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.
16/007,945	06/13/2018	John Daniel Beatty	CLVRP018	1049

146691 7590 08/19/2020
Daylight Law, P.C.
626 Jefferson Avenue
Suite 7
Redwood City, CA 94063

EXAMINER	
OUSSIR, EL MEHDI	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
08/19/2020	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):

diane@daylightlaw.com
eofficeaction@appcoll.com
eric@daylightlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JOHN DANIEL BEATTY, BRIAN JEREMIAH MURRAY,
NILENDU MISRA, and NICHOLAS POSNER

Appeal 2020-002393
Application 16/007,945
Technology Center 3600

Before JEFFREY N. FREDMAN, DEBORAH KATZ, and JOHN G. NEW, *Administrative Patent Judges*.

KATZ, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[1] seeks our review,[2] under 35 U.S.C. § 134(a), of the Examiner's decision to reject claims 1–15 (Appeal Br. 6–7.) 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 Clover Network, Inc. (*See* Appeal Br. 3.)

[2] We consider the Specification dated November 27, 2018 ("Spec."), Final Office Action issued March 21, 2019 ("Final Act."), the Appeal Brief filed August 21, 2019 ("Appeal Br."), the Examiner's Answer issued December 4, 2019 ("Ans."), and the Reply Brief filed February 3, 2020 ("Reply Br.").

INTRODUCTION

Appellant's Specification provides methods for utilizing and managing tokens in a payment system. (Spec. ¶ 7.) Point of sale (POS) systems may obtain a token as a proxy for a payment account number, e.g., credit card or debit card number. (*Id.* ¶ 2.) The token may be stored in a merchant's POS system without placing the payment account number at risk of theft. (*See id.*) To obtain a token, the POS system sends an encrypted payment account number to a tokenization service, which decrypts the account number and returns a token to the POS system. (*Id.* ¶ 3.) A multi-pay token is a specific type of token that allows a merchant to retain the token for future transactions by the same customer, without re-entering payment account information. (*Id.* ¶ 6.)

The Specification describes a process of "salting" a token by adding data to the token before encrypting the token. (Spec. ¶ 11.) The data "salt" may include meaningful data associated with the token, such as, merchant identifier, store identifier, or commerce channel, e.g., physical retail, online, mail order. (*Id.*) The POS system may include a secure processor for encrypting the salted token. (*Id.* ¶¶ 12, 40.) The secure processor may also map the encrypted salted token to the payment account number and store the map and encrypted salted token in a memory. (*Id.*)

Appellant's claim 1 recites:

> A method comprising:
>
> transmitting a tokenization request with an encrypted payment account number from a point of sale device to a tokenization service;
>
> receiving a token from the tokenization service in response to the tokenization request, wherein the token is

> a tokenized version of the encrypted payment account number;
>
> salting the token with data to produce a salted token;
>
> encrypting the salted token using a secure processor on the point of sale device;
>
> mapping the encrypted salted token to the payment account number in a map,
>
> wherein the payment account number is mapped using at least a portion of the payment account number; and
>
> storing the map and the encrypted salted token in a memory on the secure processor on the point of sale device.

(Appeal Br. 26.)

The Examiner rejects the claims as follows[3]:

Claims Rejected	35 U.S.C. §	Basis	Final Office Action
3	112(a)	Written description	5–6
1–15	112(b)	Indefinite	6–7
1–3, 5, 6, 10–14	103	McGuire,[4] Cronic[5]	7–13
4, 7, 8, 15	103	McGuire, Cronic, Ivey[6]	13–16

[3] The Examiner withdrew the rejection of claim 3 under 35 U.S.C. § 112(b) as being indefinite. (Ans. 3.)

[4] McGuire et al., U.S. Patent Application Publication 2010/0257612 A1, published October 7, 2010.

[5] Cronic et al., U.S. Patent Application Publication 2013/0191289 A1, published July 25, 2013.

[6] Ivey et al., U.S. Patent Application Publication 2016/0005029 A1, published January 7, 2016.

Claims Rejected	35 U.S.C. §	Basis	Final Office Action
9	103	McGuire, Cronic, Ivey, Park[7]	16–17

ANALYSIS

Claims 1–15 rejected under 35 U.S.C. § 112(b) as indefinite

The Examiner rejects claims 1–15 under 35 U.S.C. § 112(b) as indefinite. (Ans. 7.) The Examiner finds that the limitation "storing the map and the encrypted salted token in a memory on the secure processor of the point of sale device" is indefinite because "[a] processor or secure processor is different and distinct from a memory." (*Id.*, emphasis omitted) The Examiner finds "it is not known whether the map and the encrypted salted token are stored in the memory or whether they are stored in a memory on a secure processor." (*Id.*)

Appellant argues that the claimed secure processor "refers to a piece of hardware which includes a secure memory for storing cryptographic keys and other information in memory." (Appeal Br. 15.) Appellant argues the Specification discloses a hardware security module ("HSM") as an example of a secure processor. (*Id.* at 16, citing Spec. ¶ 40.)

We are persuaded by Appellant's argument because the Specification describes a secure processor including a memory. For example, the Specification describes storing encrypted tokens using a secure element on the POS device. (*See* Spec. ¶¶ 12, 40.) The secure element may be a secure

[7] Park et al., U.S. Patent Application Publication 2016/0253651 A1, published September 1, 2016.

processor, such as an HSM, which includes a memory as explained by Appellant. (*Id.* ¶ 40.) A secure processor is not a generic processor distinct from a memory. Accordingly, we do not sustain the Examiner's rejection.

Claim 3 rejected under 35 U.S.C. § 112(a) as lacking written description

The Examiner rejects claim 3 under 35 U.S.C. § 112(a) as lacking written description. (Ans. 3.) The Examiner finds the Specification does not support the limitation of "restricting the initiation of the second payment on the second point of sale device: (i) without decrypting the salted encrypted token; and (ii) based on the data." (*Id.* at 5, emphasis omitted) The Examiner finds that the Specification does not describe how to restrict initiation of a second payment without decrypting the salted encryption token, as recited by claim 3, when claim 1 "recites that the entire salted token is encrypted." (*Id.*)

Appellant argues that the Specification describes using a format preserving algorithm ("FPA") for obtaining data salt values without decrypting the "whole encrypted token." (Appeal Br. 12, citing Spec. ¶ 11.) For example, the FPA may read values directly by inspecting the salted encrypted token, or excise and decrypt only a portion of the salted encrypted token. (Spec. ¶ 11.) The FPA may append the data salt in a format preserving encrypted ("FPE") string, so that the data salt can be located without decrypting the token map. (*See id.* ¶ 44.) Appellant argues that the appended data may add values recognized throughout the POS network (Appeal Br. 12), so that "if the data that restricted use of the token was accessible via direct analysis of an FPE salted encrypted token, failure at the first authorization level would prevent the needless exposure of the token through decryption for a transaction that was already denied." (Spec. ¶ 47.)

We are persuaded that the original Specification provides written description support for claim 3. We begin with the language of the claim. Contrary to the Examiner's finding, claim 1 does not appear to recite encrypting the "entire salted token." (*See* Appeal Br. 26.) Accordingly, claim 3 does not appear to conflict with claim 1.

The Specification describes restricting a second use of a token based on a previous denial without decrypting the token. (*See* Spec. ¶ 47.) Original claim 6 recites a method similar to claim 3, further including the limitation of evaluating a field of a salted encrypted token without decrypting the token. (*See* Specification dated June 13, 2018, Claims App'x. 2.) "The claims as filed are part of the specification, and may provide or contribute to compliance with § 112." *Hyatt v. Boone*, 146 F.3d 1348, 1352 (Fed. Cir. 1998). Although the original Specification does not describe claim 3 exactly, we find that persons of ordinary skill in the art would recognize from the disclosure that Appellant invented a process including restricting the initiation of a second payment without decrypting the salted encrypted token. *See In re Wertheim*, 541 F.2d 257, 262 (CCPA 1976). Accordingly, we do not sustain the Examiner's rejection.

Claims 1–15 rejected under 35 U.S.C. § 103

The Examiner rejects claims 1–3, 5, 6, and 10–14 under 35 U.S.C. § 103 as obvious over McGuire and Cronic. Because the Examiner applies the combination of McGuire and Cronic to reject all of the claims, our analysis of claim 1 applies to all of the claims.

The Examiner finds McGuire teaches tokenizing an encrypted payment account number and salting the token with data to produce a salted token. (Final Act. 8, citing McGuire Abstr., ¶¶ 51, 56, 90, Fig. 1.) The Examiner finds McGuire teaches encrypting the salted token using a secure processor on the point of sale device and mapping the encrypted salted token to the payment account number in a map. (*Id.* at 8–9, citing McGuire Abstr., ¶¶ 3, 35, 44–45, 56, Fig. 1, 3–5.) The Examiner acknowledges that McGuire does not explicitly teach storing the map and encrypted salted token in a memory on a secure processor, but finds that Cronic teaches the missing limitation. (*Id.* at 9, citing Cronic ¶¶ 3, 48, 87, 98, 199.)

Appellant argues that McGuire does not teach the limitation of "mapping the encrypted salted token to the payment account number in a map, wherein the payment account number is mapped using at least a portion of the payment account number." (Reply Br. 5.) Specifically, Appellant argues that: (1) McGuire does not teach encrypting tokens; (2) McGuire's map includes unencrypted tokens; and (3) McGuire's transmitting a temporarily encrypted token through a secure socket layer does not involve mapping an encrypted salted token in map. (*See id.* at 5–6.) Appellant argues that McGuire teaches mapping a relationship between an account number and an unencrypted token. (Appeal Br. 20.)

We are persuaded by Appellant's argument. McGuire teaches a POS device (input module 140) that transmits a payment-card number to a tokenizer, "which returns a token for input module 140 to send to application module 150 along with other transaction data." (McGuire ¶ 51.) McGuire does not describe the "other transaction data," nor combining the other transaction data with the token, i.e., salting the token. (*See id.*) McGuire further teaches a look-up table with encrypted payment card numbers matching corresponding tokens. (*See id.* ¶¶ 32, 35.) McGuire does not teach encrypting the tokens nor storing and mapping encrypted tokens. (*See id.*) Because McGuire does not appear to teach at least the limitation of mapping an encrypted salted token to a payment account number in a map, we do not sustain the Examiner's rejections.

CONCLUSION

Upon consideration of the record and for the reasons given, we reverse the Examiner's rejections.

In summary:

Claims Rejected	**35 U.S.C. §**	**Reference(s)/Basis**	**Affirmed**	**Reversed**
3	112(a)	Written description		3
1–15	112(b)	Indefinite		1–15
1–3, 5, 6, 10–14	103	McGuire, Cronic		1–3, 5, 6, 10–14
4, 7, 8, 15	103	McGuire, Cronic, Ivey		4, 7, 8, 15
9	103	McGuire, Cronic, Ivey, Park		9
Overall Outcome				**1–15**

REVERSED