitations:

> 9. Transaction method of transmitting anonymous electronic cash between a first entity (U) identified by a public key ($pk_u$) and a second entity (M) for providing anonymity revocation comprising:
>
> storing a divisible coin of value $n^L$ in an electronic device;
>
> assigning the divisible coin of value $n^L$ to a tree of L+2 levels, each node having exactly n direct descendants except the $n^{L+1}$ leaves (at level L+2), such that the value of the tree root at level 1 is $n^L$, the nodes of levels between level 2 and level L+1 each have a value corresponding to 1/n of the value of their parent node, and the nodes of level L+2 have no value;
>
> constructing a root key (K1) associated with the root node of the tree by using a secret (s) known by said first entity (U);
>
> computing respective node keys (LKey, RKey) for the n direct descendant nodes of a parent node, by using a verifiable one-way function (F), wherein said computed keys (LKey, RKey) for said n direct descendant nodes are unlinkable between them without the knowledge of the parent node key;
>
> *generating a ciphertext (T) in the electronic device by encrypting the public key (pku) associated with the first entity (U) with the key of a selected node of a fraction of the divisible coin of electronic cash to be transmitted to said second entity*

> *(M) by using a verifiable randomized encryption scheme (E);* and
>
> transmitting, from the electronic device to said second entity (M), a fraction of the divisible coin of electronic cash with said ciphertext (T), the keys of the direct descendants of the selected node and a proof (ϕ) of validity of a correct computing of said ciphertext (T) and said keys of said direct descendants.

In a Final Rejection, the Examiner rejects claims 2–6 and 9 as directed to non-statutory subject matter under 35 U.S.C. § 101. The Examiner rejects claims 2–9 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.[2] The Examiner rejects claims 2– 9 under 35 U.S.C. § 112, second paragraph, as indefinite. The Examiner also rejects claims 2–9 under 35 U.S.C. § 103(a) as obvious over Jacobsson[3], Nakanishi[4], and Gentry[5]. Final Action, hereafter "Final Act.," 3–12, mailed October 1, 2012; *see also*, Answer, hereafter "Ans." 3–8, mailed June 19, 2013.

## DISCUSSION

We will address the Appellants' arguments related to the respective rejections in turn.

*35 U.S.C. § 101*

The Examiner finds that claims 2–6 and 9 are patent ineligible as directed to non-statutory subject matter. Final Act. 3. The Examiner finds that because the claims recite an abstract idea with insufficient recitation of a

[2] The current application was filed prior to the effective date of the AIA (America Invents Act), and therefore the pre-AIA statute is applicable.
[3] US Patent 6,157,920, issued December 5, 2000.
[4] Toru Nakanishi, *et. al.*, "Unlinkable Divisible Electronic Cash," ISW 2000, LNCS 1975, 121–134 (2000).
[5] US Patent 7,337,322 B2, issued February 26, 2008.

machine performing the steps, they are directed to non-statutory subject matter. *Id.* at 3–5 (citing *Bilski v. Kappos*, 130 S. Ct. 3218 (2010)). More specifically, under the machine-or-transformation test, the Examiner finds that "the step of assigning, constructing, computing, generating [of claim 9] do not require the use of a machine performing the steps. Rather, the method step could be performed by a person with human mind." *Id.* at 4. The Examiner further finds that "the claim steps of storing ... in an electronic device and transmitting, from the electronic device, the steps are insignificant activities as they represent data gathering or outputting." *Id.* The Examiner states that "[t]he claims seem to be a mere statement of a general concept of key construction and encryption technique." *Id.* at 5.

The Appellants argue that the § 101 rejection is improper because "at least three steps of the method are explicitly tied to an element of structure [an electronic device] [] used to perform the method," that is, the electronic device is used in the "storing," "generating," and "transmitting" steps. App. Br. 7. The Appellants allege that the penultimate step, that requires that a ciphertext is generated by an electronic device using a key associated with specific nodes, is "not merely data gathering or outputting," and because this step is carried out in the electronic device, and transmitted from that device, the method is tied to a particular machine. *Id.* at 7–8. The Appellants also argue that given that the claim recites that steps are carried out in the electronic device, and the result is transmitted from the electronic device in the course of a transaction, it cannot be "performed solely by a human mind, nor is it a statement of a general concept of key construction and encryption." *Id.* at 8. The Appellants contend that "[c]laim 9 as a whole is directed to a transaction method for transmitting electronic cash between a first entity and a second entity." *Id*. at 7.

At the time the Final Office Action was issued in this case, the applicable law stated "that the machine-or-transformation test is a useful and important clue, an investigative tool, for determining whether some claimed inventions are processes under § 101. The machine-or-transformation test is not the sole test for deciding whether an invention is a patent-eligible 'process.'" *Bilski v. Kappos*, 130 S. Ct. 3218, 3227 (2010).[6]

Because the machine-or-transformation test was used as the sole test for deciding whether the invention is directed to patent-eligible subject matter and we find that there is reversible error in the Examiner's related findings, we reverse the rejection of claims 2–6 and 9 under 35 U.S.C. § 101. In concluding the claims are patent-ineligible, the Examiner applies the machine-or-transformation test established under *Bilski*, however, the claims as a whole are directed to the transmission of electronic cash, and as the Appellants point out, several of the steps of the claim require that an electronic device be used. We determine that the Examiner has not demonstrated that the steps that use the electronic device are insignificant in nature, especially as to the generation of a ciphertext in the electronic

[6] After the mailing of the Examiner's Answer, the Supreme Court issued its decision in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l,* 134 S.Ct. 2347 (2014), which explains the law as it relates to patent-eligible subject matter. In *Alice*, the Supreme Court discussed its decision in *Bilski*, and used some of its rationale in the analysis determining whether the claims at issue were directed to an abstract ideas. *Id*. at 2356. Consistent with *Alice* or *Bilski*, claims directed to physical entities performing tangible functions are distinguishable from the patent-ineligible subject matter, such as laws of nature, natural phenomena, and abstract ideas.

device. Moreover, the claim itself is directed to the transmission of electronic cash and, therefore, we fail to see how an electronic device would not be integral to the claims. As such, we determine that the Examiner's findings that the claims do not require the use of a machine constitute reversible error.

Therefore, we cannot sustain the rejection of claims 2–6 and 9 under 35 U.S.C. § 101 as reciting nonstatutory subject matter.

*35 U.S.C. § 112, first paragraph*

The Examiner rejects claims 2–9 under 35 U.S.C. § 112, first paragraph, for failure to comply with the written description requirement. Final Act. 6–7. The Examiner finds that as to claims 7 and 8, the disclosure of "a smart card or a dongle," in the Specification does not reasonably convey to one of ordinary skill in the art the possession of the recited "electronic device" and "processor." *Id.* at 6; Ans. 4, 5. More specifically, the Examiner finds a discrepancy between an electronic device with a memory, when the electronic device is one of the components in the smart card. Ans. 5. The same rationale is applied to the rejection of claim 9. *Id.*

The Appellants contend that the Specification discloses the use of a "portable device," as well as that of an "electronic device," where a smart card can be the portable device, or in a disclosed embodiment, it could be an electronic device. App. Br. 8–9; Reply Br. 3–4 (citing Spec. 4:28–29). The Appellants also argue that the Specification reasonably conveys possession of the invention, and also that one of ordinary skill in the art would have known that smart cards contain a memory and microprocessor. App. Br. 8.

Claims that introduce elements or limitations which are not supported by the as-filed disclosure violate the written description requirement. *See,* *e.g.*, *Ariad Pharm., Inc. v. Eli Lilly & Co.*, 598 F. 3d 1336, 135–1354 (Fed. Cir. 2010) (en banc). The fundamental factual inquiry is whether the specification describes "an invention understandable to that skilled artisan" and shows "that the inventor actually invented the invention claimed." *Id.* at 1351. The Examiner has the burden of establishing a prima facie case that the appealed claims do not comply with 35 U.S.C. § 112, first paragraph, the written description requirement, by setting forth evidence or reasons why, as a matter of fact, the written description in Appellants' disclosure would not reasonably convey to persons skilled in the art that Appellants were in possession of the invention defined by the claims, including all of the limitations thereof, at the time the application was filed. *See, e.g.*, *In re Alton*, 76 F.3d 1168, 1172, 1175–76, (Fed. Cir. 1996), *citing In re Wertheim*, 541 F.2d 257, 262–64 (CCPA 1976).

Here, we are persuaded that the Specification sufficiently discloses possession of the invention, and more specifically, its use of "electronic devices" and "processors." *See* Spec. 4:28–29; 4:33–34. The Examiner makes some additional findings but they are related to the issue of indefiniteness, not written description.

Therefore, we cannot sustain the rejection of claims 2–9 under § 112, first paragraph.

*35 U.S.C. § 112, second paragraph*

The Examiner rejects claims 2–9 under § 112, second paragraph, finding that for the element of claims 7 and 9, reciting "by encrypting the public key (pku) associated with the first entity (U) with the key of a selected node of a fraction of the divisible coin of electronic cash . . . ," the claims are unclear because there are numerous keys identified in it. Final

Act. 8. As to "selected node," the Examiner finds that there is no function or step in the claims that relates to the identification of the selected node. *Id.* Additionally, the Examiner finds that the term "said object" of claim 8 lacks antecedent basis. *Id.*

The Appellants argue that because different keys are recited, this does not mean that the claim is unclear because the individual keys are distinguished from each other within the claims. App. Br. 10. The Appellants contend that the "public key" that is "associated with the first entity," and "the key of a selected node" are distinguishable. *Id.* at 10–11. As to the issue of the "selected node," the Appellants argue that the claim indicates that the node is associated with the "fraction of the divisible coin" to be transmitted to the "second entity," and its meaning is clear. *Id.* at 11. As to the lack of antecedent basis of "said object" in claim 8, the Appellants argue that claim 7 recites a "portable object," and claim 8's recitation of "said object" refers to the "portable object of claim 8." *Id.*

We agree with the Appellants that the indefiniteness rejection cannot be sustained. The test for definiteness under 35 U.S.C. § 112, second paragraph, is whether "those skilled in the art would understand what is claimed when the claim is read in light of the specification." *Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1576 (Fed. Cir. 1986) (citations omitted). As to the issue of the differentiation of the various keys used in the claims, we agree with the Appellants that when the use of different keys is recited in the claims, there is sufficient context therein such that the different keys can be discerned. As to the "selected node" issue, we have a similar view. On the issue of the antecedent basis of the "said object" of claim 8, it refers to the "portable object" of claim 7 when the claims are read in context. We therefore reverse the 35 U.S.C. § 112, second paragraph rejection of claims 2–9.

*35 U.S.C. § 103*

The Examiner finds that Jacobsson teaches an electronic device having a memory for storing digital cash, e.g., divisible electronic cash, with a processor to generate digital cash such as a smart card, and Nakanishi discloses a divisible electronic cash system that generates a tree and provides for unlinkability and transmits payment to a second entity. Final Act. 9–10. The Examiner finds that these references do not disclose "constructing a root key with a secret(s), e.g. public key, computing each of the node keys by using a verifiable on[e-]way function, and generating a ciphertext by encrypting the public key with a node key using a verifiable randomized encryption scheme" of claims 7 and 9. *Id.* at 10. The Examiner relies upon Gentry for that teaching, finding that it discloses constructing a root key (K1) by using a secret known by a first entity (U), computing for each direct descendant node of a parent node a key (Lkey, Rkey), and generating a private key for any of its children by using a verifiable one-way function (F). *Id.* at 10–11; Ans. 7 (citing Gentry 3:9–16, 3:22–23, 4:22–26, 5:5–6, 5:24–35, 5:46–50, 6:1–5, 6:43–53, 10:8–30, 11:25–29, 11:45–12:12, 19:32–39). The Examiner finds that the use of a key associated with a tree node fails to distinguish over the prior art because it "represents a divisible value of an electronic coin, [][that is] non-functional descriptive material, e.g. stored data." Ans. 8.

The Appellants argue that the prior art references the Examiner relies upon do not teach generating a ciphertext by encrypting a public key with a node key as required in claims 7 and 9. App. Br. 12–14. More specifically, the Appellants allege that "[w]hile the Gentry patent discloses the generation of a hierarchical set of keys, it does not disclose any relationship between those keys and the nodes of a tree that represent divisible values of an electronic coin." *Id.* at 13. The Appellants also allege that Gentry fails to disclose "a verifiable one-way function" as recited in claims 7 and 9. *Id.* It is argued that Gentry discloses a verification of a sender's signature by a recipient, but that does not relate to whether a key has been "properly generated." *Id.*

After considering each of the Appellants' contentions and the evidence presented in this Appeal, we are persuaded that the Appellants identify reversible error in the obviousness rejections, and we reverse them for failing to identify prior art that teaches the claim limitations of independent claims 7 and 9 related to generating a ciphertext by encrypting a public key with a node key and a verifiable one-way function used in computing node keys. We add the following primarily for emphasis.

We cannot agree with the Examiner that the use of a key associated with a tree node represents non-functional descriptive material and therefore fails to distinguish over the prior art. Claims 7 and 9 explicitly require that ciphertext be generated in the claimed manner, and the "key of the selected node" is not a divisible value of an electronic coin as the Examiner states, but rather is a "respective node key" that is constructed as the claim requires using a verifiable one-way function.

The "verifiable one-way function" of the computation of the node keys is also not taught by Gentry. We agree with the Appellants that the "verifiable one-way function" is used to compute the respective node keys in a certain manner, and Gentry's disclosure of the verification of a sender's signature by a recipient is not equivalent to verification of whether a key has been generated as the claims require.

We therefore cannot sustain the Examiner's obviousness rejection of independent claims 7 and 9, and claims 2–6 and 8 that depend from them.

## SUMMARY

The rejection of claims 2–6 and 9 under 35 U.S.C. § 101 is reversed.

The rejection of claims 2–9 under 35 U.S.C. § 112, first paragraph, is reversed.

The rejection of claims 2–9 under 35 U.S.C. § 112, second paragraph, is reversed.

The rejection of claims 2–9 under 35 U.S.C. § 103(a) is reversed.

## REVERSED