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.
13/968,733	08/16/2013	Hugo John Martin VINCENT	JRL-6157-3	1010

23117 7590 12/26/2019
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
MERCADO, GABRIEL S	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
12/26/2019	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):

PTOMAIL@nixonvan.com
pair_nixon@firsttofile.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte HUGO JOHN MARTIN VINCENT, KRISZTIAN FLAUTNER,
and AMYAS EDWARD WYKES PHILLIPS

Appeal 2018-005233
Application 13/968,733
Technology Center 3600

Before ERIC B. CHEN, JAMES B. ARPIN, and MICHAEL M. BARRY, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

Pursuant to 35 U.S.C. § 134(a), Appellant[2] appeals from the Examiner's decision to reject claims 1, 3–25, and 28, which are all of the claims pending. We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

[1] We refer herein to the Appeal Brief filed Oct. 26, 2017 ("Appeal Br."), the Answer mailed Feb. 21, 2018 ("Ans."), the Non-Final Office Action mailed May 1, 2017 ("Non-Final Act."), and the Specification and Figures from the Drawings filed Aug. 16, 2013 ("Spec." and "Figs.").

[2] We use "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies the real party in interest as ARM IP Limited. Appeal Br. 3.

Introduction

Appellant's Specification describes an "invention relate[d] to the field of electronic transactions between parties." Spec. 2:6–7; *see also* Figs. 1–6. Appellant discusses several issues impacting transactions performed between two parties over a network, including the use of "a trusted third party" and authentication technology. *See* Spec. 2:10–4:9. Appellant describes techniques for authenticating electronic messages that use a trusted third party along with differently cryptographically signed first and second messages sent between devices of two parties to a transaction. *See* Spec. 11:9–16:27; Fig. 1.

Claims 1, 25, and 28 are independent; claim 1 is representative of the claims on appeal:

> 1. A machine-implemented method for authenticating electronic messages exchanged between a first electronic device and a second electronic device, the method comprising:
>
> a first signing step in which a first cryptographic signature is applied to a first electronic message comprising a request and a message identifier by said first electronic device to form a first cryptographically signed message;
>
> a first transmitting step in which said first cryptographically signed message is transmitted as a signal from said first electronic device to said second electronic device;
>
> a second signing step in which said second electronic device:
>
>> forms a second electronic message that comprises the first cryptographically signed message, and
>>
>> applies a second cryptographic signature to the second electronic message to form a second cryptographically signed message;

> a second transmitting step in which said second cryptographically signed message is transmitted as a signal from said second electronic device to said first electronic device;
>
> a third transmitting step in which said second cryptographically signed message is transmitted as a signal from the first electronic device and from the second electronic device to a trusted third electronic device for authentication, wherein the first electronic device does not locally verify that the second cryptographically signed message was signed by the second electronic device, and wherein the second electronic device does not locally verify that the first cryptographically signed message was signed by the first electronic device;
>
> a first verification step in which said trusted third electronic device verifies that said second cryptographically signed message received as a signal from the first electronic device, and said second cryptographically signed message received as a signal from the second electronic device, was cryptographically signed by said second electronic device;
>
> an extracting step in which the trusted third electronic device extracts the first cryptographically signed message from the second cryptographically signed message;
>
> a second verification step in which said trusted third electronic device verifies that said first cryptographically signed message extracted from said second cryptographically signed message received as a signal from the first electronic device, and said first cryptographically signed message extracted from said second cryptographically signed message received as a signal from the second electronic device, was cryptographically signed by said first electronic device; and
>
> a request execution step in which, in response to positive verifications from said first verification step and said second verification step, said trusted third electronic device manages execution of said request specified within said second cryptographically signed message.

Appeal Br. 28–29 (Claims App'x).

The References and Rejections

The Examiner relies on the following references:

Name[3]	**Number**	**Published**
Kuroda	US 6,470,448 B1	Oct. 22, 2002
Iwamura	US 2004/0107348 A1	June 3, 2004
Soto	US 2004/0059924 A1	Mar. 25, 2004
Nagamine	US 2004/0068465 A1	Apr. 8, 2004
Samid	US 2008/0262969 A1	Oct. 23, 2008
Tie	US 2010/0262832 A1	Oct. 14, 2010
Baptist	US 2011/0161754 A1	June 30, 2011
Lucco	US 2012/0297360 A1	Nov. 22, 2012
Ronca	US 2013/0080270 A1	Mar. 28, 2013

The Examiner rejected claims 1, 3–25, and 28 under 35 U.S.C. § 101 as directed to a judicial exception, without reciting significantly more. Non-Final Act. 8–13.

The Examiner rejected claims 1, 3–25, and 28 under 35 U.S.C. § 112(a), as failing to comply with the written description requirement.[4] Non-Final Act. 13–14.

The Examiner rejected claims 1, 5–7, 11–13, 16, 18, and 20–25 under 35 U.S.C. § 103 as obvious over Kuroda, Iwamura, and Tie. Non-Final Act. 15–38; *see also id.* at 49.

[3] All reference citations are to the first listed inventor's surname.

[4] The Examiner also rejected claims 1, 3–25, and 28 under 35 U.S.C. § 112(b) as indefinite, but withdrew that rejection in the Answer. Non-Final Act. 14–15; Ans. 16.

The Examiner rejected each of claims 3, 4, 8–10, 14, 15, 17, and 19 as obvious in view of Kuroda, Iwamura, Tie, and either Soto, Nagamine, Lucco, Samid, Baptist, or Ronca. Non-Final Act. 38–44.

The Examiner rejected claim 28 as obvious in view of Kuroda and Iwamura. Non-Final Act. 44–49.

ANALYSIS

A. The Lack of Written Description Rejection

Compliance with the written description requirement is a question of fact that is context sensitive. *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc) ("[T]he level of detail required to satisfy the written description requirement varies depending on the nature and scope of the claims and on the complexity and predictability of the relevant technology."). The test is whether the disclosure "conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date." *Id.* The Specification must adequately describe the claimed subject matter, but "the exact terms need not be used *in haec verba*." *Lockwood v. Am. Airlines Inc.*, 107 F.3d 1565, 1572 (Fed. Cir. 1997).

The Examiner determines the Specification fails to provide written description support for extracting a first cryptographically signed message from a second cryptographically signed message, as recited in independent claims 1, 25, and 28. Non-Final Act. 13–14 (citing Spec. ¶ 53[5]) (explaining "the [S]pecification doesn't sufficiently disclose such step and circuitry for performing this step"). Appellant contends the Examiner errs, because

[5] Citations are to the Specification as published in US 2015/0052066 A1 (Feb. 19, 2015).

artisans of ordinary skill would have understood the Specification's disclosure of processing a first cryptographically signed message 50 that contains a second cryptographically signed message 90, as illustrated in Figure 2 and discussed in paragraphs 16, 22, 44, and 62, demonstrates Appellant was in possession of the limitations at issue. Appeal Br. 18–21. The Examiner responds that paragraph 52 of the Specification, which discusses that the trusted third party can verify whether a doubly-encrypted message has been altered by using digests, without decrypting the first encrypted message that is within the second encrypted message, demonstrates that Appellant was *not* in possession of the disputed limitation. Ans. 11–12.

Appellant's argument is persuasive. Although the Examiner is correct that the Specification's discussion of the trusted third party's use of digests for determining whether a doubly-encrypted message has been altered does not discuss decrypting the first encrypted message that is contained within the second encrypted message, the limitation at issue does not require decryption of the first encrypted message. There is no dispute that the Specification discloses that the trusted third party decrypts the second encrypted message that contains the first encrypted message in order to use the contents of the second encrypted message for verification. *Id.* This demonstrates there is written description support for the limitation at issue, because ordinarily skilled artisans understand that using the contents of the decrypted second message discloses extracting the contents of the second encrypted message, i.e., including "extract[ing] the first cryptographically signed message from the second cryptographically signed message," as claims 1, 25, and 28 recite.

Accordingly, we do not sustain the Examiner's rejection under 35 U.S.C. § 112(a) of claims 1, 3–25, and 28.

B. The Patent Eligibility Rejection

1. Patent Eligibility Law and Guidance

An invention is patent-eligible if it claims a "new and useful process, machine, manufacture, or composition of matter." 35 U.S.C. § 101. The U.S. Supreme Court, however, has long interpreted 35 U.S.C. § 101 to include implicit exceptions: "[l]aws of nature, natural phenomena, and abstract ideas" are not patentable. *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

In determining whether a claim falls within an excluded category, we are guided by the Court's two-step framework, described in *Mayo* and *Alice*. *Id.* at 217–18 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 71–73 (2012)). In accordance with that framework, we first determine what concept the claim is "directed to." *See Alice*, 573 U.S. at 219 ("On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk."); *see also Bilski v. Kappos*, 561 U.S. 593, 611 (2010) ("Claims 1 and 4 in petitioners' application explain the basic concept of hedging, or protecting against risk.").

Concepts determined to be abstract ideas, and, thus, patent ineligible, include certain methods of organizing human activity, such as fundamental economic practices (*Alice*, 573 U.S. at 219–20; *Bilski*, 561 U.S. at 611); mathematical concepts (*Parker v. Flook*, 437 U.S. 584, 594–95 (1978)); and mental processes (*Gottschalk v. Benson*, 409 U.S. 63, 67 (1972)). In *Diamond v. Diehr*, the claim at issue recited a judicial exception in the category of mathematical concepts, but the Court held that "[a] claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses a mathematical formula." 450 U.S. 175, 176 (1981).

If the claim is "directed to" an abstract idea, we turn to the second step of the *Alice* and *Mayo* framework, where "we must examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221 (internal quotation marks omitted). "A claim that recites an abstract idea must include 'additional features' to ensure 'that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].'" *Id.* (alterations in original) (quoting *Mayo*, 566 U.S. at 77). "[M]erely requir[ing] generic computer implementation[] fail[s] to transform that abstract idea into a patent-eligible invention." *Id.*

The Office has published revised guidance on the application of § 101. *See* 2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. 50–57 (Jan. 7, 2019) ("Guidance"); October 2019 Update: Subject Matter Eligibility, 84 Fed. Reg. 55942 (Oct. 17, 2019). Under the Guidance, we first look to whether the claim recites:

(1) any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain methods of organizing human activity such as a fundamental economic practice, or mental processes); and

(2) additional elements that integrate the judicial exception into a practical application (*see* Manual of Patent Examining Procedure (MPEP) § 2106.05(a)–(c), (e)–(h)).

See Guidance, 84 Fed. Reg. at 52–55. Only if a claim (1) recites a judicial exception and (2) does not integrate that exception into a practical application, do we then look to whether the claim:

(3) adds a specific limitation beyond the judicial exception that are not "well-understood, routine, conventional" in the field (*see* MPEP § 2106.05(d)); or

(4) simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception.

See Guidance, 84 Fed. Reg. at 56.

2. Patent Eligibility Analysis

For the § 101 rejection, Appellant argues the independent claims (which recite commensurate limitations) together as a group. Appeal Br. 11–18. We select claim 1 as representative. 37 C.F.R. § 41.37(c)(1)(iv).

In following the Guidance, we first consider under prong one of Step 2A whether claim 1 recites a judicial exception. Guidance, 84 Fed. Reg. at 54. For this analysis, we remain mindful that we must not express the claim's basic concept in a way that is "untethered from the language of the claims" and, accordingly, we assess what claim 1 recites at the same level of generality or abstraction expressed in the claim. *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016).

The nine recited steps are for a method of authenticating electronic messages. The first step applies a cryptographic signature to a message to form "a first cryptographically signed message." The second step transmits that cryptographically signed message from a first device to a second device. The third step creates ("forms") a second message that includes the first cryptographically signed message and then applies a second cryptographic signature to create a "second cryptographically signed message." The fourth step transmits that second cryptographically signed message from the second device to the first device. The fifth step requires both the first and second devices to transmit the second cryptographically signed message to "a trusted third electronic device for authentication." In the sixth step, the trusted third device verifies the second device's cryptographic signing of the second cryptographically signed message. In the seventh and eighth steps, the trusted third device extracts the first cryptographically signed message from the second cryptographically signed message and then verifies the first device's signing of the first cryptographically signed message. Finally, in the ninth step, the trusted third device executes a "request specified within said second cryptographically signed message."

The focus of claim 1 is on using cryptographically signed messages for verification, which is a technological idea. As the Specification explains, the use of computer technology is a fundamental aspect of cryptographic signing. *See* Spec. ¶ 41 (explaining that "[i]n general, the process of cryptographically signing a message involves generating a digest or hash of the message using a one-way hashing algorithm" and that "[a] key feature of such a hashing algorithm is that it is computationally intractable to find a different input that produces the same output"). Although cryptographic signing involves mathematical algorithms, such as hashing algorithms, the limitations of claim 1 do not recite a mathematical algorithm. There is no evidence before us that humans can implement cryptographic signing in their minds or with the assistance of pen and paper. Nor is there persuasive evidence before us that the recited steps involving cryptographic signature technology a method of organizing human activity.[6]

Thus, putting aside the novelty and obviousness issues, we agree with Appellant that claim 1 recites "a technological improvement" (Appeal Br. 17). Accordingly, because the basic focus of claim 1, as recited, is on a digital computer technology, which is neither a mathematical concept, nor a method of organizing human activity, nor a mental process, under the Guidance, and consistent with relevant precedent, we determine that claim 1 does not recite an abstract idea. *See* 84 Fed. Reg. at 52.

We further note claim 1 is analogous to the claims at issue in *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014). The common key aspect of both Appellant's claim 1 and the claim at issue in *DDR Holdings* is that these claims focus on a challenge particular to computers and computer networks. *See* 773 F.3d at 1257 (determining claims "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks" are patent eligible).

[6] To the extent claim 1 recites steps that encompass certain methods of organizing human activity that constitute an abstract idea, such as an idea based on the exchange of signed documents between people, claim 1 recites a practical application of such an idea. In particular, claim 1's limitations for forming a second cryptographically signed message that includes within it a first cryptographically signed message, along with the limitations for performing two verification steps related to the two levels of encryption, which includes a first level of decryption of the doubly-encrypted message, integrate any such "human activity" limitations into a practical application of such an idea.

Thus, at prong one of step 2A of the Guidance, we determine claim 1 does not recite a judicial exception, and we do not sustain the § 101 rejection of claims 1, 3–25, and 28.

C. The Obviousness Rejections

In rejecting claim 1 as obvious, the Examiner finds that Iwamura teaches "form[ing] a second electronic message that comprises the first cryptographically signed message; and apply[ing] a second cryptographic signature to the second electronic message" as recited. *See* Non-Final Act. 20–21 (citing Iwamura ¶ 115). Appellant contends, *inter alia*,[7] the Examiner errs in this finding. Appeal Br. 23–24 (citing Iwamura ¶¶ 43, 56, 58, 112, 114–15). In particular, Appellant argues that, in contrast with the disputed limitations' requirement for forming a second cryptographically signed message that contains ("comprises") a first cryptographically signed message, which "provide[s] two layers of authentication over the first original message," Iwamura teaches two different signatures that are for two different things. *Id.*

Appellant's argument is persuasive. The Examiner responds that "even if the signatures are placed in the document of *Iwamura* for different reasons than in the claimed invention, this does not change the fact that both inventions (instant and *Iwamura*) pertain to a digital data signed by multiple users." Ans. 13; *see also id.* at 14. This response is unpersuasive. Iwamura describes its two signatures as applied to separate data, i.e., one for the data for an "original image 12" and one for the data of the separate "history

[7] Because we reverse the Examiner's § 103 rejection based on a dispositive issue, we do not address Appellant's other contentions.

information 13" that stores modification data for the image. Iwamura ¶¶ 56, 58 (discussing Figs. 1A and 1B).

We agree with the Examiner that it is unnecessary for Iwamura's invention to be for the same purpose as Appellant's claim. But because the two cryptographic signatures in Iwamura apply to two separate sets of data (the original image and the modification history information), Iwamura's signature for the history information (which maps to claim 1's "second cryptographic signature") does not include the signed original image (which maps to claim 1's "first cryptographically signed message"), as required by the disputed limitations. Thus, Appellant persuades us that the Examiner errs in relying on Iwamura for teaching or suggesting the disputed limitations.

Thus, we do not sustain the Examiner's obviousness rejection of independent claim 1. Because independent claims 25 and 28 include commensurate limitations for which the Examiner's rejections rely on the same findings from Iwamura (*see* Appeal Br. 34–37; Non-Final Act. 36, 48), we also do not sustain the obviousness rejections of claims 25 and 28. We also, accordingly, do not sustain the obviousness rejections of the dependent claims 3–24.

CONCLUSION

In summary:

Claim(s) Rejected	**35 U.S.C. §**	**Reference(s) Basis**	**Affirmed**	**Reversed**
1, 3–25, 28	112(a)	Written Description		1, 3–25, 28
1, 3–25, 28	112(b)	Indefiniteness		1, 3–25, 28
1, 3–25, 28	101	Eligibility		1, 3–25, 28

Claim(s) Rejected	35 U.S.C. §	Reference(s) Basis	Affirmed	Reversed
1, 5–7, 11–13, 16, 18, 20–25	103	Kuroda, Iwamura, Tie		1, 5–7, 11–13, 16, 18, 20–25
3, 4	103	Kuroda, Iwamura, Tie, Soto		3, 4
8	103	Kuroda, Iwamura, Tie, Nagamine		8
9, 10	103	Kuroda, Iwamura, Tie, Lucco		9, 10
14	103	Kuroda, Iwamura, Tie, Samid		14
15	103	Kuroda, Iwamura, Tie, Baptist		15
17, 19	103	Kuroda, Iwamura, Tie, Ronca		17, 19
28	103	Kuroda, Iwamura		28
Overall Outcome				1, 3–25, 28

REVERSED