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.
14/719,014	05/21/2015	Erick Wong	79900-940985(964US02)	5963

66945 7590 07/01/2020

KILPATRICK TOWNSEND & STOCKTON LLP/VISA
Mailstop: IP Docketing - 22
1100 Peachtree Street
Suite 2800
Atlanta, GA 30309

EXAMINER
CASTILHO, EDUARDO D

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):

KTSDocketing2@kilpatrick.foundationip.com
ipefiling@kilpatricktownsend.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte ERICK WONG, CHRISTIAN AABYE,
CHRISTIAN FLURSCHEIM, and CHRISTOPHER JONES

Appeal 2019-006926
Application 14/719,014
Technology Center 3600

Before ERIC B. GRIMES, RICHARD M. LEBOVITZ, and
TAWEN CHANG, *Administrative Patent Judges.*

CHANG, *Administrative Patent Judge.*

DECISION ON APPEAL

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 1, 3, 4, 22–25, 27–30, 33–41. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

---

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies the real party in interest as Visa International Service Association. Appeal Br. 3.

BACKGROUND

Communication devices have been "used as payment instruments to conduct contactless transactions." Spec. ¶ 2. According to the Specification,

> [t]o . . . securely store account information on a portable communication device, a secure element such as subscriber identity module (SIM) card, specialized integrated chip embedded into the portable communication device, or specialized component provided as aftermarket solution[,] is used. . . . A secure element is considered secure because account information is stored in tamper-resistant hardware, which protects the account information from malware or viruses that may have infected the operating system or an application running on the portable communication device.

Id.

The Specification states that, however, "incorporating a secure element adds to the . . . cost of the portable communication device." Spec. ¶ 3. In addition, a secure element is typically not under the control of a financial institution; thus, to provision it with account credentials and payment functionalities, the issuer and/or payment processor may have to go through a "cumbersome and complex process" to establish "commercial agreements and technical connectivity" with the party controlling the secure element (e.g., the mobile network operator (MNO)). *Id.*

The Specification notes that, "[t]o further complicate the security issue, in some scenarios, obtaining authorization of a transaction from an issuer at the time of a transaction may be impractical," for instance because "a transit gate terminal may lack constant network connectivity." Spec. ¶ 5. The Specification states that, "[i]n such scenarios, credentials used to

quickly provide patrons with access [to goods or services] may require additional safeguards if they are not stored in a secure element." *Id.*

Further according to the Specification, "[e]mbodiments of the invention address the problem of security concerns with conducting transactions with a communication device that does not have or does not rely on a secure element." Spec. ¶ 6.

CLAIMED SUBJECT MATTER

The claims are directed to a method for enhancing security of a communication device when conducting a transaction offline using the communication device. Claim 1, the only independent claim, is illustrative:

> 1. A method for enhancing security of a communication device when conducting a transaction offline using the communication device, the method comprising:
>
> receiving, from a remote computer by an application installed on the communication device, a limited-use key (LUK) that is associated with a first set of one or more limited-use thresholds that limits usage of the LUK, and a signature key that is associated with a second set of one or more limited-use thresholds that limits usage of the signature key, wherein the first set of one or more limited-use thresholds includes a first limited-use threshold that is different than a second limited-use threshold included in the second set of one or more limited-use thresholds;
>
> receiving, from an access device, terminal transaction data associated with the transaction involving a good or a service;
>
> generating, by the application of the communication device:
>
> a transaction cryptogram using the LUK as an encryption key to encrypt at least a plurality of data elements from the terminal transaction data; and

a signature using at least a part of the terminal transaction data and the signature key;

sending, to the access device, a certificate authority public key index, an issuer public key certificate, and a communication device public key certificate, wherein the certificate authority public key index identifies a certificate authority public key that authenticates the issuer public key certificate, the issuer public key certificate includes an issuer public key that authenticates the communication device public key certificate, and the communication device public key certificate includes a communication device public key that authenticates the signature; and

sending, to the access device, the transaction cryptogram and the signature, the access device authenticating the application of the communication device without requiring network connectivity by verifying the signature using the communication[2] device public key, granting access to the good or service after authenticating the application of the communication device and prior to verification of the transaction cryptogram, and obtaining authorization for the transaction from an issuer by verifying the transaction cryptogram with the issuer after access to the good or service has been granted.

Appeal Br. 29 (Claims App.).

REJECTION(S)

A. Claims 1, 3, 4, 22–25, 27–30, and 33–41 are rejected under 35 U.S.C. § 101 as being directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more. Ans. 5.

[2] The Examiner notes that claim 1 in fact recites "verifying the signature using the *communicating* device public key." Ans. 47–48.

B. Claims 1, 3, 4, 22–25, 27–30, and 33–41 are rejected under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, as being indefinite.

C. Claims 1, 3, 4, 22, 23, 25, 27–29, and 33–41 are rejected under 35 U.S.C. § 103 as being unpatentable over Saxena,[3] Smets,[4] and Radu.[5] Ans. 13.

D. Claim 24 is rejected under 35 U.S.C. § 103 as being unpatentable over Saxena, Smets, Radu, and Verhoorn.[6] Ans. 24.

E. Claim 30 is rejected under 35 U.S.C. § 103 as being unpatentable over Saxena, Smets, Radu, and Ginter.[7] Ans. 25.

OPINION

A. Rejection under 35 U.S.C. § 101 (claims 1, 3, 4, 22–25, 27–30, and 33–41)

1. Issue

The Examiner asserts that "[t]he claims recite local processing of payments for goods and services," which is "within the certain methods of organizing human activity grouping of abstract ideas." Ans. 6. More particularly, the Examiner asserts that the claims "recite functions that can be performed by an individual receiving and processing documents, which is a commercial interaction; and/or an individual granting access to a good or a

---

[3] Saxena et al., US 2012/0254041 A1, published Oct. 4, 2012.
[4] Smets et al., US 2014/0263625 A1, published Sept. 18, 2014.
[5] Christian Radu, IMPLEMENTING ELECTRONIC CARD PAYMENT SYSTEMS (2002).
[6] Verhoorn et al., US 6,725,371 B1, issued Apr. 20, 2004.
[7] Ginter et al., US 5,892,900, issued Apr. 6, 1999.

service upon presentation of a valid token and/or ID, which is a fundamental economic practice." *Id.*

The Examiner asserts that the abstract ideas in the claims are not "integrated into a practical application because . . . the additional element(s) of the claim(s) . . . merely uses a computer as a tool to perform the abstract idea," which "requires no more than a computer performing functions that correspond to acts required to carry out the abstract idea." Ans. 6–7. The Examiner asserts that the additional elements do not "involve improvements to the functioning of a computer[] or . . . any other technology," "apply the abstract idea with, or by use of, a particular machine," "effect a transformation or reduction of a particular article to a different state or thing," or "apply or use the abstract idea in some other meaningful way beyond generally linking the use of the abstract idea to a particular technological environment, such that the claim[s] as a whole [are] more than a drafting effort designed to monopolize the exception." *Id.* at 7.

Finally, the Examiner asserts that "[t]he claims do not include additional elements that are sufficient to amount to significantly more" than the recited abstract idea, because "the additional elements of using a communication device to perform the steps amounts to no more than using a computer or processor to automate and/or implement the abstract idea of local processing of payments for goods or services." Ans. 8.

Appellant contends that the "characterization of the claims as being directed to fundamental economic practices and certain methods of organizing human activities overgeneralizes and oversimplifies the claims." Appeal Br. 11. Appellant further contends that the claims "provide the technical improvements of enhancing the security of the communication

device while reducing the processing time" and "should also be patent eligible under the USPTO's 2019 Guidance for integrating any alleged judicial exception in to a practical application." *Id.* at 12, 15–16.

2. Analysis

In *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66 (2012), the Supreme Court set forth a general framework for analyzing patent-eligibility questions under 35 U.S.C. § 101. As explained by our reviewing court in *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371 (Fed. Cir. 2015):

> In *Mayo* . . . , the Supreme Court 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. First, we determine whether the claims at issue are directed to a patent-ineligible concept. . . . If the answer is yes, then we next consider the elements of each claim both individually and "as an ordered combination" to determine whether additional elements "transform the nature of the claim" into a patent-eligible application. . . . The Supreme Court has described the second step of this analysis as a search for an "inventive concept"—i.e., 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."

Id. at 1375.

On January 7, 2019, the Director of the USPTO issued the "2019 Revised Patent Subject Matter Eligibility Guidance" ("Revised Guidance"), which provides further details regarding how the Patent Office analyzes patent-eligibility questions under 35 U.S.C. § 101. 84 Fed. Reg. 50–57 (Jan. 7, 2019). Under Step 2A of the Revised Guidance, the first step of the *Mayo* test, namely whether a claim is "directed to" a patent-ineligible concept, is "a two-pronged inquiry." *Id.* at 54. In prong one, we evaluate whether the

claim recites a judicial exception, such as laws of nature, natural phenomena, or abstract ideas. *Id.* If the claim recites a judicial exception, the claim is further analyzed under prong two, which requires "evaluat[ion of] whether the claim recites additional elements that integrate the exception into a practical application of that exception." *Id.* The Revised Guidance explains that, "[i]f the recited exception is integrated into a practical application of the exception, then the claim is eligible at Prong Two of . . . Step 2A [of the Revised Guidance]." *Id.*

Analyzing this case under the *Mayo* framework as articulated by the Supreme Court and as further elucidated in *Ariosa* and the Revised Guidance, we agree with Appellant that the Examiner has not established a prima facie case that the claims are patent-ineligible as being directed to a judicial exception to patent-eligible subject matter, because the claims recite additional elements that integrate any judicial exception into a practical application of that exception.

Revised Guidance Step 2A, Prong 1

Following the Revised Guidance, we first consider whether the claims recite a judicial exception. The Revised Guidance identifies three groupings of subject matter in the abstract idea exception, including "[c]ertain methods of organizing human activity," such as "fundamental economic principles or practices (including hedging, insurance, mitigating risk)" and "commercial or legal interactions (including agreements in the form of contracts; legal obligations; advertising, marketing or *sales activities or behaviors*; business relations)." 84 Fed. Reg. at 52 (emphasis added).

Claim 1, the only independent claim, recites "receiving, from an access device, terminal transaction data associated with the transaction involving a good or service," "granting access to . . . good or service after authenticating . . . the communication device," and "obtaining authorization for the transaction from an issuer." Appeal Br. 29 (Claims App.). In the context of the claims, transactions involving a good or service are sales. *See, e.g.*, Spec. 1:13–16 (describing point-of-sale (POS) terminal as an example of an access device). Thus, these steps relate to sales activities, which as discussed above are "commercial or legal interactions" that fall within "[c]ertain methods of organizing human activity" grouping of the abstract idea exception. Accordingly, we conclude that the claims recite abstract ideas.

We note that the Examiner appears to assert that the entirety of the claims recites an abstract idea. For example, the Examiner asserts that "[t]he claims recite local processing of payments for goods or services, which is an abstract idea." Ans. 6. More specifically, the Examiner asserts that claim limitations relating to "receiving . . . key . . . and a signature key . . . "; "receiving . . . data"; "generating . . . cryptogram and a signature"; "sending . . . certificate . . . "; and "sending . . . cryptogram and the signature" all recite "methods of organizing human activity" because "they recite functions that can be performed by an individual receiving and processing documents, which is a commercial interaction; and/or an individual granting access to a good or a service upon presentation of a valid token and/or ID, which is a fundamental economic practice." *Id.*

To the extent this is the Examiner's position, we are not persuaded. While certain limitations in the claims – e.g., "granting access to . . . good or

service after authenticating . . . the communication device" – may be equivalent to "granting access to a good or a service upon presentation of a valid token and/or ID," which we agree to be a fundamental economic practice and/or an abstract method of organizing human activity, the claims recite additional limitations as discussed below.

As an initial matter, the fact that a claim recites functions that *can be performed* by an individual engaging in a commercial interaction does not indicate that these functions themselves are commercial interactions and thus abstract ideas. Furthermore, we are not persuaded by the Examiner's conclusory statement that the recited limitations can be performed by an individual receiving and processing documents. For example, it is unclear how and in what circumstance such an individual would "generat[e] . . . a transaction cryptogram using the LUK as an encryption key to encrypt at least a plurality of data elements from the terminal transaction data" that can then be "verif[ied] . . . with the issuer after access to the good or service has been granted."

In response to Appellant's arguments, the Examiner asserts that, when properly construed under the broadest reasonable interpretation standard, the only claim language carrying patentable weight are the steps of:
(a) "receiving, from a remote computer by an application installed on the communication device, a limited-use key (LUK)"; (b) "receiving, from an access device, terminal transaction data"; (c) "generating, by the application of the communication device: a transaction cryptogram using the LUK as an encryption key" and "a signature using at least a part of the terminal transaction data and the signature key"; (d) "sending, to the access device, a certificate authority public key index, an issuer public key certificate, and a

communication device public key certificate"; and (e) "sending, to the access device, the transaction cryptogram and the signature." Ans. 34–35.

We are not persuaded. Assuming for the sake of argument that the only limitations having patentable weight are those recited by the Examiner, the Examiner still has not persuasively shown that all of these limitations recite a "commercial interaction" or a "fundamental economic practice," for the reasons discussed above.

Neither do we agree with the Examiner's claim construction. The Examiner asserts that claim language relating to usage limits of the limited use key or signature and/or relating to the functions of the public key index and the various public keys and certificates are "nonfunctional descriptive material" rather than "positively recited method steps" and thus carry no patentable weight. Ans. 29–30, 32–33. The Examiner similarly asserts that, in the "sending" step of claim 1, claim elements that "recit[e] what the receiving device and other recited (or unrecited) entities perform" "carr[y] no patentable weight as [they] merely represent[] the intended use of the step of 'sending'." *Id.* at 33–34. The Examiner asserts that Appellant attempts to import limitations from the Specification into the claims. *Id.* at 38.

We are not persuaded. Under the nonfunctional descriptive material doctrine, descriptive material that does not "functionally affect" the claimed system or process need not be given patentable weight. *See Ex parte Nehls*, 88 USPQ2d 1883, 1887–93 (BPAI 2008) (precedential). In *Nehls*, for example, the Board found that the particular sequence of nucleic acid recited in a system for identifying commercially important human nucleic acid fragments are nonfunctional descriptive material because "[t]here is no evidence that [the recited nucleic acid sequence(s)] affect the process of

comparing a target sequence to a database by changing the efficiency or accuracy or any other characteristic of the comparison." *Id.* at 1890.

In contrast, in this case the claim elements cited by the Examiner as "descriptive" material does functionally affect the claimed process. For example, the Specification states that "[a] 'limited-use threshold' may refer to a condition that limits the usage of a piece of information," which "may become invalid and may no longer be used" when "the limited-use threshold is exceeded or exhausted," i.e., when "the underlying condition is met." Spec. ¶ 42. The claim recites the use of the limited-use key and the signature keys to generate, respectively, a transaction cryptogram and a signature using at least part of the transaction data, which are subsequently used to authenticate the communication device and obtain authorization for the transaction from an issuer. Depending on whether the keys are associated with limited-use thresholds and whether such thresholds have been exhausted, the keys may be unable to perform the functions of authenticating the communication device and/or obtaining authorization for the transaction from an issuer.

Likewise, the claim elements that require the certificate authority public key index and the various public key certificate(s) and public key(s) to identify and/or authenticate other public key(s) and/or certificate(s) and the signature functionally affect the claimed process, because they allow the access device to verify the signature and authenticate the communication

device and subsequently to grant access to a good or service without verifying the transaction cryptogram.[8]

The Examiner asserts that, under the broadest reasonable interpretation of the claims, the claim allows for unrecited entities (rather than the communication device) to perform the steps of "receiv[ing] 'terminal transaction data' and send[ing] 'a key index, and two certificates' and 'the cryptogram and the signature'." Ans. 32. The Examiner asserts that this, "per se, is a good indication that an abstract idea is present in the claims as these steps are not even required to be performed by the recited 'machine.'" *Id.*

We are not persuaded. The Examiner cites to no authority, and we are aware of none, that a method is directed to an abstract idea merely because it does not explicitly recite the entity performing each of the recited steps.

Revised Guidance Step 2A, Prong 2

---

[8] The Examiner also asserts that, even if weight were to be given to the claim elements relating to limited usage key and signature, "it would provide a 'loose' relationship between the usage and sets of thresholds and another 'loose' relationship between the sets of thresholds and keys themselves as the claim does not recite in which manner these elements are 'associated' one to another." Ans. 29. The Examiner asserts that "the claims . . . do not limit the keys . . . to 'have different usage limits'" but only require "two keys that are each 'associated' with some set of other data and this set of other data has some sub-data that is different from the sub-data included in the set of other data 'associated' with the other key." *Id.* at 30–31. Assuming the Examiner's interpretation of these limitations is correct (i.e., that the limited-use key and signature key need not have different usage limits), the Examiner does not explain how such a construction renders these claim limitations abstract ideas.

As discussed above, although claim 1 recites an abstract idea, it would still be patent-eligible if "the claim as a whole integrates the recited judicial exception into a practical application of the exception." 84 Fed. Reg. at 53. The analysis of whether the claim integrates the judicial exception into a practical application includes "[i]dentifying . . . additional elements recited in the claim beyond the judicial exception(s)" and "evaluating those additional elements individually and in combination to determine whether they integrate the exception into a practical application." *Id.* at 54–55.

"A claim that integrates a judicial exception into a practical application will apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception." 84 Fed. Reg. at 53. An additional element may integrate an exception into a practical application if, for example, it "reflects an improvement in the functioning of a computer, or an improvement to other technology or technical field." *Id.* at 55. In contrast, "[a]n additional element . . . [that] merely includes instructions to implement an abstract idea on a computer, or merely uses a computer as a tool to perform an abstract idea" indicates that "a judicial exception has not been integrated into a practical application." *Id.*

Here, in addition to the steps that recite sales activities, claim 1 also recites (1) the communication device (a) "receiving[] from a remote computer . . . a limited-use key (LUK) . . . and a signature key" and (b) "generating . . . a transaction cryptogram using LUK as an encryption key" and "a signature using at least part of the terminal transaction data and the signature key"; (2) "sending, to the access device, a certificate authority public key index, an issuer public key certificate, and a communication device public key certificate," which respectively authenticates the issuer

public key certificate, the communication device public key certificate, and the signature; (3) "sending . . . the transaction cryptogram and the signature" to the access device; and (4) the access device (a) "authenticating . . . the communication device . . . by verifying the signature using the communication device public key" and (b) "verifying the transaction cryptogram with the issuer after access to the good or service has been granted." Appeal Br. 29 (Claims App.).

The Specification states the methods of the invention "enhance the security of a portable communication device when conducting transactions" without requiring "the use of a secure element to safeguard account credentials," because they "provision a portable communication device with limited-use account parameters that have a limited usage or lifespan" and replenish the device with new limited-use account parameters when prior parameters are exhausted. Spec. ¶ 7. Thus, "account credentials stored on a portable communication device [without a security element] becomes only a limited security risk, because stolen limited-use account parameters can at most be used for only a small number of transactions or limited monetary amount." *Id.* ¶ 25.

The Specification explains that, as compared to secure element implements, the approach of the invention "reduces the technical and commercial complexities for issuers and/or payment processors, because issuers and/or payment processors can provision account credentials and payment functionalities to a mobile application on a portable communication device without having to obtain access to a secure element through a mobile network operator." Spec. ¶ 23.

The Specification further states that the methods of the invention "include a signature key that is used to generate a signature to perform offline data authentication" and that such offline data authentication "can be useful in environments in which network connectivity is limited[] or in which there is insufficient time to obtain transaction authorization from an issuer," including by "reduc[ing] the processing time at [a] transit gate to allow more passengers to go through the transit gate in a given time frame." Spec. ¶ 58.

In short, the Specification describes the method of the claims as an improvement in the performance of electronic transactions, in that the additional elements of the claimed method recited above allow communication devices to perform such transactions with enhanced security and offline authentication, without requiring the use of a secure element. As applied to transactions using a communication device, therefore, the method of the claims represents an improvement to a technical field, and claim elements that reflect such an improvement indicate that recited judicial exception(s) have been integrated into a practical application.

In response to Appellant's arguments, the Examiner asserts that "Appellant's overgeneralization of the analysis, without specifically identifying which claim elements would transform the patent-ineligible concept into a [patent]-eligible application, is improper." Ans. 40. The Examiner asserts that the claims do not integrate the judicial exception into a practical application because "the additional elements of the claims, such as a communication device performing the steps of receiving and generating[,] merely use[] a computer as a tool to perform the abstract idea," while "[t]he

remaining steps are not even required to be performed by the 'communication device.'" *Id.*

We are not persuaded. As discussed above, the Examiner does not persuasively explain how limitations such as "generating . . . a transaction cryptogram using the LUK as an encryption key" is an abstract idea as described in the Revised Guidance. Moreover, as further noted above, we find that the Examiner's § 101 analysis is based on erroneous claim construction. Thus, we do not agree that the additional elements of the claim "merely use[] a computer as a tool to perform [an] abstract idea." Likewise, as also discussed above, we are not aware of any authority, and none are cited by the Examiner, that suggests a claimed step is necessarily an abstract idea if not explicitly described as being performed by a single recited machine.

The Examiner asserts that "[n]othing in the claim language would lead one of ordinary skill to convey that an enhancement in security is being provided" and that Appellant is inconsistent in arguing that "the claims both 'enhance the security' and 'reduces the technical complexities' (i.e., by not requiring a tamper-proof hardware[)]." Ans. 36–37. The Examiner asserts that "the data contents recited by the claims has no impact whatsoever in the security of the device," that "Appellant falls short of asserting that the solution provided by the claims enhances security when compared to conventional ways (i.e. a [']secure element')," and that "the gain in security, from the communications device perspective, is [non-]existent" because "storing a key outside of the confines of a secure element per se is less secure than storing the same key inside the secure element, regardless of the key contents." *Id.* Finally, the Examiner asserts that any "reduc[tion of]

processing time by deferring verification of the transaction cryptogram without sacrificing security" is an "intended result . . . far outside the scope of the claim" and that "[t]he gain obtained by a device outside of the scope of the claim shouldn't impact . . . the analysis of the subject matter of the claims at issue." Ans. 39.

We are not persuaded. While not dispositive, and without construing the preamble as limiting, we note that the preamble of claim 1 recites "[a] method for enhancing security of a communication device when conducting a transaction offline using the communication device." Appeal Br. 29 (Claims App.).

Moreover, while the element(s) that confer the improvement must be in the claims, we do not agree that the claims must recite what the improvement is. As an example, our reviewing court found in *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016) that claims to a self-referential table for a computer database are directed to an improvement of an existing technology, based on the *specification*'s teachings that, as compared to traditional databases, the claimed invention "does not require a programmer to preconfigure a structure to which a user must adapt data entry" and "achieves other benefits . . . such as increased flexibility, faster search times, and smaller memory requirements." *Id.* at 1337. Finally, we note that a "reduc[tion of] processing time . . . without sacrificing security" is, in fact, an improvement to a method of "conducting a transaction . . . using [a] communication device" rather than "[a] gain obtained by a device outside of the scope of the claim," as the Examiner asserts.

Nor are we persuaded by the Examiner's conclusory statements that the invention of the claims do not in fact provide an improvement over

conventional technology. A claimed invention may be directed to an improvement over conventional technology in one aspect, even if it is not superior to conventional technology in all aspects. For this reason, we also see no inconsistency in Appellant simultaneously arguing that the claims both reduce technical complexity (by reducing the need for a "secure element") and enhance security (by using limited-use keys and signature keys associated with limited-use thresholds).

Accordingly, we conclude that the claims are patent eligible and reverse the Examiner's rejection of the claims under 35 U.S.C. § 101 as directed to a judicial exception without significantly more.

B. Indefiniteness rejection (claims 1, 3, 4, 22–25, 27–30, and 33–41)

1. Issue

Claim 1 recites among other things:

> generating, by the application of the communication device:
> a transaction cryptogram using the LUK as an encryption key to encrypt at least a plurality of data elements from the terminal transaction data; and
> *a signature* using at least a part of the terminal transaction data and the signature key;
> . . .
> sending, to the access device, the transaction cryptogram and the signature, the access device authenticating the application of the communication device *without requiring network connectivity* by verifying the signature using the communication device public key, *granting access to the good or service after authenticating the application of the communication device and prior to verification of the transaction cryptogram, and obtaining authorization for the transaction from an issuer* by verifying the transaction cryptogram *with the issuer* after access to the good or service has been granted.

Appeal Br. 29 (Claims App.) (emphasis added).

The Examiner asserts that "it is unclear whether 'and a signature . . . '" in the claim limitation, "generating . . . a transaction cryptogram . . . and a signature" refers to "the step of 'generating' . . . or . . . the intended use of the encryption key." Ans. 11–12.

The Examiner also asserts that, since network connectivity is not required, the step of "sending . . . the transaction cryptogram and the signature" is unclear. Ans. 10. The Examiner asserts that "[c]laim 1 . . . attempts to limit the step of 'sending, to the access device, the transaction cryptogram and the signature' by actions performed by the receiving device," but "the scope of claim is unclear" because the Specification states that "the steps performed by the access device are not part of the claimed steps performed by the communication device." Ans. 10–11.

The Examiner further asserts that "it is unclear whether the steps of 'granting . . . and obtaining" recited in claim 1 are performed by the communications device or the access device and that "it is unclear which entity or entities performs the 'verifying the transaction cryptogram with the issuer' (i.e. communications device, access device, issuer or a combination of these entities)." Ans. 12.

Appellant contends that "the claim language reasonably defines the metes and bounds of the claims." Appeal Br. 19.

The issue with respect to this rejection is whether a preponderance of evidence supports the Examiner's conclusion that the claims are indefinite.

2. Analysis

We agree with Appellant that the Examiner has not established a prima facie case that the claims are indefinite.

As to the Examiner's assertion that, since network connectivity is not required, the step of "sending . . . the transaction cryptogram and the signature" to the access device is unclear, Ans. 10, we note that the claim requires the access device to authenticate the application of the communication device without requiring network connectivity, but does not require that the transaction cryptogram and the signature to be sent without requiring network connectivity.

In response to Appellant's similar argument that the claim does not require that "the access device receives the transaction cryptogram and signature without requiring network connectivity," Appeal Br. 16, the Examiner states that "Examiner agrees that the claims do not require the 'receiving' step, and for this specific reason the claims do not require the access device to be in possession of the data sent by the required method step of sending" and that "[t]his remark by Appellant further illustrates the claim scope issue identified by the subsequent rejection as discussed below." Ans. 43–44.

We are not persuaded. The Examiner's response does not address Appellant's point that, given the claim does not recite that the transaction cryptogram and signature be sent to the access device without requiring network connectivity, there is no inconsistency in the claim both requiring the cryptogram and signature to be sent to the access device and that the access device authenticates the application of the communication device without requiring network connectivity. As to the Examiner's point, we note that the claim requires a step of "sending, to the access device, the transaction cryptogram and the signature" and a step in which "the access device authenticat[e] the application of the communication device without

requiring network connectivity by verifying the signature using the communication device public key." Thus, the access device needs to at least be in possession of the signature to the extent of being able to verify it using the communication device public key.

We also note that, assuming that the claim requires the transaction cryptogram and signature to be sent without requiring network connectivity, a skilled artisan would understand that this may be accomplished through the use of other contact or contactless mode of operation that do not require network connectivity. Spec. 8:25–9:4 (explaining that "[a]n access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a portable communication device," including using optical scanners, bar code readers, or magnetic strip readers interact with a portable communication device).

The Examiner acknowledges Appellant's argument that "the 'connectivity' necessary for the sending steps" is different than the recited "network connectivity." Ans. 41. The Examiner asserts, however, that Appellant's argument is problematic because (1) according to Appellant's interpretation, the claims are attempting to improperly "limit the step of 'sending,' by an undisclosed device/entity by reciting structural limitations of the receiving device (network characteristics of the access device)"; and (2) it is unclear by the claim language "which entity does not 'require' network connectivity, the undisclosed sending device, the receiving (access)

device, or both," and further unclear whether "without requiring network connectivity" refers to structural elements or actions. *Id.* at 42.[9]

We are not persuaded. We agree with Appellant that the language of the claim makes it clear that "without requiring network connectivity" refers to the step of "authenticating the application of the communication device . . . by verifying the signature suing the communication device public key." Reply Br. 11–12.

As to the Examiner's assertion that the scope of the claims are unclear because claim 1 "attempts to limit the step of 'sending, to the access device, the transaction cryptogram and the signature' by actions performed by the receiving device," even though such actions are not "part of the claimed

---

[9] Appellant contends that, even if the transaction cryptogram and signature must be sent to the access device without requiring network connectivity, such a limitation can be satisfied by sending the cryptogam and signature "using a local communication technology" such as "NFC, Bluetooth, etc." because such local communication channel does not require the access device to have network connectivity to access networks 192 and 194. Appeal Br. 17. The Examiner asserts that a skilled artisan would understand that "a 'local communication technology' also provides 'network connectivity' between two devices," because "[i]t is well known in the art that the minimal configuration of a client/server network or architecture has a server component and a client component requiring 'network connectivity' between them." Ans. 43. We acknowledge the Examiner's apparent position that the term "network" itself may be indefinite. However, and without determining whether the term is in fact indefinite, we find that, to the extent the Examiner's rejection is based on the position that the term "network" itself is indefinite because it could be understood to include or exclude connections through technologies such as, e.g., Bluetooth or near field communication, the Examiner has not established a prima facie case of indefiniteness because the Examiner has not attempted to construe the term in light of the Specification.

steps performed by the communication device," Ans. 10–11, we are unpersuaded. The Examiner cites no authority, and we are aware of none, that a method claim may only recite steps performed by a single component.

The Examiner asserts in response to Appellant's arguments that,

> [f]rom an infringement perspective, one of ordinary skill in the art would not be able to reasonably convey where infringement of the "sending" step occurs: at the sending step? at the authenticating step? at the undisclosed sending device? at the (receiving) access device? at the nonrequired interaction between devices? The claim further recites "verifying with . . . with [sic] the issuer . . .". [D]oes the issuer further modifies the method step of sending or not? Can the issuer infringe on the claimed sending step?

Ans. 44.

We are not persuaded. The limitation of "sending, to the access device, the transaction cryptogram and the signature" is met when the sending device sends the recited data to the access device, i.e., at the sending step, regardless of whether or not an accused method also meets the authenticating and verifying steps. The mere fact that different steps of a method claim are accomplished by different devices do not render the claim indefinite.

We are likewise unpersuaded by the Examiner's assertion that "it is unclear whether 'and a signature . . . '" in the claim limitation, "generating . . . a transaction cryptogram . . . and a signature," refers to "the step of 'generating' . . . or . . . the intended use of the encryption key." Ans. 11–12. We agree with Appellant that the grammar, formatting, and punctuation of the claim make clear that the signature is generated by the application of the communication device, rather than being encrypted by the LUK encryption key. Appeal Br. 18. Furthermore, "during examination proceedings, claims

are given their broadest reasonable interpretation *consistent with the specification*." *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000). The Examiner has not persuasively explained how the alternative construction of the claim the Examiner offers – interpreting "signature" as an "intended result" of the encryption key (i.e., requiring the use of the limited use key as an encryption key to encrypt a signature) – is consistent with the Specification.

The Examiner asserts that "[w]hile the formatting presented by Appellant in the claim at issue would lead one of ordinary skill in the art that the generating step comprises both a cryptogram and a signature, there is no guarantee that this formatting is going to be preserved through future rounds of prosecution and an eventual allowance," and is further "unpersuaded that the indentations and punctuations . . . are sufficient to resolve the clarity issue presented by the claim language." Ans. 46.

We are not persuaded. As Appellant notes, the Examiner appears to concede that the claim as currently drafted and formatted is definite, because "the formatting . . . in the claim at issue would lead one of ordinary skill in the art [to understand] that the generating step comprises both a cryptogram and a signature." Appeal Br. 15; Ans. 46. Rejections should be based on the claim as it exists, not as it may be amended. Neither has Examiner cited any authority – and we are unaware of any – that formatting and punctuation of a claim should not be considered in an indefiniteness rejection.

The Examiner further asserts that "the contents of the Specification cannot resolve the issue that the claim language does not particularly points out and distinctly claims the subject matter which Appellant regards as his invention." Ans. 46–47. We are not persuaded. As discussed above, during

prosecution a claim is construed under the broadest reasonable interpretation *consistent with the specification*. Thus, although care must be taken not to import limitations into the claim, the specification nevertheless has a role in evaluating whether a claim is indefinite.

The Examiner next asserts that it is unclear which device (the communications device, the access device, the issuer, and/or a combination) is performing the steps of "granting access to the good or service" and "obtaining authorization for the transaction from an issuer by verifying the transaction cryptogram with the issuer" recited in claim 1. Ans. 12. The Examiner also asserts that it is unclear whether "the 'sending' step, performed by an undisclosed device, [is] being modified by the language 'verifying' . . . i.e. [whether] the undisclosed device that performs the sending [is] the same as the device that performs 'verifying' or [if] verifying is performed by some other entity/device." Ans. 48–49.

We agree with Appellant that the language of the claim, when read in light of the Specification, makes it clear that it is the access device that "authenticat[es] the application of the communication device . . . , grant[s] access to the good or service after authenticating . . . , and obtain[s] authorization for the transaction from an issuer." Appeal Br. 18.

In response to Appellant's arguments, the Examiner agrees that "which entity is performing which function goes to the breadth of the claim rather than indefiniteness," but asserts that

> the step of "sending", the steps of "granting" and "obtaining" need to be at least identified as being performed by the same (undisclosed) entity that performs the "sending" step or by any other recited or unrecited entity/device, as this significantly impacts in the construction of the claimed step of "sending", performed broadly by an undisclosed device or entity (i.e. are

> the steps of sending, granting, and obtaining being performed by the same undisclosed device or not?). By opting to leave these functions disconnected from the sending step, as presented, one of ordinary skill in the art would not be able to reasonably convey what specifically the "sending" step comprises.

Ans. 47–48.[10]

We are not persuaded. We find that, under the broadest reasonable interpretation standard *consistent with the specification*, a skilled artisan would understand that the granting and obtaining steps are performed by the access device.[11]

C. Obviousness rejections (claims 1, 3, 4, 22–25, 27–30, and 33–41)

1. Issue

The same issue is dispositive for all of the obviousness rejections; we therefore consider them together. The Examiner finds that the combination

---

[10] The Examiner notes that claim 1 recites "verifying the signature using the communicating device public key" and that "communicating device" lacks antecedent basis. Ans. 47–48. However, the Examiner does not appear to have based any rejection on such lack; thus, we do not address this issue in our opinion.

[11] Appellant argues that "which entity is performing which function goes to the breadth of the claim rather than indefiniteness." Appeal Br. 18. We do not agree with this argument to the extent the claim may be interpreted to either (1) require the access device to perform the steps of granting and obtaining or (2) allow any device to perform the steps of granting and obtaining, the claim may be invalid. *Ex parte Miyazaki*, 2008 WL 5105055, at *5 (BPAI 2008) (precedential) ("[I]f a claim is amenable to two or more plausible claim constructions, the USPTO is justified in requiring the applicant to more precisely define the metes and bounds of the claimed invention by holding the claim unpatentable under 35 U.S.C. § 112, second paragraph, as indefinite.").

of Saxena and Smets discloses many of the limitations of claim 1, but does not disclose, among other things:

> [receiving a] limited-use key (LUK) . . . associated with a first set of one or more limited-use thresholds that limits usage of the LUK[, and] a signature key that is associated with a second set of one or more limited-use thresholds that limits usage of the signature key, wherein the first set of one or more limited-use thresholds includes a first limited-use threshold that is different than a second limited-use threshold included in the second set of one or more limited-use thresholds.

Ans. 16.

However, the Examiner finds that Radu discloses a method of implementing an electronic card payment system comprising a limited-use key associated with a first set of limited-use threshold(s) that limits the use of the key and a signature key associated with a second set of limited-use threshold(s) that limits the usage of the key, wherein at least one of the first limited-use threshold(s) is different than one of the second limited-use threshold(s). Ans. 17. The Examiner concludes that it would have been obvious to a skilled artisan to "incorporate the offline combined dynamic data authentication/Application cryptogram as disclosed by Radu in the method of [Saxena and Smets], the motivation being to enable anyone with an authentic copy of the ICC public key, especially the terminal at the point of service, to verify the application cryptogram." *Id.* at 18.

Appellant contends that, because Radu's ICC private key, which the Examiner cites as the limited-use key, and its private signing key, which the Examiner cites as the signature key, refer to the same key, Radu (and therefore the cited combination of prior art) does not teach a method

comprising "receiving both: (1) a LUK; and (2) a signature key," as recited in the first step of claim 1. Appeal Br. 19.

Appellant further contends that,

> even if one is to assume that the ICC private key and the private signing key KS_{card} are referring to different keys, the combination of Radu and the other cited references does not describe a communication device as receiving both the ICC private key and KS_{card}, and using the ICC private key and KS_{card} to generate a transaction cryptogram and a signature, respectively, for the same transaction. Moreover, nothing in Radu indicates that the ICC private key has a limited-use threshold that is different than a limited-use threshold of the private signing key KS_{card}. As such, even under the unfounded assumption that the ICC private key and KS_{card} are different keys, Radu still fails to teach the attributes and functions of the LUK and signature key as claimed.

Id. at 20.

Finally, Appellant contends that the cited prior art combination does not teach the limitation of "the access device . . . obtaining authorization for the transaction from an issuer by verifying the transaction cryptogram with the issuer after access to the good or service has been granted," because "the cryptogram being generated [in Radu] is the digital signature, and there is no separate and distinct transaction cryptogram being sent to the access device in addition to the signature." Appeal Br. 20–21. Similarly, Appellant contends that Radu does not describe a scenario where the communication device generates both: (1) "a signature . . . locally verified by the access device to grant access . . . ; and (2) a transaction cryptogram . . . verified with an issuer after access . . . has been granted." *Id.* at 21.

The issue with respect to the obviousness rejections is whether a preponderance of the evidence of record supports the Examiner's conclusion

that claim 1, the only independent claim, is obvious over the combination of Saxena, Smets, and Radu.

2. *Analysis*

We agree with Appellant that the Examiner has not established a prima facie case that claim 1 is obvious over Saxena, Smets, and Radu, at least because the Examiner has not established a prima facie case that the cited combination of prior art suggests both a limited-use key and a signature key, associated with, respectively, a first and second set of one or more limited-use thresholds, wherein the first set includes a first limited-use threshold that is different than a second limited-use threshold included in the second set, as required by the first step of claim 1.

The Examiner appears to point to private key 527 and shared secret 525 in Saxena as the limited-use key. Ans. 13, 52. However, while Saxena teaches the use of a one-time credit card number, which is associated with a limited-use threshold, the passages in Saxena cited by the Examiner does not suggest that private key 527 and shared secret 525 are associated with a limited-use threshold (i.e., a condition that limits their usage).

For example, with respect to the shared secret 525, the passage of Saxena cited by the Examiner states only that:

> [t]he one-time credit card number application **515** can implement a shared secret **525,** which is available at both the issuer device **520** and the customer device **510**. In practice, the shared secret **525** can be embedded into the application **515** to avoid the customer tampering with it. Thus, the application **515** can be a personalized software program for a specific individual (e.g., the customer) that has a shared secret **525** between the issuer and the respective individual. The shared secret can be embedded into the application **515** (e.g., in the form of executables). . . .

> . . .
> The shared secret **525** stored at the issuer device **520** can be associated with an identity of the customer or customer device **510** so that it can be retrieved for use during purchase transactions involving the customer or customer device **510.**

Saxena ¶¶ 90–92.

With respect to private key 527, the passage of Saxena cited by the Examiner states only that, "[t]o support . . . digital signature technologies," "public key/private key cryptographic techniques can be implemented" wherein "the customer device **510** has access to a private key **527** (e.g., stored on the customer device **510**), and a public key **577** of the customer is published (e.g., made available to others, including the issuer)." Saxena ¶ 91.

In response to Appellant's arguments, the Examiner first asserts that, under the broadest reasonable interpretation of the claims, "[t]he description of the keys or the loose 'association' to some other data does not further limit the keys in any manner," and the rejection is proper because "[t]he combination of references recites receiving two keys (LUK and signature key)." Ans. 51.

We are not persuaded. In general, "every limitation positively recited in a claim must be given effect." *In re Wilder*, 429 F.2d 447, 450 (CCPA 1970). The Examiner has not provided any persuasive reason – e.g., that the claim elements are merely the intended use or result of other positively recited limitations – why limitations relating to the limited use threshold should be given no patentable weight.

The Examiner next asserts, in response to Appellant's argument that Radu does not disclose both a LUK and a signature key as recited in the claim, that LUK is anticipated by Saxena, including by disclosures in

Saxena's paragraph 52, while the signature key is disclosed by Radu. Ans. 50–51.

We are not persuaded. As discussed above, the passages of Saxena initially cited by the Examiner does not teach that either shared secret 525 or private key 527 meets the limitation of a limited-use key *that is associated with a first set of one or more limited-use thresholds that limits usage of the LUK*. Neither do we find Saxena's paragraph 52 to disclose such a key. In particular, paragraph 52 states:

> Credit card security codes can be generated according to issuer convention, such as encrypting card information (e.g., credit card number, expiration date, and service code) with an encryption key. The expiration date can be set for the current month or some other date. Alternatively, a special card security code or codes can be used for one-time credit card numbers.

Saxena ¶ 52.

We agree that the credit card security codes may be associated with one or more limited-use thresholds, e.g., an expiration date and/or the number of times the code may be used (for codes used for one-time credit card numbers). However, the Examiner does not persuasively explain how such codes are used as a *key* (e.g., to encrypt at least a plurality of data elements from the terminal transaction data to generate a transaction cryptogram, as required later in claim 1). To the extent the Examiner is relying on the "encryption key" mentioned in paragraph 52 of Saxena as the LUK recited in claim 1, the Examiner has not persuasively explained how such encryption key encrypt "at least a plurality of data elements from the terminal transaction data" to generate a transaction cryptogram, as recited in claim 1.

The Examiner further asserts that, in addition to Saxena, Radu also discloses "characteristics of the LUK similar to the language describing the data" and discloses receiving a distinct LUK. Ans. 50, 52.

We are not persuaded. The Examiner appears to cite the integrated circuit card (ICC) private key disclosed in Radu as the "limited-used key (LUK) . . . associated with a first set of one or more limited-use thresholds that limits usage of the LUK" and the "private signing key" as the signature key. Ans. 17, 52. However, Radu describes the ICC private key as being used to "produce a signature s on the terminal dynamic data and other data from the ICC" and further teaches that, when the ICC private key computes an application cryptogram as a digital signature, "the dynamic authentication of the card is performed with a digital signature-based [dynamic data authentication (DDA)]," discussed in Section D.7.2 of Appendix D. Radu 167, Fig. 6.6, 212. Section D.7.2 of Appendix D then discusses using a private signing key to compute a dynamic authenticator as a digital signature. *Id.* at 396.

Thus, the ICC private key and the private signing key appear to refer to the same key. In appropriate circumstances, a single element in the reference could suggest two elements recited in a claim. *Cf. Powell v. Home Depot U.S.A., Inc.*, 663 F.3d 1221, 1231 (Fed. Cir. 2011) (finding claim reciting "cutting box interior in fluid communication with dust collection structure for collecting dust" to be infringed by accused product in which the rear portion of the cutting box serves to collect sawdust and woodchips). In this case, however, claim 1 also recites that the set of one or more limited-use thresholds that limits usage of LUK includes a first limited-use threshold that is different than a second limited-use threshold included in the second

set of threshold that limits usage of the signature key. The Examiner appears to cite to the same limited-use threshold – i.e., public key certificate expiration date – for both the ICC private key and the private signing key. Ans. 23, 52. Thus, the Examiner has not persuasively shown that the ICC private key and the private signing key in Radu are two separate keys having, respectively, a first and second set of one or more limited-use thresholds that limits their usage, "wherein the first set of one or more limited-use thresholds includes a first limited-use threshold that is different than a second limited-use threshold included in the second set of one or more limited-use thresholds."

We note that the Examiner asserts that the claims "do not limit the keys themselves to 'have different usage limits.'" Ans. 50. In contrast, Appellant contends that "the claim language . . . requires the two sets [of limited-use thresholds] to have at least one limited-use threshold that is different." Reply Br. 16. We are not persuaded that either position is entirely correct. The claim requires that "the first set of one or more limited-use thresholds includes a first limited-use threshold that is different than a second limited-use threshold included in the second set of one or more limited-use thresholds." Where the two sets each include multiple limited-use thresholds, the sets arguably meet the claim limitation even if they have the same thresholds (e.g., A, B, and C), because the first set includes a first limited-use threshold (i.e., A) that is different than a second limited-use threshold included in the second set (i.e., B or C). We need not decide this claim construction issue, however, because where the sets only contain one limited-use threshold (e.g., the public certificate expiration date), as they do

in the Examiner's rejection, they must contain different limited-use thresholds in order to meet the claim limitation.

Accordingly, we reverse the Examiner's rejection of independent claim 1 as obvious over the combination of Saxena, Smets, and Radu. We likewise reverse the rejection of claims 3, 4, 22, 23, 25, 27–29, and 33–41, which depend directly or indirectly from claim 1, for the same reasons discussed with respect to claim 1. *In re Fine*, 837 F.2d 1071, 1076 (Fed. Cir. 1988) ("Dependent claims are nonobvious under section 103 if the independent claims from which they depend are nonobvious."). Examiner rejects claim 24 and 30 over the combination of Saxena, Smets, Radu, and, respectively, Verhoorn and Ginter. The Examiner appears to cite Verhoorn and Ginter only for the additional dependent claim limitations. Accordingly, we also reverse the rejections of claims 24 and 30 for the same reasons as discussed with respect to claim 1.

CONCLUSION

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)/ Basis	Affirmed	Reversed
1, 3, 4, 22–25, 27–30, 33–41	101	Eligibility		1, 3, 4, 22–25, 27–30, 33–41
1, 3, 4, 22–25, 27–30, 33–41	112(b) or 112 (pre-AIA), second paragraph	Indefiniteness		1, 3, 4, 22–25, 27–30, 33–41
1, 3, 4, 22, 23, 25, 27–29, 33–41	103	Saxena, Smets, Radu		1, 3, 4, 22, 23, 25, 27–29, 33–41
24	103	Saxena, Smets, Radu,		24

Claims Rejected	35 U.S.C. §	Reference(s)/ Basis	Affirmed	Reversed
		Verhoorn		
30	103	Saxena, Smets, Radu, Ginter		30
Overall Outcome				1, 3, 4, 22–25, 27–30, 33–41

REVERSED