



# 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.
14/636,467	03/03/2015	Cristian Radu	P01515-US- UTIL (M01.361)	7390
125619	7590	07/01/2020	EXAMINER	
Mastercard International Incorporated c/o Buckley, Maschoff & Talwalkar LLC 50 Locust Avenue New Canaan, CT 06840			ASGARI, SIMA	
			ART UNIT	PAPER NUMBER
			3685	
			NOTIFICATION DATE	DELIVERY MODE
			07/01/2020	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):

colabella@bmtpatent.com  
martin@bmtpatent.com  
szpara@bmtpatent.com

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

*Ex parte* CRISTIAN RADU, MEHDI COLLINGE,  
and  
JOHN GAITANOS

---

Appeal 2020-001837  
Application 14/636,467<sup>1</sup>  
Technology Center 3600

---

Before JOSEPH L. DIXON, DAVID M. KOHUT, and  
JON M. JURGOVAN, *Administrative Patent Judges*.

JURGOVAN, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant seeks review under 35 U.S.C. § 134(a) from a Non-Final Rejection of claims 1, 8, and 25–28, which are all the claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.<sup>2</sup>

---

<sup>1</sup> We use the word “Appellant” to refer to “applicant(s)” as defined in 37 C.F.R. § 1.42. The real party in interest is Mastercard International Incorporated. (Appeal Br. 2.)

<sup>2</sup> Our Decision refers to the Specification (“Spec.”) filed March 3, 2015, the Non-Final Office Action (“Non-Final Act.”) mailed April 1, 2019, the Appeal Brief (“Appeal Br.”) filed August 12, 2019, the Examiner’s Answer (“Ans.”) mailed November 22, 2019, and the Reply Brief (“Reply Br.”) filed

## CLAIMED INVENTION

The claims are directed to a mobile computing device and method “allowing [the] mobile device to operate as a payment device securely without a requirement for secure hardware.” (Spec. 1:9–12.) A processor of the mobile computing device is programmed with a mobile transaction application, a memory of the mobile computing device comprises a local database to hold data items for use by the mobile transaction application, and the mobile transaction application “is adapted to encrypt data items for storage in the local database [] and to decrypt data items stored in the local database [] using white-box cryptographic techniques.” (Abstract.)

Independent claims 1 and 25, reproduced below, are illustrative of the claimed subject matter:

1. A mobile computing device configured for performing payment transactions, the mobile computing device comprising:
  - a processor; and
  - a memory associated with the processor;
    - the memory storing a local database, the local database including a plurality of entries, each of said entries including:
      - (a) an index, (b) an application sequence counter value; and
      - (c) an encrypted parameter;
    - the memory storing program instructions, the processor controlled by the program instructions to perform functions as follows:
      - retrieving the index and the application sequence counter value from one of the entries contained in the local database;
      - deriving an entry-specific key  $K_i$  based on (i) a system key  $K_{SYS}$ , (ii) the retrieved index, and (iii) the retrieved sequence counter value; said system key  $K_{SYS}$  having been included in embedded form in said program instructions; and

using the derived entry-specific key  $K_i$  to decrypt the encrypted parameter included in said one of the entries contained in the local database;

the memory further storing a mobile transaction application, the processor controlled by the mobile transaction application such that the mobile computing device performs a payment transaction using the decrypted parameter.

25. A method of performing payment transactions, the method comprising:

storing a local database in a memory in a mobile computing device, the local database including a plurality of entries, each of said entries including: (a) an index, (b) an application sequence counter value; and (c) an encrypted parameter;

retrieving the index and the application sequence counter value from one of the entries contained in the local database;

deriving an entry-specific key  $K_i$  based on (i) a system key  $K_{SYS}$ , (ii) the retrieved index, and (iii) the retrieved sequence counter value; said system key  $K_{SYS}$  having been included in embedded form in program instructions stored in the mobile computing device;

using the derived entry-specific key  $K_i$  to decrypt the encrypted parameter included in said one of the entries contained in the local database; and

performing a payment transaction with the mobile computing device using the decrypted parameter.

(Appeal Br. 18–19 (Claims App.).)

## REFERENCES

The prior art relied upon by the Examiner is:

Name	Reference	Date
Cooper	US 5,563,946	October 8, 1996
Ginter	US 5,892,900	April 6, 1999
Flitcroft	US 2003/0028481 A1	February 6, 2003
Pourfallah	US 2012/0253852 A1	October 4, 2012

## REJECTIONS

Claims 1, 8, and 25–28 stand rejected under 35 U.S.C. § 112(a) as failing to comply with the written description requirement. (Non-Final Act. 8–10.)

Claims 1, 8, and 25–28 stand rejected under 35 U.S.C. § 112(b) as being indefinite. (Non-Final Act. 10–12.)

Claims 1, 8, and 25–28 stand rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter. (Non-Final Act. 4–7.)

Claims 1 and 8 stand rejected under 35 U.S.C. § 102(a)(1)/(a)(2) as anticipated by Cooper. (Non-Final Act. 13–14.)

Claims 1, 25, and 28 stand rejected under 35 U.S.C. § 103 based on Cooper and Flitcroft. (Non-Final Act. 15–17.)

Claims 8 and 26 stand rejected under 35 U.S.C. § 103 based on Cooper, Flitcroft, and Ginter. (Non-Final Act. 17.)

Claim 27 stands rejected under 35 U.S.C. § 103 based on Cooper, Flitcroft, and Pourfallah. (Non-Final Act. 18.)

## ANALYSIS

### ***§ 112(a) Written Description Rejections***

The written description “must ‘clearly allow persons of ordinary skill in the art to recognize that [the inventor] invented what is claimed.’” *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1345, 1351 (Fed. Cir. 2010)

(en banc) (citation omitted). 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.*

Moreover, the Federal Circuit also stated that the written description clause of section 112 has been construed to mandate that the specification satisfy two closely related requirements—it must describe the manner and process of making and using the invention so as to enable a person of skill in the art to make and use the full scope of the invention without undue experimentation and “it must describe the invention sufficiently to convey to a person of skill in the art that the patentee had possession of the claimed invention at the time of the application, i.e., that the patentee invented what is claimed.” *LizardTech, Inc. v. Earth Resource Mapping, Inc.*, 424 F.3d 1336, 1344–45 (Fed. Cir. 2005) (while the inventor had the intent to cover generic methods with his patent, he did not disclose enough in the specification to enable one skilled in the art to make and use the generic invention and thus did not show possession of the generic claims). The Federal Circuit has explained that:

The test for determining compliance with the written description requirement is whether the disclosure of the application as originally filed reasonably conveys to the artisan that the inventor had possession at that time of the later claimed subject matter, rather than the presence or absence of literal support in the specification for the claim language.

*In re Kaslow*, 707 F.2d 1366, 1375 (Fed. Cir. 1983) (citations omitted).

In cases where functional claim language recites merely a desired result, the claim “may do so without describing species that achieve that result[, b]ut the specification must demonstrate that the applicant has made a generic

invention that achieves the claimed result . . . by showing that the applicant has invented species sufficient to support a claim to the functionally-defined genus.” *Ariad Pharms.*, 598 F.3d at 1349.

The Examiner rejected independent claims 1 and 25 as failing to comply with the written description requirement because the Specification lacks sufficient written description for particular limitations recited in these claims. (Non-Final Act. 8–9; Ans. 7–9.) Specifically, with respect to claim 1, the Examiner asserts:

[T]he claim[] recite[s] “. . . processor controlled by the program instructions . . .”, and “. . . processor controlled by the mobile transaction application . . .” without clearly defining how the “controlled . . .” is performed. An algorithm or steps/procedure taken to perform the function “controlled” must be described with sufficient detail so that one of ordinary skill in the art would understand how the inventor intended the function to be performed.

(Non-Final Act. 8–9; *see also* Ans. 7–8.) And, with respect to claim 25, the Examiner asserts:

[T]he claim recites “storing . . .”, “retrieving . . .”, “deriving . . .”, “using . . .”, and “performing . . .” However, the claim limitations are silent to what component(s) perform the “storing . . .”, “retrieving . . .”, “deriving . . .”, “using . . .”, and “performing . . .” Therefore, the claim limitations are broader than the Specification.

(Non-Final Act. 9 (citing *LizardTech Inc.*, 424 F.3d at 1344–45); *see also* Ans. 9.)

We agree with the Examiner. Both claims 1 and 25 recite “retrieving the index and the application sequence counter value from one of the entries contained in the local database,” “deriving an entry-specific key  $K_i$  based on

(i) a system key  $K_{SYS}$ , (ii) the retrieved index, and (iii) the retrieved sequence counter value; said system key  $K_{SYS}$  having been included in embedded form in said program instruction,” and “using the derived entry-specific key  $K_i$  to decrypt the encrypted parameter included in said one of the entries contained in the local database.” (See Appeal Br. 18–19 (claims 1 and 25).) Thus, claims 1 and 25 recite functional language specifying a desired result (generation of a decrypted parameter). However, Appellant’s Specification does not sufficiently describe how the retrieving, deriving, and decrypting are performed. For example, page 7, line 31 to page 8, line 2, page 8, lines 8–23, page 16, lines 3–22, page 17, lines 2–16, and Figure 9 in the Specification (cited by Appellant as support, *see* Appeal Br. 11 and Reply Br. 2) restate functions/steps recited in the claims and provide generic descriptions for key derivation and parameter decryption, but do not describe with sufficient detail the algorithms or operations that perform the claimed retrieving, deriving, and using/decrypting steps. For example, page 7, line 31 to page 8, line 2, and page 8, lines 8–23 in the Specification merely describe components of a mobile computing device, but do not describe which cryptographic, encryption, and decryption techniques to use and how to use them to perform the parameter’s encryption, the subsequent derivation of an entry-specific key, and the encrypted parameter’s decryption. Page 16, lines 3–22, page 17, lines 2–16, and Figure 9 in the Specification describe how to generically derive an entry-specific key based on three elements (system key, retrieved index, and retrieved sequence counter value), but do not explain (i) *which entry* (of the plurality of entries) in the local database is selected for retrieval of its *index* and *application sequence counter value*, or *how is the index selected* for retrieval from the plurality of the entries’



indices, and (ii) *which cryptographic, encryption, and decryption techniques would be used, and how would they be used to prepare the encrypted parameter, to derive the entry-specific key, and to decrypt the encrypted parameter.* The Specification (at page 16, lines 3–22, page 17, lines 2–16, Figure 9, and elsewhere) references generic cryptographic frameworks and encryption/decryption algorithms—including a “static white-box algorithm” (SWB), “suitable cryptographic algorithms” such as AES-256, “white-box cryptography (WBC)” and “white-box cryptographic techniques,” “dynamic white-box (DWB) cryptography,” “a key derivation algorithm in encryption and storage of data in the local encrypted database,” “grey-box (GB) model” and “grey-box techniques,” SWB AES 256-E, AES 256-I, AES-128 E (*see* Spec. 4:5–6, 11:2–19, 12:25–27, 13:19–22, 15:6–7, 16:3–28, 17:2–19, 18:10–19, 18:27–28)—but the Specification does not provide sufficient detail regarding *which of these cryptographic, encryption, and decryption techniques are to be used and more particularly, how are they to be used to prepare the encrypted parameter EPARAM<sub>i</sub> (see Spec. 16:10, 16:13) and to derive the entry-specific key K<sub>i</sub> based on system key, retrieved index, and retrieved sequence counter value so that the derived key K<sub>i</sub> enables decryption of the encrypted parameter.*

Appellant’s response to the Examiner’s written description rejections of claims 1 and 25 (*see* Appeal Br. 11–12, Reply Br. 2) does not provide evidence that a skilled artisan would understand the applicant to have invented, and been in possession of, the full scope of the invention as broadly and generically recited in claims 1 and 25. *See LizardTech, Inc.*, 424 F.3d at 1345 (citing *O’Reilly v. Morse*, 56 U.S. 62, 112–13 (1853)). Appellant’s response asserts that the language of claims 1 and 25 is

supported in the Specification, and identifies pages of the Specification providing such support. (Appeal Br. 11–12; Reply Br. 2.) However, the issue is not whether the literal language is recited in the Specification, but whether sufficient functional detail is disclosed in the Specification to show that the Appellant had possession of the broad features recited in claims 1 and 25. (*See* Non-Final Act. 8–9; Ans. 7–9.) Here, there is insufficient detail about how the claimed “retrieving,” “deriving,” and “using . . . to decrypt” operate—e.g., *about how* the index is retrieved from the local database (e.g., which entry is selected for retrieval of its index and sequence counter value, or how is the index selected from the plurality of entries’ indices) and *how* an algorithm for “deriving an entry-specific key  $K_i$ ” would operate to produce a key that enables decryption of the “encrypted parameter”—so that one of ordinary skill in the art could conclude that the inventor invented a cryptographic technique for payment transactions in the manner claimed. (*Id.*). Particularly, it is not clear why the Specification’s generic reference to a multiplicity of cryptographic frameworks and encryption/decryption algorithms (e.g., SWB, WBC, DWB, GB model, AES-256, SWB AES 256-E, AES 256-I, and AES-128 E) would entitle the inventor to claim any and all combinations of such algorithms and frameworks for achieving the deriving and decrypting steps in claims 1 and 25.

We are thus persuaded by the Examiner’s arguments that Appellant has not provided sufficient evidence to demonstrate that the inventor possesses the full scope of the invention as claimed in claims 1 and 25. Accordingly, we sustain the § 112(a) written description rejections of claims

1 and 25, and of dependent claims 8 and 26–28 for the reasons stated for claims 1 and 25 from which they depend. *See* 37 C.F.R. § 31.47(c)(1)(iv).<sup>3</sup>

---

<sup>3</sup> In the event of any further prosecution, we suggest the Examiner analyze whether Appellant’s Specification also *enables* the full scope of independent claims 1 and 25 as required by 35 U.S.C. § 112(a). In particular, we suggest the Examiner analyze whether Appellant’s original Specification contains sufficient information to enable one skilled in the art to make and use the claimed invention without undue experimentation—more particularly, to teach one skilled in the art how to first prepare/encrypt the encrypted parameter for storage in the local database, and how to derive the entry-specific key  $K_i$  based on system key, retrieved index, and retrieved sequence counter value so that the derived entry-specific key  $K_i$  enables decryption of the encrypted parameter. For example, the Examiner should analyze whether the Specification provides an enabling description of key deriving techniques that are covered by the generically claimed “deriving” recited in claims 1 and 25. The Examiner should also analyze whether Appellant’s Specification apprises one skilled in the art of the techniques/algorithms that may be used to encrypt the encrypted parameter for storage in the local database, and to derive the entry-specific key  $K_i$  based on system key  $K_{SYS}$ , retrieved index, and retrieved sequence counter value so that the derived key  $K_i$  can perform decryption of the encrypted parameter. For example, the Examiner should analyze whether the Specification’s references to generic encryption/decryption algorithms (AES-256, SWB AES 256-E, AES 256-I, AES-128 E, *see* Spec. 15:7, 16:28, 18:10–28) and reference to generic cryptographic techniques (e.g., “use [of] static white-box cryptography and use[ of] a key derivation algorithm in encryption and storage of data in the local encrypted database,” “static white-box (SWB) and dynamic white-box (DWB) cryptography,” and “grey-box (GB) model,” *see* Spec. 4:4–6, 11:1–20, 12:25–27, 13:19–27, 17:17–19) provide sufficient information to enable a skilled artisan to understand which cryptographic, encryption, and decryption techniques to use and how to use them to perform the PARAMi’s encryption and the subsequent derivation of an entry-specific key  $K_i$ . *See In re Knowlton*, 500 F.2d 566, 572 (CCPA 1974) (any patent or publication cited to provide evidence that a particular programming technique is well-known in the programming art does not demonstrate that one of ordinary skill in the art could make and use correspondingly disclosed programming techniques unless both the known and disclosed programming techniques are

We note the Examiner asserted additional written description rejections (with respect to particular limitations in dependent claims 8 and 27) with which we do not agree. In particular, the Examiner asserted claim 8 lacks written description support because the Specification is silent regarding, and lacks an algorithm or steps/procedure for, storing a system key “‘by the memory’ and ‘. . . in a manner utilizing [software obfuscation],” and claim 27 lacks written description support because “the claim limitations are silent to what component(s) perform the ‘emulating.’” (Non-Final Act. 9–10; Ans. 8–9.) We agree with Appellant, however, that the Specification demonstrates Appellant possessed the limitation of claim 8 and adequately describes how a key may be stored in memory in a manner utilizing software obfuscation. (Appeal Br. 11–12; *see* Spec. 9:10–15, 10:4–5, 10:15–16, 11:15–22, 12:21–22, 12:26–27, 14:10–15, 15:1–29, 17:6–12, 18:10–15.) The Specification also demonstrates Appellant possessed the limitation of claim 27, and adequately describes how a mobile computing device emulates a contactless payment card. (*See* Spec. 2:7–11, 2:27–30, 6:18–20, 7:1–2, 8:13–17, 8:24–28, 11:25–27, 22:29–30.)

### **§ 112(b) Indefiniteness Rejections**

The Examiner rejected claims 1 and 8 as “indefinite” on the ground that they are hybrid claims because the claims are “directed to a product (a

---

of approximately the same degree of complexity); *In re Scarbrough*, 500 F.2d 560, 565 (CCPA 1974) (any cited patents which are used by the applicant to demonstrate that particular box diagram hardware or software components are old must be analyzed as to whether such patents are germane to the instant invention and as to whether such patents provide better detail of disclosure as to such components than an applicant’s own disclosure); M.P.E.P. 2164, 2164.06(c).

mobile computing device)” but “also recite[] method steps . . . that are not attributed to an element of the product.” (Non-Final Act. 10–11 (citing *In re Katz Interactive Call Processing Patent Litig.*, 639 F.3d 1303, 1318 (Fed. Cir. 2011)); Ans. 10.)

Appellant argues the Examiner’s “hybrid” claim rejections are in error because claims 1 and 8 cover an apparatus capable of particular functionality, whereby “[i]n claim 1, all of the recited functions are attributed to a component, namely the processor,” while “in claim 8, the term ‘is stored’ as used in the claim would be understood by those skilled in the art to be an attribute of the system key, and not to denote a method step.” (Appeal Br. 13.)

We agree with Appellant that the Examiner’s “hybrid” claim rejections of claims 1 and 8 should be reversed. While it is true “a single claim covering both an apparatus and a method of use of that apparatus” has been held indefinite, our reviewing court has repeatedly drawn a distinction between such claims, and claims that “merely use permissible functional language to describe capabilities of the claimed system” and are, therefore, not indefinite. *MasterMine Software, Inc. v. Microsoft Corp.*, 874 F.3d 1307, 1313–1316 (collecting and analyzing cases applying *IPXL Holdings LLC v. Amazon.com Inc.*, 430 F.3d 1377 (Fed. Cir. 2005)). Claims 1 and 8 fall into this second category. Claim 1 recites a “mobile computing device” comprising a “processor” and a “memory,” the “memory” (i) storing program instructions (including the embedded system key) that cause the “processor . . . to perform [the retrieving, deriving, and using] functions,” and (ii) storing a mobile transaction application that controls the “processor . . . such that the mobile computing device [that includes the processor]

performs a payment transaction.” Thus, claim 1 is directed to a mobile computing device whose components (i.e., processor and memory) have particular configuration and capabilities, as claimed. Claim 8 is similarly directed to the mobile computing device whose memory is recited as securely storing (by software obfuscation storage) particular data (the system key).

Accordingly, we do not sustain the Examiner’s § 112(b) “hybrid claim” rejections of claims 1 and 8.

The Examiner also rejects independent claims 1 and 25 for having unclear scope for the reasons that (i) “[i]t is unclear whether the claim[s] 1 and 25] . . . [are] directed to the mobile computing device or to the combination mobile computing device and local database” or “to the local database (or the system key),” (ii) “[i]t is unclear whether the claims [1 and 25] are directed to the mobile computing device or to the combination mobile computing device and program instructions [that include the system key],” and (iii) claim 1 is “directed to ‘a mobile computing device’ and the phrase ‘such that the mobile computing device performs . . .’ describes the mobile computing device in terms of the mobile computing device itself” but “a device cannot comprise itself.” (Non-Final Act. 11–12; Ans. 10–11.)

Appellant argues the scope of claims 1 and 25 is clear. (Appeal Br. 13.) We agree with Appellant. Particularly, we agree with Appellant that “[a] person of ordinary skill in the art would readily grasp that claim 1 is directed to a mobile computing device, and that the phrase in question [pertaining to a local database] further defines characteristics of the local database stored in the device memory.” (Appeal Br. 13.) Thus, the scope of the subject matter embraced by claim 1 is clear, as claim 1 identifies that it is

directed to *a mobile computing device* having various components that include *a memory* “storing a local database [of entries],” *the memory* also “storing program instructions [including an embedded system key].” (*See* Appeal Br. 18 (claim 1).) We also agree with Appellant that “a person of ordinary skill would also readily grasp that claim 25 is directed to a method of performing payment transactions” using various pieces of data stored in a database. (Appeal Br. 13.) The scope of the subject matter embraced by claim 25 is clear, as claim 25 identifies that it is directed to a method of performing payment transactions by steps of retrieving, deriving, using, and performing. (*See* Appeal Br. 19 (claim 25).)

We also disagree with the Examiner that claim 1 is unclear because it “describes the mobile computing device in terms of the mobile computing device itself.” (*See* Non-Final Act. 12.) As Appellant explains, “a person of ordinary skill would readily understand from the context of this phrase [(“such that the mobile computing device performs”)], that it aids in further defining functions performed by the processor.” (Appeal Br. 13.) The scope of the subject matter embraced by claim 1 is clear, as claim 1 identifies functionality of the mobile computing device’s components whereby (i) the processor (of the mobile computing device) is controlled to enable the mobile computing device to perform a payment transaction, with (ii) the processor being controlled as such by an application stored on the mobile computing device’s memory. (*See* Appeal Br. 18 (claim 1).)

Based on the foregoing, we do not sustain the Examiner’s § 112(b) “unclear scope” rejections of independent claims 1 and 25, and of their associated dependent claims 8 and 26–28.

The Examiner also rejects independent claims 1 and 25 for “insufficient antecedent basis for ‘the decrypted parameter’ in the claim[s], because the previous limitation merely recites ‘using . . . to decrypt the encrypted parameter . . .’ Therefore, the decryption was never performed.” (Non-Final Act. 12.)

Appellant states the claims’ recitation of “using the derived entry-specific key . . . to decrypt the encrypted parameter” provides antecedent basis for the claimed “decrypted parameter,” as a “person of ordinary skill in the art would readily comprehend that a result of this function/method step” [(i.e., the “using the derived entry-specific key . . . to decrypt the encrypted parameter”)] is decryption of the parameter, thereby providing ample antecedent basis for [the decrypted parameter].” (Appeal Br. 14.) We agree with Appellant. In light of the claimed “using the derived entry-specific key  $K_i$  to decrypt the encrypted parameter” (as recited in claims 1 and 25), one of ordinary skill in the art would understand that the recited “*decrypted parameter*” indicates the data that is generated by the claimed *decrypting the encrypted parameter*. (See Appeal Br. 18–19 (claims 1 and 25).)

Based on the foregoing, we do not sustain the Examiner’s § 112(b) rejection of independent claims 1 and 25 for insufficient antecedent basis.

### ***35 U.S.C. § 101 Rejection***

Patent eligibility is a question of law that is reviewable *de novo*. *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1333 (Fed. Cir. 2012). Accordingly, we review the Examiner’s § 101 determinations concerning patent eligibility under this standard.

Patentable subject matter is defined by 35 U.S.C. § 101, as follows:



Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

In interpreting this statute, the Supreme Court emphasizes that patent protection should not preempt “the basic tools of scientific and technological work.” *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972) (“*Benson*”); *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 71 (2012) (“*Mayo*”); *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014) (“*Alice*”). The rationale is that patents directed to basic building blocks of technology would not “promote the progress of science” under the U.S. Constitution, Article I, Section 8, Clause 8, but instead would impede it. Accordingly, laws of nature, natural phenomena, and abstract ideas, are not patent-eligible subject matter. *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1346 (Fed. Cir. 2017) (citing *Alice*, 573 U.S. at 216).

The Supreme Court set forth a two-part test for subject matter eligibility in *Alice* (573 U.S. at 217–18). The first step is to determine whether the claim is directed to a patent-ineligible concept. *Id.* (citing *Mayo*, 566 U.S. at 76–77). If so, then the eligibility analysis proceeds to the second step of the *Alice/Mayo* test in which we “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) (quoting *Mayo*, 566 U.S. at 72, 79). There is no need to proceed to the second step, however, if the first step of the *Alice/Mayo* test yields a determination that the claim is directed to patent-eligible subject matter.

The Patent Office has recently revised its guidance for how to apply the *Alice/Mayo* test in the *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50 (January 7, 2019) (“the Revised Guidance”). Under the Revised Guidance, we first look to whether the claim recites:

- (1) any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, mental processes, or certain methods of organizing human activity such as a fundamental economic practice or managing personal behavior or relationships or interactions between people); 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)).

84 Fed. Reg. at 51–52, 55.

A claim that integrates a judicial exception into a practical application applies, relies on, or uses the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception. 84 Fed. Reg. at 54. When the judicial exception is so integrated, then the claim is not directed to a judicial exception and is patent-eligible under § 101. 84 Fed. Reg. at 54. Only if a claim (1) recites a judicial exception and (2) does not integrate that exception into a practical application, do we then evaluate whether the claim provides an inventive concept. 84 Fed. Reg. at 56; *Alice*, 573 U.S. at 217–19, 221. Evaluation of the inventive concept involves consideration of whether an additional element or combination of elements (1) adds a specific limitation or combination of limitations that are not well-understood, routine, conventional activity in the field, which is indicative that an inventive concept may be present; or (2) simply appends well-understood, routine, conventional activities previously known to the

industry, specified at a high level of generality, to the judicial exception, which is indicative that an inventive concept may not be present.

Appellant argues claims 1, 8, and 25–28 together, presenting arguments directed to independent claim 25. (Appeal Br. 8–11.) As a result, we select independent claim 25 as the illustrative claim for the group and address Appellant’s arguments thereto. Independent claim 1 contains similar limitations.

### Step 1

Applying Step 1 of the Revised Guidance (which is unchanged from the prior guidance) to the present case, we determine independent claim 25 recites a “method,” which is a form of “process,” thereby falling within one of the categories enumerated under § 101 and satisfying Step 1 of the Revised Guidance.

### Step 2A—Prong One (Does the Claim Recite a Judicial Exception?)

We proceed to apply Step 2A of the Revised Guidance to determine if claim 25 is “directed to” a judicial exception. As discussed *supra*, Prong One of Step 2A under the Revised Guidance is to determine whether the claim recites a judicial exception including (a) mathematical concepts; (b) certain methods of organizing human activity; and (c) mental processes.

Reviewing claim 25, we note the claim involves commercial interactions and sales activities that “perform[] payment transactions,” and more particularly the activity of “performing a payment transaction with [a] mobile computing device.” (See Appeal Br. 19 (claim 25).) The claim therefore recites one of the certain methods of organizing human activity identified in the Revised Guidance, and therefore, an abstract idea. (See Revised Guidance, 84 Fed. Reg. at 51–52 (describing an abstract idea

category of “Certain methods of organizing human activity—fundamental economic principles or practices (including hedging, insurance, mitigating risk); commercial or legal interactions (including . . . sales activities or behaviors; business relations)”); Non-Final Act. 6; Ans. 4.)

Step 2A—Prong Two (Integration into Practical Application)

Although claim 25 recites an abstract idea of a method of organizing human activity, as provided for in the Revised Guidance, such a claim may nonetheless be patentable if it recites a particular, practical application of the abstract idea embodied therein. *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1352 (Fed. Cir. 2016).

Accordingly, we proceed to the Prong Two of Step 2A, where we inquire whether an additional element of the claim integrates the method of organizing human activity into a practical application. Revised Guidance, 84 Fed. Reg. at 54–55. Such an additional element may reflect an improvement in the functioning of a computer, or an improvement to another technology or technical field. *Id.* at 55; *see also McRO, Inc. v. Bandai Namco Games America Inc.*, 837 F.3d 1299 (Fed. Cir. 2016); *Finjan Inc. v. Blue Coat Systems, Inc.*, 879 F.3d 1299 (Fed. Cir. 2018); and *Core Wireless Licensing, S.A.R.L. v. LG Electronics, Inc.*, 880 F.3d 1356 (Fed. Cir. 2018) (claims were directed to improvements instead of abstract ideas).

Having reviewed the evidence, we disagree with the Examiner’s findings that

This judicial exception is not integrated into a practical application because the additional element(s) of the claim(s) such as a memory, a computing device, and a processor, and decrypting the data, merely use a computer as a tool to perform an abstract idea. . . . the additional claim elements “using a key to decrypt data” is[sic] not indicative of integration into a

practical application, because the “decryption” does not improve the functioning of an apparatus (e.g., the processor), or any other technology or technical field. . . . the claims do not. . . . effect an improvement in any other technology or technical field.

(Non-Final Act. 6–7; *see also* Ans. 4–5.) Rather, we agree with Appellant that claim 25 *integrates* the abstract idea *into a practical application* under the Prong Two of Step 2A. (Revised Guidance, 84 Fed. Reg. at 54–55; *see* Appeal Br. 6, 9–10; Reply Br. 2.) Particularly, we agree with Appellant that claim 25 *integrates* the abstract idea *into a practical application* that “improve[s] the functioning of the apparatus by providing sufficiently robust security for payment account parameters such that a secure element need not be incorporated in a payment-enabled mobile device.” (Appeal Br. 9.)

Appellant more particularly explains:

As stated at page 16, line 23 to page 17, line 1 of the specification, and as would be inferred generally from the disclosure as a whole by those who are skilled in the art, software features of the invention provide improved cyber-security for payment applications, such that, with the claimed software features, adequate protection from fraudulent attacks is provided without incorporating a secure element (SE) in a payment-enabled mobile device. This is an improvement in the technical field of cyber-security.

(Reply Br. 2.)

Claim 25 recites a combination of additional elements including:

[D]eriving an entry-specific key  $K_i$  based on (i) a system key  $K_{SYS}$ , (ii) the retrieved index [from one of the entries contained in the local database], and (iii) the retrieved sequence counter value [from the entry contained in the local database]; said system key  $K_{SYS}$  having been included in embedded form in program instructions stored in the mobile computing device; [and]

using the derived entry-specific key  $K_i$  to decrypt the encrypted parameter included in said one of the entries contained in the local database,

which improve security of a payment transaction executed by the mobile computing device, by using the decrypted parameter in a payment transaction. (*See* Appeal Br. 19 (claim 25); Spec. 14:19–23, 16:3–22, 17:5–23, 18:10–32.) Appellant’s Specification explains that security of mobile payments is improved even for a mobile payment application and associated local database located within a mobile device’s application processor such that “neither [the payment application nor the local database] rely on the security domain 105 provided within the SIM/USIM 104 [of the mobile device] or on any other security domain protected by secure hardware.” (*See* Spec. 8:19–23, 11:8–22, 13:22–27, Fig. 2.) The Specification explains that transaction security is improved by using an index, application sequence counter value, and encrypted parameter associated with the mobile payment application’s operation on the mobile device:

[The] mobile application 101 [for use in a payment device for making contactless transactions] is adapted to write to (41) and read from (42) the encrypted local database 102. The encrypted local database 102 may contain any parameter needed for the operation of the mobile application 101 that is potentially sensitive to the user or any other party, such as a card issuer or a merchant. . . . [E]ach entry 43 in the encrypted local database 102 has three items: an index 44; an application sequence counter value 45; and an encrypted parameter 46. . . . The index 44 fixes the position in the encrypted local database 102 where one specific parameter is stored. The application sequence counter (represented pictorially as ASN) value 45 provides a reference to the transaction during which a relevant operation (resulting in, typically, writing of the parameter to the database) was performed. The encrypted parameter (EPARAM) 46 contains

encrypted content in an appropriate format (such as TLV) for long term protection.

The inventors have determined that using this approach, it is possible for the mobile transaction application 101 to be a generic application that is not initially differentiated for each user. This means that the application can be downloaded by the user from an application store and installed in main memory in the same manner as a normal mobile application.

(Spec. 11:24–12:17.) The Specification provides that Appellant’s mobile payment technique “allows the use of a generic transaction application [on a mobile device] that is not personalised to a user without compromising user or issuer security.” (Spec. 3:29–31, 4:19–21 (“the mobile transaction application is downloaded to the mobile computing device without customisation to the mobile computing device or its user”), 16:23–17:12.)

Thus, Appellant’s claim 25 integrates a technique for performing payment transactions into a process rooted in computer and network technologies. (*See* Spec. 11:24–12:17, 16:3–17:16; *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257–58 (Fed. Cir. 2014) (holding patent-eligible a claim that “address[es] a business challenge (retaining website visitors)” by enabling visitors “to purchase products from the third-party merchant without actually entering that merchant’s website,” thus providing a “claimed solution . . . necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks”).) Similar to claim 25, independent claim 1 integrates performance of payment transactions into a process rooted in computer and network technologies. (*See* Appeal Br. 18 (claim 1).)

Because claims 1 and 25 integrate the judicial exception into a practical application, we find claims 1 and 25, and their dependent claims 8

and 26–28 are directed to patent-eligible subject matter under § 101. Accordingly, we do not address Step 2B of the Revised Guidance (corresponding to step two of the *Alice/Mayo* test).

For these reasons, we do not sustain the Examiner’s rejection of claims 1, 8, and 25–28 as directed to non-statutory subject matter under 35 U.S.C. § 101.

### **§ 102 Rejection**

“Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim.” *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548 (Fed. Cir. 1983); *see also In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009); *In re Buszard*, 504 F.3d 1364, 1366 (Fed. Cir. 2007); *In re Paulsen*, 30 F.3d 1475, 1478–79 (Fed. Cir. 1994). Anticipation is a factual issue. *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997).

The Examiner rejects claim 1 as anticipated by Cooper. (Non-Final Act. 13–14.) The Examiner does not, however, make findings that Cooper discloses certain functionality recited in claim 1 that the Examiner determines “indicate[s] the intended use of the processor.” (*Id.* at 14.)

For example, the Examiner makes no findings that Cooper discloses “the processor controlled by the mobile transaction application [stored by the memory] such that the mobile computing device performs a payment transaction using the decrypted parameter,” as recited in claim 1. (*Id.*) Rather, the Examiner concludes that “the recitation: ‘the processor controlled . . . to . . .’ indicate[s] the intended use of the processor, as it does not require that the processor perform an operation.” (*Id.*) The Examiner



then determines that “the processor taught by Cooper et al. reads on the claim,” as “the intended use will not differentiate the claim from the teaching of Cooper.” (*Id.* (citing Cooper 7:13–8:62, 13:6–14:15, Figs. 2–3 and 18).)

Appellant argues the Examiner’s anticipation rejection is in error because the Examiner does not identify in Cooper the claimed functions, which are “positively recited functions performed by the processor.” (Appeal Br. 14.) We agree.

Claim 1 recites a mobile computing device comprising a processor controlled by programmed instructions to perform certain functions. For example, the processor in claim 1 is “controlled by the mobile transaction application” (stored in the mobile computing device’s memory) “such that the mobile computing device performs a payment transaction using the decrypted parameter.” (Appeal Br. 18 (Claim 1).)

When functional language in a claim is associated with programming or some other structure required to perform the function, that programming or structure must be present in order to meet the claim limitation. *See Typhoon Touch Techs., Inc. v. Dell, Inc.*, 659 F.3d 1376, 1380–81 (Fed. Cir. 2011) (discussing *Microprocessor Enhancement Corp. v. Texas Instruments, Inc.*, 520 F.3d 1367 (Fed. Cir. 2008)); *see also In re Noll*, 545 F.2d 141, 148 (CCPA 1976) (“[T]he claimed invention . . . comprises physical structure, including storage devices and electrical components uniquely configured to perform specified functions through the physical properties of electrical circuits to achieve controlled results. Appellant’s programmed machine is structurally different from a machine without that program.”). Regardless of the structure of the device, the steps of the method (e.g., that the device is

controlled to perform) recite functions that must be considered. *See In re Lowry*, 32 F.3d 1579, 1582 (Fed. Cir. 1994) (“The Patent and Trademark Office (PTO) must consider all claim limitations when determining patentability of an invention over the prior art.”) (citing *In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983)).

Because the Examiner fails to clearly articulate the reasons as to how claim 1’s recited functions are disclosed by Cooper “with such information and references as may be useful in judging of the propriety of continuing the prosecution of [the] application” (35 U.S.C. § 132), the Examiner’s “rejection is so uninformative that it prevents the applicant from recognizing and seeking to counter the grounds for rejection” (*Chester v. Miller*, 906 F.2d 1574, 1578 (Fed. Cir. 1990)). Thus, the Examiner has not set forth a prima facie case of unpatentability, and we do not sustain the anticipation rejection of independent claim 1, and of the associated dependent claim 8, on the basis discussed above.

### ***§ 103 Rejections***

The Examiner finds Cooper’s method of transferring encrypted files (trial versions of software packages) from a source computer to a target computer via computer-accessible memory media (such as diskettes or CD-ROMs to be used on the target computer) teaches steps of the method recited in claim 25, including the claimed (i) storing a local database including entries with an index, an application sequence counter value, and an encrypted parameter, (ii) retrieving the index and the application sequence counter value from one of the entries contained in the local database, and (iii) deriving an entry-specific key  $K_i$  based on a system key  $K_{SYS}$  and based

on the retrieved index and the retrieved sequence counter value. (Non-Final Act. 15–16 (citing Cooper 7:13–8:62, 13:6–16:11, 14:15, Fig. 18); Ans. 11–12.) In particular, the Examiner finds “Cooper . . . teaches a computer accessible memory media with a file management program (local database) that stores values such as machine identification, customer number, real key, interval data.” (Ans. 12 (citing Cooper 14:15–16:16, Figs. 14–20).) The Examiner also finds:

Cooper further teaches retrieving *an index (e.g., a customer number), and a sequence counter value (e.g., a machine ID)* from the local database (e.g., computer accessible memory media), and *deriving an entry-specific key (e.g., real key) based on a system key (e.g. product key), the retrieved index (e.g., customer number), and the retrieved sequence counter value (e.g., machine ID).*

(*Id.* (emphases added).) The Examiner then finds “[t]he derived real key of Cooper is later used to decrypt an encrypted parameter (e.g. encrypted validation text),” thereby teaching the claimed decryption of the encrypted parameter. (*Id.* (citing Cooper 16:17–17:14, Fig. 21); *see also* Non-Final Act. 16.) We do not agree.

We agree with Appellant that the Examiner has not shown that Cooper teaches “retrieving the index and the application sequence counter value from one of the entries contained in the local database” and “deriving an entry-specific key  $K_i$  based on (i) a system key  $K_{SYS}$ , (ii) the retrieved index, and (iii) the retrieved sequence counter value” as recited in claim 25. (Appeal Br. 15–16.) As Appellant explains, “Cooper is primarily concerned with transfers of files in encrypted form, using a key that is unique to a transfer medium, such as a diskette” but “Cooper is not concerned with decrypting encrypted parameters stored in database entries” and “fails to

disclose or suggest retrieving an index and application sequence counter from an entry in a local database.” (*Id.* at 15.)

More particularly, Cooper’s *customer number* is a number assigned by a software vendor to a customer, the number provided by the vendor to customer via phone, fax, or mail. (*See* Cooper 11:41–43, 13:25–27, 15:17–19.) In contrast, Appellant’s Specification explains that a *database index* “fixes the position in the encrypted local database . . . where one specific parameter is stored.” (*See* Spec. 12:4–6, 16:2–5, 16:13–16 (referring to “the row entry identified by Index *i*”).) Thus, we disagree with the Examiner’s finding that Cooper’s *customer number* assigned by vendor to customer teaches the claimed *database index*. (*See* Ans. 12; *see also* Appeal Br. 15.) We also disagree with the Examiner’s finding that Cooper’s *machine ID* (which identifies a customer’s computer) teaches the claimed *application sequence counter value*. (*See* Ans. 12.) More particularly, Cooper’s *machine ID* is “a unique machine identification” of the “user-controlled data processing system” where a trial software version can be installed. (*See* Cooper 11:16–20, 11:43–50, 13:35–38.) In contrast, Appellant’s Specification describes an *application sequence counter value* as a value that “provides a reference to the transaction during which a relevant operation (resulting in, typically, writing of the parameter to the database) was performed.” (*See* Spec. 12:6–9, 16:5–6 and 18–20 (referring to “the number of the current transaction performed by the application, namely the application sequence number (ASN)” at a write operation, and “the number of the transaction when the writing was performed by the application, namely the then ASN”).) The Examiner’s interpretation of the claimed term “application sequence counter value” as reading on Cooper’s “machine ID”

is unduly broad. (*See* Ans. 12.) Thus, we agree with Appellant that the Examiner’s reference to Cooper’s *machine ID* has not shown that Cooper teaches *retrieving an application sequence counter value from an entry in the local database* as claimed.

We further agree with Appellant that “[t]he ‘real key’ described in Cooper is not derived using a retrieved index for a database entry” and “is not derived based on a sequence counter value retrieved from the database entry.” (Appeal Br. 16.) The Examiner’s reference to Cooper’s customer number and machine ID to produce a key has not shown that Cooper *derives a key based on a retrieved database index and based on a retrieved application sequence counter value from a local database* as required by claim 25.

The Examiner does not rely upon the additional teachings of Flitcroft, Pourfallah, and Ginter to cure the above-noted deficiencies of Cooper. As the Examiner has not identified sufficient evidence to support the rejection of claim 25, we do not sustain the Examiner’s § 103 rejection of independent claim 25, independent claim 1 argued for substantially the same reasons as claim 25, and claims 8 and 26–28 dependent from one of claims 1 and 25. (Appeal Br. 14, 16.)<sup>4</sup>

---

<sup>4</sup> In the event of any further prosecution, the Examiner may want to perform an additional prior art search in the cryptography art, including art in Class 380 (Cryptography, including Subclasses 247–250 (cellular telephone cryptographic authentication), Subclasses 255–276 (communication using cryptography), Subclasses 277–286 (key management), and Subclass 287 (electronic signal modification)), Class 711 (Electrical Computers and Digital Processing Systems: Memory, including Subclass 164 (memory access requiring authorization code information) and Subclass 216 (hashing)), Class 713 (Electrical Computers and Digital Processing Systems: Support, including Subclass 150 (multiple computer communication using

### CONCLUSION

The Examiner's rejection of claims 1, 8, and 25–28 under 35 U.S.C. § 112(a), as failing to comply with the written description requirement, is AFFIRMED.

The Examiner's rejection of claims 1, 8, and 25–28 under 35 U.S.C. § 112(b) as being indefinite, is REVERSED.

The Examiner's rejection of claims 1, 8, and 25–28 under 35 U.S.C. § 101 is REVERSED.

The Examiner's rejection of claims 1 and 8 under 35 U.S.C. § 102(a)(1)/(a)(2) is REVERSED.

The Examiner's rejections of claims 1, 8, and 25–28 under 35 U.S.C. § 103 are REVERSED.

In summary:

<b>Claims Rejected</b>	<b>35 U.S.C. §</b>	<b>Reference(s)/Basis</b>	<b>Affirmed</b>	<b>Reversed</b>
1, 8, 25–28	101	Eligibility		1, 8, 25–28
1, 8, 25–28	112(a)	Written Description	1, 8, 25–28	
1, 8, 25–28	112(b)	Indefiniteness		1, 8, 25–28
1, 8	102(a)(1)/ (a)(2)	Cooper		1, 8

---

cryptography) and Subclass 182 (system access control based on user identification by cryptography)), and Class 726 (Information Security, including Subclass 2 (access control or authentication) and Subclass 26 (prevention of unauthorized use of data including prevention of piracy, privacy violations, or unauthorized data modification)). *See also* further specifics of CPC G06F than just 21/00 and 21/10.

Appeal 2020-001837  
Application 14/636,467

1, 25, 28	103	Cooper, Flitcroft		1, 25, 28
8, 26	103	Cooper, Flitcroft, Ginter		8, 26
27	103	Cooper, Flitcroft, Pourfallah		27
<b>Overall Outcome</b>			1, 8, 25– 28	

Because we have affirmed at least one ground of rejection with respect to each claim on appeal, the Examiner’s decision is affirmed.

*See* 37 C.F.R. § 41.50(a)(1).

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