



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
61/413,926	11/15/2010	Joseph Zipperer	26629-17764

25315
LOWE GRAHAM JONES, PLLC
701 FIFTH AVENUE
SUITE 4800
SEATTLE, WA 98104

CONFIRMATION NO. 1652
POA ACCEPTANCE LETTER



Date Mailed: 08/13/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/03/2012.

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.

/tpetros/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☒ Practitioners associated with the Customer Number: 25315

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☒ The address associated with Customer Number: 25315

OR

☐ Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		

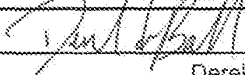
Assignee Name and Address:

Media IP, LLC
220 W. Mercer Street, Suite W-430
Seattle, WA 98119

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	5/2/2012
Name	Derek de Bakker	Telephone	206-979-1045
Title	Manager		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.31 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Media IP, LLC

Application No./Patent No.: 61/413,926

Filed/Issue Date: November 15, 2010

Titled: VIRTUAL SECURE DIGITAL CARD

Media IP, LLC, a limited liability company

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;
2. ☐ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or
3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

- A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy therefore is attached.

OR

- B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Joseph Zipperer et al. To: MOD Systems Incorporated

The document was recorded in the United States Patent and Trademark Office at
Reel 025672, Frame 0625, or for which a copy thereof is attached.

2. From: MOD Systems Incorporated To: MOD Asset Preservation LLC

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

3. From: MOD Asset Preservation LLC To: Media IP, LLC

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

- ☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Ellen M. Bierman/

Signature

August 3, 2012

Date

Ellen M. Bierman

Printed or Typed Name

Attorney of Record

Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ACKNOWLEDGMENT AND ASSIGNMENT

WHEREAS, MOD Systems Incorporated (hereinafter referred to as MOD), MOD Asset Preservation LLC (hereinafter referred to as MAP), and Media IP, LLC (hereinafter referred to as Media IP), collectively the Parties, wish to avoid any uncertainty with regard to ownership of the Patents and Patent Applications listed in the attached Schedule A (hereinafter referred to collectively as INVENTIONS) and wish to transfer all rights in the INVENTIONS to Media IP;

WHEREAS, MOD, whose office was located at 1301 2nd Avenue, #501, Seattle, WA 98101, was the owner of the INVENTIONS;

WHEREAS, MOD surrendered its business and assets, including the INVENTIONS, as part of a Surrender of Collateral, Consent to Strict Foreclosure, and Release Agreement (UCC 9A-620) dated on or about March 22, 2011 to MAP, having an address of 220 West Mercer Street, Suite W-430, Seattle, WA 98119;

WHEREAS, Media IP, a Washington Limited Liability Company having a principal address at 220 W. Mercer Street, Suite W-430, Seattle, WA 98119, desires the entire right, title and interest in and to the INVENTIONS; and

WHEREAS, the Parties hereto wish to provide, via this Assignment, a complete and formal transfer of all rights, to the extent any exist from MOD and MAP, to Media IP in a form suitable for recordation with the U.S. Patent and Trademark Office;

NOW, THEREFORE, for ten U.S. dollars (\$10.00) and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, MOD and MAP (collectively ASSIGNORS) hereby sell, assign and transfer to Media IP, individually and collectively, their entire right, title and interest in and to the INVENTIONS, and any and all applications and letters patent which may be granted for the INVENTIONS in the United States of America and its territorial possessions and in any and all other countries, and in any and all divisions, reissues and continuations thereof, including the right to file applications directly in the name of Media IP and to claim priority rights deriving from said United States application to which said foreign applications are entitled by virtue of international convention, treaty or otherwise, said INVENTIONS, applications and all letters patent on said INVENTIONS to be held and enjoyed by Media IP and its successors and assigns as fully and entirely as the same would have been held and enjoyed by ASSIGNORS had this assignment, transfer and sale not

been made. ASSIGNORS hereby authorize and request the Commissioner of Patents and Trademarks to issue all letters patent on said INVENTIONS to Media IP.

MOD and MAP each agree to execute all instruments and documents as may be reasonably required by Media IP for the making and prosecution of applications for United States and foreign letters patent on said INVENTIONS, or for the purpose of protecting title to said INVENTIONS or letters patent therefor.

MOD Systems Incorporated

Date: June 26, 2012 By: Julia DeHaan

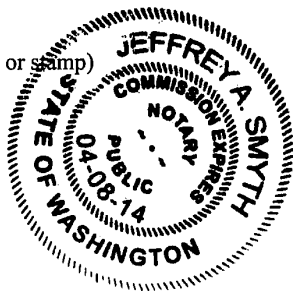
Julia DeHaan, Director, for MOD Systems Incorporated

STATE OF Washington)
COUNTY OF King) ss.

I certify that I know or have satisfactory evidence that Julia DeHaan is the person who appeared before me and signed this instrument and acknowledged such signature to be a voluntary act for the purposes mentioned in the instrument.

Dated: 6-26-12

(Seal or Stamp)



Signature: [Signature]
Printed Name: JEFF SMYTH
Notary Public
My appointment expires 4-8-14

MOD Asset Preservation LLC

Date: June 26, 2012 By: Julia de Haan

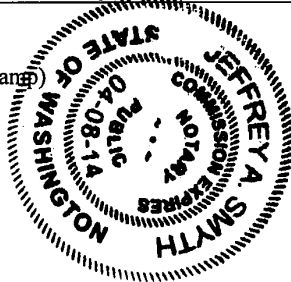
Julia DeHaan, Manager, for MOD Asset
Preservation LLC

STATE OF Washington)
) ss.
COUNTY OF King)

I certify that I know or have satisfactory evidence that Julia DeHaan is the person who appeared before me and signed this instrument and acknowledged such signature to be a voluntary act for the purposes mentioned in the instrument.

Dated: 6-26-12

(Seal or stamp)



[Signature]
Signature
Printed Name: JEFF SMYTH
Notary Public
My appointment expires 4-8-14

Media IP, LLC

Date: June 26, 2012 By: Derek de Bakker

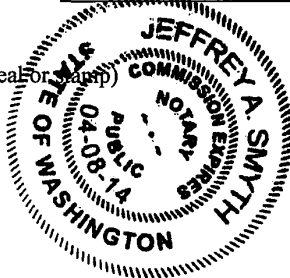
Derek de Bakker, Manager, for Media IP, LLC

STATE OF Washington)
) ss.
COUNTY OF King)

I certify that I know or have satisfactory evidence that Derek de Bakker is the person who appeared before me and signed this instrument and acknowledged such signature to be a voluntary act for the purposes mentioned in the instrument.

Dated: 6-26-12

(Seal or stamp)



[Signature]
Signature
Printed Name: JEFF SMYTH
Notary Public
My appointment expires 4-8-14

SCHEDULE A

Application No.	App. Date	Publication No.	Pub. Date	Patent No.	Issue Date	Title
61/474,671	4/12/11					KIOSK DISTRIBUTION OF LICENSED CONTENT TO PORTABLE DEVICES WITHIN DVD AVAILABILITY WINDOW
61/478,204	4/22/11					ACCESS CONTROLS FOR KNOWN CONTENT
61/413,926	11/15/10					VIRTUAL SECURE DIGITAL CARD
13/078,323	4/1/11					VIRTUAL SECURE DIGITAL CARD
13/073,802	3/28/11					READ AND WRITE OPTIMIZATION FOR PROTECTED AREA OF MEMORY
61/294,070	1/11/10					CONTENT AND IDENTITY DELIVERY SYSTEM FOR PORTABLE PLAYBACK OF CONTENT AND STREAMING SERVICE INTEGRATION
13/004,806	1/11/11					CONTENT AND IDENTITY DELIVERY SYSTEM FOR PORTABLE PLAYBACK OF CONTENT AND STREAMING SERVICE INTEGRATION
61/253,777	10/21/09					RESUME POINT FOR DIGITAL MEDIA PLAYBACK
12/906,949	10/18/10	US11/0091187	4/21/11			RESUME POINT FOR DIGITAL MEDIA PLAYBACK



Application No.	App. Date	Publication No.	Pub. Date	Patent No.	Issue Date	Title
61/253,792	10/21/09					CONTEXTUAL CHAPTER NAVIGATION
12/906,941	10/18/10	US11/0197131	8/11/11			CONTEXTUAL CHAPTER NAVIGATION
61/253,789	10/21/09					HIGH-SPEED SECURE CONTENT TRANSFER TO SD CARD FROM KIOSK
12/906,938	10/18/10	US11/0093622	4/21/11			HIGH-SPEED SECURE CONTENT TRANSFER TO SD CARD FROM KIOSK
PCT/US10/53118	10/19/10	WO 11/049902	4/28/11			HIGH-SPEED SECURE CONTENT TRANSFER TO SD CARD FROM KIOSK
60/851,631	10/13/06					DIGITAL CONTENT DELIVERY SYSTEM
11/974,918	10/15/07	US08/0133546	6/5/08	7,779,064	8/17/10	METHOD AND SYSTEM FOR EFFICIENT AND DYNAMICALLY ADAPTABLE DIGITALLY-ENCODED-INFORMATION DISTRIBUTION

Electronic Acknowledgement Receipt	
EFS ID:	13419009
Application Number:	61413926
International Application Number:	
Confirmation Number:	1652
Title of Invention:	Virtual Secure Digital Card
First Named Inventor/Applicant Name:	Joseph Zipperer
Customer Number:	758
Filer:	Ellen M Bierman/Kimberly Papp
Filer Authorized By:	Ellen M Bierman
Attorney Docket Number:	26629-17764
Receipt Date:	03-AUG-2012
Filing Date:	15-NOV-2010
Time Stamp:	19:14:04
Application Type:	Provisional

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	MDIP-5-1001XPOA.pdf	621505	no	2
			13188915de48d86d28825c971385a5cd2924f01		

Warnings:

Information:

2	Assignee showing of ownership per 37 CFR 3.73(b).	MDIP-1-1403SB96.pdf	428500	no	2				
			906392cb8de2fc3c866de428b9d5c4c8ce67dd86						
Warnings:									
Information:									
3	Assignee showing of ownership per 37 CFR 3.73(b).	MDIP-5-1001XAsgn.pdf	457580	no	5				
			8f1782bd3415e2eb2fa3b6c39f2f384d5466b375						
Warnings:									
Information:									
Total Files Size (in bytes):			1507585						
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.									



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
61/413,926	11/15/2010		220	26629-17764		

CONFIRMATION NO. 1652

758
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

FILING RECEIPT



OC000000045026909

Date Mailed: 12/27/2010

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. 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**

Applicant(s)

Joseph Zipperer, Seattle, WA;
John Calixto, Seattle, WA;

Power of Attorney:

Rajiv Patel--39327

If Required, Foreign Filing License Granted: 12/17/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/413,926**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No
Title

Virtual Secure Digital Card

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

page 1 of 3

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 (1-866-999-4158).

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).

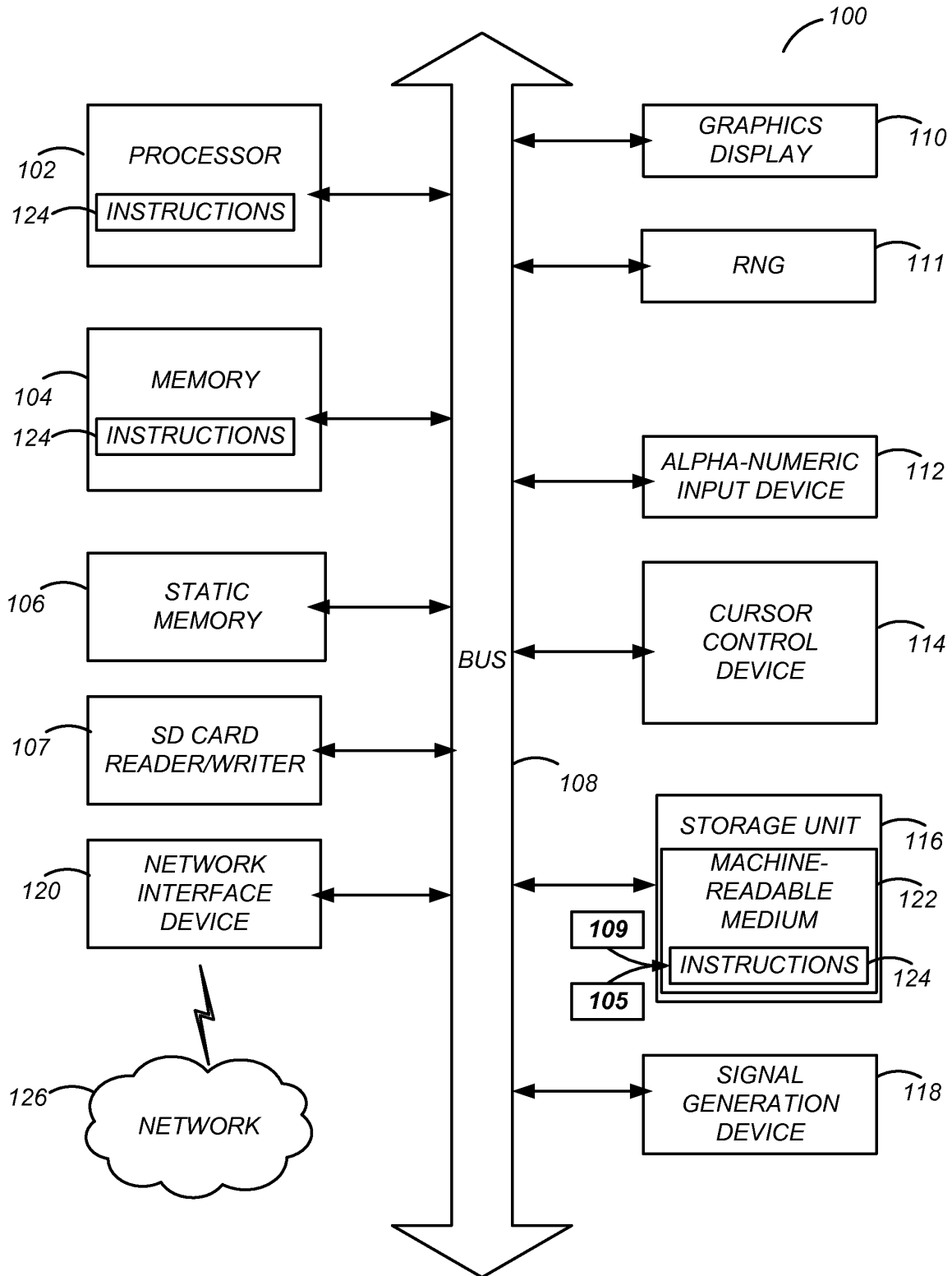


FIG. 1a

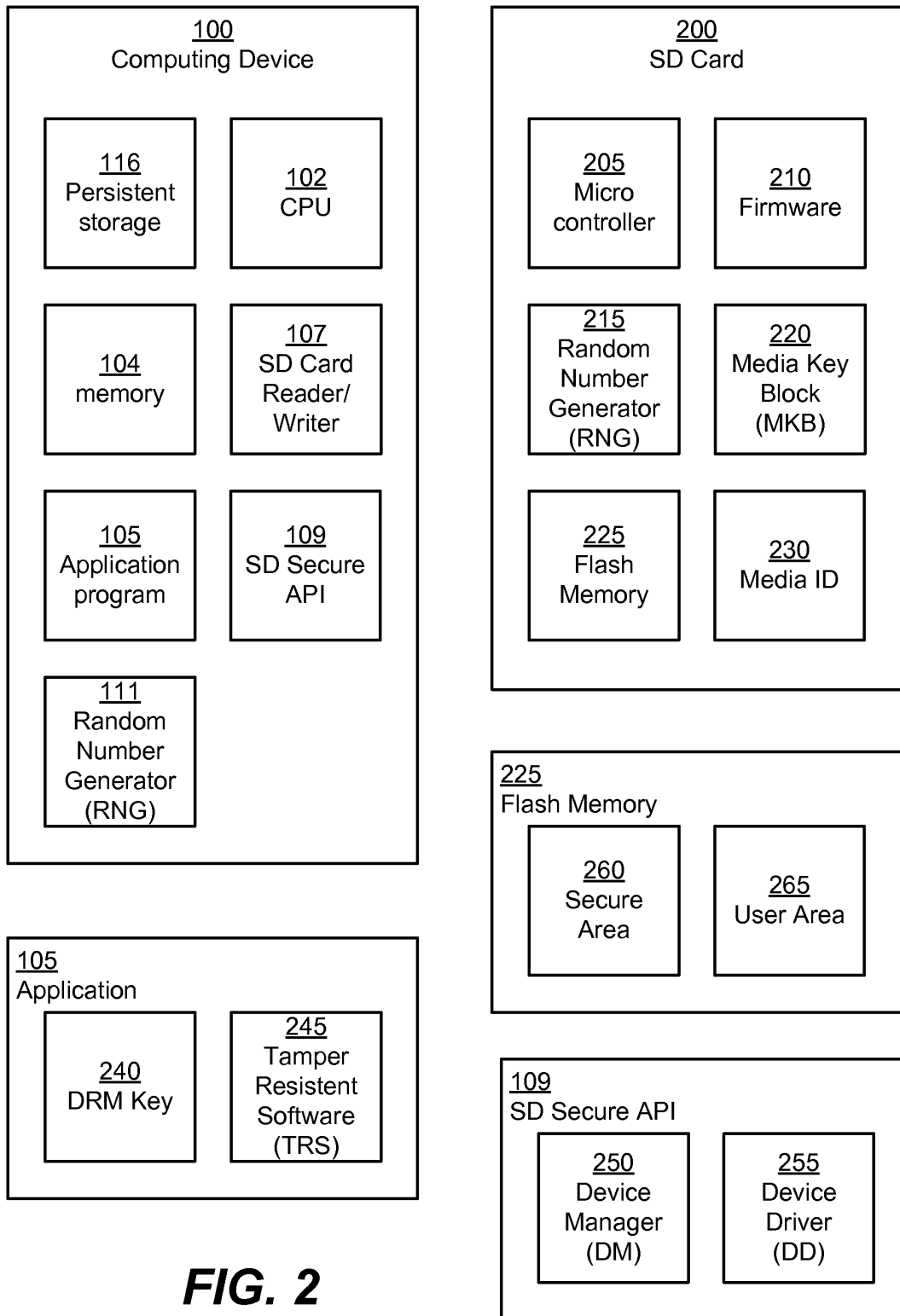


FIG. 2

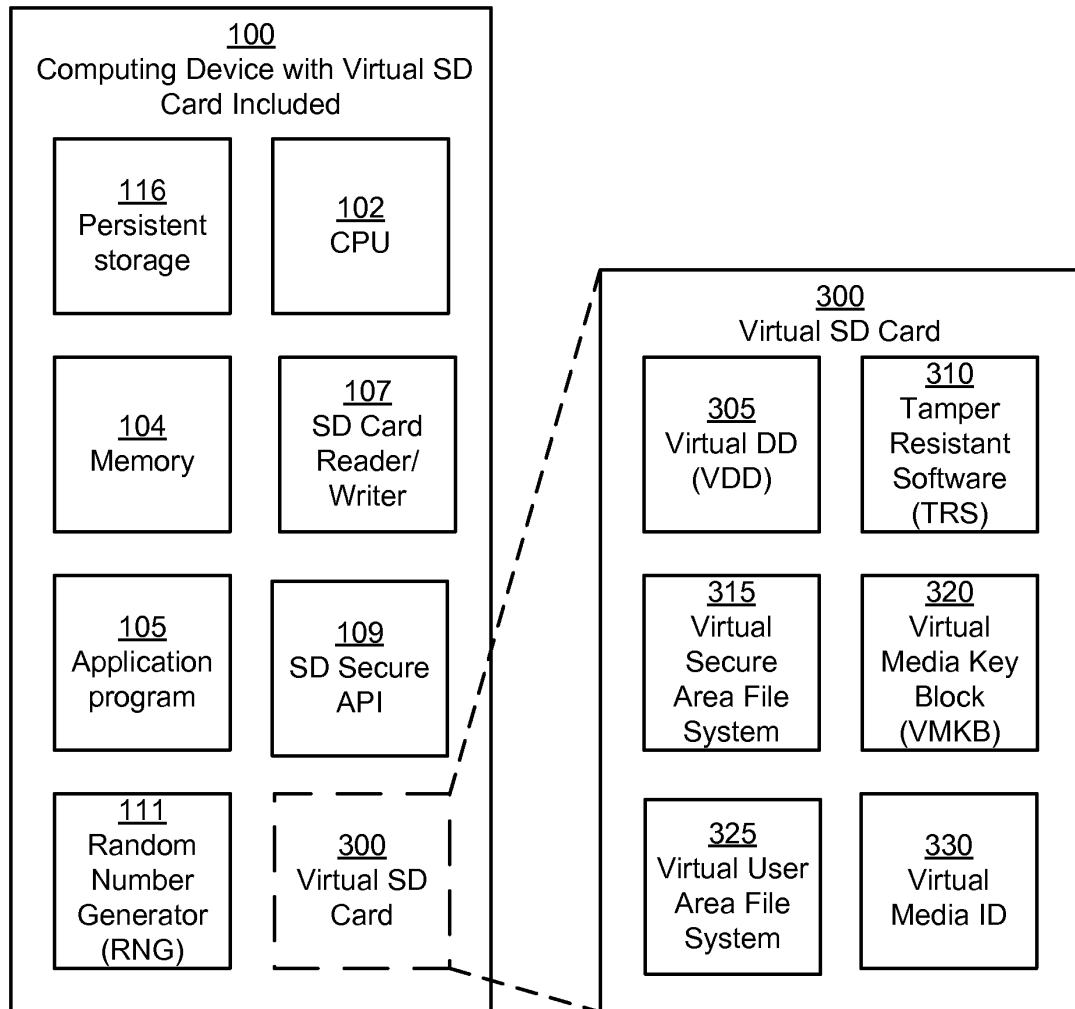


FIG. 3

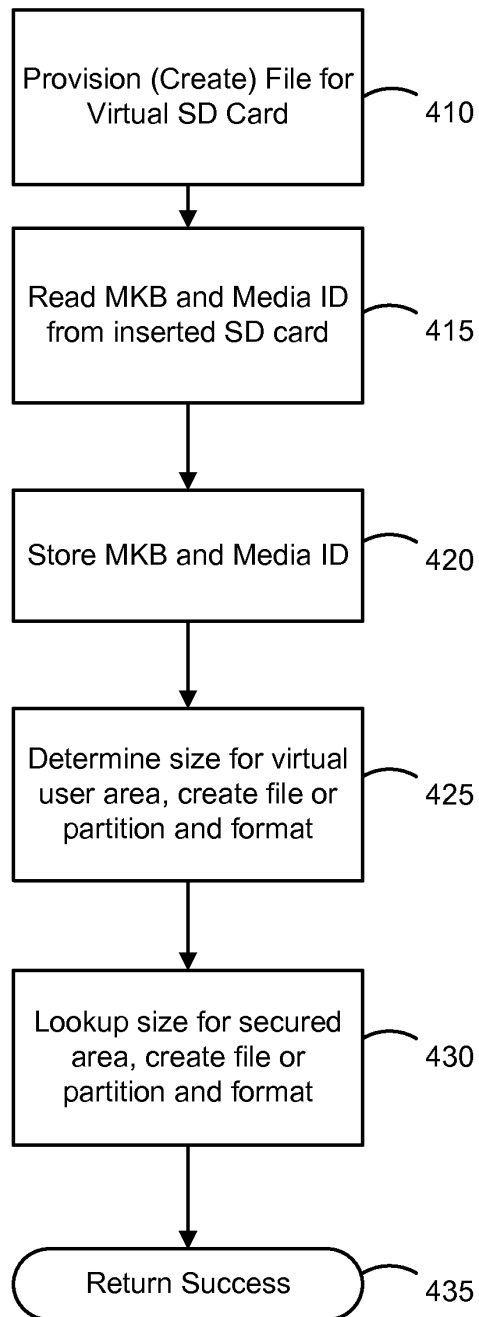


FIG. 4

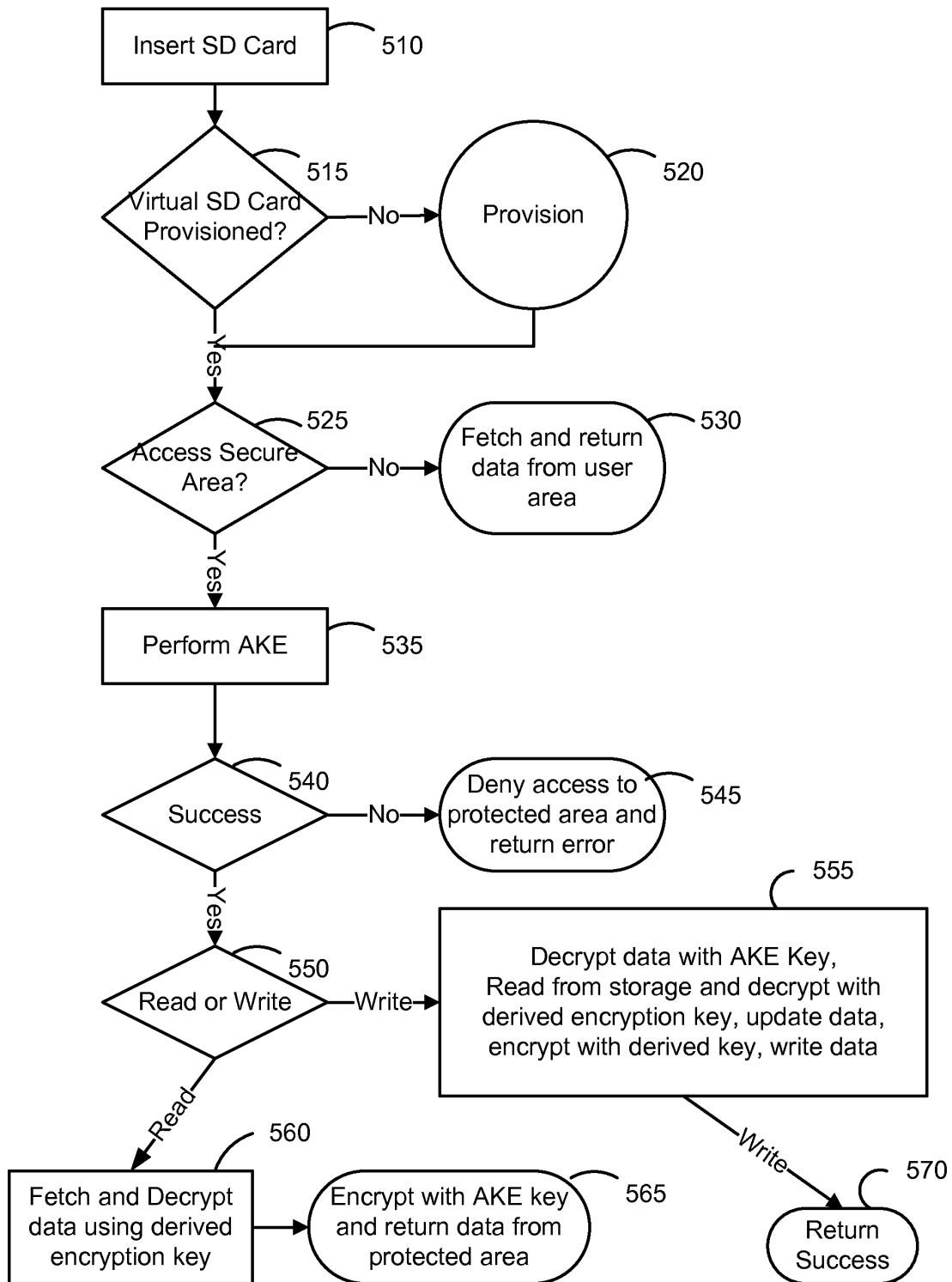


FIG. 5

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name	Middle Name	Family Name	City	State	Country i
Joseph		Zipperer	Seattle	WA	US

Inventor 2

Remove

Given Name	Middle Name	Family Name	City	State	Country i
John		Calixto	Seattle	WA	US

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.**Add****Title of Invention**

Virtual Secure Digital Card

Attorney Docket Number (if applicable)

26629-17764

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number ☐ Firm or Individual Name

Customer Number

00758

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Entity Status

Applicant claims small entity status under 37 CFR 1.27

☐ Yes, applicant qualifies for small entity status under 37 CFR 1.27☒ No**Warning**

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Rajiv P. Patel/			Date (YYYY-MM-DD)	2010-11-15
First Name	Rajiv P.	Last Name	Patel	Registration Number (If appropriate)	39327

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to a n other federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

VIRTUAL SECURE DIGITAL CARD

INVENTORS:
JOSEPH ZIPPERER
JOHN CALIXTO

BACKGROUND

1. FIELD OF ART

[0001] The disclosure generally relates to the field of memory devices, and more particularly, generation of virtual memory devices.

2. DESCRIPTION OF THE RELATED ART

[0002] Today, Secure Digital (SD) cards are in wide use for many storage applications including audio (MP3 players), pictures (digital cameras), and full motion video (camcorders and HD camcorders). The SD card provides an acceptable portable storage medium to transfer unprotected content between different devices, especially for the video capture devices mentioned above. The content stored on SD cards can be transferred or archived to devices with larger storage capacities and additional processing capabilities. One such additional processing capability allows consumers to create and manage a digital archive of consumer generated content.

[0003] Consumers are familiar with the storage capabilities, but there are a very few applications which take advantage of the security (the S in secure digital) features of the SD card. Today's applications that use the security features are enable digital rights management (DRM) to protect the content from copying or other forms of piracy. Examples of DRM applications include still images (Gallery Player) and full-motion video (1-seg and GreenPlay). DRM protected content on the aforementioned SD cards cannot be archived easily. The DRM protection must remain intact during generation, transfer, and archival. While an SD card is suited for generation and transfer, it is not as well suited for the archival aspect.

[0004] While SD cards are suited to purchasing and transporting content, they are not a suitable method for creating a digital library. The main reasons correspond to the primary use of SD cards as a portable storage medium. Accordingly, the size and the lack of labeling on the SD

card results in an undesirable format for a digital library. Although SD cards are available currently in up to 64 gigabyte (GB) capacity, a typical digital rights management (DRM)-protected commercial video is approximately 2 GB. Therefore, only 32 DRM-protected commercial videos can be stored on any single SD card. Multiple SD cards are therefore required in order to create a digital library of any significant capacity. In contrast, hard disk drives are in abundant supply in sizes ranging from several hundred gigabytes to few tens of terabytes. These allow for storing upwards of 5000 DRM-protected commercial videos.

[0005] DRM configurations used by SD cards can be legally moved and/or copied to other DRM-compliant devices because the anti-piracy mechanism is maintained, but technical hurdles have prevented this. For example, a DRM license agreement specifies the process requirements for moving content to/from the SD card, but does not specify the file formats for the non-SD card device. In addition, file structures and data to implement the DRM are complex and have many entities. A typical secure exchange to move/copy content may require a minimum of 150 secure operations for the DRM portion alone. Maintaining the complex relationships within a new file structure presents a substantial processing and memory resources challenges in addition to the effort of developing software code to maintain and manage the process. Another challenge is software security architecture external to SD cards is only defined for personal computer (PC) architectures. It is not defined for other software or hardware architectures including may devices which utilize SD cards that need to implement DRM such as mobile phones, TV, set top boxes, and Blu-ray disc players and the like. Further, many devices may not implement internal SD card for a variety of reasons including cost, space considerations for connectors, and the lack of software drivers implementing secure access. These devices include dedicated flash for storage applications, but lack the security feature included within the SD card. Thus, these devices become unsuitable for storage according to the DRM license agreement. Moreover, conventional external storage does not support securely storing data. Due to the lack of random number generators (RNGs) in the conventional external storage replay detection cannot be provided making the DRM much more easily hacked/cracked.

BRIEF DESCRIPTION OF DRAWINGS

[0006] The disclosed embodiments have other advantages and features that will be more readily apparent from the detailed description, the appended claims, and the accompanying figures (or drawings). A brief introduction of the figures is below.

[0007] Figure (FIG.) 1 illustrates one example embodiment of components of an example machine able to read instructions from a machine-readable medium and execute them in a processor (or controller).

[0008] FIG. 2 illustrates one example embodiment of a computing configuration for use with a digital right management (DRM) environment.

[0009] FIG. 3 illustrates one example embodiment of a computing device with virtual Secure Digital (SD) card.

[0010] FIG. 4 illustrates one example embodiment of a process for provisioning a virtual SD card.

[0011] FIG. 5 illustrates one example embodiment of a process for using a virtual SD card.

DETAILED DESCRIPTION

[0012] The Figures (FIGS.) and the following description relate to preferred embodiments by way of illustration only. It should be noted that from the following discussion, alternative embodiments of the structures and methods disclosed herein will be readily recognized as viable alternatives that may be employed without departing from the principles of what is claimed.

[0013] Reference will now be made in detail to several embodiments, examples of which are illustrated in the accompanying figures. It is noted that wherever practicable similar or like reference numbers may be used in the figures and may indicate similar or like functionality. The figures depict embodiments of the disclosed system (or method) for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles described herein.

CONFIGURATION OVERVIEW

[0014] One embodiment of a disclosed system (or method and computer readable storage medium) that generates a virtual secure digital (SD) card. In one example configuration the system detects an SD card and reads a media key block and media identification for the SD card. The system stores the media key block and the media identification. The system creates a file system for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card and creates a file system for user data on the storage device for storage of user data corresponding to a user data area of the SD card. In addition, the system uses the virtual secure digital (SD) card. The system determines if the virtual SD card is provisioned and provisions it if not. The system accesses the data stored in the secure area of the provisioned virtual SD card. The system extracts the data from the secured area of the provisioned virtual SD card.

COMPUTING MACHINE ARCHITECTURE

[0015] FIG. (Figure) 1 is a block diagram illustrating components of an example machine able to read instructions from a machine-readable medium and execute them in a processor (or microcontroller). Specifically, FIG. 1 shows a diagrammatic representation of a machine in the

example form of a computer system 100 within which instructions 124 (e.g., software) for causing the machine to perform any one or more of the methodologies discussed herein may be executed. In alternative embodiments, the machine operates as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the machine may operate in the capacity of a server machine or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment.

[0016] The machine may be a server computer, a client computer, a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a cellular telephone, a smartphone, a web appliance, a network router, switch or bridge, a gaming console, a Blu-ray Disc player, or any machine capable of executing instructions 124 (sequential or otherwise) that specify actions to be taken by that machine. In addition, the machine may be configured to include instructions stored as firmware. Further, while only a single machine is illustrated, the term “machine” shall also be taken to include any collection of machines that individually or jointly execute instructions 124 to perform any one or more of the methodologies discussed herein.

[0017] The example computer system 100 includes a processor 102 (e.g., a central processing unit (CPU), a graphics processing unit (GPU), a digital signal processor (DSP), one or more application specific integrated circuits (ASICs), one or more radio-frequency integrated circuits (RFICs), or any combination of these), a main memory 104, and a static memory 106, which are configured to communicate with each other via a bus 108. The computer system 100 may further include graphics display unit 110 (e.g., a plasma display panel (PDP), a liquid crystal display (LCD), a projector, or a cathode ray tube (CRT)). The computer system 100 may also include alphanumeric input device 112 (e.g., a keyboard), a cursor control device 114 (e.g., a mouse, a trackball, a joystick, a motion sensor, or other pointing instrument), a persistent storage unit 116, a signal generation device 118 (e.g., a speaker), and a network interface device 120, which also are configured to communicate via the bus 108. The computer system 100 also may include a random number generator (RNG) 111. The random number generator 111 can be implemented in either hardware or software.

[0018] The storage unit 116 includes a machine-readable medium 122 on which is stored instructions 124 (e.g., software) embodying any one or more of the methodologies or functions

described herein. The instructions 124 (e.g., software) may also reside, completely or at least partially, within the main memory 104 or within the processor 102 (e.g., within a processor's cache memory) during execution thereof by the computer system 100, the main memory 104 and the processor 102 also constituting machine-readable media. The instructions 124 (e.g., software) may be transmitted or received over a network 126 via the network interface device 120.

[0019] Also included in the computing system 100 is a secure digital (SD) card reader/writer 107. The SD card reader/writer in one embodiment may be a physical device that accepts SD card in various physical formats (SD card, mini SD, or micro SD) and interfaces the electrical characteristics such that the storage on the SD card can be accessed by the computing device. The card reader may be internal to the computing device or external using adapters such as a USB-SD card reader, PC card-card reader, express card reader, or any other electrical interface such that the computing device can communicate with an SD card.

[0020] While machine-readable medium 122 is shown in an example embodiment to be a single medium, the term "machine-readable medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, or associated caches and servers) able to store instructions (e.g., instructions 124). The term "machine-readable medium" shall also be taken to include any medium that is capable of storing instructions (e.g., instructions 124) for execution by the machine and that cause the machine to perform any one or more of the methodologies disclosed herein. The term "machine-readable medium" includes, but not be limited to, data repositories in the form of solid-state memories, optical media, and magnetic media.

[0021] In one example embodiment, the instructions 124 correspond to an application program 105. The application program 105 include a set of machine readable instructions to carry out key exchange and data transfer specifications as further described herein. In one example, the application program 105 may work with a digital rights management (DRM) key and tamper resistant software.

[0022] In addition, the example computer system 100 may include a SD secure application programming interface (API) 109. The SD API is a software component that facilitates access to the SD card's secure area. The software architecture of the computer systems assumes that the

SD card is capable of responding to the commands from the application program using the SD Secure API architecture.

[0023]

DIGITAL RIGHTS MANAGEMENT COMPUTING ENVIRONMENT

[0024] FIG. 2 illustrates one example embodiment of a computing configuration for use with a digital right management (DRM) environment. The DRM environment includes the computer system 100 and a Secure Digital (SD) card 200. The SD card 200 includes a microcontroller 205, a firmware 210, a random number generator (RNG) 215, a media key block (MKB) 220, a flash memory 225, and a media identifier (MID) 230.

[0025] The application program 105 and the SD secure API 109 of the computer system 100 are further broken out for illustration purposes to show additional components. Specifically, the application program 105 includes a DRM key 240 and a tamper resistant software (TRS) 245. The SD secure API 109 includes a device manager (DM) 250 and a device driver (DD) 255. Similarly, the flash memory 225 is further broken out for illustration purposes to show a secure (or protected) area 260 and a user area 265.

[0026] Turning now to the application program 105, the DRM key 240 stored in the computer system 100 and used to complete a key exchange with the SD card 200. Specifically, the key exchange is used to gain access the SD card secure area 260 in accordance with the Content Protection for Recordable Media (CPRM) specification for use with SD cards. The application is provisioned with the DRM key either at initial installation or contained within the program itself. The random number generator 111 in the computer system 100 provides random numbers for replay protection required by the Authenticated Key Exchange (AKE) specification.

[0027] The key exchange process is subject to hackers (unauthorized or rogue applications) attempting to obtain the data stored on the secure area 260 of the SD card 200 that is transferred into the application program 105. The tamper resistant software 245 protects against the attacks. The tamper resistant software 245 comprises software code that may include techniques which remain proprietary to their respective vendors but may include such items as code obfuscation, anti-debugging, and code duplication.

[0028] Next, referring to the SD secure API 109, it comprises a software component that

facilitates access to the secure area 260 on the SD card 200. The software architecture of the computer system 100 assumes that the SD card is capable of responding to the commands from the application program 105 using the SD secure API 109 architecture.

[0029] As noted previously, the SD secure API 109 includes the device manager (DM) 250 and the device driver (DD) 255. The device manager (DM) 250 identifies SD card readers attached to the computer system 100. Once card readers are identified, the device manager 250 matches the corresponding device driver 255 with the specific physical card reader, or readers, attached to the computer system 100. The device driver 255 provides a device independent interface to card readers. It formats secure commands specifically for card readers and returns data to the application program 105. The device driver 255 provides a conduit for communicating with card readers, which in turn communicate directly with the secure area 260 of the SD card 200.

[0030] Turning now to the SD card 200, the SD card may be SD card, mini SD, or micro SD. The SD card 200 must conform to the specifications developed and enforced by the SD CARD ASSOCIATION. The general construct of the SD card 200 is illustrated to provide a general idea of how an SD card may be internally constructed so that the functionality assigned to the virtual SD card can be better understood. The decomposition is not intended to reveal any specific trade secrets or patents of the many SD card vendors. The SD card itself can be thought of as an application specific computing platform, as opposed to the general purpose computing platform of a computing device. The specific application is to transfer data to/from the computer system 100, and if required, to securely store data by restricting access to applications that can complete the Authenticated Key Exchange (AKE) in order to access the secure data.

[0031] In the SD card 200, a microcontroller device 205 is configured to receive requests for data from a card reader. In the case of user area 265 access (insecure access) data is returned without completing the Authenticated Key Exchange. The firmware 210 comprises software machine instructions by the microcontroller 205 to interpret card reader commands and return data to the card reader. The firmware includes the necessary algorithms (cryptograph and hash) in accordance with SD CARD ASSOCIATION and CPRM specifications to implement the Authenticated Key Exchange (AKE) protocol. Firmware may be implemented in silicon or can be a program that is interpreted by a microcontroller 205.

[0032] The random number generator 215 that provides random numbers for replay protection required by AKE protocol. The random number generator 215 can be implemented in either hardware or software. It is noted that the random number generator 111 in the computer system 100 and the random number generator 215 in the SD card 200 are both used for the AKE protocol. The media key block (MKB) 220 is structured in accordance with the CPRM specification for SD Cards. Specifically, multiple keys are included in SD cards and are provisioned by the SD card manufacturer at manufacturing time. The media key block 220 includes DRM keys that may change due to key revocations. Specific keys are used with the key exchange protocol that must be completed prior to accessing the secure flash area.

[0033] As noted previously, the SD card contains flash memory 225 that is partitioned into two separate regions. One is a secure area 260 and the other is a user (unsecured) area 265. The secured area 260 may be implemented as a physical or logical device within the SD card as chosen by the SD card original equipment manufacturer (OEM). The size of the secure area 260 size is determined at manufacturing time according to the SD card specifications. Requests to access the data from the secured area 260 must first complete the AKE process. The user (or unsecured) area 265 may be implemented in the same manner as the secure area 260. The user (or unsecured) area 265 also may be either physical or logical partitions depending on implementation within the SD card. Request for data from the user area 265 does not require AKE process to complete.

[0034] The flash memory 225 is configured to store secure data in the secure area 260 and unsecured data in the user area 265. Both the secure data and the unsecure data are stored in a persistent manner so that it can be retrieve at a later time. It is noted that every SD card is provisioned with a secure area 260, even if it is never used by any application.

[0035] The Media ID 230 is used in accordance with the AKE protocol. The DRM key of the media key block (MKB) 220 and media ID 230 are required for the AKE processes. These items are provisioned by the SD card manufacturer during the manufacturing process.

[0036] When executing, the application program 105 uses a DRM key , the random number generator 111 of the computer system 100 , the media key block 220, and the media ID 230 when transferring data through the device manager 250 and device driver 255 in order to complete the security exchange with the SD card 200. The SD card 200 uses the media key

block 220, the random number generator 215, the media ID 230, and data sent by the application program 105 to calculate the AKE process result. The exchange process includes mutual authentication whereby both the SD card 200 and application program 105 authenticate each other before accessing the secure area 260 of the SD card 200. The process completes when both the SD card 200 has authenticated the application program 105 and the application program 105 has authenticated the SD card 200. Here, the SD card 200 performs the same operations as the application program 105 and if both achieve the same AKE process result, mutual authentication is achieved and both the application program 105 and SD card 200 can proceed to access the data in the secure area 260 within the flash memory 225 of the SD card 200.

VIRTUAL SD CARD CONFIGURATION

[0037] FIG. 3 illustrates one example embodiment of the computing device 100 including a virtual Secure Digital (SD) card 300. In this example, virtual SD card 300 can be configured within internal storage 116 or may be configured within an external storage that is coupled with the computer system 100. By way of example, the external storage can be a hard disk drive or a RAID storage that is coupled to the computer system 100 via a wired connection, e.g., IEEE 1394 or USB. Another example of the external storage can be storage accessible by the computer system 100 through a storage area network that is wired or wirelessly coupled. Yet another example of the external storage is a storage location accessible by the computer system 100 in a network cloud, e.g., accessible through an internet connection. For ease of discussion, the virtual SD card 300 is described in the context of a configuration within the storage 116, but it would be understood that the configuration is applicable to external storage coupled with the computer system 100.

[0038] In FIG 3, the virtual SD card 300 includes a virtual device driver 305, tamper resistant software 310, a virtual secure area file system 315, a virtual media key block 320, virtual user area file system 325, a virtual media identification (ID) 330. The virtual device driver 305 is configured to interface the device manager 250, which is the interface to the device driver 255. The device manager 250 and device driver 255 interfaces remain unchanged from the specification for SD cards. The virtual secured area file system 315 is secured using the tamper resistant software 310. The tamper resistant software 310 functions similar to the tamper

resistant software 245. The virtual device driver 305 functions similar to the device driver 255.

[0039] The secured area file system 315 is configured as a storage area for secure data. This may be implemented as a physical or logical storage area within external storage 300. Because the file system can be accessed by the computer system 100 without using the virtual SD card 300, the data within the secure area is protected using an encryption key. The encryption key is derived from the computing device's unique information (e.g., processor serial number, bios serial number, device serial number), and hidden information effectively binding the file systems to the computer system 100. This prevents transfer of data to another device for access. In one example embodiment, to further enhance security the encryption key is not stored but rather derived. A size of the secured area file system 315 is determined at manufacturing time according to the SD card specifications. It is preferable that the secured area file system 315 is stored within a non-removable storage device to further assist in replay-attack prevention. These methods bind the file systems to a specific computer that cannot be transferred to another computer. If an attempt is made to transfer the bound file systems, the derived encryption key is different and the data is lost. The size of the virtual secured area file system 315 is a table lookup from SD ASSOCIATION specifications based on the size of the virtual user area file system 325.

[0040] The virtual media key block (MKB) 320 is equivalent to media key block 220. The virtual media key block 320 is provisioned either at software load time or when a first SD card, e.g., 200, is read by the computer system 100 utilizing the media key block 220 from the SD card 220. The media key block 220 is stored using the process described previously, e.g., with respect to the virtual secured area file system 315.

[0041] The user area file system file system 325 is a storage area for unsecured data. The virtual user area file system 325 is maintained on the storage device 116 in a physical or logical partition. Unlike the secure area, encryption and non-removable storage are not required. The virtual media ID 330 is functionally similar to the media ID 230. The virtual media ID 330 is provisioned either at software load time or when a first SD card is read by the computer system 100 utilizing the media ID 220 from the SD card 200. The virtual media ID 330 is stored using the process described previously, e.g., with respect to the virtual secured area file system 315.

[0042] By leveraging storage 116 of the computer system 100 to create the virtual SD card,

the file storage layouts and data implementations can replicate a physical SD card implementation. This simplifies the software implementation to a unified storage algorithm for data on SD cards and on virtual SD archives. It is noted that in the virtual SD card 300 configuration, the card reader interface 107 is no longer necessary because there is no communication with a physical SD card. Rather, the virtual device driver 305 is configured to include the firmware 210 of the original SD card specification and based on the AKE specification. It is noted that the encryption keys for protecting data in physical storage are derived prior to use and the encryption key is not stored.

[0043] The virtual SD card 300 implements in software the functionality previously implemented by SD card 200 in hardware. The functional components of the computer system 100 are used by the virtual SD card 300 implementation. For example, within the computer system 100, the virtual SD card 300 includes the virtual device 305 as previously described. Through this configuration, instead of the microcontroller 205 responding to the System on a Chip (SoC)/CPU to create the security association. The virtual SD card 300 provides not only the interface to device manager 250, but also the processing that would normally take place in the microcontroller 205 on the SD card 220 while executing the firmware 210 of the SD card 230. In addition, rather than send data protocol commands to the SD card 220, the virtual device driver 305 interfaces directly with the virtual secured area file system 315 and the virtual user area file system 325.

[0044] The virtual secured area file system 315 and the virtual user area file system 325 can be implemented as file systems within an encrypted file. This provides the same level of protection as a physical SD card 220 implementation. They can also be implemented as physical or logical partitions on the same or separate devices, with or without encryption depending on the overall system security requirements. However, unlike physical SD cards, the virtual SD card 300 allows for storage of larger volumes of DRM media typically stored on physical SD cards. Moreover, this configuration allows for additional media management such as layering media management system to organize and interface with one or more stored virtual SD cards using a user interface accessible through the computer system 100.

[0045] Turning now to FIG. 4, it illustrates one example embodiment of a process for provisioning a virtual SD card 300. The provisioning process for creating the virtual SD card

300 following by defining/assembling the components for the virtual SD card 300. The process detects the SD card 200 in the SD card reader/writer 107 of the computer system 100. The SD card reader/writer 107 reads the media key block 220 and media ID 230 from the SD card 200 and stores 420 them in the storage unit 116 as the Virtual Media Key Block 320 and the Virtual Media ID 330 for access by the virtual SD card 300

[0046] The process determines 425 the size for a virtual user area 325 on the virtual SD card 300 and creates a file or partition on the storage 116 that is accordingly formatted for the virtual user area 325. Based on the virtual user area 325 on the virtual SD card 300, the process conducts a lookup 430 to determine the size of the virtual secured area 315 in the virtual SD card 300. The process creates a file or partition on the storage 116 that is accordingly formatted for the virtual secured area 315. Once completed the process is returned as successful 435. With the virtual SD card 300 provisioned, it is now ready to be used.

[0047] FIG. 5 illustrates one example embodiment of a process for using the virtual SD card 300. In this example, the process detects insertion of a SD card 200 in the SD card reader/writer 107 of the computer system 100. The process determines 515 if the virtual SD card 300 is provisioned. If it is not provisioned, the process provisions 520 the SD card, for example, as described in FIG. 4.

[0048] The process determines 525 if it can access the secured area 315 of the virtual SD card. If it cannot, the process only fetches and returns 530 data from the user area 325. If the secured area can be accessed, the process performs 535 a key exchange using AKE. If the process determines 540 key exchange is not successful, the process denies 545 access to the secure area and may return an error on a display of the computer system 100. If the key exchange is successful, the process determines 550 whether a read or a write operation will be performed. If a write operation, the process decrypts 555 data with the key derived during AKE, reads from the storage, decrypts with encryption key derived from the computing devices unique information, updates data, encrypts with the key derived from the computing device unique information, and writes data to the virtual secure area file system 315 of the virtual SD card 300. It is noted that there are two encryption keys. One encryption key is for physical storage that is derived from the computing device unique information prior to use. This key is constant but is not stored. The second key is the key calculated during AKE. This key protects data during

transport between the virtual SD card and the application program. If successful, an indication 570 of success is returned. If a read operation, the process fetches and decrypts 560 data from the virtual secure area file system 315 using the key derived from the computing device unique information. The process encrypts 565 the data with the AKE key for transport to the application program 105. The process returns (or retrieves or extracts) data from the virtual secure area 315 to the application program 105.

ADDITIONAL CONFIGURATION CONSIDERATIONS

[0049] Throughout this specification, plural instances may implement components, operations, or structures described as a single instance. Although individual operations of one or more methods are illustrated and described as separate operations, one or more of the individual operations may be performed concurrently, and nothing requires that the operations be performed in the order illustrated. Structures and functionality presented as separate components in example configurations may be implemented as a combined structure or component. Similarly, structures and functionality presented as a single component may be implemented as separate components. These and other variations, modifications, additions, and improvements fall within the scope of the subject matter herein.

[0050] Certain embodiments are described herein as including logic or a number of components, modules, or mechanisms. Modules may constitute either software modules (e.g., code embodied on a machine-readable medium or in a transmission signal) or hardware modules. A hardware module is tangible unit capable of performing certain operations and may be configured or arranged in a certain manner. In example embodiments, one or more computer systems (e.g., a standalone, client or server computer system) or one or more hardware modules of a computer system (e.g., a processor or a group of processors) may be configured by software (e.g., an application or application portion) as a hardware module that operates to perform certain operations as described herein.

[0051] In various embodiments, a hardware module may be implemented mechanically or electronically. For example, a hardware module may comprise dedicated circuitry or logic that is permanently configured (e.g., as a special-purpose processor, such as a field programmable gate array (FPGA) or an application-specific integrated circuit (ASIC)) to perform certain operations.

A hardware module may also comprise programmable logic or circuitry (e.g., as encompassed within a general-purpose processor or other programmable processor) that is temporarily configured by software to perform certain operations. It will be appreciated that the decision to implement a hardware module mechanically, in dedicated and permanently configured circuitry, or in temporarily configured circuitry (e.g., configured by software) may be driven by cost and time considerations.

[0052] The various operations of example processes described herein, e.g., as described with FIGS. 3, 4 and 5, may be performed, at least partially, by one or more processors that are temporarily configured (e.g., by software) or permanently configured to perform the relevant operations. Whether temporarily or permanently configured, such processors may constitute processor-implemented modules that operate to perform one or more operations or functions. The modules referred to herein may, in some example embodiments, comprise processor-implemented modules.

[0053] The one or more processors may also operate to support performance of the relevant operations in a “cloud computing” environment or as a “software as a service” (SaaS). For example, at least some of the operations may be performed by a group of computers (as examples of machines including processors), these operations being accessible via a network (e.g., the Internet) and via one or more appropriate interfaces (e.g., application program interfaces (APIs).)

[0054] The performance of certain of the operations may be distributed among the one or more processors, not only residing within a single machine, but deployed across a number of machines. In some example embodiments, the one or more processors or processor-implemented modules may be located in a single geographic location (e.g., within a home environment, an office environment, or a server farm). In other example embodiments, the one or more processors or processor-implemented modules may be distributed across a number of geographic locations.

[0055] Some portions of this specification are presented in terms of algorithms or symbolic representations of operations on data stored as bits or binary digital signals within a machine memory (e.g., a computer memory). These algorithms or symbolic representations are examples of techniques used by those of ordinary skill in the data processing arts to convey the substance

of their work to others skilled in the art. As used herein, an “algorithm” is a self-consistent sequence of operations or similar processing leading to a desired result. In this context, algorithms and operations involve physical manipulation of physical quantities. Typically, but not necessarily, such quantities may take the form of electrical, magnetic, or optical signals capable of being stored, accessed, transferred, combined, compared, or otherwise manipulated by a machine. It is convenient at times, principally for reasons of common usage, to refer to such signals using words such as “data,” “content,” “bits,” “values,” “elements,” “symbols,” “characters,” “terms,” “numbers,” “numerals,” or the like. These words, however, are merely convenient labels and are to be associated with appropriate physical quantities.

[0056] Unless specifically stated otherwise, discussions herein using words such as “processing,” “computing,” “calculating,” “determining,” “presenting,” “displaying,” or the like may refer to actions or processes of a machine (e.g., a computer) that manipulates or transforms data represented as physical (e.g., electronic, magnetic, or optical) quantities within one or more memories (e.g., volatile memory, non-volatile memory, or a combination thereof), registers, or other machine components that receive, store, transmit, or display information.

[0057] As used herein any reference to “one embodiment” or “an embodiment” means that a particular element, feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment.

[0058] Some embodiments may be described using the expression “coupled” and “connected” along with their derivatives. For example, some embodiments may be described using the term “coupled” to indicate that two or more elements are in direct physical or electrical contact. The term “coupled,” however, may also mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other. The embodiments are not limited in this context.

[0059] As used herein, the terms “comprises,” “comprising,” “includes,” “including,” “has,” “having” or any other variation thereof, are intended to cover a non-exclusive inclusion. For example, a process, method, article, or apparatus that comprises a list of elements is not necessarily limited to only those elements but may include other elements not expressly listed or

inherent to such process, method, article, or apparatus. Further, unless expressly stated to the contrary, “or” refers to an inclusive or and not to an exclusive or. For example, a condition A or B is satisfied by any one of the following: A is true (or present) and B is false (or not present), A is false (or not present) and B is true (or present), and both A and B are true (or present).

[0060] In addition, use of the “a” or “an” are employed to describe elements and components of the embodiments herein. This is done merely for convenience and to give a general sense of the invention. This description should be read to include one or at least one and the singular also includes the plural unless it is obvious that it is meant otherwise.

[0061] Upon reading this disclosure, those of skill in the art will appreciate still additional alternative structural and functional designs for a system and a process for provisioning and using a virtual Secure Digital card through the disclosed principles herein. Thus, while particular embodiments and applications have been illustrated and described, it is to be understood that the disclosed embodiments are not limited to the precise construction and components disclosed herein. Various modifications, changes and variations, which will be apparent to those skilled in the art, may be made in the arrangement, operation and details of the method and apparatus disclosed herein without departing from the spirit and scope defined in the appended claims.

CLAIMABLE SUBJECT MATTER

CLAIMABLE SUBJECT MATTER AND ADDITIONAL WRITTEN DESCRIPTION INCLUDES, BUT IS NOT LIMITED TO, THE FOLLOWING:

- A1. A method generating a virtual secure digital (SD) card, the method comprising:
 - reading a media key block and media identification for an SD card;
 - storing the media key block and the media identification;
 - creating a file system for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card; and
 - creating a file system for user data on the storage device for storage of user data corresponding to a user data area of the SD card.
- A2. The method of claim A1, wherein a size of the file system for secure data is determinant on a size of the file system for user data, the determination based on a lookup table providing a relationship between the sizes.
- A3. The method of any one of claim A1 and A2, wherein the file system for secure data is encrypted.
- A4. The method of any one of claim A1 through A3, wherein an encryption key is derived from a computer system information, the encryption key not stored by the computer system.
- A5. The method of any one of claim A1 through A4, wherein the encryption key is derived from a computer system and stored by the computer system.
- A6. The method of any one of claim A1 through A5, wherein the media identification comprises random data not allocated from the SD card.

- A7. The method of any one of claim A1 through A6, wherein the file system for secure data and the file system for user data are located on different physical partitions of the storage device.
- A8. The method of any one of claim A1 through A7, wherein the file system for secure data and the file system for user data are located on different logical partitions of the storage devices
- A9. The method of any one of claim A1 through A8, wherein the file system for secure data and the file system for user data are within an existing file system.
- A10. The method of any one of claim A1 through A9, where the media key block and the media identification are assigned to the device and not from the SD card.
- B1. A method using a virtual secure digital (SD) card, the method comprising:
determining if the virtual SD card is provisioned;
provisioning the SD card in response to the virtual SD card not being provisioned;
accessing the data stored in the secure area of the provisioned virtual SD card; and
extracting the data from the secured area of the provisioned virtual SD card.
- B2. The method of claim B1, further comprising performing an authentication using Authenticated Key Encryption (AKE) before accessing the data in the secure area of the provisioned virtual SD card.
- B3. The method of claim B1 or B2, wherein data received from an application program through Authenticated Key Encryption (AKE) is first decrypted.

- B4. The method of any one of claim B1 through B3, wherein data received from an application program through Authenticated Key Encryption (AKE) is encrypted with another key before storing the data in the secure area of the provisioned virtual SD card.
- C1. A computer readable medium configured to store instructions, the instructions when executed cause at least one processor to:
- read a media key block and media identification for an SD card;
 - store the media key block and the media identification;
 - create a file system for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card; and
 - create a file system for user data on the storage device for storage of corresponding to a user data area of the SD card.
- C2. The computer readable medium of claim C1, wherein a size of the file system for secure data is determinant on a size of the file system for user data, the determination based on a lookup table providing a relationship between the sizes.
- C3. The computer readable medium of claim C1 or C2, wherein the file system for secure data is encrypted.
- C4. The computer readable medium of any one of claim C1 through C3, wherein an encryption key is derived from a computer system information, the encryption key not stored by the computer system.
- C5. The computer readable medium of any one of claim C1 through C4, wherein the encryption key is derived from a computer system and stored by the computer system

- C2. The computer readable medium of claim C1, further comprising instructions that cause the processor to
- D1. A computer readable medium configured to store instructions, the instructions when executed cause at least one processor to:
- determine if the virtual SD card is provisioned;
 - provision the SD card in response to the virtual SD card not being provisioned;
 - access the data stored in the secure area of the provisioned virtual SD card; and
 - extract the data from the secured area of the provisioned virtual SD card.
- D2. The computer readable medium of claim D1, further comprising performing an authentication using Authenticated Key Encryption (AKE) before accessing the data in the secure area of the provisioned virtual SD card.
- D3. The computer readable medium of claim D1 or D2, wherein data received from an application program through Authenticated Key Encryption (AKE) is first decrypted.
- D4. The computer readable medium of any of claim D1 through D3, wherein data received from an application program through Authenticated Key Encryption (AKE) is encrypted with another key before storing the data in the secure area of the provisioned virtual SD card.

ABSTRACT

A system (and a method) are disclosed for generating a virtual secure digital (SD) card. The system detects an SD card and reads a media key block and media identification for the SD card. The system stores the media key block and the media identification. The system creates a file system for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card and creates a file system for user data on the storage device for storage of user data corresponding to a user data area of the SD card. In addition, the system uses the virtual secure digital (SD) card. The system determines if the virtual SD card is provisioned and provisions it if not. The system accesses the data stored in the secure area of the provisioned virtual SD card. The system extracts the data from the secured area of the provisioned virtual SD card.

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		VIRTUAL SECURE DIGITAL CARD		
First Named Inventor/Applicant Name:		Joseph Zipperer		
Filer:		Rajiv P. Patel/Nubia Morad		
Attorney Docket Number:		26629-17764		
Filed as Large Entity				
Provisional Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Provisional application filing	1005	1	220	220
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				220

Electronic Acknowledgement Receipt	
EFS ID:	8842352
Application Number:	61413926
International Application Number:	
Confirmation Number:	1652
Title of Invention:	VIRTUAL SECURE DIGITAL CARD
First Named Inventor/Applicant Name:	Joseph Zipperer
Customer Number:	00758
Filer:	Rajiv P. Patel
Filer Authorized By:	
Attorney Docket Number:	26629-17764
Receipt Date:	15-NOV-2010
Filing Date:	
Time Stamp:	20:37:49
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$220
RAM confirmation Number	6840
Deposit Account	192555
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Drawings-only black and white line drawings	17764_drawings.pdf	77021	no	5
			73bd219768ab0dfc31ad7a50eb191a79c2b4e668		

Warnings:

Information:

2	Provisional Cover Sheet (SB16)	17764_Provisional_cover.pdf	1060169	no	3
			d2edc2f61aea4f722897e6eabd2773dceac94429		

Warnings:

Information:

3	Specification	17764_US_Specification.pdf	138903	no	22
			1c23cd871aaeeb4f70f10147706ab258d59ae992		

Warnings:

Information:

4	Fee Worksheet (PTO-875)	fee-info.pdf	29650	no	2
			00255c53656552a2fb5b2e5f84b4f12ed5b51c6e		

Warnings:

Information:

Total Files Size (in bytes):

1305743

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.