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.
13/750,742	01/25/2013	Quentin Liu	DCERT.056C1	1095

20995 7590 04/16/2018

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER
DAVIS, ZACHARY A

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
04/16/2018	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):

jayna.cartee@knobbe.com
efiling@knobbe.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte QUENTIN LIU, MARC WILLIAMS, and RICHARD F. ANDREWS

Appeal 2017-009975
Application 13/750,742
Technology Center 2400

Before ALLEN R. MacDONALD, BETH Z. SHAW, and DAVID J. CUTITTA II, *Administrative Patent Judges*.

MacDONALD, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from a rejection of claims 1, 3–11, and 13–20. Appellants cancelled claims 2 and 12. App. Br. 10, 14. We have jurisdiction under 35 U.S.C. § 6(b).

---

[1] Appellants state the real party in interest for this appeal is Symantec Corporation. App. Br. 2.

Representative Claim

Representative claim 1 under appeal reads as follows (emphasis, formatting, and brackets added).

1. A method comprising:

[A.] ***receiving***, over a network, one or more certificate signing requests;

[B.] ***extracting***, by at least one computer processor, a first name and a second name from an existing digital certificate stored in a memory,

wherein extracting the first and second names comprises extracting

[i.] the first name from a Subject field of the existing digital certificate and

[ii.] the second name from a SubjectAltName extension of the existing digital certificate; and

[C.] in response to the receiving, ***provisioning***, over the network, by the at least one computer processor,

[i.] a first digital certificate with the first name and

[ii.] a second digital certificate with the second name,

wherein the first name is stored in a Subject field of the first digital certificate, and

wherein the second name is stored in a Subject field of the second digital certificate.

Rejection

The Examiner rejected claims 1, 3–11, and 13–20 under 35 U.S.C. § 101 "because the claimed invention is directed to non-statutory subject matter" (Oct. 6, 2016 Final Act. 7), i.e., for being patent-ineligible subject matter.[2]

Issue on Appeal

Did the Examiner err in rejecting claim 1 for being directed to patent-ineligible subject matter?

Appellants' Admissions

1. Appellants state in their Background:

> X.509 certificates, also referred to as digital certificates, are used in a wide variety of applications. These digital certificates provide a method to verify the identity of a user, are a component of a secure communications channel, and deliver authentication information based on these capabilities.
>
> X.509 certificates are defined by the Telecommunication Standardization Sector (ITU-T) of the International Telecommunication Union (ITU) as part of the Directory (X.500) series.

Spec. ¶¶ 2–3.

2. Appellants also state in their Background:

> The structure of an X.509 v3 digital certificate is as follows:
>
> - Certificate
> - o Version
> - o Serial Number

[2] We select claim 1 as representative. Separate patentability, in compliance with 37 C.F.R. § 41.37(c)(iv), is not argued for claims 3–11 and 13–20. Except for our ultimate decision, we do not discuss the rejection of claims 3–11 and 13–20 further herein.

- o Algorithm ID
- o Issuer
- o Validity
  - • Not Before
  - • Not After
- o Subject
- o Subject Public Key Info
  - • Public Key Algorithm
  - • Subject Public Key
- o Issuer Unique Identifier (Optional)
- o Subject Unique Identifier (Optional)
- o Extensions (Optional)
  - • . . .

• Certificate Signature Algorithm
• Certificate Signature

Spec. ¶ 4.

3. Appellants further state in his Background:

> X.509 certificates bind the name of an entity in the real world, such as a company "VeriSign," to a public key. The "Subject" field of the certificate provides a location for storage of the name, which is bound to the public key stored in the certificate. The subject name is in the form of an X.500 or LDAP directory name and is often identical to the entity's directory name, e.g., the fully qualified domain name of the website: www.verisign.com. . . . Many digital certificates contain only one name, which is stored in the Subject field.
>
> Starting with X.509 v3 certificates, the subject alternative name extension was provided to allow identities to be bound to the subject of the certificate. These identities may be included in addition to or in place of the identity in the subject field of the certificate. Defined.

Spec. ¶¶ 5–6 (emphasis added).

DEFINITIONS[3]

Symantec

Digital certificate – A digital certificate is an electronic document which confirms the identity of an entity – which could be a user, a server, a company, a program on a client, just about anything – and associates that entity with a public key. The digital certificate is the entity's identification to the public key infrastructure. Each party to a TLS-secured communication can evaluate the contents of the certificate. The most examined field is the Common Name.

White Paper - Best Practices and Applications of TLS/SSL; Larry Seltzer; Symantec; page 4; 2014.

https://www.symantec.com/content/en/us/enterprise/white_papers/b-best-practices-applications-of-tls-ssl_WP.pdf. (Accessed 4/5/2018).

Wikipedia

Digital certificate –In cryptography, a public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject. In email encryption, code signing, and e-signature systems, a certificate's subject is typically a person or organization. However, in Transport Layer Security

[3] Dictionary.com. Dictionary.com Unabridged. Random House, Inc. http://www.dictionary.com (accessed: March 9, 2018).

(TLS) a certificate's subject is typically a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices. TLS, sometimes called by its older name Secure Sockets Layer (SSL), is notable for being a part of HTTPS, a protocol for securely browsing the web.

The most common format for public key certificates is defined by X.509. Because X.509 is very general, the format is further constrained by profiles defined for certain use cases, such as Public Key Infrastructure (X.509) as defined in RFC 5280.

https://en.wikipedia.org/wiki/Public_key_certificate (accessed 4/2/2018).

Microsoft Press

Digital certificate – A user identity card or "driver's license" for cyberspace. Issued by a certificate authority (CA), a digital certificate is an electronic credential that authenticates a user on the Internet and intranets. Digital certificates ensure the legitimate online transfer of confidential information, money, or other sensitive materials by means of public encryption technology. A digital certificate holder has two keys (strings of numbers): a private key held only by the user, for "signing" outgoing messages and decrypting incoming messages; and a public key, for use by anyone, for encrypting data to send to a specific user. See also certificate authority, encryption, private key, public key.

Microsoft Computer Dictionary.--5th ed.; page 158; 2002.

ANALYSIS

We have reviewed the Examiner's rejections in light of Appellants' arguments (Appeal Brief and Reply Brief) that the Examiner has erred. We disagree with Appellants' conclusions and concur with the conclusions reached by the Examiner. Except as noted below, we adopt as our own the reasoning set forth by the Examiner in the Examiner's Answer. We highlight the following points.

A. *Section 101*

Under 35 U.S.C. § 101, a patent may be obtained for "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." The Supreme Court has "long held that this provision contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable." *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2354 (2014) (quoting *Ass'n for Molecular Pathology* v. *Myriad Genetics, Inc.*, 133 S. Ct. 2107, 2116 (2013)). The Supreme Court in *Alice* reiterated the two-step framework previously set forth in *Mayo Collaborative Services* v. *Prometheus Laboratories, Inc.*, 132 S. Ct. 1289, 1300 (2012), "for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of these concepts." *Alice*, 134 S. Ct. at 2355. The first step in that analysis is to "determine whether the claims at issue are directed to one of those patent-ineligible concepts," such as an abstract idea. For example, a fundamental economic practice is an abstract idea.

> [In *Bilski v. Kappos*], the Court grounded its conclusion that all of the claims at issue were abstract ideas in the understanding that risk hedging was a " 'fundamental economic practice.' " 561 U.S., at 611, 130 S.Ct. 3218.

Alice, 134 S. Ct. at 2357.

The Court acknowledged in *Mayo* that "all inventions at some level embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas." *Mayo*, 132 S. Ct. at 1293. We, therefore, look to whether the claims focus on a specific means or method that improves the relevant technology or are instead directed to a result or effect that itself is the abstract idea and merely invoke generic processes and machinery. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336 (Fed. Cir. 2016). If the claims are not directed to an abstract idea, the inquiry ends. Otherwise, the inquiry proceeds to the second step where the elements of the claims are considered "individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 134 S. Ct. at 2355 (quoting *Mayo*, 132 S. Ct. at 1298, 1297).

B. *Alice/Mayo - Step 1*

The Examiner concludes:

> Claim 1 is directed to a method that only recites receiving requests, extracting names from a certificate, and provisioning certificates. Extracting names from a certificate could be performed entirely by a person and is an abstract step. Similarly, provisioning new certificates is an abstract step because it merely involves compiling and separating data. These are abstract because they are directed to general methods of organizing human activities and data. . . . Because the claims recite (i.e. set forth or describe) abstract ideas of extracting names and provisioning certificates, the claims are directed to abstract ideas in the meaning of the subject matter eligibility test set forth in the [2014] Interim Guidance [on Patent Subject Matter Eligibility] (see section I.A.1).

Final Act. 7.

1

a

Appellants contend claim 1 is not directed to an abstract idea because:

> The Examiner has asserted that the claims are directed to various abstract ideas, including "using categories to organize, store, and transmit data" and "data recognition and storage" (Office Action), or the "movement, manipulation, and organization of data" (Advisory Action). However, while the claims involve those general concepts, ***it is inappropriate to ask*** whether claims "*involve* a patent-ineligible concept." *Enfish, LLC. v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016). Instead, the appropriate inquiry is whether the ***claims as a whole*** are directed to excluded subject matter. *Id.*

App. Br. 4 (emphasis added).

Appellants correctly point out that the Examiner has misstated the holding in *Enfish*. However, Appellants then doubly misstate the *Enfish* holding. *Enfish* does not state, "***it is inappropriate to ask*** whether claims '*involve* a patent-ineligible concept'" as argued by Appellants. App. Br. 4 (emphasis added). Rather, *Enfish* states "[t]he 'directed to' inquiry [] ***cannot simply ask*** whether the claims *involve* a patent-ineligible concept." *Enfish,* 822 F.3d at 1335 (emphasis added). Also, *Enfish* does not state "the appropriate inquiry is whether the ***claims as a whole*** are directed to excluded subject matter'" as argued by Appellants. App. Br. 4 (emphasis added). Rather, *Enfish* states "the 'directed to' inquiry applies a stage-one filter to claims, considered in light of the specification, based on whether '***their character as a whole*** is directed to excluded subject matter.'" *Enfish,* 822 F.3d at 1335 (emphasis added).

Our review under *Alice/Mayo* step 1 looks to the character of claim 1 as a whole.

b

Appellants contend:

> Claim 1 . . . is directed to a ***specific method*** for splitting a digital certificate. Because, ***in the claimed invention***, the user already has been verified and approved for possession of certificates containing all of the requested names (in one certificate), efficiency in the certificate splitting process can be achieved while ***maintaining security without requiring a re-verification of identity***. See Specification as Filed at [0025], [0013]-[0014].

App. Br. 4 (emphasis added).

Appellants also contend:

> It is also inappropriate to oversimplify claims by "looking at them generally and ***failing to account for the specific requirements of the claims***." See *McRO, Inc. v. Bandai Namco Games America*, [837 F.3d 1299, 1313 (Fed. Cir. 2016)].
>
> Here, the ***specific requirements*** of the claims have been ignored. The claims are not directed to organizing and storing data, or to manipulation of data, but rather ***to specific ways*** in which data manipulation and storage may be used to achieve a non-abstract goal – splitting a single digital certificate with multiple names owned by a single entity into multiple certificates with single names owned by that same entity, ***without needing to re-verify or certify the identity of the entity and without requiring repetitive requests***. Rather than being directed to the abstract idea of manipulating data, or even to an abstract idea of splitting certificates if such were indeed abstract, which it is not, the claims as a whole are directed to a ***specific transformation*** achieving a new and useful result. Contrary to the Federal Circuit's instructions in Enfish and McRO, the Examiner has oversimplified the claims and looked at what they involve, rather than what they are directed to as a whole, in order to find an abstract idea. The claims are focused on a "***specific means or***

> ***method*** that improves the relevant technology," and not to a result which is itself the abstract idea, and thus are not directed to an abstract idea.

App. Br. 4–5 (emphasis added).

Appellants further contend:

> Here . . . the Examiner has ignored the focus of the claimed advance, which provides ***specific advantages and distinctions*** over conventional certificate issuance, in order to assert that the claims are directed to the automation of conventional activity. In particular, the claims allow for a technique that enables providing multiple separate certificates when a primary certificate with multiple owners previously existed. ***Other such techniques exist***; but this particular technique ***provides a specific way*** to achieve this result, and thus does not constitute an abstract idea.

App. Br. 5–6 (emphasis added).

Appellants further contend:

> Similar to *Enfish*, the claimed invention provides a particular and ***specific improvement*** (a particular set of rules for taking a source certificate and provisioning multiple certificates from the source certificate) to the way computers previously could be used to provision multiple certificates. Further, similar to McRO, the claimed invention uses a combined order of ***specific rules*** (receiving a source certificate and extracting information from it in specified ways) that renders information into a ***specific format*** (first and second names) that is then used and applied to create desired results (multiple provisioned certificates).

App. Br. 7 (emphasis added).

The Examiner responds:

> Appellant does not specify what requirements of the claims are alleged to have been ignored [and] . . . does not specify what the focus of the claimed advance is with reference to the claim language[.] [R]ather, Appellant only states that "the claims allow for a technique that enables providing multiple separate certificates when a primary certificate with multiple owners previously existed" and makes the conclusory statement that

> "this particular technique provides a specific way to achieve this result, and thus does not constitute an abstract idea".

Ans. 2–3.

The Examiner further responds:

> [F]irst, it is noted that in *McRO*, the rules were explicitly recited as "rules" to be used in the claim, which is not equivalent to the present claims, as the present claims do not explicitly recite any "rules". Further, Appellant's summary of the claim, as rendering information into a specific format (extracting names from the certificates) and using that to create desired results of provisioned certificates, again highlights the similarity to gathering data (the names) from one collection of information (the existing certificate) and then organizing the information into a new form (using the data to result in the two new certificates), which was identified as abstract in *Digitech*.

Ans. 4–5.

We are unpersuaded by Appellants' arguments. Contrary to Appellants' assertion, we conclude the character of claim 1 as a whole is "directed to general methods of organizing human activities and data" as the Examiner concludes. Final Act. 7.

Contrary to the specific limitations argued by Appellants, we do not find in claim 1 splitting a digital certificate "without needing to re-verify or certify the identity of the entity and without requiring repetitive requests" (App. Br. 5); or "specific rules" and "specific format" (App. Br. 7). The argued negative limitation is simply not set forth as a requirement of claim 1; nor are specific rules or a specific format. At most, claim 1 sets forth specific data (names) and a general format (Subject and SubjectAltName fields) which Appellants have admitted are known in the prior art (Appellants' admissions 1–3). Although Appellants repeatedly assert claim 1 is directed to a specific method, specific advantage; specific distinction,

specific transformation, specific way; or specific improvement; we find no such specifics in claim 1. Rather, we agree with the Examiner that these are conclusory statements (Ans. 3) without sufficient support in Appellants' arguments or claim 1.

C. *Alice/Mayo - Step 2*

Turning to the second part of the *Alice/Mayo* analysis, the Examiner concludes:

> Although the claim recites that the operations are performed "by a data processor", this constitutes, at most, mere instructions to implement the abstract idea on a computer. It is noted that the broadest interpretation of a "data processor" also encompasses a person that processes data; however, even if the claim were more explicitly limited to a computer, microprocessor, or other hardware data processor performing the steps, this would still constitute mere instructions to implement the abstract idea on a computer. . . . The claims require no more than a generic computer to perform generic computer functions that are well-understood, routine, and conventional activities, namely receiving and compiling data, and this does not add significantly more to the abstract idea. . . . The step of receiving one or more certificate signing requests is also a generic computer function (i.e. receiving a request for processing to be performed). Further, the limitations that the receiving and provisioning are performed over a network merely amount to a link to a particular field of use (i.e. computer networks). . . . The additional steps, whether considered individually or as an ordered combination, do not amount to significantly more than the abstract idea, and therefore, the claim as a whole is not directed to significantly more than the abstract idea.

Final Act. 8.

Appellants contend:

> The claims here are ***fundamentally*** tied to computer technology as digital certificates for identity are ***fundamentally*** a technology

> that arose out of the need to provide secure identification techniques in the online environment, a need which does not exist in the same way in the physical world. The claims describe a process by which the routine and conventional approach to certificates, requiring one signing request per certificate desired, is overridden and an improved process results. ***The claimed invention is not merely directed to the routine and conventional applied by a computer, but rather to a new way of using that computer***. As a result, the present claims are similar to those in *DDR Holdings* and thus not simply directed to an abstract idea but rather fundamentally tied to computer technology.

App. Br. 6 (emphasis added).

The Examiner responds:

> [A] digital certificate is not a "technology". Rather, a digital certificate is defined only as a set of certain data (usually including, for example, an identity, issuer, public key, and issuer signature on the other fields of the certificate) and is therefore intangible as such, as noted with respect to *Elec. Power Grp*.

Ans. 4.

We are unpersuaded by Appellants' arguments. Symantec Corporation (the Real Party in Interest for this appeal; App. Br. 2) states that a digital certificate is an electronic document (above Definitions); and Appellants admit that the known structure of an X.509 v3 digital certificate includes a Subject and a subject alternative name extension (Appellants' Admissions 1–3). Appellants' assert that the claim 1 digital certificate process is an improvement of computer technology which provides secure identification techniques in the online environment. We disagree. We conclude that the claimed rearranging of the "existing digital certificate" data so as to provision new first and second digital certificates ***does not*** change or improve the actual computer technology which provides secure identification techniques in the online environment. Our review finds

neither the prior art secure identification techniques, which apply the digital certificate, nor any new variation thereof are recited in claim 1. Rather, claim 1 limits itself to merely splitting the contents of the existing electronic document into new first and second documents. Although data content is split, we do not find where claim 1 requires that the new documents be in any other way different in format that the existing document.

Appellants also overlook that our reviewing court has cautioned against Appellants' position in the *DDR Holdings* decision.

> We caution, however, that not all claims purporting to address Internet-centric challenges are eligible for patent. For example, in our recently-decided *Ultramercial* opinion, the patentee argued that its claims were "directed to a specific method of advertising and content distribution that was previously unknown and never employed on the Internet before." 772 F.3d at 714. But this alone could not render its claims patent-eligible. In particular, we found the claims to merely recite the abstract idea of "offering media content in exchange for viewing an advertisement," along with "routine additional steps such as updating an activity log, requiring a request from the consumer to view the ad, restrictions on public access, and use of the Internet." *Id.* at 715–716.

DDR Holdings, LLC v. Hotels.com, L.P, 773 F.3d at 1258 (Fed. Cir. 2014). The *DDR Holdings* decision required more from a "solution" before finding a claim to be rooted in computer technology.

> The '399 patent's claims are different enough in substance from those in *Ultramercial* because they do not broadly and generically claim "use of the Internet" to perform an abstract business practice (with insignificant added activity). Unlike the claims in *Ultramercial*, the claims at issue here specify ***how interactions*** with the Internet ***are manipulated*** to yield a desired result—a result that ***overrides the routine and conventional sequence of events*** ordinarily triggered by the click of a hyperlink. Instead of the computer network operating in its

> normal, expected manner by sending the website visitor to the third-party website that appears to be connected with the clicked advertisement, the claimed system generates and directs the visitor to the above-described hybrid web page that presents product information from the third-party and visual "look and feel" elements from the host website. When the limitations of the '399 patent's asserted claims are taken together as an ordered combination, the claims recite ***an invention that is not merely the routine or conventional use of the Internet***.

773 F.3d at 1258–59 (emphasis added). In other words, the claimed invention in *DDR Holdings* did not merely use the Internet but rather changed how interactions on the Internet operated.

D. *Other 101 Arguments*

1

Appellants contend claim 1 "does not ***pre-empt*** the field of certificate splitting." App. Br. 7 (emphasis added). Appellants' pre-emption argument overlooks that the Court's *Alice* two-step (abstract idea/ significantly more) analysis is the Court's framework for determining pre-emption.

> [W]e set forth a framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts.

Alice, 134 S. Ct. at 2355. Contrary to Appellants' argument, the Examiner applied this *Alice* framework in the Final Action.

2

Appellants also contend as to claim 1:

> [T]he limitations of claim 1 represent significantly more than the abstract idea, as the functionality is not well-understood, routine, and conventional (as evidenced by the ***lack of any prior art cited***

> ***by the Examiner disclosing or rendering obvious the claimed invention***).

App. Br. 9 (emphasis added).

We are not persuaded by Appellants' argument. Although the second step in the *Alice/Mayo* analysis includes a search for an inventive concept, the analysis is not an evaluation of novelty or nonobviousness, but rather, a search for "an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Alice*, 134 S. Ct. at 2355 (quoting *Mayo*, 132 S. Ct. at 1294). A novel and nonobvious claim directed to a purely abstract idea is, nonetheless, patent-ineligible. *See Mayo*, 132 S. Ct. at 1304 (rejecting the suggestion that Sections 102, 103, and 112 might perform the appropriate screening function and noting that in *Mayo* such an approach "would make the 'law of nature' exception . . . a dead letter"). Further, "under the *Mayo/Alice* framework, a claim directed to a newly discovered law of nature (or natural phenomenon or abstract idea) cannot rely on the novelty of that discovery for the inventive concept necessary for patent eligibility." *Genetic Techs. Ltd. v. Merial L.L.C.*, 818 F.3d 1369, 1376 (Fed. Cir. 2016).

CONCLUSION

(1) The Examiner has not erred in rejecting claims 1, 3–11, and 13–20 under 35 U.S.C. § 101, as being directed to patent-ineligible subject matter.

(2) Claims 1, 3–11, and 13–20 are not patentable.

DECISION

We **affirm** the Examiner's rejection of claims 1, 3–11, and 13–20.

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)(iv).

AFFIRMED