

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	79314.5
		Application Number	
Title of Invention	METHODS, DEVICES, AND SYSTEMS FOR SECURE PROVISIONING, TRANSMISSION, AND AUTHENTICATION OF PAYMENT DATA		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2(Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	--

Inventor Information:

Inventor 1						Remove	
Legal Name							
Prefix	Given Name	Middle Name		Family Name		Suffix	
	Enyang			Huang			
Residence Information (Select One)		☒ US Residency		☐ Non US Residency		☐ Active US Military Service	
City	Andover	State/Province	MA	Country of Residence	US		
Mailing Address of Inventor:							
Address 1		4 Gregory Circle					
Address 2							
City	Andover	State/Province		MA			
Postal Code	01810	Country	i	US			
Inventor 2						Remove	
Legal Name							
Prefix	Given Name	Middle Name		Family Name		Suffix	
	William	Wang		Graylin			
Residence Information (Select One)		☒ US Residency		☐ Non US Residency		☐ Active US Military Service	
City	Winchester	State/Province	MA	Country of Residence	US		
Mailing Address of Inventor:							
Address 1		14 Robinson Park					
Address 2							
City	Winchester	State/Province		MA			
Postal Code	01890	Country	i	US			
Inventor 3						Remove	
Legal Name							
Prefix	Given Name	Middle Name		Family Name		Suffix	
	George			Wallner			

Application Data Sheet 37 CFR 1.76		Attorney Docket Number		79314.5	
		Application Number			
Title of Invention	METHODS, DEVICES, AND SYSTEMS FOR SECURE PROVISIONING, TRANSMISSION, AND AUTHENTICATION OF PAYMENT DATA				
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Miami Beach	State/Province	FL	Country of Residence	US
Mailing Address of Inventor:					
Address 1		17 N. Hibiscus Drive			
Address 2					
City	Miami Beach	State/Province	FL		
Postal Code	33139	Country	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button. Add					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	71130		
Email Address	bosippto@seyfarth.com	Add Email	Remove Email

Application Information:

Title of the Invention	METHODS, DEVICES, AND SYSTEMS FOR SECURE PROVISIONING, TRANSMISSION, AND AUTHENTICATION OF PAYMENT DATA		
Attorney Docket Number	79314.5	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	12	Suggested Figure for Publication (if any)	

Filing By Reference

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	79314.5
		Application Number	
Title of Invention	METHODS, DEVICES, AND SYSTEMS FOR SECURE PROVISIONING, TRANSMISSION, AND AUTHENTICATION OF PAYMENT DATA		

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	71130		
Additional Representative Information blocks may be generated within this form by selecting the Add button.			

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.			
Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).			
			Remove
Application Number	Country i	Filing Date (YYYY-MM-DD)	Access Code (if applicable)

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	79314.5
		Application Number	
Title of Invention	METHODS, DEVICES, AND SYSTEMS FOR SECURE PROVISIONING, TRANSMISSION, AND AUTHENTICATION OF PAYMENT DATA		

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	79314.5
		Application Number	
Title of Invention	METHODS, DEVICES, AND SYSTEMS FOR SECURE PROVISIONING, TRANSMISSION, AND AUTHENTICATION OF PAYMENT DATA		

Applicant 1								
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.								
Clear								
☒ Assignee	☐ Legal Representative under 35 U.S.C. 117	☐ Joint Inventor						
☐ Person to whom the inventor is obligated to assign.	☐ Person who shows sufficient proprietary interest							
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:								
Name of the Deceased or Legally Incapacitated Inventor :								
If the Applicant is an Organization check here. ☒								
Organization Name	LoopPay, Inc.							
Mailing Address Information:								
Address 1	400 Trade Center							
Address 2	Suite 5900							
City	Woburn	State/Province	MA					
Country i	US	Postal Code	01801					
Phone Number		Fax Number						
Email Address								
Additional Applicant Data may be generated within this form by selecting the Add button.								

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.	
Assignee 1	
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.	
If the Assignee or Non-Applicant Assignee is an Organization check here ☒	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	79314.5
		Application Number	
Title of Invention	METHODS, DEVICES, AND SYSTEMS FOR SECURE PROVISIONING, TRANSMISSION, AND AUTHENTICATION OF PAYMENT DATA		

Organization Name	LoopPay, Inc.
-------------------	---------------

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	400 Trade Center		
Address 2	Suite 5900		
City	Woburn	State/Province	MA
Country i	US	Postal Code	01801
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/Brian Michaelis/				
First Name	Brian	Last Name	Michaelis	Registration Number	34221
Additional Signature may be generated within this form by selecting the Add button.					

CLAIMS

What is claimed is:

1. A method for creating dynamic card data, comprising:
receiving, by a device, card track data;
encrypting, by the device, the card track data using a first key;
sending, by the device, the encrypted card track data to a server;
receiving, by the device, a working key;
generating, by the device, modified card track data including a time-dependent CVV
using the working key; and
sending, by the device, the modified card track data to a point of sale terminal or causing
the modified card track data to be displayed to a user for use in an e-commerce transaction.
2. The method of claim 1, wherein an expiration date, a registered primary account
number, or a portion of a discretionary field of the modified track data indicates to a card issuer
or a third party service provider that the modified card track data is dynamic-CVV (dCVV) card
track data and authorization is to be performed in a dCVV mode.
3. The method of claim 1, wherein the sending the modified card track data to the
point of sale terminal includes sending the time-dependent CVV, and a dynamic mode indicator.
4. The method of claim 3, wherein the dynamic mode indicator is a primary account
number, an expiration date, or a separate dynamic mode indicator of the modified track data.
5. The method of claim 4, wherein the dynamic mode indicator indicates to a card
issuer or third party service provider, that the modified card track data is dynamic-CVV (dCVV)
card track data and authorization is to be performed in a dCVV mode.
6. The method of claim 1, wherein the device is a magnetic stripe storage and
transmission device or a mobile communication device.

7. A method for provisioning dynamic financial card data by issuer, comprising:
receiving, by a server, a request for provisioning card track data;
requesting, by the server, an authentication of a user corresponding to the card track data from a card issuer server, wherein the card issuer server corresponds to a card issuer of the card track data;
receiving, by the server, an authentication result from the card issuer server; and
generating, by the server, a working key for the generation of dynamic card track data.

8. The method of claim 7, wherein the requesting the authentication of the user from the card issuer server includes sending a primary account number and at least one of a CVV-2, a name, a date of birth, a username and password, and an answer to a challenge question to the card issuer server for authentication.

9. The method of claim 7, further comprising securely sending the working key to a wallet server.

10. The method of claim 7, further comprising receiving a request for verification of a dynamic-CVV (dCVV) in response to initiation of a payment transaction, wherein the dCVV is based on the working key.

11. The method of claim 10, wherein the receiving the request for verification of the dCVV includes receiving a primary account number, an expiration date, a service code, a time-stamp, and a mode indicator.

12. The method of claim 11, further comprising comparing the received time-stamp with a stored time-stamp or current time on the server for verifying a transaction.

13. The method of claim 12, further comprising sending an authorization failure in response to the stored time-stamp or current time corresponding to a time greater than the received time-stamp.

14. A method for performing dynamic-CVV (dCVV), comprising:
generating, by a server, a working key for card track data;
receiving, by a magnetic stripe storage and transmission device (MST), the working key;
generating, by the MST, modified card track data including a dCVV component based on original card track data, a time-stamp or counter and the working key;
sending the modified card track data to a point of sale terminal or e-commerce website for payment processing;
receiving, by the server, a request for verification of the dCVV from a card issuer server or a third party service provider in response to initiation of the payment processing, wherein the request includes the modified card track data;
performing, by the server, a verification of the dCVV component; and
sending, by the server, a verification failure or final verification based on the verification of the dCVV component.

15. The method of claim 14, wherein the modified card track data includes the dCVV component, a primary account number, an expiration date, a service code, the time-stamp or counter, and optionally a separate mode indicator when the expiry date or the primary account number is not used to indicate that authorization is to be performed in a dCVV mode.

16. The method of claim 15, wherein the mode indicator indicates to the card issuer server that the modified card track data is dCVV card track data and authorization is to be performed in a dCVV mode.

17. The method of claim 15, wherein the performing the verification includes comparing a received time-stamp or received counter with a stored time-stamp or a current time of the server or stored counter.

18. The method of claim 17, wherein the sending the verification failure or final verification includes sending the verification failure in response to the stored time-stamp or current time of the server corresponding to a time greater than the received time-stamp.

19. The method of claim 15, wherein the performing the verification includes: independently computing, by the server, a dCVV value using the working key; and comparing the computed dCVV value with the dCVV component.

20. The method of claim 19, wherein the sending the verification failure or final verification includes sending the final verification in response to the computed dCVV value matching the received dCVV component.

21. The method of claim 14, further comprising sending, by the server, the original card track data to the card issuer server for processing via the card issuer server's normal processing methods to complete a transaction, wherein the original card track data corresponds to data of a card issuer corresponding to the card issuer server.



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.
14/511,994	10/10/2014	Enyang Huang	73745.6	3622

71130 7590 07/14/2017
SEYFARTH SHAW LLP
WORLD TRADE CENTER EAST
TWO SEAPORT LANE, SUITE 300
BOSTON, MA 02210-2028

EXAMINER

MARTINEZ-HERNAND, EDGAR R

ART UNIT	PAPER NUMBER
----------	--------------

3685

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

07/14/2017

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):

bosippto@seyfarth.com

Office Action Summary	Application No. 14/511,994	Applicant(s) HUANG ET AL.	
	Examiner EDGAR R. MARTINEZ	Art Unit 3685	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 3/27/2017.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

- 5) ☒ Claim(s) 1-21 is/are pending in the application.
5a) Of the above claim(s) 1-13 is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 14-21 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) ☐ All b) ☐ Some** c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date 12/28/2016; 4/13/2017; 6/9/2017.
- 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 4) ☐ Other: ____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Response to Amendment

2. The Amendment filed on 3/27/2017, by Brian L. Michaelis (hereinafter referred to as "Applicant"), has been entered.

a. Claims 14-17 and 19-21 have been amended. The Examiner has confirmed no new matter has been added.

b. Claims 1-13 remain withdrawn from further consideration as being drawn to a non-elected invention.

3. Claims 14-21 are pending in the application and the status of the application is currently pending.

4. Applicant's amendments to the Claims have overcome each and every objection previously set forth in the previous office action mailed 12/27/2016.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads 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.

6. Claims 14-21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more.

7. The two-step Subject Matter Eligibility Test was conducted, which is described in the 2014 Interim Guidance on Patent Subject Matter Eligibility and further discussed in the July 2015 Update to the Interim Eligibility Guidance. The test further includes the latest quick reference sheet April 2017 Decisions holding claims eligible and identifying abstract ideas. When considering subject matter eligibility under 35 U.S.C. 101, the first step is to determine whether the claims are “directed to one of the four statutory categories of invention” (process, machine, manufacture, or composition of matter). If the claims are directed to one of the statutory categories, the next step is to determine if the claims “are not wholly directed to subject matter encompassing a judicially recognized exception”. *See MPEP 2106*. In this step, first it must be determined whether the claims are directed to the concept of a judicial exception (i.e. law of nature, natural phenomenon, and abstract idea). If a judicial exception is determined, it must additionally be determined whether the claims are a patent-eligible application of the judicial exception. In the case where the judicial exception present in the claims is an abstract idea, a patent-eligible application is determined if any additional element in each claim taken individually or a combination of additional elements from the claims can be defined as sufficient to ensure that the claims amount to significantly more than the judicial exception itself. Examples of abstract ideas include fundamental economic practices, certain methods of organizing human activities,

Art Unit: 3685

an idea 'of itself' and mathematical relationships/formulas. *See Alice Corporation Pty. Ltd. v. CLS Bank International, et al.*, 573 U.S. __, 134 S. Ct. 2347 (2014).

8. In the first step of the test, the claims are reviewed for statutory category. The claims were found to be directed to one of the four statutory categories, which is a process to verify a dynamic card validation value (dCVV). Step 1 is confirmed YES.

9. In the next test step, the claims are reviewed for a judicial exception. Claim 14 was found to be directed to the concept of "verifying a dynamic value", defined by the limitations:

- a. receiving a request for provisioning of a working key, the request comprising card track data;
- b. generating the working key for the card track data received with the request;
- c. sending the working key as a response to the request for provisioning;
- d. receiving the working key;
- e. generating a dCVV based on the card track data, a time-stamp, and the working key;
- f. sending modified card track data to the POS terminal [...] for payment processing, or to an e-commerce website for payment processing;
- g. sending the modified card track data to a card issuer server or a third party service provider for authorization;
- h. sending a request for verification of the dCVV, the request including the modified card track data / receiving the request for verification of the dCVV from the card issuer server or third party service provider;

Art Unit: 3685

- i. performing a verification of the dCVV in response to the request for verification;
- j. sending a verification failure or final verification based on the verification of the dCVV.

10. The steps of "receiving a request for a work key", "generating a work key" and "sending the work key" are interpreted to be part of a registration process that is well-understood, routine and conventional actions previously known in the art of token registration for authentication, which is evidenced in the prior art. The steps of "receiving the working key" and "generating a dCVV" are interpreted to be further part of the registration process, considering the "MST" recited in the claim is a card scanner, and where the steps are interpreted to be well-understood, routine and conventional actions previously known in the art of generating a secured value through the use of an algorithm. The steps of "sending modified card track data", "sending a request for verification", "performing a verification" and "sending a response based on the verification" are interpreted as part of a payment transaction approval protocol that is well-understood, routine and conventional actions previously known in the art of credit card authentications, which is evidenced in the prior art. The "verification" step is further specified in dependent claim 17 ("comparing a received time-stamp or received counter with a stored time-stamp or a current time") and dependent claim 19 ("independently computing a dCVV value using the working key; and comparing the computed dCVV value with the dCVV component"). In combination, the process steps are interpreted to be part of a payment transaction approval protocol, where a smart card is used to perform the claimed method steps. The concept as described defines a judicial exception, an abstract

Art Unit: 3685

idea, similar to “an idea of itself” (the courts found similar concepts relating to processes of comparing data that can be performed mentally as abstract, such as *obtaining and comparing intangible data (CyberSource)*; see also *In re Grams*, 888 F.2d 835, 840-41 (Fed. Cir. 1989); and *In re Meyer*, 688 F.2d 789, 794-95 (C.C.P.A. 1982)). In the two-step test, Step 2A is confirmed YES. Due to their dependence, claims 15-21 are also directed to the abstract idea.

11. In the next test step, the claims are reviewed for their additional elements. The claims recite the additional elements of “a server”, “a magnetic stripe storage and transmission device”, “a point of sale terminal” and “a card issuer server or a third party service provider”. The additional elements are recited in a high level of generality where the claims require no more than a generic computer to perform the generic functions that are well-understood, routine and conventional activities previously known in the industry. These conventional activities merely improve the abstract idea of “verifying a dynamic value”. Introducing these elements into the analysis of the concept of claim 14, shown above, the additional elements do not change the interpretation of the concepts that were found to be similar to an abstract idea. While the additional elements limit the abstract idea to a specific field, there is no improvement to the functioning of the generic computer nor is there an improvement to another technology or technical field.

12. Considering the additional elements individually, the claims do not include elements that are sufficient to amount to significantly more than the judicial exception. Considering the additional elements in combination does not add anything more than the elements

Art Unit: 3685

analyzed individually that is significantly more than the abstract idea. In the two-step test, Step 2B is confirmed NO for all claims. Therefore, the claims are not patent eligible.

Claim Rejections - 35 USC § 112

13. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

(a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

14. **Claims 14-21 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.**

15. Claim 14 recites “receiving, by a server, a request for provisioning of a working key...”, where a general server is recited. The claim further recites “receiving, by the server, the request for verification of the dCVV...”, where again a general server is recited. The Specification discloses “the wallet server may determine whether the card is eligible for

Art Unit: 3685

dCVV” (see ¶ [0051]), which is specific to an embodiment of the claimed invention. The Specification further recites “The provisioning and authentication server may identify that the request, from step 508, is from the wallet server...”, where the request is for verification (see ¶ [0054]). The claim as amended is broader than the Specification when it is reciting that a server, as in ‘any’ server, can perform the method steps of “provisioning” and “verification” while the Specification discloses two specific servers in two unique circumstances performing the claimed method steps. Thus, the claim does not comply with the written description requirement where the embodiment recited in the claim is broader than the Specification.

16. Due to their dependence, claims 15-21 are also rejected with claim 14 because they do not comply with the written description requirement.

17. The following is a quotation of 35 U.S.C. 112(b):

(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

18. Claims 14 is rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Art Unit: 3685

19. Claim 14 recites “generating, by the MST, a dCVV based on the card track data...” and further recites “sending modified card track data to the POS...”. It is unclear where or when the MST received the card track data in the method steps. Where the claim recites “receiving, by a server, a request for provisioning of a working key, the request comprising card track data”, the claim is not clear on where the card data comes from, whether from a card scan or from the wallet server. Further, the Specification recites “In this aspect, at each transmission, the MST constructs, for example, modified track 2 data (MT) containing a dCVV, which is derived from the card data” (see at least ¶ [0069]), which clarifies the modified card track data is constructed by the MST and includes the dCVV. Thus, there is insufficient antecedent basis for the recitation of “the card track data” in the claim.

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

21. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

22. This application currently names joint inventors. In considering patentability of the claims the examiner presumes that the subject matter of the various claims was commonly owned as of the effective filing date of the claimed invention(s) absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and effective filing dates of each claim that was not commonly owned as of the effective filing date of the later invention in order for the examiner to consider the applicability of 35 U.S.C. 102(b)(2)(C) for any potential 35 U.S.C. 102(a)(2) prior art against the later invention.

23. Claims 14, 15, and 17-21 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Von Mueller (US 2006/0049256, hereinafter referred to as "Von Mueller"), further in view of Ward (US 2010/0098246, hereinafter referred to as "Ward") and further in view of Faith (US 2008/0120236, hereinafter referred to as "Faith").

24. **Regarding Claim 14**, Von Mueller teaches

- a. receiving, by a server, a request for [updating the] working key, the request comprising card track data ("the MSR module generates a new key, encrypts that key with the command or current key, and sends the packet formatted in the applications conventional format with certain clear text information..." See at least ¶ [0020]-[0022]);

Art Unit: 3685

- b. [decrypting and storing] the working key for the card track data received with the request (See ¶ [0020]-[0022]);
- c. sending, by the server, [...] a response to the request (See ¶ [0020]-[0022]);
- d. generating, by the MST, [converted data] based on original card track data, a time-stamp or counter and the working key, wherein the MST increments a counter value contained in the time-stamp at each transaction ("Nineteen digits of the remaining card data are converted to an 8 byte binary value, a time function is added 206 and the result TDES encrypted using an electronic code book (ECB) block encryption 209, The 8 bytes of encrypted data are converted to a 20 digit base 10 number, the least significant 19 digits replace the selected card digits. The last digit is 0 or 1 and is added predefined to a bank field. A new mod 10 character is generated 210 and placed into the selected card digit." See ¶ [0095]; in a similar embodiment, see the transaction block including the encryption key, a time or counter and track data encrypted together and finally modified, seen in Fig. 5; "The time stamped in the encrypted transaction is compared with the transaction processing server and if out of date the transaction is rejected and a new card swipe requested. If the new card swipe date stamp is equal to the previous data a fraudulent transaction is flagged. If the date stamp is out of date by an amount equal to the duration between stamps, the transaction is allowed and the date inaccuracy noted in the servers transition data base. In the same manner, if a real time clock is not available the secure module increments a counter for each transaction the reader makes. The

- processing server compares the count in the current encrypted transaction request to the last received count." See ¶ [0035]; example includes a signature for authentication: "In an alternate method the POS server forwards the encrypted card and signature to an enabled transaction server to both authenticate and decrypt the card data." See at least ¶ [0094]);
- e. sending modified card track data to the POS terminal as magnetic pulses transmitted by the MST for payment processing, or to an e-commerce website for payment processing, the [converted data] comprising [...] a portion of the card track data, the [converted data] having a format similar to an original format of the card track data (starting from Fig. 5, device 44, moving data to server 151, in Fig. 22; "multiple PDAs 111, table mounted POS terminal with secure module for order entry and payment along with internet access 150, and a point of sale register with wireless capabilities are all connected to a wireless local area network (WAN) 152. This WAN, and any hard wired POS registers communicate with a local POS application server 151 which is connected via the Internet and secure connections to a TDES encryption database and transaction processing server." See at least ¶ [0094]; "The 8 bytes of encrypted data are converted to a 20 digit base 10 number, the least significant 19 digits replace the selected card digits." See at least ¶ [0095]);
- f. sending, by the POS terminal or e-commerce website, the [converted data] to a card issuer server or a third party service provider for authorization (see ¶ [0101]-[0102]);

Art Unit: 3685

- g. sending, by the card issuer server or third party service provider, a request for verification of [the signature], the request including the [converted data] (see ¶ [0101]-[0102]);
- h. receiving, by the server, the request for verification of [the signature] from the card issuer server or third party service provider ("the local POS application server either requests the authentication sever to verify the cards authenticity and sends that response along with the encrypted card data to the new transaction server or additionally requests the encryption keys and formats the data for a legacy transaction server." See at least ¶ [0094]);
- i. performing, by the server, a verification of [the signature] in response to the request for verification (one example including authentication: "The selected keys are used to decode signature data along with a hash code generated by the secure module from the card data account number. The hash value generated from the card data is used to index the secure stripe database to retrieve the card signature. The database signature is then compared to the decrypted transaction signature and based on the comparison the transaction is sent to the processing bank indicated in the signature database or a message is sent back to the card holder requesting verification of the card's authenticity which may be in the form of a re-swipe of the card or entry of additional information such as billing zip code at which point the transaction is sent to the processing bank using standard formats or declined." See ¶ [0116]);

- j. sending, by the server, a verification failure or final verification based on the verification of the [signature] (see ¶ [0116]).

25. Von Mueller further teaches receiving a request for a new key (as recited in the claim, the function of “receiving a request” is interpreted as a result of an action performed with the MST: “In the case of the new key request command, the card is swiped while the head module is connected to the handheld computing device which is browsing the WAP site supporting this application.” See ¶ [0020]).

26. The limitation “the MST comprising a driver and an inductor configured to transmit magnetic pulses to a point of sale (POS) terminal” is a recitation of the intended use of the claimed invention. This recitation must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. It has been held that a recitation with respect to the manner in which a claimed apparatus is intended to be employed does not differentiate the claimed apparatus from a prior art apparatus satisfying the claimed structural limitations. *Ex parte Masham*, 2 USPQ2d 1647 (1987). If the prior art structure is capable of performing the intended use, then it meets the claim. *See MPEP §2106*. In this case, Von Mueller does teach an MST comprising a driver and an inductor (see Fig. 1 - Fig. 3).

27. Von Mueller does not expressly teach generating the working key and providing the working key in response to the request.

28. However, Ward does teach receiving a request to generate an encryption key, generating the encryption key and providing the encryption key in response to the request (“FIG. 3 shows an example of a method 300 of generating an encryption key using an EKMS

Art Unit: 3685

(e.g., the EKMS 100 of FIG. 1) in accordance with certain implementations of the disclosed technology. At 302, the EKMS receives a request to create an encryption key. ... At 304, the EKMS obtains seed material (e.g., n-bits of random data) using a random sequence generator, for example. At 306, the EKMS obtains the X509 certificate's private key. At 308, the EKMS uses an encryption key generation algorithm to generate the requested encryption key. The algorithm can be used to generate encryption keys given an X509 certificate and associated private key. ... At 310, the EKMS returns the generated encryption key to the requestor." See ¶ [0045]-[0052]).

29. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "generating an encryption key at a request", as taught by Ward, by modifying the process to generate the key at the server instead of at the card reader, to further improve the process of securing the account data for smart cards that may be used in card-not-present transactions or online transactions.

30. Von Mueller does not explicitly teach generating, by the MST, the dCVV based on a time-stamp.

31. However, Faith does teach generating a dCVV based on a counter ("Portable consumer device 30 generates a verification value using the counter and/or other dynamic data elements (step 220). The verification value and a portion of the counter are embedded in payment data that is in the form of Track data." See at least ¶ [0073]).

32. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "a verification

value generator", as taught by Faith, as part of the process of generating converted data in the card reader, to further improve the secure authentication of a personal account number for any transaction.

33. **Regarding Claim 15**, Von Mueller, in view of Ward and further in view of Faith, teaches the limitations of claim 14. Von Mueller further teaches the modified card track data includes a primary account number, an expiration date and a service code (Account Number, Expire Date and Bank Fields, see Fig. 23) and a time-stamp or counter ("It is yet a further advantage of the present invention to allow the encrypted magnetic head module to communicate with a real time clock or a global positioning system (GPS) receiver either internal to the phone or reader to tag all data transaction with date, time and location information. This is especially required in POS financial transaction that are mobile to verify where and when the transaction that the transaction occurred. Stamping the data with the date and time prevents the encrypted card information from being recorded and used to make multiple transactions at a later date. The time stamped in the encrypted transaction is compared with the transaction processing server and if out of date the transaction is rejected and a new card swipe requested." See ¶ [0035] and Fig. 23).

34. Von Mueller, in view of Ward, does not explicitly teach the dCVV.

35. However, Faith does teach a verification value created for the verification of the card data ("Server 72 of service provider 70 retrieves its counter stored in counter database 76 and uses it to calculate a verification value (step 250) using an algorithm. The algorithm may follow steps similar to those shown in FIG. 2 to calculate the verification value. The

Art Unit: 3685

calculated verification value is compared to the verification value received in the Track data." See at least ¶ [0078]].

36. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "a verification value generator", as taught by Faith, used in the modified card track data, to further improve the secure authentication of a personal account number for any transaction.

37. **Regarding Claims 17 and 18**, Von Mueller, in view of Ward and further in view of Faith, teaches the limitations of claim 14. Von Mueller further teaches comparing a received time-stamp or received counter with a stored time-stamp or a current time of the server or stored counter ("The time stamped in the encrypted transaction is compared with the transaction processing server and if out of date the transaction is rejected and a new card swipe requested. If the new card swipe date stamp is equal to the previous data a fraudulent transaction is flagged. If the date stamp is out of date by an amount equal to the duration between stamps, the transaction is allowed and the date inaccuracy noted in the servers transition data base." See ¶ [0035]) and sending the verification failure in response to the stored time-stamp or current time of the server corresponding to a time greater than the received time-stamp ("In the same manner, if a real time clock is not available the secure module increments a counter for each transaction the reader makes. The processing server compares the count in the current encrypted transaction request to the last received count. If the count is greater than the previous count, the transaction is accepted and the new count stored in the transaction data base. In addition to providing for testing for reused previously recorded transaction data, the counter is used to change the encrypted

transaction data. The output for swiping the same card multiple times will always be different. Therefore any data stolen from the merchant's servers cannot be reused to make a duplicate transaction." See ¶ [0035]].

38. **Regarding Claim 19**, Von Mueller, in view of Ward and further in view of Faith, teaches the limitations of claim 14. Von Mueller further teaches comparing the [signature] to determine authenticity ("The application server requests the Authentication database server or service 130 to verify the magnetic stripe authenticity using the account hash code to index the stored signature value for the magnetic stripe. The results of the signature comparison are used to determine if the card transaction should be terminated or forwarded to the legacy transaction processor based on acceptance rules contained within the encryption database 121." See at least ¶ [0087]).

39. Von Mueller, in view of Ward, does not expressly teach independently computing, by the server, a dCVV value using the working key in response to receiving the request for verification.

40. However, Faith does teach independently computing, by the server, a dCVV value ("Server 72 of service provider 70 retrieves its counter stored in counter database 76 and uses it to calculate a verification value (step 250) using an algorithm. The algorithm may follow steps similar to those shown in FIG. 2 to calculate the verification value. The calculated verification value is compared to the verification value received in the Track data." See at least ¶ [0078]).

41. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "computing a

Art Unit: 3685

dCVV value by the server", as taught by Faith, used in the comparison for authentication of data to further protect the account number during the authentication of the card used in any transaction.

42. **Regarding Claim 20**, Von Mueller, in view of Ward and further in view of Faith, teaches the limitations of claim 14. Von Mueller further teaches sending the final verification in response to the [stored signature] matching the received [signature] ("The database signature is then compared to the decrypted transaction signature and based on the comparison the transaction is sent to the processing bank indicated in the signature database or a message is sent back to the card holder requesting verification of the card's authenticity which may be in the form of a re-swipe of the card or entry of additional information such as billing zip code at which point the transaction is sent to the processing bank using standard formats or declined." See example in ¶ [0116]).

43. Von Mueller, in view of Ward, does not expressly teach the dCVV used in the comparison for authentication.

44. However, Faith does teach a dCVV created for the verification of the card data (See ¶ [0078]-[0080]).

45. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "a dCVV generator", as taught by Faith, used in the comparison for authentication of data to further protect the account number during the authentication of the card used in any transaction.

46. **Regarding Claim 21**, Von Mueller, in view of Ward and further in view of Faith, teaches the limitations of claim 14. Von Mueller further teaches replacing dynamic content

Art Unit: 3685

included in the modified track data, including the dCVV, with original track content to restore original card track data, and sending the original card track data to the card issuer server for processing via the card issuer server's normal processing methods to complete the transaction, wherein the original card track data corresponds to the card track data as originally issued by a card issuer, the card issuer corresponding to the card issuer server ("The application server requests the encryption key database server or service 121, which is located on the same intranet or within the same computer, to accept the encrypted data and return decrypted transaction data. The returned decrypted transaction data is formatted by the WAP application server suitable to the required transaction processor 116 and the transaction processed using current bank rules." See ¶ [0088]-[0089] and [0096] and Fig. 16-23).

47. Claim 16 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Von Mueller, further in view of Ward, further in view of Faith and further in view of Brown (US 2007/0136211, hereinafter referred to as "Brown").

48. Regarding Claim 16, Von Mueller, in view of Ward and further in view of Faith, teaches the limitations of claim 14. Von Mueller, in view of Ward and further in view of Faith, does not explicitly teach the modified card track data further includes a separate mode indicator, when the expiry date or the primary account number is not used, to indicate that authorization is to be performed in a dCVV mode that includes the verification of the dCVV, and that the mode indicator indicates to the card issuer server that the modified card track data is dCVV card track data and authorization is to be performed in a dCVV mode.

Art Unit: 3685

49. However, Brown does teach an indicator field ("The ISO 7810/7816 specifications and ABA/1ATA stripe data fields describe a "discretionary field", and "other data field" that can be used exclusively for the issuing bank. These can be used to place operators, which can be as simple as a single status bit." See ¶ [0076] and Fig. 4F) as a plain text indicator that indicates the modified card track data is dCVV card track data (includes cryptograms and plaintext used in CVx type authentication, see at least ¶ [0137]-[0140]) and authorization is to be performed in a dCVV mode (identification of a CVQ (card verification number) cryptogram is followed by the process in Fig. 6, "CVx authentication uses data that is on Track2. The remote server can only authenticate using data on-hand and the bank key." See at least ¶ [0141]-[0147]).

50. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "a dCVV component code (CVQ) and performing a dCVV authorization", as taught by Brown, to further secure the account number during an authentication of the account for any transaction.

Response to Arguments

51. Applicant's arguments, filed 3/27/2017, with respect to the rejections under 35 USC 101 and 35 USC 103(a) have been fully considered.

52. Regarding the rejection under 35 USC 101, the Examiner has considered the amendments to the claims and considered the arguments.

53. The Applicant argues: "On page 7 of the Action, SmartGene is cited for the idea that "The concept as described defines a judicial exception, an abstract idea, similar to an idea 'of itself (the courts found similar concepts relating to processes of comparing data that can be performed mentally as abstract, such as 'comparing new and stored information an using rules to identify options.'" Unlike the amended claim 14, the claim in SmartGene lacked any specificity as to how data was processed, preempting the use of an abstract concept so as to encompass any method for processing the data."

54. In response, the amended claims were tested using the rationale defined in the 2014 Guidance and the 2015 Update for the Two-Step Subject Matter Eligibility Test. The previous office action was completed at the time the courts defined the precedential and non-precedential cases. An update to the results of the test has been provided in the current action. The test includes the court cases defined in the May 2017 reference sheet, which points out the newest court cases to define an abstract idea as well as define the precedential and non-precedential court cases. The current interpretation of the limitations that define the abstract idea were further explained in the rejection above, and only the precedential court cases were used to compare the abstract idea in the claims.

55. The Applicant further argues: "Also on page 7 of the Action, the assertion is made that "the [claim] elements are recited in a high level of generality that allows the claim to require no more than a generic computer to perform generic functions that are well-understood, routine and conventional activities previously known in the industry (generating a key, receiving the key, generating and sending modified card track data, receiving a request, performing a verification, sending a failure or final verification, etc.)."

Art Unit: 3685

Characterizing the clauses as being routine and conventional diminishes that most of what computers do is process information. This can be said about every computer program in existence.

56. “Among other improved technological results, the claimed MST (which itself is a hardware component “comprising a driver and an inductor configured to transmit magnetic pulses to a point of sale (POS) terminal” and is certainly not a “mental process”) generates a different dCVV for every transaction, and uses a transaction format that is format-compatible with the standard card formats expected by POS terminals and e-commerce websites. Also, by virtue of the counter value being incremented by the MST itself, a provisioned MST can generate a new dCVV for each transaction and execute the transaction even when no network connection exists. See, e.g., [0035].”

57. In response, the technology in the claims, including the MST, are recited performing functions that are conventional actions previously known in the art, as is explained in the rejection above. The affirmation of the limitation “the claimed MST generates a different dCVV for every transaction” follows the description of the generation of a dynamic CVV or CVV-2, as taught by Brown. The MST is performing functions that are conventional to secure the payment card data, which is evidenced in the prior art. Therefore, the results of the test are supported by the further explanation and are evidenced in the prior art.

58. The Applicant further argues: “Throughout § 101 rejection, the claimed elements are characterized as a “routine” computer implementation of an abstract idea.

Reconsideration is requested in view of the claim amendments, since that sort of broad

Art Unit: 3685

generalization about the amended claims would overlook the specific limitations recited therein, and thus fail to consider the claimed subject matter as a whole.”

59. In response, the test results have been provided with further explanation as to how each limitation individually and as a whole are considered as an abstract idea, are rooted in the technology but do not provide a technical solution to the technical problem, and do not recite elements that would be significantly more than the abstract idea.

60. **Regarding the rejection under 35 USC 112(b)**, the Examiner has considered the amendments and the arguments in view of the prior art. The amendments to claim 14 have overcome the 112 rejection from the previous action, and have therefore been withdrawn. The new 112 rejection proposed in the current action are in regards to the current amended claims.

61. **Regarding the rejection under 35 USC 103(a)**, the Examiner has considered the amendments and the arguments in view of the prior art.

62. The Applicant argues: “Applicant has amended claim 14 to better define the invention. As amended, there are several distinctions relative to the applied references.

63. The applied references fail to teach generating the working key “for the card track data received with the request.” The “current key” in Von Mueller is specific to the MSR module, rather than to the card track data. See Mueller [0020] to [0022]. Likewise, in Dorsey, the cryptographic key is associated with the card reader 514. See Dorsey [0281]. And in Brown, the encryption key used to encrypt the encryption tables 132 is not shared with the payment card having the crypto table. See Brown [0058].”

Art Unit: 3685

64. In response, the art of Von Mueller does teach a method to create new keys, the method which can be implemented during a transaction, which improves the security of the transaction as the key is not related to any part of the account number stored in the card. However, the method in Von Mueller is explained in a way that allows other methods to be applied. The art of Ward was introduced in order to teach a method of receiving a request to generate a key, using the card account information as the mentioned "seed material" to generate the key, and providing the key for use. One of ordinary skill in the art would be motivated to include the method of Ward into the method of Von Mueller to further secure the account data for smart cards that may be used in card-not-present transactions or online transactions.

65. The Applicant further argues: "Further, Von Mueller and Dorsey both relate to encoding card data by a magnetic stripe reader, whereas Brown relates to a pre-programmed smart card. Referring to FIG. 2 in Brown, Von Mueller and Dorsey both relate to what would be merchant infrastructure in Brown. Applicant submits that if Von Mueller and/or Dorsey were combined with Brown, the suggested combination would be to infrastructure rather than the Brown's pre-programmed payment card. And if the pre-programmed crypto-table 205 used for the dynamic CVVs in Brown were added to Von Mueller, then there still would be no suggestion, nor motivation to modify each of the references in different ways, to generate the dCVV in the manner claimed. As illustrated in Von Mueller's FIGS. 5 and 23, the card data is encrypted by the card reader. See Von Mueller [0021] and [0095]. Absent hindsight (and the benefit of Applicant's disclosure), applicant submits the result flowing from the teaching of the references would be to

encrypt Brown's dynamic CVV with the rest of the card data, rather than generate the dCVV in the manner particularly claimed."

66. In response, it has been mentioned in the rejections above that "the MST generating a dCVV" is interpreted as a function of an algorithm. The Specification recites the MST generates the dCVV and includes the dCVV in the modified card data based on instructions from the wallet server. Von Mueller teaches the use of hardware components (see Fig. 11 and 12) and the software (see example ¶ [0095]) to convert the card data as is required to secure the data before transmission through an unsecure network. Brown teaches the method to generate a dCVV that is used in the detection of fraud, which is interpreted as a method of authentication. The combination of the dCVV algorithm taught by Brown into the conversion method of Von Mueller does teach the elements that are recited in the claims, motivated by adding the element of the dCVV in the scanned card data to further secure the account data for authentication for a transaction.

67. The Applicant further argues: "Further, claim 14 now recites that the MST increments a counter value contained in the time-stamp at each transaction, such that the dCVV would be different for each transaction. While Von Mueller stamps the data with the date and time (see Von Mueller [0035]), that does not suggest generating a dCVV based on the time-stamp. Nor does Brown suggest this feature, as the dynamic CVV in Brown is pre-computed and stored in a table (see Brown [0058]), with the next cryptogram pulled from the table one to five minutes after a swipe, rather than for each transaction (see Brown [0142]).

Art Unit: 3685

68. In response, it is shown above that Von Mueller does teach the use of a time-stamp or a counter to create a different modified card data for every transaction (see Von Mueller ¶ [0096]). It should be understood that even though numerous characteristics and advantages are set forth in the art of Von Mueller, together with details of the structure and function of the invention, the disclosure is illustrative only, and changes may be made in detail, especially in matters of shape, size, construction, materials, chemistry and arrangement of parts within the principal of the invention to the full extent indicated by the broad general meaning of the terms in which the appended claims are expressed. (See Von Mueller ¶ [0121]). The art of Faith is combined with Von Mueller to teach using a counter value to generate a verification value, which changes with every transaction, even with every swipe of the card, providing a further secure transaction without fraudulent activity.

Prior Art Made of Record

69. The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure, and is listed in the attached form PTO-892 (Notice of References Cited). Unless expressly noted otherwise by the Examiner, all documents listed on form PTO-892 are cited in their entirety.

Interview

70. The Examiner respectfully welcomes a telephonic interview with Applicant to discuss any items that will advance prosecution.

Conclusion

71. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDGAR R. MARTINEZ whose telephone number is (571)270-0658. The examiner can normally be reached on MON - FRI at 9:00 AM-5:00 PM EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John W. Hayes, can be reached on MON - FRI at 571-272-6708. The fax phone

Art Unit: 3685

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/EDGAR R. MARTINEZ/
Examiner, Art Unit 3685

/MAMON OBEID/
Primary Examiner, Art Unit 3685

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Enyang Huang, *et al.* Art Unit: 3685
Application No.: 14/511,994 Confirmation No.: 3622
Filed: October 10, 2014 Examiner: Edgar R. Martinez-Hernande
For: METHODS, DEVICES, AND SYSTEMS FOR SECURE
PROVISIONING, TRANSMISSION, AND AUTHENTICATION OF
PAYMENT DATA

CERTIFICATE OF TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being electronically submitted with the United States Patent Office on the date shown below via EFS-Web:

By: /Seema S. White/

Date: October 10, 2017

Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.116

Commissioner,

In response to the Final Office Action dated July 14, 2017 in the above referenced patent application, applicant requests entry of the following claim amendments and remarks. This response is not filed with a petition for extension of time, as none is believed necessary. However, this response is being filed with a Request for Continued Examination (RCE). Authorization is hereby given to charge Deposit Account No. 19-1351 in connection with any fees necessary to permit entry of this response.

Claim Amendments begin on page 2 of this paper.

Remarks begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Withdrawn) A method for creating dynamic card data, comprising:
receiving, by a device, card track data;
encrypting, by the device, the card track data using a first key;
sending, by the device, the encrypted card track data to a server;
receiving, by the device, a working key;
generating, by the device, modified card track data including a time-dependent CVV using the working key; and
sending, by the device, the modified card track data to a point of sale terminal or causing the modified card track data to be displayed to a user for use in an e-commerce transaction.
2. (Withdrawn) The method of claim 1, wherein an expiration date, a registered primary account number, or a portion of a discretionary field of the modified track data indicates to a card issuer or a third party service provider that the modified card track data is dynamic-CVV (dCVV) card track data and authorization is to be performed in a dCVV mode.
3. (Withdrawn) The method of claim 1, wherein the sending the modified card track data to the point of sale terminal includes sending the time-dependent CVV, and a dynamic mode indicator.
4. (Withdrawn) The method of claim 3, wherein the dynamic mode indicator is a primary account number, an expiration date, or a separate dynamic mode indicator of the modified track data.
5. (Withdrawn) The method of claim 4, wherein the dynamic mode indicator indicates to a card issuer or third party service provider, that the modified card track data is dynamic-CVV (dCVV) card track data and authorization is to be performed in a dCVV mode.
6. (Withdrawn) The method of claim 1, wherein the device is a magnetic stripe storage and transmission device or a mobile communication device.

7. (Withdrawn) A method for provisioning dynamic financial card data by issuer, comprising: receiving, by a server, a request for provisioning card track data;
requesting, by the server, an authentication of a user corresponding to the card track data from a card issuer server, wherein the card issuer server corresponds to a card issuer of the card track data;
receiving, by the server, an authentication result from the card issuer server; and
generating, by the server, a working key for the generation of dynamic card track data.
8. (Withdrawn) The method of claim 7, wherein the requesting the authentication of the user from the card issuer server includes sending a primary account number and at least one of a CVV-2, a name, a date of birth, a username and password, and an answer to a challenge question to the card issuer server for authentication.
9. (Withdrawn) The method of claim 7, further comprising securely sending the working key to a wallet server.
10. (Withdrawn) The method of claim 7, further comprising receiving a request for verification of a dynamic-CVV (dCVV) in response to initiation of a payment transaction, wherein the dCVV is based on the working key.
11. (Withdrawn) The method of claim 10, wherein the receiving the request for verification of the dCVV includes receiving a primary account number, an expiration date, a service code, a time-stamp, and a mode indicator.
12. (Withdrawn) The method of claim 11, further comprising comparing the received time-stamp with a stored time-stamp or current time on the server for verifying a transaction.
13. (Withdrawn) The method of claim 12, further comprising sending an authorization failure in response to the stored time-stamp or current time corresponding to a time greater than the received time-stamp.

14. (Currently Amended) A method for performing dynamic Card Validation Value (dCVV) verification, comprising:

receiving, by a provisioning and authentication server, a request for provisioning of a working key, the request comprising card track data from a wallet server;

generating, by the provisioning and authentication server, the working key for the card track data received with the request;

sending, by the provisioning and authentication server, the working key as a response to the request for provisioning;

receiving, by a magnetic stripe storage and transmission device (MST), the working key, the MST comprising a driver and an inductor configured to transmit magnetic pulses to a ~~point-of sale (POS)~~transaction terminal;

generating, by the MST, a dCVV based on the card track data from the wallet server, a time-stamp, and the working key, wherein the MST increments a counter value contained in the time-stamp at each transaction;

sending modified card track data to the ~~[[POS]]~~transaction terminal as magnetic pulses transmitted by the MST for ~~payment~~ processing, or to an e-commerce website for ~~payment~~ processing, the modified card track data comprising the dCVV and a portion of the card track data, the modified card track data having a format similar to an original format of the card track data;

sending, by the ~~[[POS]]~~transaction terminal or e-commerce website, the modified card track data to a card issuer server or a third party service provider for authorization;

sending, by the card issuer server or third party service provider, a request for verification of the dCVV, the request including the modified card track data;

receiving, by the provisioning and authentication server, the request for verification of the dCVV from the card issuer server or third party service provider;

performing, by the provisioning and authentication server, a verification of the dCVV in response to the request for verification; and

sending, by the provisioning and authentication server, a verification failure or final verification based on the verification of the dCVV.

15. (Previously Presented) The method of claim 14, wherein the modified card track data includes the dCVV, a primary account number, an expiration date, a service code, the time-stamp or counter value.

16. (Previously Presented) The method of claim 15, wherein the modified card track data further includes a separate mode indicator when the expiry date or the primary account number is not used to indicate that authorization is to be performed in a dCVV mode that includes the verification of the dCVV, the mode indicator indicates to the card issuer server that the modified card track data is dCVV card track data and authorization is to be performed in the dCVV mode.

17. (Previously Presented) The method of claim 15, wherein the performing of the verification includes comparing a received time-stamp or received counter value with a stored time-stamp or a current time of the server or stored counter value.

18. (Original) The method of claim 17, wherein the sending the verification failure or final verification includes sending the verification failure in response to the stored time-stamp or current time of the server corresponding to a time greater than the received time-stamp.

19. (Previously Presented) The method of claim 16, wherein the performing of the verification in the dCVV mode includes:

independently computing, by the server, a dCVV value using the working key in response to receiving the request for verification; and

determining whether the computed dCVV value [[with]] matches the dCVV received in the request for verification.

20. (Previously Presented) The method of claim 19, wherein the sending of the verification failure or final verification includes sending the final verification in response to the computed dCVV value matching the received dCVV.

21. (Previously Presented) The method of claim 14, further comprising the server, after the verification indicates that the dCVV is valid:

replacing dynamic content included in the modified track data, including the dCVV, with original track content to restore original card track data; and

sending the original card track data to the card issuer server for processing via the card issuer server's normal processing methods to complete the transaction,

wherein the original card track data corresponds to the card track data as originally issued by a card issuer, the card issuer corresponding to the card issuer server.

REMARKS

In view of the remarks below, Applicants believe the pending application is in condition for allowance.

Claims 14-21 are currently pending.

Amendment or cancellation of the claims during the prosecution is not to be construed as acquiescence to any of the objections/rejections set forth in the Office Actions and was done solely to expedite prosecution of the application. Applicants hereby expressly reserve the right to pursue the claims as originally filed or similar claims, in this or one or more patent applications.

Applicants respectfully request reconsideration and withdrawal of the claim rejections in view of the amendments and remarks presented herein.

Claim Rejections under 35 U.S.C. § 101

On pages 3-7 of the Office Action, the Examiner rejects claims 14-21 under 35 U.S.C. § 101 as being directed to a judicial exception without significantly more. Applicants submits these rejections are herein overcome.

Determining patent subject matter eligibility requires examining the claims in a two-step inquiry. Step 1 determines if the claims are directed to a process, machine, manufacture, or composition of matter, which is explained in MPEP 2106(I). The present claims, according to the Office Action at p. 4, satisfy Step 1 of the subject matter eligibility framework. The Office Action, pages 4, takes the position that claims 14-21 are directed to a process to verify a dynamic card validation value (dCVV).

If Step 1 is satisfied, the claims are examined in Step 2 to determine if they are directed to an unpatentable judicial exception. Step 2 involves a two prong analysis based on the Supreme Court decision in *Alice Corp. v. CLS Bank Int'l*. Step 2A determines whether the claims are directed to a judicial exception—laws of nature, natural phenomena, and abstract ideas. Examples of abstract ideas include fundamental economic practices, certain methods of organizing human activity, an idea “of itself,” and mathematical relationships. Here, the Office Action asserts on pages 5-6 that claims 14-21 are directed to judicial exception, an abstract idea, similar to “an idea of itself”. Applicants respectfully disagree as explained below.

If the claims are not *directed to* a judicial exception, the claims are subject matter eligible. If the claims are found to be directed to a judicial exception, the claims may still be patent subject matter eligible under Step 2B, which determines if any claim element, or a combination of claim elements, is sufficient to ensure that the claim as a whole amounts to significantly more than the judicial exception. *See* 2014 Interim Eligibility Guidance Quick Reference Sheet. The Office Action, pages 6-7, asserts that the claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the additional elements recited in the claims do not amount to significantly more than the abstract idea. Applicants also respectfully disagree as explained below.

Applicants emphasize that the claimed invention solves a technical problem using a technical solution. Currently, CVV1 and CVV2 values are static and can be compromised by many different methods, such as skimming devices and sniffing devices (paragraph [0007], Specification). Further, when the security measures (i.e., CVV1 and CVV2 values) associated with magnetic strip or chip card data are compromised, they can be continually used in fraudulent transactions (paragraph [0007], specification). In contrast, the inventors of the subject patent application have invented a new method for performing dynamic Card Validation Value (dCVV) verification, implemented in the context of an improved computer system or device that, among other things, generates modified card track data that includes a dynamic CVV (dCVV) component based on a number of components. Accordingly, embodiments of the claimed invention solves the problem of card security by automatically converting static card data into dynamic one time use card data that can be authenticated by a payment network or processor on behalf of thousands of card issuers as a service, without infrastructure change and integration by each user. In other words, the methods and systems for performing dynamic Card Validation Value verification can provide more security for magnetic strip or chip cards.

The Court of Appeals for the Federal Circuit has recognized that specific technologic modifications to solve a problem are generally patent-eligible subject matter. For example, in *McRo, Inc. v. Bandai Namco Games America, Inc.*, 837 F.3d 1299, 1315-16 (Fed. Cir. 2016), the court upheld a claimed process of improving existing technological processes using a combined order of rules in animation as patent eligible for being not directed to patent ineligible abstract idea in step one of the 2-step framework of *Alice*. In addition, an invention that improves the way computers operate was found to be patent eligible in step one of the 2-step framework of

Alice. See *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1334 (Fed. Cir. 2016) (the invention uses a self-referential table to improve the operation of the computers). In a more recent case, the Court of Appeals for the Federal Circuit has held that claims directed to a non-conventional technique of improving systems of tracking an object on a moving platform as patent eligible in step one of the *Alice* analysis, wherein the improvement is that the technique tracks the object more efficiently (*Thales Visionix Inc. v. United States*, Case No. 2015-5150, decided March 8, 2017; <http://www.cafc.uscourts.gov/sites/default/files/opinions-orders/15-5150.Opinion.3-6-2017.1.PDF>).

The Court also held that claimed inventions “that overcome a problem specifically arising in the realm of computer networks” are patent eligible in step two of the 2-step framework of *Alice*, wherein the invention solves a technology-based problem. See *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014) (the invention addresses the problem of retaining website visitors by creating a hybrid webpage; “the claimed solution amounts to an inventive concept for resolving particular Internet-centric problem”). A claim to an abstract idea of filtering content on the internet by locating a filter in a non-conventional position remote from the end-users thereby overcoming existing problems with other internet filtering systems was held to be patent eligible by passing step two of the 2-step framework of *Alice*. See *Bascom Global Internet Services, Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1351 (Fed. Cir. 2016). Furthermore, the Court held that a claim to a computer program that solves a technological problem of massive data flow congestion forming bottlenecks in computer networks, having an unconventional distributed architecture of distributing the data instead of having all the data stored in a central location, is patent eligible, passing step two of the 2-step framework of *Alice* by providing a sufficient inventive concept because having the generic computer components operate in an unconventional fashion improves computer functionality. See *Amdocs (Israel) Limited v. Openet Telecom, Inc.*, 841 F.3d 1288, 1300-1302 (Fed. Cir. 2016).

In the case law summarized above, the claimed inventions which were found by the court to be patent eligible, under either step of the 2-step framework of *Alice*, have a common theme that the claimed inventions solve certain technological problems. Similar to the case law summarized above, the technical problem and solution detailed above as related to the claimed invention of the subject patent application would render the claims as not “directed to” an abstract idea or law of nature under step one of the 2-step framework of *Alice* because the

claimed invention solves the problem of complexity and cost associated with securing static magnetic strip or chip card data. The claimed method for performing dynamic-Card Validation Value verification is not “directed to” an abstract idea or law of nature. Thus, the claimed subject matter is patent eligible.

Even if the subject claims were considered to be “directed to” an abstract idea under step one of the 2-step framework of *Alice*, the claims would pass step two of the 2-step framework of *Alice* by providing significantly more than the abstract idea since the claimed invention solves a problem of complexity and cost associated with securing static magnetic strip or chip card data. As pointed out above, static magnetic strip or chip card data can be compromised using a number of different methods. In contrast, the method of performing dynamic Card Validation Value verification according to the claimed invention, which is implemented in the context of an improved computer device or system, generates a dCVV based on the card track data from the wallet server, a time-stamp, and the working key, wherein an magnetic stripe storage and transmission device (MST) increments a counter value contained in the time-stamp at each transaction and performs a verification of the dCVV in response to the request for verification, among other things. The combined claim elements use technology to help solve a security issue associated with magnetic strip and chip card data.

Applicants would like to draw the Examiner’s attention to the *Bascom* case, 827 F.3d 1341, 1351 (Fed. Cir. 2016), wherein **solving problems** of existing internet filtering systems by locating a filter **in a non-conventional position** was held by the court to contribute significantly more than an abstract idea and consequently patent eligible in step two of the 2-step framework of *Alice*. Similarly, **solving a technological problem** of data congestion in existing computer networks by having **an unconventional distributed architecture** for data distribution was held by the court to be patent eligible in step two of the 2-step framework of *Alice*. See *Amdocs (Israel) Limited v. Openet Telecom, Inc.*, 841 F.3d 1288, 1300-1302 (Fed. Cir. 2016). The systems and methods of generating an alternative security code of the claimed invention resembles the inventions of *Bascom* and *Amdocs* in that, in the context of an improved computing system/device, it solves a technological problem of securing magnetic strip and chip card data via a technological system and method to generate and verify dynamic Card Validation Values without infrastructure change and integration by each user. Therefore, the claimed invention provides significantly more than an abstract idea, and rises to the level of “inventive

concept,” achieving a status of patent eligibility at least in step two of the 2-step framework of *Alice*.

In light of the reasoning above, withdrawal of the rejection under 35 USC § 101 is respectfully requested.

Claim Rejections under 35 U.S.C. § 112

Claims 14-21 under 35 U.S.C. § 112(a)

On pages 7-8 of the Office Action, the Examiner rejected claims 14-21 under 35 U.S.C. § 112(a). Claim 14 has been amended to specifically recite the applicable server that overcomes the rejection. Support for the amendment can be found, at least, in paragraph [0066], [0067], and [0071] of the specification. The rejections of dependent claims 15-21 are also overcome due to their dependence from independent claim 14.

Claim 14 under 35 U.S.C. § 112(b)

On pages 8-9 of the Office Action, the Examiner rejected claim 14 under 35 U.S.C. § 112(a) for lack of antecedent basis of “the card track data”. Claim 14 has been amended in a manner that overcomes the rejection. Support for the amendment can be found, at least, in paragraph [0066] of the specification.

Claim Rejections under 35 U.S.C. § 103

Claims 14, 15, and 17-21 over Von Mueller, Ward, and Faith

On pages 10-20 of the Office Action, the Examiner rejected claims 14, 15, and 17-21 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication Number 2006/0049256 to von Mueller et al. (hereinafter “von Mueller”), in view of U.S. Patent Publication Number 2010/0098246 to Ward (hereinafter “Ward”), and further in view of U.S. Patent Publication No. 2008/0120236 to Faith et al. (hereinafter “Faith”). Applicant respectfully traverses this rejection.

The claimed invention, as set forth in representative amended claim 14, recites:

14. A method for performing dynamic Card Validation Value (dCVV) verification, comprising:
 - receiving, by a provisioning and authentication server, a request for provisioning of a working key, the request comprising card track data from a wallet server;
 - generating, by the provisioning and authentication server, the working key for the card track data received with the request;

sending, by the provisioning and authentication server, the working key as a response to the request for provisioning;

receiving, by a magnetic stripe storage and transmission device (MST), the working key, the MST comprising a driver and an inductor configured to transmit magnetic pulses to a transaction terminal;

generating, by the MST, a dCVV based on the card track data from the wallet server, a time-stamp, and the working key, wherein the MST increments a counter value contained in the time-stamp at each transaction;

sending modified card track data to the transaction terminal as magnetic pulses transmitted by the MST for processing, or to an e-commerce website for processing, the modified card track data comprising the dCVV and a portion of the card track data, the modified card track data having a format similar to an original format of the card track data;

sending, by the transaction terminal or e-commerce website, the modified card track data to a card issuer server or a third party service provider for authorization;

sending, by the card issuer server or third party service provider, a request for verification of the dCVV, the request including the modified card track data;

receiving, by the provisioning and authentication server, the request for verification of the dCVV from the card issuer server or third party service provider;

performing, by the provisioning and authentication server, a verification of the dCVV in response to the request for verification; and

sending, by the provisioning and authentication server, a verification failure or final verification based on the verification of the dCVV.

In order for the combination of von Mueller, Ward, and Faith to teach the Applicants' claimed invention, the combination of von Mueller, Ward, and Faith must teach each of the elements claimed. Otherwise, the combination cannot be said to teach that element if none of von Mueller, Ward, or Faith disclose that particular element. Applicant respectfully urges, however, that von Mueller, Ward, and Faith do not disclose, at least the recited limitation, ***generating, by the MST, a dCVV based on the card track data from the wallet server, a time-stamp, and the working key, wherein the MST increments a counter value contained in the time-stamp at each transaction.***

More specifically, the Applicants' claimed invention recites an improved method that can

be used to securely perform dynamic Card Validation Value verification. In particular, the claimed invention discloses and particularly claims generating, by the MST, ***a dCVV based on the card track data from the wallet server, a time-stamp, and the working key***, wherein the MST increments a counter value contained in the time-stamp at each transaction. The claimed invention generates a dynamic cryptogram, also called the dynamic-CVV (dCVV), based on each of card track data, a time stamp, and a newly generated working key. As a result, the claimed invention secures magnetic strip and chip card data via a technological system and method to generate and verify dynamic Card Validation Values without infrastructure change and integration by each user.

The Examiner correctly asserts on page 14 of the Office Action that Von Mueller does not teach or suggest among other things, generating a dCVV based on the card track data from the wallet server, a time-stamp, and the working key. Accordingly, Von Mueller does not teach the claimed invention that includes generating, by the MST, a dCVV based on the card track data from the wallet server, a time-stamp, and the working key, wherein the MST increments a counter value contained in the time-stamp at each transaction.

Further, Ward does not rectify the deficiencies of von Mueller. Ward also fails to teach or suggest generating a dCVV based on the card track data from the wallet server, a time-stamp, and the working key, wherein the MST increments a counter value contained in the time-stamp at each transaction. In particular, Ward teaches a device that includes an encryption key management system used to generate encryption keys using seed material. In other words, Ward only teaches using seed material to generate encryption keys rather than a dynamic-CVV, based on each of card track data, a time stamp, and a newly generated working key such as Applicants particularly claim.

In addition, Faith does not rectify the deficiencies of von Mueller and Ward. Faith teaches a method for authenticating a transaction using the verification value and the portion of a counter embedding in the payment data that is in the form of Track data. More specifically, Faith teaches generating a verification value using the counter value that is embedded in the payment data. In other words, Faith only teaches using a single element to generate the verification. Accordingly, Faith like von Mueller and Ward, does not teach or suggest the claimed invention since Faith does not teach or suggest generating, by the MST, a dCVV based on the card track data from the wallet server, a time-stamp, and the working key, wherein the

MST increments a counter value contained in the time-stamp at each transaction as Applicants particularly claim.

Thus, von Mueller, Ward, and Faith taken in any combination, do not disclose or suggest Applicant's presently claimed invention and therefore they do not render the claimed invention obvious under 35 U.S.C. § 103.

Claims 15-21 are dependent claims that depend from allowable independent claim 14. Accordingly, claims 15-21 are also in condition for allowance at least due to their dependency on independent claim 14.

Claim 16 over Von Mueller, Ward, Faith, and Brown

On pages 20-21 of the Office Action, the Examiner rejected claim 16 under 35 U.S.C. § 103(a) as obvious over von Mueller, in view of Ward, further in view of Faith, and further in view of U.S. Patent Publication No. 2007/0136211 to Brown et al. (hereinafter "Brown"). Applicant respectfully traverses this four-way rejection.

First, as discussed above regarding independent claim 1, von Mueller, Ward, and Faith do not teach or suggest, among other things, generating, by the MST, a dCVV based on the card track data from the wallet server, a time-stamp, and the working key, wherein the MST increments a counter value contained in the time-stamp at each transaction.

Further, Brown does not rectify the deficiencies of von Mueller, Ward, and Faith. In particular, Brown was merely relied upon to allegedly cure additional deficiencies the Office Action acknowledges exist in von Mueller.

Thus, von Mueller, Ward, Faith, and Brown do not establish prima facie obviousness under 35 U.S.C. § 103.

Furthermore, claims 16 depends from allowable independent claim 14. Accordingly, claim 16 is in condition for allowance at least due to its dependency on independent claim 14.

CONCLUSION

Should any matters remain, Applicant requests that the undersigned be contacted by phone in order to expedite the allowance of the present case.

If any fees are due in connection with this application, the Patent Office is authorized to deduct the fees from Deposit Account No. 19-1351 as required. If such withdrawal is made, please indicate the attorney docket number (73745.6) on the account statement.

Respectfully submitted,

October 10, 2017
Dated:

/Brian Michaelis/
Brian Michaelis (Reg. No. 34,221)
Customer No. 71130
Counsel for Applicant
SEYFARTH SHAW LLP
World Trade Center East
Two Seaport Lane, Suite 300
Boston, MA 02210
Tel: 617-946-4901
Fax: 617 946-4801
E-mail: bosippto@seyfarth.com



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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/511,994	10/10/2014	Enyang Huang	73745.6

71130
SEYFARTH SHAW LLP
WORLD TRADE CENTER EAST
TWO SEAPORT LANE, SUITE 300
BOSTON, MA 02210-2028

CONFIRMATION NO. 3622
POWER OF ATTORNEY NOTICE



OC000000100331079

Date Mailed: 06/18/2018

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/13/2018.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/cvorachack/



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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/511,994	10/10/2014	Enyang Huang	0210-0271

CONFIRMATION NO. 3622

POA ACCEPTANCE LETTER

68103
Jefferson IP Law, LLP
1130 Connecticut Ave., NW, Suite 420
Washington, DC 20036



Date Mailed: 06/18/2018

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/13/2018.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/cvorachack/



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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
14/511,994	10/10/2014	3685	840	0210-0271	21	3

CONFIRMATION NO. 3622
CORRECTED FILING RECEIPT

68103
Jefferson IP Law, LLP
1130 Connecticut Ave., NW, Suite 420
Washington, DC 20036



Date Mailed: 06/18/2018

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Enyang Huang, Andover, MA;
William Wang Graylin, Winchester, MA;
George Wallner, Miami Beach, FL;

Applicant(s)

Samsung Electronics Co., Ltd., Suwon-si, KOREA, REPUBLIC OF;

Power of Attorney: The patent practitioners associated with Customer Number 68103

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/974,696 04/03/2014
and claims benefit of 61/942,681 02/21/2014

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 10/16/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/511,994**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

Title

METHODS, DEVICES, AND SYSTEMS FOR SECURE PROVISIONING, TRANSMISSION, AND AUTHENTICATION OF PAYMENT DATA

Preliminary Class

705

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



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.
14/511,994	10/10/2014	Enyang Huang	0210-0271	3622
68103	7590	06/28/2018		
Jefferson IP Law, LLP 1130 Connecticut Ave., NW, Suite 420 Washington, DISTRICT OF COLUMBIA 20036 UNITED STATES OF AMERICA			EXAMINER MARTINEZ-HERNANDE, EDGAR R	
			ART UNIT	PAPER NUMBER
			3685	
			NOTIFICATION DATE	DELIVERY MODE
			06/28/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

usdocketing@jeffersonip.com

DETAILED CORRESPONDENCE

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission, filed on 10 of October of 2017, has been entered.

Response to Amendment

3. The following detailed action acknowledges the amendments of the response filed on 10 of October of 2017, by Brian Michaelis (hereinafter referred to as "Applicant's Representative"). The amendments in the filed response have been entered.
 - a. Claim 14 has been amended. The Examiner has confirmed no new matter has been added.
 - b. Claims 1-13 remain withdrawn from consideration.
4. The detailed action further acknowledges amendments to the Claims have overcome the objections and the rejections of the previous application as follows:

- a. The amendment to claim 14 has been fully considered and is persuasive to overcome the rejection under 35 USC 101 for being directed to a judicial exception without significantly more. The claim still recites a statutory category after the amendment, the claims do not recite an abstract idea that can be reasonably determined to be similar to any court case defined by the courts to be abstract, and the claim recites additional elements that are considered significantly more than any abstract idea. Thus, the rejection under 35 USC 101 of claims 14-21 has been withdrawn.
 - b. The amendment to claim 14 has been fully considered and is persuasive to overcome the rejection under 35 USC 112(a). The amendment positively recites the specific servers that perform the functions in the recited method as it is recited in the Specification. The rejection under 112(a) of claims 14-21 has been withdrawn.
 - c. The amendments to claim 14 has been fully considered and is persuasive to overcome the rejection under 35 USC 112(b). The amendment positively recites specific information that clarifies the conditions for the MST to construct modified track 2 data. The rejection under 112(b) of claims 14-21 has been withdrawn.
5. Claims 14-21 are pending in the application and the status of the application is currently pending.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. This application currently names joint inventors. In considering patentability of the claims the examiner presumes that the subject matter of the various claims was commonly owned as of the effective filing date of the claimed invention(s) absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and effective filing dates of each claim that was not commonly owned as of the effective filing date of the later invention in order for the examiner to consider the applicability of 35 U.S.C. 102(b)(2)(C) for any potential 35 U.S.C. 102(a)(2) prior art against the later invention.

9. Claims 14, 15 and 17-21 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Von Mueller (US 2006/0049256, hereinafter "Von Mueller"), further in view of Spodak (US 2013/0024372, hereinafter "Spodak"), further in view of Ward (US 2010/0098246, hereinafter "Ward") and further in view of Faith (US 2008/0120236, hereinafter "Faith").

10. Regarding Claim 14, Von Mueller teaches

- a. Receiving [...] a request for provisioning a working key, the request comprising card track data [...] ("the MSR module generates a new key, encrypts that key with the command or current key, and sends the packet formatted in the applications conventional format with certain clear text information..." See at least ¶ [0020]-[0022]);
- b. [decrypting and storing] the working key for the card track data received with the request (See ¶ [0020]-[0022]);
- c. Sending [...] a response to the request for provisioning (See ¶ [0020]-[0022]);
- d. generating, by the MST, [converted data] based on the card track data [...], a time-stamp, and the working key, wherein the MST increments a counter value contained in the time-stamp at each transaction ("Nineteen digits of the remaining card data are converted to an 8 byte binary value, a time function is added 206 and the result TDES encrypted using an electronic code book (ECB) block encryption 209, The 8 bytes of encrypted data are converted to a 20 digit base 10 number, the least significant 19 digits replace the selected card digits. The last digit is 0 or 1 and is added predefined to a bank field. A new mod 10 character is generated 210 and placed into the selected card digit." See ¶ [0095]; in a similar embodiment, see the

transaction block including the encryption key, a time or counter and track data encrypted together and finally modified, seen in Fig. 5; "The time stamped in the encrypted transaction is compared with the transaction processing server and if out of date the transaction is rejected and a new card swipe requested. If the new card swipe date stamp is equal to the previous data a fraudulent transaction is flagged. If the date stamp is out of date by an amount equal to the duration between stamps, the transaction is allowed and the date inaccuracy noted in the servers transition data base. In the same manner, if a real time clock is not available the secure module increments a counter for each transaction the reader makes. The processing server compares the count in the current encrypted transaction request to the last received count." See ¶ [0035]; example includes a signature for authentication: "In an alternate method the POS server forwards the encrypted card and signature to an enabled transaction server to both authenticate and decrypt the card data." See at least ¶ [0094]);

- e. sending modified card track data to the transaction terminal as magnetic pulses transmitted by the MST for processing, or to an e-commerce website for processing, the modified card track data comprising [...] a portion of the card track data, the modified card track data having a format similar to an original format of the card track data (starting from Fig. 5, device 44, moving data to server 151, in Fig. 22; "multiple PDAs 111, table mounted POS terminal with secure module for order entry and payment along with internet access 150, and a point of sale register with wireless capabilities are all connected to a wireless local area network (WAN) 152. This WAN, and any hard wired POS registers communicate with a local POS

application server 151 which is connected via the Internet and secure connections to a TDES encryption database and transaction processing server." See at least ¶ [0094]; "The 8 bytes of encrypted data are converted to a 20 digit base 10 number, the least significant 19 digits replace the selected card digits." See at least ¶ [0095]);

- f. sending, by the transaction terminal or e-commerce website, the modified card track data to a card issuer server or a third party service provider for authorization (see ¶ [0101]-[0102]);
- g. sending, by the card issuer server or third party service provider, a request for verification of [the signature], the request including the modified card track data (see ¶ [0101]-[0102]);
- h. receiving [...] the request for verification of [the signature] from the card issuer server or third party service provider ("the local POS application server either requests the authentication sever to verify the cards authenticity and sends that response along with the encrypted card data to the new transaction server or additionally requests the encryption keys and formats the data for a legacy transaction server." See at least ¶ [0094]);
- i. performing [...] a verification of [the signature] in response to the request for verification (one example including authentication: "The selected keys are used to decode signature data along with a hash code generated by the secure module from the card data account number. The hash value generated from the card data is used to index the secure stripe database to retrieve the card signature. The database signature is then compared to the decrypted transaction signature and based on the comparison the transaction is sent to the processing bank indicated in the signature

database or a message is sent back to the card holder requesting verification of the card's authenticity which may be in the form of a re-swipe of the card or entry of additional information such as billing zip code at which point the transaction is sent to the processing bank using standard formats or declined." See ¶ [0116]);

- j. sending [...] a verification failure or final verification based on the verification of [signature] (see ¶ [0116]).

11. Von Mueller further teaches the Authentication database server or service and an encryption key database server or service (See at least Fig. 17). Von Mueller further teaches receiving a request for a new key (as recited in the claim, the function of "receiving a request" is interpreted as a result of an action performed with the MST: "In the case of the new key request command, the card is swiped while the head module is connected to the handheld computing device which is browsing the WAP site supporting this application." See ¶ [0020]).

12. Von Mueller does not expressly teach acquiring card track data from a wallet server. However, it is obvious for one of ordinary skill in the art to exchange the use of a card swiped in a card reader with functions of a digital wallet application. The limitation is interpreted to obviously include a digital wallet application running locally on the local device that comprises the MST, and is further interpreted to obviously include a network connection between the wallet application and the wallet server. It is known in the art that a digital wallet can store data from any payment method, which includes a financial account card (bank card or credit card). An example of using either or both the e-wallet and a payment card interchangeably is in Spodak (US 2013/0024372, hereinafter "Spodak") in Figs 15A – 15C.

13. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to “use a dynamic payment card with a wallet application”, as taught by Spodak, since the examiner takes Official Notice of the equivalence of “a payment card stored in a digital wallet” and “a physical payment card” for their use in “receiving a request for provisioning a working key, the request comprising card track data” and the selection of any of these known equivalence would be within the level of ordinary skill in the art.

14. Von Mueller, in view of Spodak, does not expressly teach generating the working key and providing the working key in response to the request.

15. However, Ward does teach receiving a request to generate an encryption key, generating the encryption key and providing the encryption key in response to the request (“FIG. 3 shows an example of a method 300 of generating an encryption key using an EKMS (e.g., the EKMS 100 of FIG. 1) in accordance with certain implementations of the disclosed technology. At 302, the EKMS receives a request to create an encryption key.... At 304, the EKMS obtains seed material (e.g., n-bits of random data) using a random sequence generator, for example. At 306, the EKMS obtains the X509 certificate's private key. At 308, the EKMS uses an encryption key generation algorithm to generate the requested encryption key. The algorithm can be used to generate encryption keys given an X509 certificate and associated private key.... At 310, the EKMS returns the generated encryption key to the requestor.” See ¶ [0045]-[0052]).

16. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include “generating an encryption key at a request”, as taught by Ward, by modifying the process to generate the

key at the server instead of at the card reader, to further improve the process of securing the account data for smart cards that may be used in card-not-present transactions or online transactions.

17. Von Mueller, in view of Spodak and in view of Ward, does not explicitly teach generating the dCVV based on a time-stamp.

18. However, Faith does teach generating a dCVV based on a counter ("Portable consumer device 30 generates a verification value using the counter and/or other dynamic data elements (step 220). The verification value and a portion of the counter are embedded in payment data that is in the form of Track data." See at least ¶ [0073]).

19. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "a verification value generator", as taught by Faith, as part of the process of generating converted data in the card reader, to further improve the secure authentication of a personal account number for any transaction.

20. **Regarding Claim 15**, Von Mueller, in view of Spodak, in view of Ward and in view of Faith, teaches the limitations of claim 14. Von Mueller further teaches the modified card track data includes a primary account number, an expiration date and a service code (Account Number, Expire Date and Bank Fields, see Fig. 23) and a time-stamp or counter ("It is yet a further advantage of the present invention to allow the encrypted magnetic head module to communicate with a real time clock or a global positioning system (GPS) receiver either internal to the phone or reader to tag all data transaction with date, time and location information. This is especially required in POS financial transaction that are mobile to verify where and when the transaction that the transaction occurred. Stamping

the data with the date and time prevents the encrypted card information from being recorded and used to make multiple transactions at a later date. The time stamped in the encrypted transaction is compared with the transaction processing server and if out of date the transaction is rejected and a new card swipe requested." See ¶ [0035] and Fig. 23).

21. Von Mueller, in view of Ward, does not explicitly teach the dCVV.

22. However, Faith does teach a verification value created for the verification of the card data ("Server 72 of service provider 70 retrieves its counter stored in counter database 76 and uses it to calculate a verification value (step 250) using an algorithm. The algorithm may follow steps similar to those shown in FIG. 2 to calculate the verification value. The calculated verification value is compared to the verification value received in the Track data." See at least ¶ [0078]).

23. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "a verification value generator", as taught by Faith, used in the modified card track data, to further improve the secure authentication of a personal account number for any transaction.

24. **Regarding Claim 17 and 18**, Von Mueller, in view of Spodak, in view of Ward and in view of Faith, teaches the limitations of claim 14. Von Mueller further teaches comparing a received time-stamp or received counter with a stored time-stamp or a current time of the server or stored counter ("The time stamped in the encrypted transaction is compared with the transaction processing server and if out of date the transaction is rejected and a new card swipe requested. If the new card swipe date stamp is equal to the previous data a fraudulent transaction is flagged. If the date stamp is out of date by an amount equal to the duration between stamps, the transaction is allowed and the date inaccuracy noted in the

servers transition data base." See ¶ [0035]] and sending the verification failure in response to the stored time-stamp or current time of the server corresponding to a time greater than the received time-stamp ("In the same manner, if a real time clock is not available the secure module increments a counter for each transaction the reader makes. The processing server compares the count in the current encrypted transaction request to the last received count. If the count is greater than the previous count, the transaction is accepted and the new count stored in the transaction data base. In addition to providing for testing for reused previously recorded transaction data, the counter is used to change the encrypted transaction data. The output for swiping the same card multiple times will always be different Therefore any data stolen from the merchant's servers cannot be reused to make a duplicate transaction." See ¶ [0035]).

25. **Regarding Claim 19**, Von Mueller, in view of Spodak, in view of Ward and in view of Faith, teaches the limitations of claim 14. Von Mueller further teaches comparing the [signature] to determine authenticity ("The application server requests the Authentication database server or service 130 to verify the magnetic stripe authenticity using the account hash code to index the stored signature value for the magnetic stripe. The results of the signature comparison are used to determine if the card transaction should be terminated or forwarded to the legacy transaction processor based on acceptance rules contained within the encryption database 121." See at least ¶ [0087]).

26. Von Mueller, in view of Spodak and in view of Ward, does not expressly teach independently computing, by the server, a dCVV value using the working key in response to receiving the request for verification.

27. However, Faith does teach independently computing, by the server, a dCVV value ("Server 72 of service provider 70 retrieves its counter stored in counter database 76 and uses it to calculate a verification value (step 250) using an algorithm. The algorithm may follow steps similar to those shown in FIG. 2 to calculate the verification value. The calculated verification value is compared to the verification value received in the Track data." See at least ¶ [0078]).

28. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "computing a dCVV value by the server", as taught by Faith, used in the comparison for authentication of data to further protect the account number during the authentication of the card used in any transaction.

29. **Regarding Claim 20**, Von Mueller, in view of Spodak, in view of Ward and in view of Faith, teaches the limitations of claim 14. Von Mueller further teaches sending the final verification in response to the [stored signature] matching the received [signature] ("The database signature is then compared to the decrypted transaction signature and based on the comparison the transaction is sent to the processing bank indicated in the signature database or a message is sent back to the card holder requesting verification of the card's authenticity which may be in the form of a re-swipe of the card or entry of additional information such as billing zip code at which point the transaction is sent to the processing bank using standard formats or declined." See example in ¶ [0116]).

30. Von Mueller, in view of Spodak and in view of Ward, does not expressly teach the dCVV used in the comparison for authentication.

31. However, Faith does teach a dCVV created for the verification of the card data (See ¶ [0078]-[0080]).

32. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "a dCVV generator", as taught by Faith, used in the comparison for authentication of data to further protect the account number during the authentication of the card used in any transaction.

33. **Regarding Claim 21**, Von Mueller, in view of Spodak, in view of Ward and in view of Faith, teaches the limitations of claim 14. Von Mueller further teaches replacing dynamic content included in the modified track data, including the dCVV, with original track content to restore original card track data, and sending the original card track data to the card issuer server for processing via the card issuer server's normal processing methods to complete the transaction, wherein the original card track data corresponds to the card track data as originally issued by a card issuer, the card issuer corresponding to the card issuer server ("The application server requests the encryption key database server or service 121, which is located on the same intranet or within the same computer, to accept the encrypted data and return decrypted transaction data. The returned decrypted transaction data is formatted by the WAP application server suitable to the required transaction processor 116 and the transaction processed using current bank rules." See ¶ [0088]-[0089] and [0096] and Fig. 16-23).

34. **Claim 16 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Von Mueller, further in view of Spodak, further in view of Ward, further in view of Faith and further in view of Brown (US 2007/0136211, hereinafter referred to as "Brown").**

35. **Regarding Claim 16**, Von Mueller, in view of Spodak, in view of Ward and in view of Faith, teaches the limitations of claim 14. Von Mueller, in view of Spodak, in view of Ward and in view of Faith, does not explicitly teach the modified card track data further includes a separate mode indicator, when the expiry date or the primary account number is not used, to indicate that authorization is to be performed in a dCVV mode that includes the verification of the dCVV, and that the mode indicator indicates to the card issuer server that the modified card track data is dCVV card track data and authorization is to be performed in a dCVV mode.

36. However, Brown does teach an indicator field ("The ISO 7810/7816 specifications and ABA/1ATA stripe data fields describe a "discretionary field", and "other data field" that can be used exclusively for the issuing bank. These can be used to place operators, which can be as simple as a single status bit." See ¶ [0076] and Fig. 4F) as a plain text indicator that indicates the modified card track data is dCVV card track data (includes cryptograms and plaintext used in CVx type authentication, see at least ¶ [0137]-[0140]) and authorization is to be performed in a dCVV mode (identification of a CVQ (card verification number) cryptogram is followed by the process in Fig. 6, "CVx authentication uses data that is on Track2. The remote server can only authenticate using data on-hand and the bank key." See at least ¶ [0141]-[0147]).

37. It would have been obvious to a person having ordinary skill in the art at the time the invention was filed to modify the teachings of Von Mueller to include "a dCVV component code (CVQ) and performing a dCVV authorization", as taught by Brown, to further secure the account number during an authentication of the account for any transaction.

Response to Arguments

38. Applicant's arguments, filed 10 of October of 2017, with respect to the rejections under 35 USC 103 have been fully considered.

39. **Regarding the rejection under 35 USC 103(a)**, the Examiner has considered the amendments and the arguments in view of the prior art.

40. The Applicant argues: "Applicant respectfully urges, however, that von Mueller, Ward, and Faith do not disclose, at least the recited limitation, generating, by the MST, a dCVV based on the card track data from the wallet server, a time-stamp, and the working key, wherein the MST increments a counter value contained in the time-stamp at each transaction. More specifically, the Applicants' claimed invention recites an improved method that can be used to securely perform dynamic Card Validation Value verification. In particular, the claimed invention discloses and particularly claims generating, by the MST, a dCVV based on the card track data from the wallet server, a time-stamp, and the working key, wherein the MST increments a counter value contained in the time-stamp at each transaction. The claimed invention generates a dynamic cryptogram, also called the dynamic-CVV (dCVV), based on each of card track data, a time stamp, and a newly generated working key. As a result, the claimed invention secures magnetic strip and chip card data via a technological system and method to generate and verify dynamic Card Validation Values without infrastructure change and integration by each user."

41. In response to applicant's arguments against the references individually (See Remarks), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

42. In response to the arguments against the references in combination, Claim 14 recites functions of various elements that in combination provide a result that is similar to the results of each element individually. For example, the acquisition of data from a wallet server result in the acquisition of the card data as if the card was swiped in a portable device. Spodak teaches this function and the results are the same even if the elements were interchanged in the art of Von Mueller. In another example, the device that includes an MST is similar to the device that includes an NFC, where a specific application running on said device is capable of converting the received data to a secure format, which in this case is encrypted with a key, and then transmits the data through a magnetic field that is possible for the NFC as well as for the MST. Ward teaches the generation of an encryption key as per request and Faith teaches generating a dynamic verification value using a counter and other dynamic elements. Faith specifically teaches the creation of a dCVV based on a counter that changes after every transaction is a conventional function previously known in the art (See Faith in ¶ [0006]). Thus, the combination of Von Mueller, Spodak, Ward and Faith teach the elements recited in the claim in combination provide the result of protecting magnetic stripe data in transit from the magnetic stripe reader to a host computer while maintaining compatibility with the data format contained within the magnetic stripe data, which is the same as the result from Von Mueller, Spodak, Ward and Faith individually. One would be motivated to combine the claimed inventions of Von Mueller, Spodak, Ward and Faith to encourage multiple versions of securing personal account information prior to use in a transaction to deter theft and fraudulent use of the personal account information.

43. The Prior Art made of record and not relied upon is considered pertinent to Applicant's disclosure, and is listed in the attached form PTO-892 (Notice of References Cited). Unless expressly noted otherwise by the Examiner, all documents listed on form PTO-892 are cited in their entirety.

44. The Examiner respectfully welcomes a telephonic interview with Applicant to discuss any items that will advance prosecution. A suggested topic is the use of the claimed invention in a transaction.

Conclusion

45. Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDGAR R MARTINEZ-HERNANDEZ whose telephone number is (571)270-0658. The examiner can normally be reached on M-F from 9:00 am - 5:00 pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, JOHN W. HAYES can be reached on 571-272-6708. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/EDGAR R MARTINEZ-HERNANDEZ/
Examiner, Art Unit 3685

/MAMON OBEID/
Primary Examiner, Art Unit 3685