FILE HISTORY
US 6,088,802

PATENT:	6,088,802
INVENTORS:	Bialick, William P. Sutherland, Mark J. Dolphin Peterson, Janet L. Rowland, Thomas K. Skeba, Kirk W. Housley, Russell D.
TITLE:	Peripheral device with integrated security functionality
APPLICATION NO:	US1997869305A
FILED:	04 JUN 1997
ISSUED:	11 JUL 2000
COMPILED:	03 OCT 2016

08/869305 PTO

ISSUE CLASSIFICATION	
Class	Subclass
713	200

[redacted]

6088802

UTILITY SERIAL NUMBER	PATENT DATE JUL 11 2000	PATENT NUMBER 6088802

SERIAL NUMBER	FILING DATE	CLASS	SUBCLASS	GROUP ART UNIT	EXAMINER
08/869,305	06/04/97	~~380~~ 713	200	~~242~~	

APPLICANTS: WILLIAM P. BIALICK, CLARKSVILLE, MD; MARK J. SUTHERLAND, MILPITAS, CA; JANET L. DOLPHIN-PETERSON, BELVEDERE, CA; THOMAS K. ROWLAND, LOS GATOS, CA; KIRK W. SKEBA, FREMONT, CA; RUSSELL D. HOUSLEY, HERNDON, VA.

BEST COPY

CONTINUING DATA*******************
VERIFIED

none BDL 11/10/98

FOREIGN APPLICATIONS**********
VERIFIED

none BDL 11/10/98

FOREIGN FILING LICENSE GRANTED 11/13/97 ***** SMALL ENTITY *****

Foreign priority claimed 35 USC 119 conditions met Verified and Acknowledged	□ yes ☑ no □ yes ☑ no BDL 11/10/98 Examiner's Initials	AS FILED	STATE OR COUNTRY	SHEETS DRWGS.	TOTAL CLAIMS	INDEP. CLAIMS	FILING FEE RECEIVED	ATTORNEY'S DOCKET NO.
			MD	7	32	12	$460.00	SPY-004

ADDRESS
DAVID R GRAHAM
1337 CHEWPON AVENUE
MILPITAS CA 95035

TITLE
PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY

U.S. DEPT. OF COMM./ PAT. & TM—PTO-436L (Rev.12-94)

PARTS OF APPLICATION FILED SEPARATELY

Applications Examiner 6/8/99

NOTICE OF ALLOWANCE MAILED		CLAIMS ALLOWED	
6-7-99	Assistant Examiner	Total Claims 39	Print Claim 1

ISSUE FEE	
Amount Due	Date Paid
$605.00	9-14-99

LY V. HUA
PRIMARY EXAMINER
Primary Examiner

DRAWING		
Sheets Drwg.	Figs. Drwg.	Print Fig.
7	11	6

ISSUE BATCH NUMBER U04

Label Area

PREPARED FOR ISSUE

WARNING: The information disclosed herein may be restricted. Unauthorized disclosure may be prohibited by the United States Code Title 35, Sections 122, 181 and 368. Possession outside the U.S. Patent & Trademark Office is restricted to authorized employees and contractors only.

Form PTO-436A
(Rev. 8/92)

ISSUE FEE IN FILE

Formal Drawings (___shts) set

6,088,802

PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY

Transaction History

Date	Transaction Description
06-04-1997	Workflow - Drawings Finished
06-04-1997	Workflow - Drawings Matched with File at Contractor
06-04-1997	Workflow - Drawings Received at Contractor
07-14-1997	Initial Exam Team nn
08-07-1997	IFW Scan & PACR Auto Security Review
11-04-1997	Notice Mailed--Application Incomplete--Filing Date Assigned
03-05-1998	Application Is Now Complete
03-12-1998	Application Dispatched from OIPE
03-12-1998	Application Dispatched from OIPE
04-07-1998	Case Docketed to Examiner in GAU
08-15-1998	Information Disclosure Statement (IDS) Filed
08-15-1998	Information Disclosure Statement (IDS) Filed
10-08-1998	Information Disclosure Statement (IDS) Filed
10-08-1998	Information Disclosure Statement (IDS) Filed
11-23-1998	Non-Final Rejection
12-11-1998	Mail Non-Final Rejection
03-15-1999	Response after Non-Final Action
03-18-1999	Supplemental Response
03-25-1999	Date Forwarded to Examiner
03-30-1999	Information Disclosure Statement (IDS) Filed
03-30-1999	Information Disclosure Statement (IDS) Filed
04-01-1999	Date Forwarded to Examiner
06-07-1999	Mail Notice of Allowance
06-07-1999	Notice of Allowance Data Verification Completed
06-23-1999	Workflow - Drawings Received at Contractor
06-24-1999	Workflow - Drawings Sent to Contractor
09-13-1999	Workflow - Incoming Correspondence - Finish
09-13-1999	Workflow - Incoming Correspondence - Begin
09-13-1999	Information Disclosure Statement (IDS) Filed
09-13-1999	Information Disclosure Statement (IDS) Filed
09-13-1999	UnMatched Papers in Pubs
09-13-1999	UnMatched Papers in Pubs
09-14-1999	Issue Fee Payment Verified
12-16-1999	Mail Miscellaneous Communication to Applicant
12-16-1999	Miscellaneous Communication to Applicant - No Action Count
01-04-2000	Workflow - File Sent to Contractor
05-26-2000	Workflow - Complete WF Records for Drawings
05-28-2000	Application Is Considered Ready for Issue
06-23-2000	Issue Notification Mailed
07-11-2000	Recordation of Patent Grant Mailed
06-25-2008	Correspondence Address Change
01-12-2012	ENTITY STATUS SET TO UNDISCOUNTED (INITIAL DEFAULT SETTING OR STATUS CHANGE)
03-02-2015	Change in Power of Attorney (May Include Associate POA)
03-02-2015	Correspondence Address Change
09-29-2016	File Marked Found

PATENT APPLICATION

08869305

APPROVED FOR LICENSE □

INITIALS ________

CONTENTS

Date Entered or Counted		Date Received or Mailed
	1. Application 7 papers.	
	2. Ltr. unsigned Dec./Fee	11/4/97
	3. Dec. Surch. Fee	1-12-98
	4. I.D.S.	10. 8. 98
	5. Prior Art	Aug 15, 1997
11/23	6. Rej. 3 mos.	12. 11. 98
3/25/99	7. Amdt A	Mar. 15, 1999 m 3/21
4/1/99	8. Supp. Amdt B	Mar 18, 1999
	9. Prior Art	Mar 30, 1999
6/7	10. Notice of Allow	6-2-99
	11. Prior Art + fee	Sep 13, 1999
	12. Letter	12-16-99
	13.	
4-11-00	14. Formal Drawings	6-4-97
	15.	
	16.	
	17.	
	18.	
	19.	
	20.	
	21.	
	22.	
	23.	
	24.	
	25.	
	26.	
	27.	
	28.	
	29.	
	30.	
	31.	
	32.	

Class	Subclass
713	200

R
05

ned
ons met
fledged

APPLIC
ARATEL
ALLOV

-99

ISSUE

Labe
Area

PATENT NUMBER

ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
713	200

APPLICATION SERIAL NUMBER
08/869,305

APPLICANT'S NAME (PLEASE PRINT)
BIALICK ET AL.

IF REISSUE, ORIGINAL PATENT NUMBER

INTERNATIONAL CLASSIFICATION					
G	0	6	K		14/67
					/
					/
					/

CROSS REFERENCE(S)				
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)			
713	201	202		

GROUP ART UNIT
2785

ASSISTANT EXAMINER (PLEASE STAMP OR PRINT FULL NAME)

PRIMARY EXAMINER (PLEASE STAMP OR PRINT FULL NAME)
LY V. HUA

PTO 270
(REV. 5-91)

ISSUE CLASSIFICATION SLIP

U.S. DEPARTMENT OF COMM
PATENT AND TRADEMARK

Claim		Date							
Final	Original	11/20/9	6/3/99						
	1	✓							
2	2	+	=						
3	3	+	=						
4	4	✓	=						
5	5	+	=						
1	6	0	=						
6	7	0	=						
11	8	✓	=						
12	9	+	=						
15	10	+	=						
19	11	✓	=						
22	12	+	=						
23	13	0	=						
24	14	✓	=						
25	15	+	=						
28	16	+	=						
32	17	✓	=						
35	18	+	=						
	~~19~~	+							
14	20	+	=						
	~~21~~	+							
17	22	+	=						
18	23	+	=						
	~~24~~	✓							
20	25	✓	=						
21	26	✓	=						
	~~27~~	+							
	~~28~~	✓							
36	29	✓	=						
37	30	✓	=						
38	31	✓	=						
39	32	✓	=						
7	33		=						
8	34		=						
9	35		=						
10	36		=						
13	37		=						
16	38		=						
26	39		=						
27	40		=						
29	41		=						
30	42		=						
31	43		=						
33	44		=						
34	45		=						
	46								
	47								
	48								
	49								
	50								

SYMBOLS
✓ .... Rejected
= .... Allowed
- (Through numberal) Canceled
+ .... Restricted
N .... Non-elected
I .... Interference
A .... Appeal
O .... Objected

Claim		Date							
Final	Original								
	51								
	52								
	53								
	54								
	55								
	56								
	57								
	58								
	59								
	60								
	61								
	62								
	63								
	64								
	65								
	66								
	67								
	68								
	69								
	70								
	71								
	72								
	73								
	74								
	75								
	76								
	77								
	78								
	79								
	80								
	81								
	82								
	83								
	84								
	85								
	86								
	87								
	88								
	89								
	90								
	91								
	92								
	93								
	94								
	95								
	96								
	97								
	98								
	99								
	100								

713 Class | 200 Subclass

ied
ns met
ledged

APPLIC
RATEI
ALLO
-99
ISSUE

Lab
Are

POSITION		ID NO.	DATE
CLASSIFIER		5	5/5/98
EXAMINER		10270	11/3/99
TYPIST			
VERIFIER			
CORPS CORR.			
SPEC. HAND		704	3-6
FILE MAINT.		10270	11/3/99
DRAFTING			

INDEX OF CLAIMS

Claim		Date							
Final	Original	11/20/98	6/3/99						
	1	✓							
2	2	+	=						
3	3	+	=						
4	4	✓	=						
5	5	+	=						
1	6	O	=						
6	7	O	=						
11	8	✓	=						
12	9	+	=						
15	10	+	=						
19	11	✓	=						
22	12	+	=						
23	13	C	=						
24	14	✓	=						
25	15	+	=						
28	16	+	=						
32	17	✓	=						
35	18	+	=						
	19	+							
14	20	+	=						
	21	+							
17	22	+	=						
18	23	+	=						
	24	✓							
20	25	✓	=						
21	26	✓	=						
	27	+							
	28	✓							
36	29	✓	=						
37	30	✓	=						
38	31	✓	=						
39	32	✓	=						
7	33		=						
8	34		=						
9	35		=						
10	36		=						
13	37		=						
16	38		=						
26	39		=						
27	40		=						
29	41		=						
30	42		=						
31	43		=						
33	44		=						
34	45		=						
	46								
	47								
	48								
	49								
	50								

SYMBOLS

✓ .... Rejected
= .... Allowed
– (Through numberal) Canceled
+ .... Restricted
N .... Non-elected
I .... Interference
A .... Appeal
O .... Objected

Claim		Date							
Final	Original								
	51								
	52								
	53								
	54								
	55								
	56								
	57								
	58								
	59								
	60								
	61								
	62								
	63								
	64								
	65								
	66								
	67								
	68								
	69								
	70								
	71								
	72								
	73								
	74								
	75								
	76								
	77								
	78								
	79								
	80								
	81								
	82								
	83								
	84								
	85								
	86								
	87								
	88								
	89								
	90								
	91								
	92								
	93								
	94								
	95								
	96								
	97								
	98								
	99								
	100								

[redacted]

SEARCHED

Class	Sub.	Date	Exmr.
395	188.01	11/10/98	LuH
|	187.01.	11/10/98	LuH
|	186	11/10/98	LuH
380	4	11/10/98	LuH
|	25	|	|
|	49		
713	200	6/1/99	LuH
713	201	|	|
713	202		
update	Search	6/1/99	LuH
the above		|	|
subclasses	of		
Class	380		

31

INTERFERENCE SEARCHED

Class	Sub.	Date	Exmr.
713	200	6/2/99	LuH
713	201	6/2/99	LuH
713	202	6/2/99	LuH

SEARCH NOTES

	Date	Exmr.
MAYA	9/17/98	LuH
APS	11/10/98	LuH

US006088802A

United States Patent [19]

Bialick et al.

[11] **Patent Number: 6,088,802**

[45] **Date of Patent: Jul. 11, 2000**

[54] **PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY**

[75] Inventors: **William P. Bialick**, Clarksville, Md.; **Mark J. Sutherland**, Milpitas, Calif.; **Janet L. Dolphin-Peterson**, Belvedere, Calif.; **Thomas K. Rowland**, Los Gatos, Calif.; **Kirk W. Skeba**, Fremont, Calif.; **Russell D. Housley**, Herndon, Va.

[73] Assignee: **Spyrus, Inc.**, Santa Clara, Calif.

[21] Appl. No.: **08/869,305**

[22] Filed: **Jun. 4, 1997**

[51] **Int. Cl.**^{7} **G06K 14/67**

[52] **U.S. Cl.** **713/200**; 713/201; 713/202

[58] **Field of Search** 395/188.01, 187.01, 395/186; 380/4, 25, 49; 713/200, 201, 202

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,709,136	11/1987	Watanabe	235/379
4,910,776	3/1990	Dyke	380/25
5,191,611	3/1993	Lang	380/25
5,282,247	1/1994	McLean et al.	380/4
5,297,206	3/1994	Orton	380/30
5,442,704	8/1995	Holtey	380/23
5,457,590	10/1995	Barrett et al.	360/133
5,473,692	12/1995	Davis	380/25
5,491,827	2/1996	Holtey	395/800
5,524,134	6/1996	Gustafson et al.	379/58
5,537,544	7/1996	Morisawa et al.	395/188.01
5,546,463	8/1996	Caputo et al.	380/25
5,548,721	8/1996	Denslow	395/187.01
5,610,981	3/1997	Mooney et al.	380/25
5,630,174	5/1997	Stone, III et al.	395/883
5,640,302	6/1997	Kikinis	361/687
5,694,335	12/1997	Hollenberg	364/514
5,742,683	4/1998	Lee et al.	380/23
5,770,849	6/1998	Novis et al.	235/492
5,790,674	8/1998	Houvener et al.	380/23
5,828,832	10/1998	Holden et al.	395/187.01
5,878,142	3/1999	Caputo et al.	380/25

FOREIGN PATENT DOCUMENTS

WO 82/03286	9/1982	WIPO .
WO 97/29416	8/1997	WIPO .

OTHER PUBLICATIONS

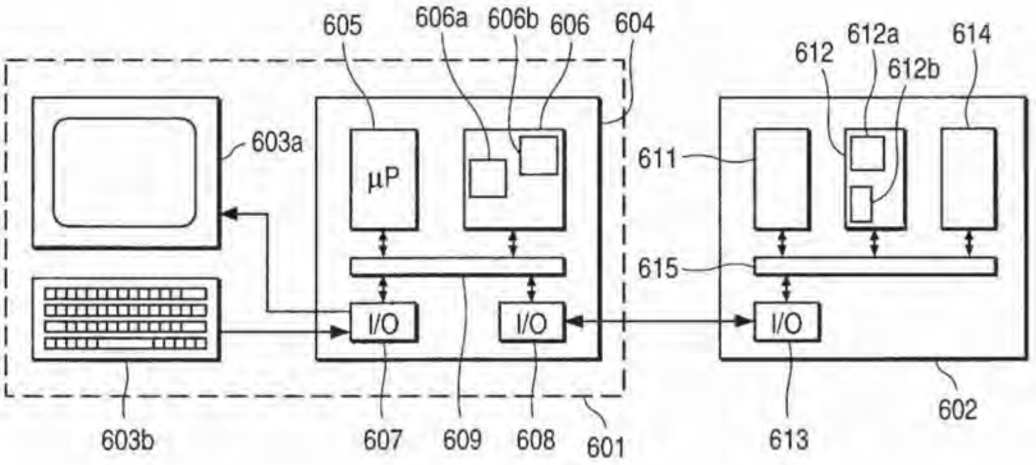
U.S. application No. 08/869,120, Bialick et al., filed Jun. 4, 1997, pending.

Primary Examiner—Ly V. Hua
Attorney, Agent, or Firm—David R. Graham

[57] **ABSTRACT**

The invention enables a peripheral device to communicate with a host computing device to enable one or more security operations to be performed by the peripheral device on data stored within the host computing device, data provided from the host computing device to the peripheral device (which can then be, for example, stored in the peripheral device or transmitted to yet another device), or data retrieved by the host computing device from the peripheral device (e.g., data that has been stored in the peripheral device, transmitted to the peripheral device from another device or input to the peripheral device by a person). In particular, the peripheral device can be adapted to enable, in a single integral peripheral device, performance of one or more security operations on data, and a defined interaction with a host computing device that has not previously been integrated with security operations in a single integral device. The defined interactions can provide a variety of types of functionality (e.g., data storage, data communication, data input and output, user identification). The peripheral device can also be implemented so that the security operations are performed in-line, i.e., the security operations are performed between the communication of data to or from the host computing device and the performance of the defined interaction. Moreover, the peripheral device can be implemented so that the security functionality of the peripheral device is transparent to the host computing device.

39 Claims, 9 Drawing Sheets



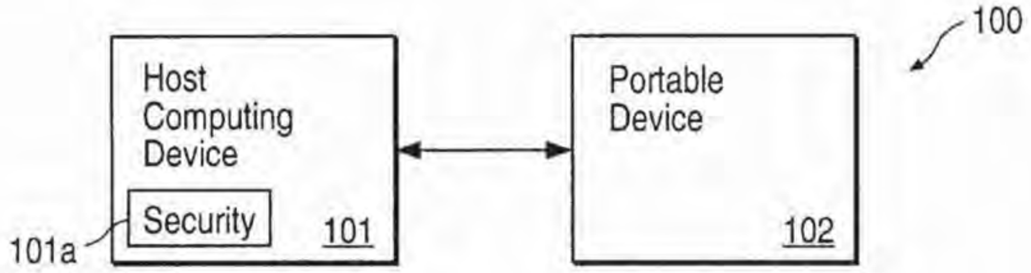


FIG. 1
(PRIOR ART)

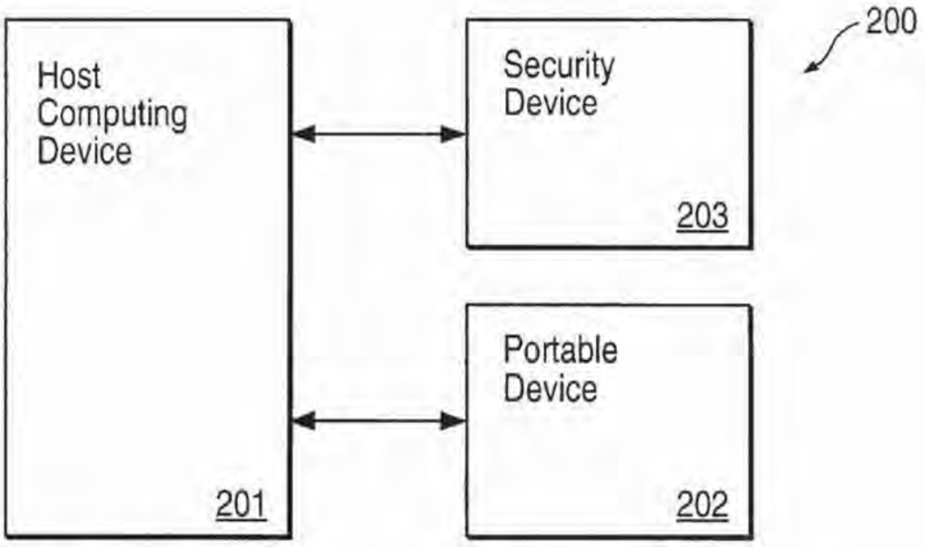


FIG. 2
(PRIOR ART)

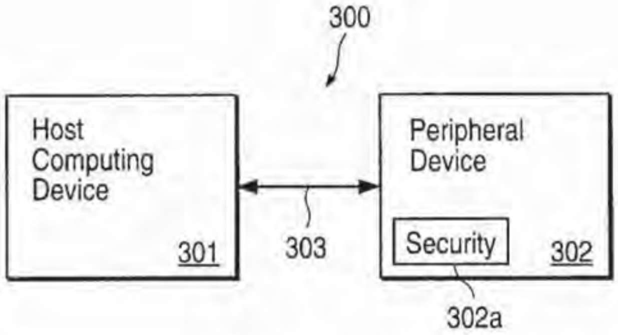

300
Host Computing Device
301
303
Peripheral Device
Security
302
302a

FIG. 3A

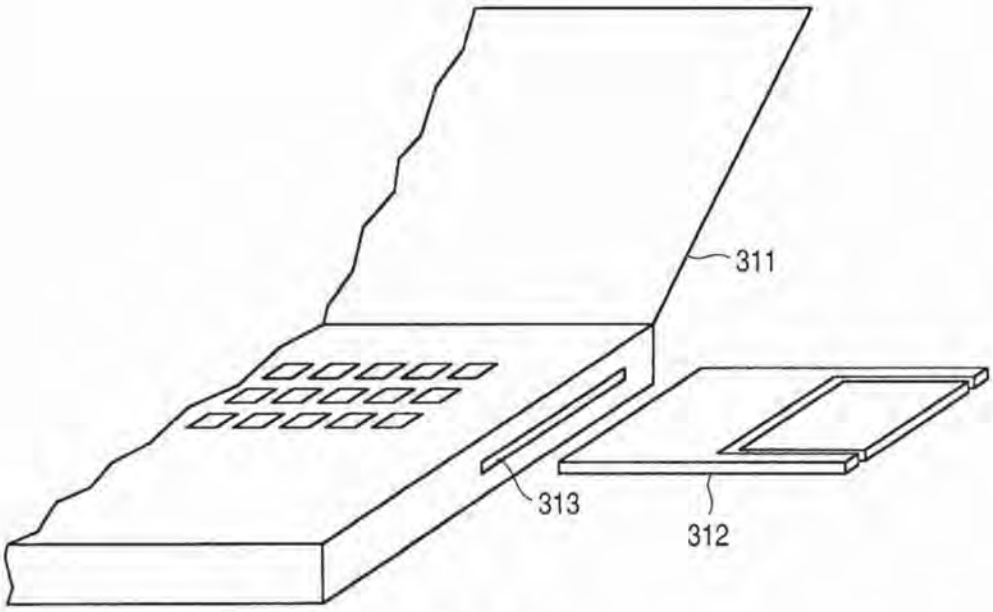

311
313
312

FIG. 3B

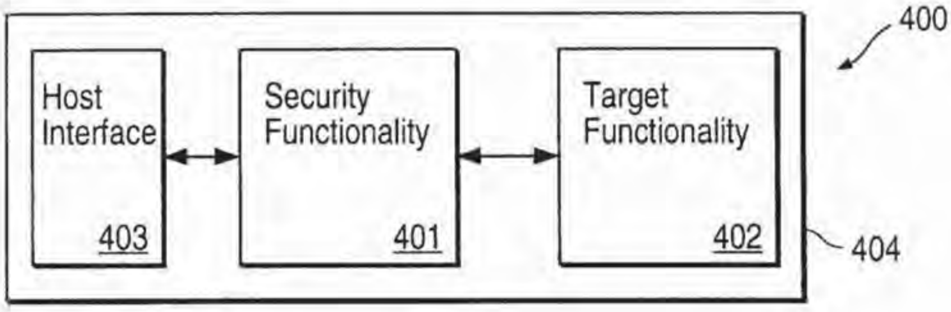

400
Host Interface
403
Security Functionality
401
Target Functionality
402
404

FIG. 4

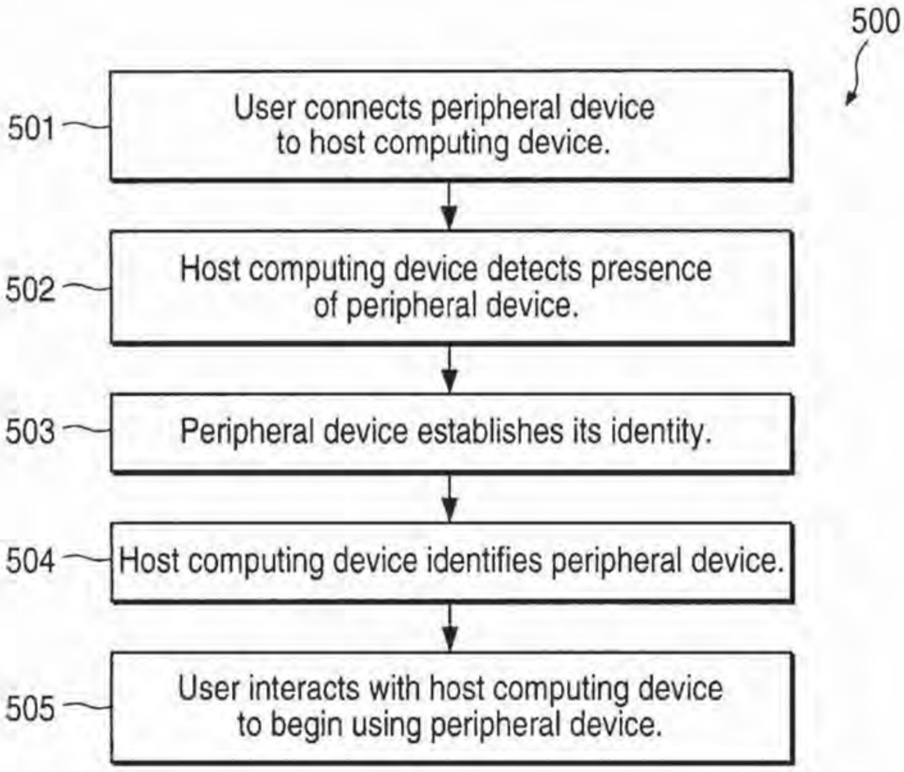

500
501
User connects peripheral device to host computing device.
502
Host computing device detects presence of peripheral device.
503
Peripheral device establishes its identity.
504
Host computing device identifies peripheral device.
505
User interacts with host computing device to begin using peripheral device.

FIG. 5

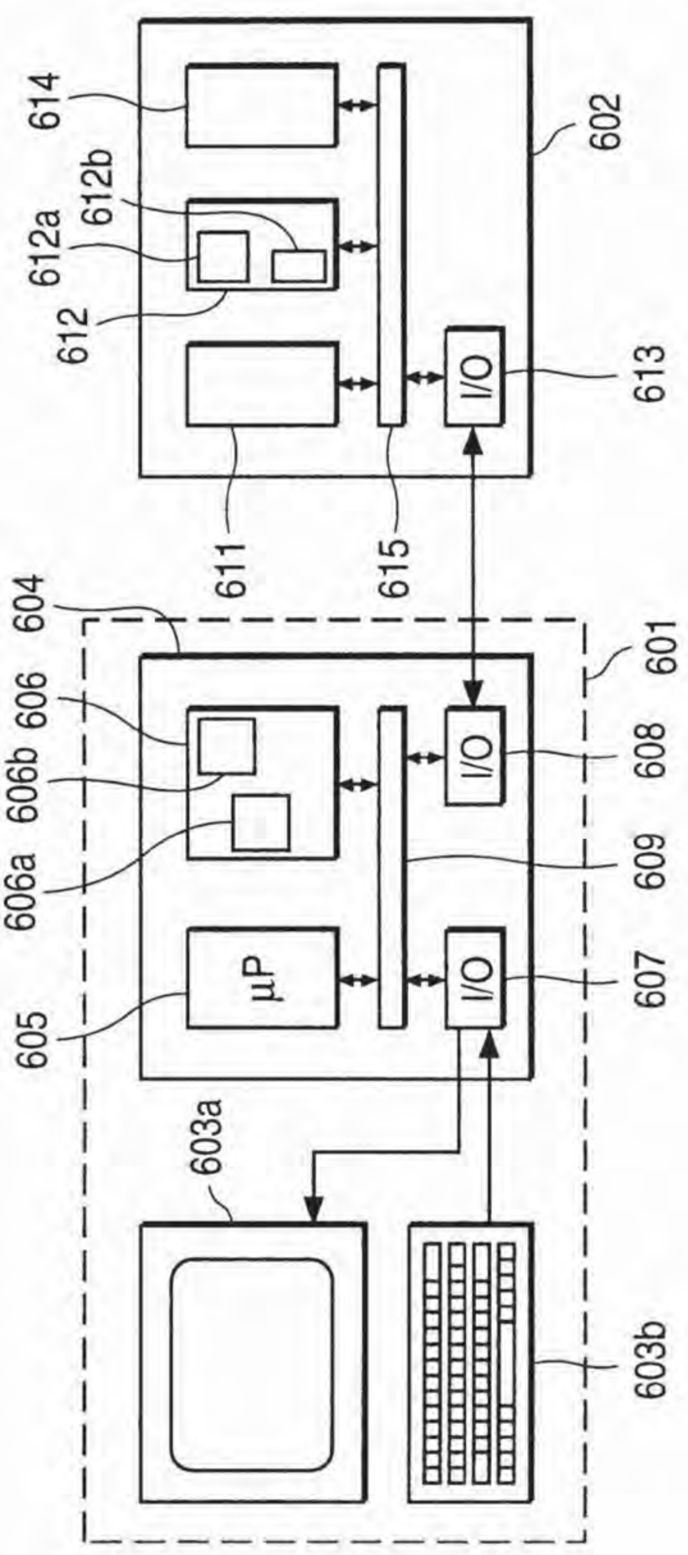

614
612b
612a
612
602
I/O
613
611
615
604
606
606b
606a
605
μP
601
I/O
608
609
I/O
607
603a
603b

FIG. 6

FIG. 7A

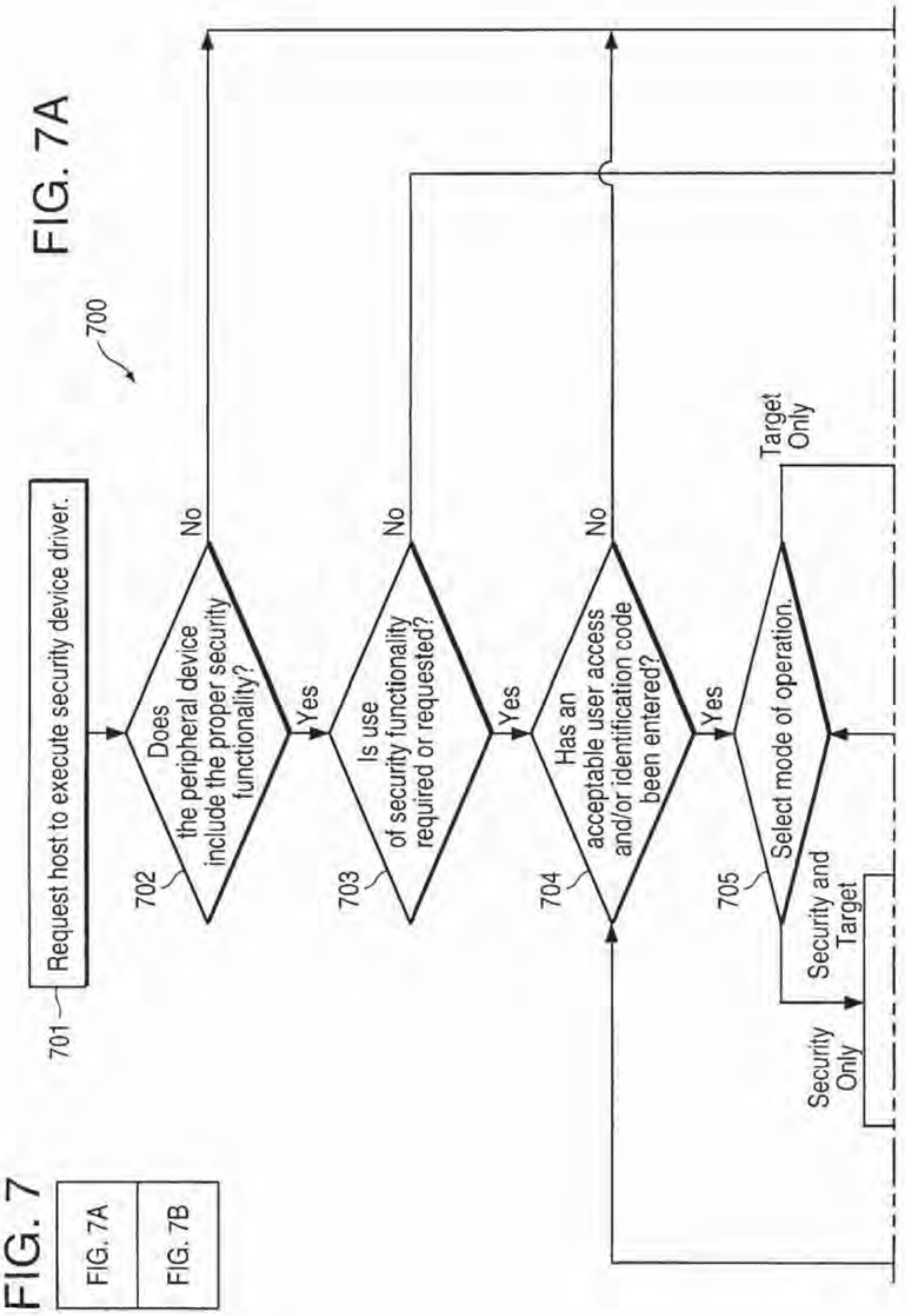

700
701
Request host to execute security device driver.
702
Does the peripheral device include the proper security functionality?
No
Yes
703
Is use of security functionality required or requested?
No
Yes
704
Has an acceptable user access and/or identification code been entered?
No
Yes
705
Select mode of operation.
Target Only
Security and Target
Security Only

FIG. 7

FIG. 7A

FIG. 7B

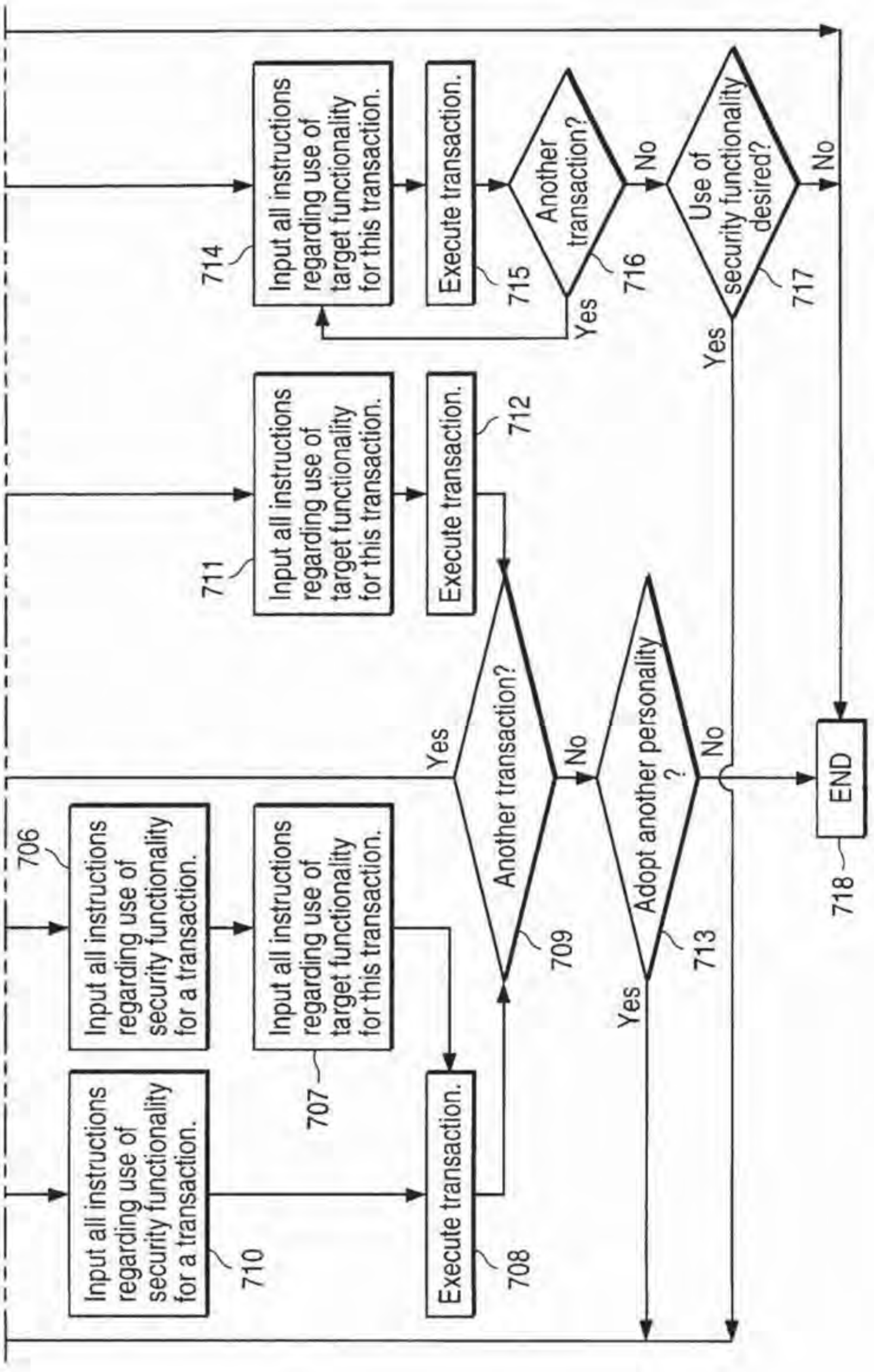

Input all instructions regarding use of security functionality for a transaction.
710
Input all instructions regarding use of security functionality for a transaction.
706
Input all instructions regarding use of target functionality for this transaction.
707
Execute transaction.
708
Another transaction?
709
Yes
No
Adopt another personality ?
713
Yes
No
Input all instructions regarding use of target functionality for this transaction.
711
Execute transaction.
712
Input all instructions regarding use of target functionality for this transaction.
714
Execute transaction.
715
Another transaction?
716
Yes
No
Use of security functionality desired?
717
Yes
No
END
718

FIG. 7B

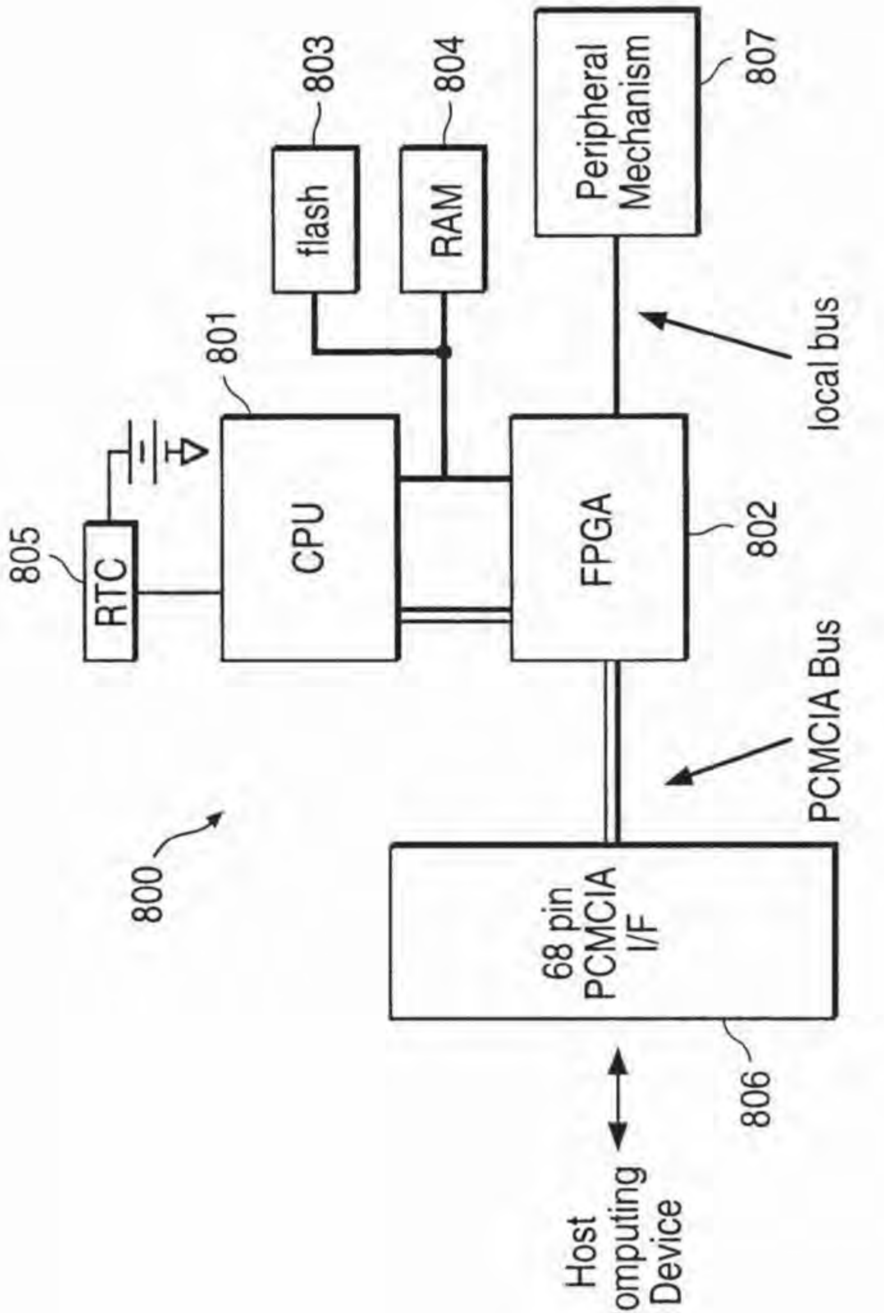

800
805
RTC
CPU
801
flash
803
RAM
804
FPGA
802
Peripheral Mechanism
807
local bus
PCMCIA Bus
68 pin PCMCIA I/F
806
Host Computing Device

FIG. 8

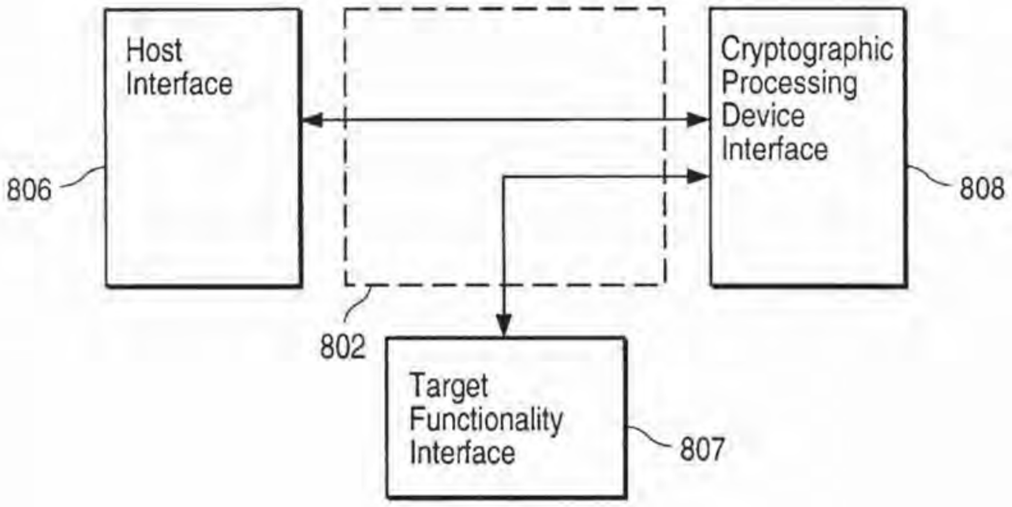

Host Interface
806
Cryptographic Processing Device Interface
808
802
Target Functionality Interface
807

FIG. 9A

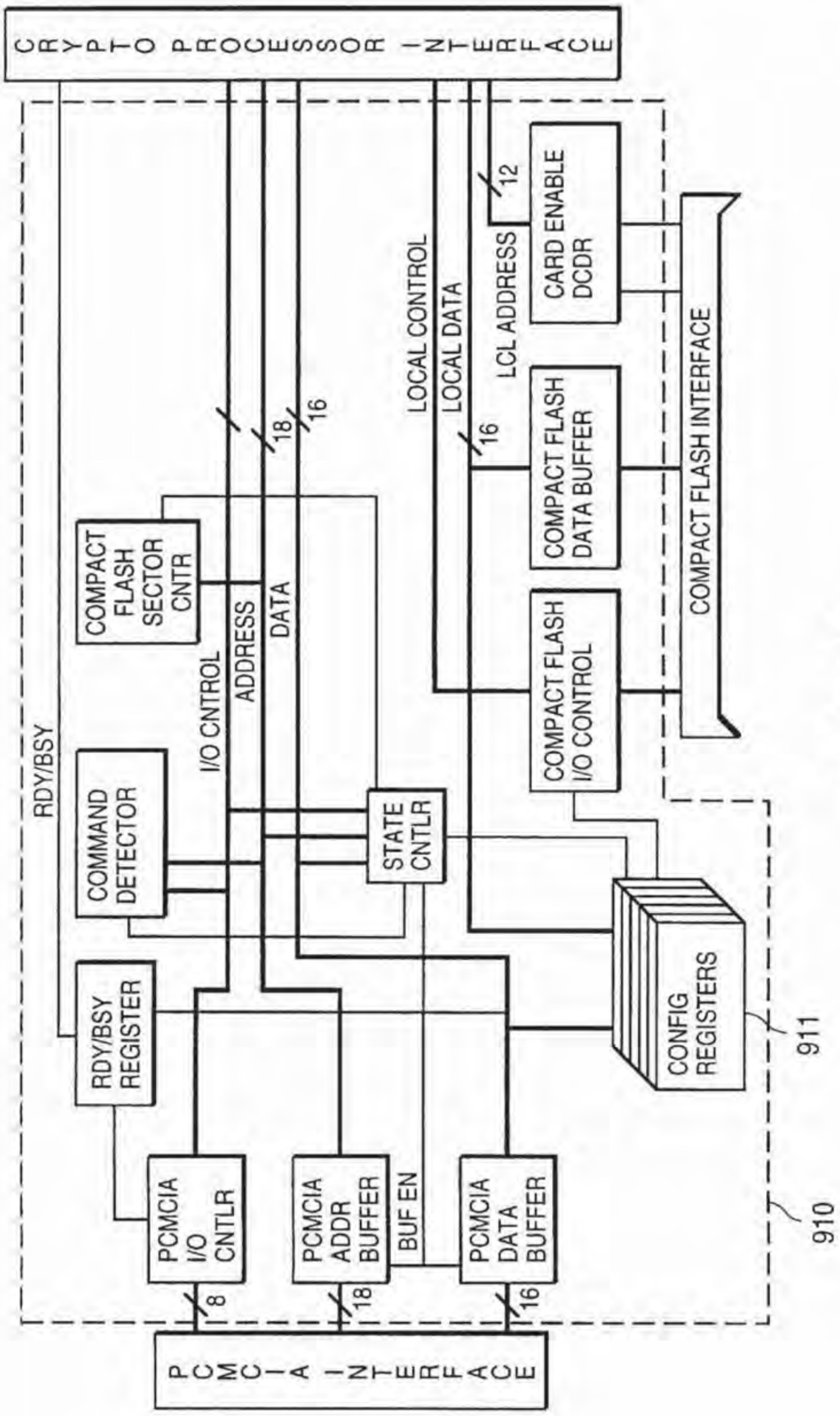

CRYPTO PROCESSOR INTERFACE
RDY/BSY
I/O CNTROL
ADDRESS
DATA
18
16
LOCAL CONTROL
LOCAL DATA
LCL ADDRESS
16
12
CARD ENABLE DCDR
COMPACT FLASH DATA BUFFER
COMPACT FLASH I/O CONTROL
COMPACT FLASH INTERFACE
COMPACT FLASH SECTOR CNTR
COMMAND DETECTOR
STATE CNTLR
RDY/BSY REGISTER
CONFIG REGISTERS
911
PCMCIA I/O CNTLR
PCMCIA ADDR BUFFER
BUF EN
PCMCIA DATA BUFFER
910
8
18
16
PCMCIA INTERFACE

FIG. 9B

PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY

CROSS-REFERENCE TO RELATED APPLICATION

This application is related to the commonly owned, co-pending United States patent Application entitled "Modular Security Device," by William P. Bialick, Mark J. Sutherland, Janet L. Dolphin-Peterson, Thomas K. Rowland, Kirk W. Skeba and Russell D. Housley, filed on the same date as the present application and having Attorney Docket No. SPY-003, the disclosure of which is incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to a peripheral, often portable, device (as well as the methods employed by such a peripheral device, and systems including such a peripheral device and a host computing device with which the peripheral device communicates) that can communicate with a host computing device to enable one or more security operations to be performed by the peripheral device on data stored within the host computing device, data provided from the host computing device to the peripheral device, or data retrieved by the host computing device from the peripheral device.

2. Related Art

Computing capability is becoming increasingly portable. In particular, there are more and more portable peripheral devices that are adapted for communication with a host computing device (e.g., desktop computer, notebook computer or personal digital assistant) to enable particular functionality to be achieved. These portable peripheral devices can take a variety of physical forms (e.g., PCMCIA cards, smart cards, CD-ROMs) and can perform an assortment of functions (e.g., storage, communications and cryptography).

However, while portable computing affords a number of advantages, it has a significant disadvantage in that the computational environment (including the portable peripheral devices, the host computing devices in which they are used, and any other computational devices that communicate with those devices) is more susceptible to security breaches, i.e., unauthorized access to, or modification of, programs and/or data resident within the environment. Consequently, cryptographic devices and methods have been developed for use with such computational environments (as well as other computational environments) to enable increased levels of environment security to be obtained.

FIG. **1** is a block diagram of a prior art system for enabling a host computing device to provide secured data to, and retrieve secured data from, a portable device. In FIG. **1**, a system **100** includes a host computing device **101** and a portable device **102**. The host computing device **101** and portable device **102** are adapted to enable communication between the devices **101** and **102**. The host computing device **101** includes a security mechanism **101***a* (which can be embodied by appropriately configured hardware, software and/or firmware, such as, for example, a general purpose microprocessor operating in accordance with instructions of one or more computer programs stored in a data storage device such as a hard disk) which can be directed to perform one or more cryptographic operations.

In the system **100**, if it is desired to provide secured data from the host computing device **101** to the portable device **102**, the host computing device **101** causes the security mechanism **101***a* to perform appropriate cryptographic operations on data before the data is transferred to the portable device **102**. Similarly, the host computing device **101** can receive secured data from the portable device **102** and perform appropriate cryptographic operations on the data to convert the data into a form that enables the data to be accessed and/or modified by a person who is authorized to do so.

A significant deficiency of the system **100** is that the security mechanism **101***a* is itself typically not adequately secure. It is commonly accepted that the components (including hardware, software and/or firmware) of most host computing devices are inherently insecure. This is because the system design of host computing devices is, typically, intentionally made open so that components made by different manufacturers can work together seamlessly. Thus, an unauthorized person may obtain knowledge of the operation of the security mechanism **101***a* (e.g., identify a cryptographic key), thereby enabling that person to gain access to, and/or modify, the (thought to be secured) data.

FIG. **2** is a block diagram of another prior art system for enabling a host computing device to provide secured data to, and retrieve secured data from, a portable device. In FIG. **2**, a system **200** includes a host computing device **201**, a portable device **202** and a security device **203**. The host computing device **201**, the portable device **202** and security device **203** are adapted to enable communication between the devices **201** and **202**, and between the devices **201** and **203**. The security device **203** includes appropriately configured hardware, software and/or firmware which can be directed to perform one or more cryptographic operations.

In the system **200**, if it is desired to provide secured data from the host computing device **201** to the portable device **202**, the host computing device **201** first causes data to be transferred to the security device **203**, where appropriate cryptographic operations are performed on the data. The secured data is then transferred back to the host computing device **201**, which, in turn, transfers the secured data to the portable device **202**. Similarly, the host computing device **201** can receive secured data from the portable device **202** by, upon receipt of secured data, transferring the secured data to the security device **203**, which performs appropriate cryptographic operations on the data to convert the data into a form that enables the data to be accessed and/or modified by a person who is authorized to do so, then transfers the unsecured data back to the host computing device **201**.

The system **200** can overcome the problem with the system **100** identified above. The security device **203** can be constructed so that the cryptographic functionality of the device **203** can itself be made secure. (Such a security device is often referred to as a security "token.") An unauthorized person can therefore be prevented (or, at least, significantly deterred) from obtaining knowledge of the operation of the security device **203**, thereby preventing (or significantly deterring) that person from gaining access to, and/or modifying, the secured data.

However, the system **200** may still not always ensure adequately secured data. In particular, unsecured data may be provided by the host computing device **201** to the portable device **202** if the host computing device **201**—whether through inadvertent error or deliberate attack by a user of the host computing device **201**, or through malfunction of the host computing device **201**—fails to first transfer data to the security device **203** for appropriate cryptographic treatment before providing the data to the portable device **202**.

Additionally, the system **200** requires the use of two separate peripheral devices (portable device **202** and security device **203**) to enable the host computing device **201** to exchange secured data with the portable device **202**. For several reasons, this may be inconvenient. First, both devices **202** and **203** may not be available at the time that it is desired to perform a secure data exchange (e.g., one may have been forgotten or misplaced). Second, even if both devices **202** and **203** are available, it may not be possible to connect both devices **202** and **203** at the same time to the host computing device **201**, making use of the devices **202** and **203** cumbersome and increasing the likelihood that unsecured data is provided by the host computing device **201** to the portable device **202**.

SUMMARY OF THE INVENTION

A peripheral device according to the invention can be used to communicate with a host computing device to enable one or more security operations to be performed by the peripheral device on data stored within the host computing device, data provided from the host computing device to the peripheral device (which can then be, for example, stored in the peripheral device or transmitted to yet another device) or data retrieved by the host computing device from the peripheral device (e.g., data that has been stored in the peripheral device, transmitted to the peripheral device from another device or input to the peripheral device by a person). In particular, the peripheral device can be adapted to enable, in a single integral peripheral device, performance of one or more security operations on data, and a defined interaction with a host computing device that has not previously been integrated with security operations in a single integral device. The defined interactions can provide a variety of types of functionality (e.g., data storage, data communication, data input and output, user identification), as described further below. The peripheral device can be implemented so that the peripheral device can be operated in any one of multiple user-selectable modes: a security functionality only mode, a target functionality mode, and a combined security and target functionality mode. The peripheral device can also be implemented so that the security operations are performed in-line, i.e., the security operations are performed between the communication of data to or from the host computing device and the performance of the defined interaction. Moreover, the peripheral device can be implemented so that the security functionality of the peripheral device is transparent to the host computing device.

A peripheral device according to the invention can advantageously enable application of security operations to a wide variety of interactions with a host computing device. In particular, a peripheral device according to the invention can accomplish this without necessity to use two peripheral devices: one that performs the security operations and one that performs the defined interaction. This can, for example, minimize the possibility that the device adapted to perform the defined interaction will be used with the host computing system without proper application of security operations to that interaction. Moreover, the provision of in-line security in a peripheral device according to the invention enables a more secure exchange of data between a host computing device and the peripheral device, overcoming the problems identified above in previous systems for performing security operations on data exchanged between such devices. Additionally, implementing a modular device according to the invention so that the performance of security operations by the modular device is transparent can reduce or eliminate the need to modify aspects of the operation of the host computing device (e.g., device drivers of the host computing device), making implementation and use of a data security system including the modular device simpler and easier. Thus, the possibility that a user will use the system incorrectly (e.g., fail to apply security operations to an interaction with the host computing device, or apply the security operations incorrectly or incompletely) is reduced. Making the security operations transparent can also enhance the security of those operations.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a prior art system for enabling a host computing device to provide secured data to, and retrieve secured data from, a portable device.

FIG. **2** is a block diagram of another prior art system for enabling a host computing device to provide secured data to, and retrieve secured data from, a portable device.

FIG. **3A** is a block diagram of a system according to the invention.

FIG. **3B** is a perspective view of a physical implementation of the system of FIG. **3A** according to one embodiment of the invention.

FIG. **4** is a block diagram of a peripheral device according to an embodiment of the invention.

FIG. **5** is a flow chart of a method, according to an embodiment of the invention, for initiating use of a system according to the invention.

FIG. **6** is a block diagram of a system, according to an embodiment of the invention, illustrating operation of the system during a method according to the invention as in FIG. **5**.

FIGS. **7A** and **7B** is a flow chart of a method, according to an embodiment of the invention, for using a peripheral device according to the invention.

FIG. **8** is a block diagram of a peripheral device according to another embodiment of the invention.

FIG. **9A** is a block diagram illustrating the flow of data through the interface control device of FIG. **8**.

FIG. **9B** is a block diagram of a particular embodiment of an interface control device for use in a peripheral device according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

FIG. **3A** is a block diagram of a system **300** according to the invention. The system **300** includes a host computing device **301** and a peripheral device **302** that communicate via a communications interface **303**. Herein, "peripheral device" can refer to any device that operates outside of a host computing device and that is connected to the host computing device. The peripheral device **302** includes a security mechanism **302***a* that enables security operations (examples of which are described in more detail below) to be performed on data that is stored within the host computing device **301**, data that is transmitted from the host computing device **301** to the peripheral device **302**, or data that is transmitted from the peripheral device to the host computing device **301**. As explained in more detail below, the peripheral device **302** also provides additional functionality (referred to herein as "target functionality") to the system **300**, such as, for example, the capability to store data in a solid-state disk storage device, the capability to enable communications from the host computing device **301** to another device, the capability to accept biometric input to enable user authentication to the host computing device **301**, and the capability to receive and read a smart card inserted into the peripheral device **302**.

Generally, the communications interface **303** can be any embodied by any of a variety of communication interfaces, such as a wireless communications interface, a PCMCIA interface, a smart card interface, a serial interface (such as an RS-232 interface), a parallel interface, a SCSI interface or an IDE interface. Each embodiment of the communications interface **303** includes hardware present in each of the host computing device **301** and peripheral device **302** that operates in accordance with a communications protocol (which can be embodied, for example, by software stored in a memory device and/or firmware that is present in the host computing device **301** and/or peripheral device **302**) appropriate for that type of communications interface, as known to those skilled in the art. Each embodiment of the communications interface **303** also includes mechanisms to enable physical engagement, if any, between the host computing device **301** and peripheral device **302**.

Generally, the security mechanism **302***a* can be configured to perform any electronic data security operation (herein, referred to simply as "security operation") including, for example, operations that provide one or more of the basic cryptographic functions, such as maintenance of data confidentiality, verification of data integrity, user authentication and user non-repudiation. Particular security operations that can be implemented in a peripheral device according to the invention are described in more detail below.

The security mechanism **302***a* can be, for example, embodied as a security token. Herein, "security token" refers to a device that performs security operations and that includes one or more mechanisms (such as, for example, use of a hardware random number generator and/or protected memory) to provide security for the content of those operations.

FIG. **3**B is a perspective view of a physical implementation of the system **300** of FIG. **3**A, according to one embodiment of the invention. In FIG. **3**B, the peripheral device **302** is embodied as a card **312** that can be inserted into a corresponding slot **313** formed in a portable computer **311** that, in FIG. **3**B, embodies the host computing device **301**. Often a peripheral device according to the invention is a portable device, such as the card **312** shown in FIG. **3**B. Herein, "portable device" can refer generally to any device that is capable of being easily carried by hand.

FIG. **4** is a block diagram of a peripheral device **400** according to an embodiment of the invention. The peripheral device **400** includes security functionality **401**, target functionality **402** and a host interface **403** that are formed together as part of a single physical device. For example, the security functionality **401** and target functionality **402** can be enclosed in a single, card-like housing (designated in FIG. **4** by the numeral **404**) conforming to a PCMCIA card or smart card standard.

The peripheral device **400** can have a number of advantageous characteristics. The peripheral device **400** can be implemented in a manner that enables the security operations of the security functionality **401** to be performed in a manner that is transparent to a host computing device (and, depending upon the particular implementation of the peripheral device **400**, to a user of a system including the peripheral device **400**) of a system according to the invention, so that the host computing device (and, perhaps, user) is aware only of the presence of the target functionality **402**. Additionally, the peripheral device **400** can be implemented so that security operations are performed "in-line," i.e., the security operations are performed between the communication of data to or from the host computing device and the performance of the target functionality provided by the peripheral device. Further, the peripheral device **400** enables a wide variety of secure target functionality to be easily provided to a host computing device.

FIG. **5** is a flow chart of a method **500**, according to an embodiment of the invention, for initiating use of a system according to the invention. The method **500** enables an aspect of the invention in which the presence of security functionality as part of a peripheral device is not detected by a host computing device, thus making the security functionality transparent to the host computing device and, depending upon the particular manner in which the security functionality is implemented, to a user of the system.

FIG. **6** is a block diagram of a system **600**, according to an embodiment of the invention, illustrating operation of the system **600** during a method according to the invention such as the method **500** of FIG. **5**. The system **600** includes a host computing device **601** and a peripheral device **602**. The host computing device **601** includes a display device **603***a* (e.g., a conventional computer display monitor) and user input device **603***b* (e.g., a keyboard, mouse, trackball, joystick or other appropriate device), referred to collectively hereinafter as user interface device **603**. The host computing device **601** also includes, mounted within a housing **604**, a processing device **605**, a memory device **606**, an input/output (I/O) device **607** for enabling communication with the user interface device **603**, and an input/output (I/O) device **608** for enabling communication with peripheral device **602**. The devices **605**, **606**, **607** and **608** can each be implemented by conventional such devices and can communicate with each other via a conventional computer bus **609**, as is well known and understood. The peripheral device **602** includes security functionality **611**, a memory device **612**, an input/output (I/O) device **613** for enabling communication with the host computing device **601** and target functionality **614**. The security functionality **611**, memory device **612**, I/O device **613** and target functionality **614** can each be implemented by conventional devices and can communicate with each other via a conventional computer bus **615**, as is well known and understood. The host computing device **601** and the peripheral device **602** are shown in simplified form in FIG. **6** to facilitate clarity in illustration of this aspect of the invention; as described in more detail below and as understood by those skilled in the art, the host computing device **601** and the peripheral device **602** can—and typically will—include other devices not shown in FIG. **6**.

Returning to FIG. **5**, use of a system according to the invention begins when, as shown by step **501**, a user of the system connects a peripheral device according to the invention to a host computing device. Such connection can occur in any manner that enables the peripheral device to communicate with the host computing device. Frequently, this will occur as a result of a physical connection of the peripheral device to the host computing device. (In general, such physical connection can occur either before or after the host computing device begins operating; however, in the former case, subsequent steps of the method **500**—with the exception of, depending upon the implementation of the peripheral device, the step **503**—cannot be performed until the host computing device begins operating.) For example, the peripheral device can be embodied in a card or disk (e.g., a card conforming to a PCMCIA form factor as established by the appropriate standard) that is inserted into a corresponding socket formed in the host computing device. Or, the peripheral device can be embodied in a housing from which a cord extends, a plug of the cord being inserted into a mating receptacle formed in the host computing device. However, such physical connection need not necessarily occur; the peripheral device can also be connected to the host computing device by any type of wireless communication for which the host computing device contains an appropriate interface.

Once connection between the peripheral device and the host computing device is made, the host computing device detects the presence of the peripheral device, as shown by step **502**. Such detection of the presence of a peripheral device is typically enabled as a standard aspect of the operating system software of the host computing device.

Typically, once the presence of a new peripheral device is detected by the operating system software of the host computing device, the operating system software (or companion software program) also identifies the type of the peripheral device. This can be accomplished, for example, by a standard software device driver (hereinafter, "host driver") for devices of the type that use the host computing device interface that is being used by the peripheral device **602**. In FIG. **6**, the host driver is shown stored in the memory section **606***a* of the memory device **606** of the host computing device **601**. (The Card Services or Socket Services programs that often are bundled with the Windows95™ operating system software for use in performing various "housekeeping" functions associated with a PCMCIA interface are examples of such drivers.) However, in the method **500**, before the operating system software can perform such identification, the peripheral device according to the invention suspends operation of this aspect of the operating system software, so that the peripheral device can establish its identity, as shown by step **503**, and explained further below. As will be apparent from that explanation, performance of the step **503** advantageously enables the peripheral device to assume the identity of the target functionality that is part of the peripheral device. Since, as described elsewhere herein, a peripheral device according to the invention can include a variety of types of target functionality, the peripheral device can take a variety of identities.

The particular manner in which operation of the operating system software is suspended so that the peripheral device can establish its identity can depend on the characteristics of the operating system software and/or the device interface. However, for many combinations of operating system software and device interface, the operating system software waits for confirmation that the device connected to the device interface is ready for further interaction with the operating system software before the operating system software seeks to identify the type of the device connected to the interface (the standard for PCMCIA interfaces, for example, specifies such operation). In such cases, the peripheral device can be configured to delay informing the operating system software that the peripheral device is ready for further interaction until the peripheral device has established its identity.

The following description of one way in which the step **503** can be implemented can best be understood by reference to the system **600** shown in FIG. **6**. One way in which the operating system software of a host computing device can identify the type of a peripheral device is to access a known memory section of a memory device of the peripheral device, as established by an interface standard developed for that type of peripheral device, that stores data representing the type of the peripheral device. This is true for a variety of types of peripheral devices, such as, for example, peripheral devices that conform to the PCMCIA standard. (The PCMCIA standard, for example, includes a specification, called the Card Information Structure, that defines, among other things, a location in a portion of memory of a PCMCIA card, denoted as "attribute memory", that stores data identifying the type of the PCMCIA card.) In the system **600**, the peripheral device **602** is such a device. The memory section of the memory device **612** of the peripheral device **602** which the host computing device **601** seeks to access is shown in FIG. **6** as the memory section **612***a*, and the data stored therein is referred to herein as "peripheral device identification data."

The peripheral device **602** can be implemented so that the peripheral device **602** assumes the identity of the target functionality **614** (whether or not the security functionality of the peripheral device is also being used). This enables the host computing device **601** to interact with the peripheral device **602** as though the peripheral device **602** were a device of the type of the target functionality **614**, without recognizing that security functionality **611** is present that may be performing security operations. Thus, the need to modify aspects of the operation of the host computing device (e.g., the host device driver) to enable performance of security operations is reduced or eliminated, making implementation and use of a data security system including the peripheral device **602** simpler and easier. Since use of the data security system is easier (e.g., a user need not provide input to cause the host driver to be appropriately tailored to enable desired interaction with a security device), the possibility that a user will use the system incorrectly (e.g., fail to apply security operations to an interaction with the host computing device, or apply the security operations incorrectly or incompletely) is reduced.

Though, as shown in FIG. **6**, the peripheral device **602** includes security functionality **611** and target functionality **614**, the system **600** can be operated so that only the security functionality **611** is used. The peripheral device **602** and peripheral device driver (discussed below) can be implemented so that, when the peripheral device **602** is operated in that way, the peripheral device identification data stored in the memory location **612***a* identifies the peripheral device **602** as a security device.

Returning to FIG. **5**, after the peripheral device has established its identity, the host computing device identifies the peripheral device, as shown by step **504**. This can be implemented as part of the host driver, as indicated above.

Once the host computing device has identified the peripheral device (and other host computing device operating system software operations concluded, if applicable), the user can begin using the peripheral device (in particular, the security functionality of the peripheral device), as shown by step **505** of the method **500**. Such use can be enabled by one or more software programs (referred to collectively hereinafter as a "peripheral device driver," though such programs can include programs in addition to those conventionally termed "drivers," such as programs conventionally termed "applications") that are executed by the host computing device.

The use of a separate driver to control and interact with the security functionality of a peripheral device according to the invention can be advantageous because it reduces or eliminates the need to modify the host driver. As a practical matter, such modification of the host driver can likely only be accomplished by requiring a user to interact with a standard host driver to appropriately modify the standard host driver. This is undesirable because the user may forget to modify the driver or modify the driver incorrectly or incompletely.

The peripheral device driver can have previously been installed on a data storage device (e.g., hard disk) of the host computing device (in FIG. **6**, the peripheral device driver is shown stored in the memory section **606***b* of the memory device **606** of the host computing device **601**), or can be made accessible to the host computing device via an appropriate interface (such as a floppy disk drive, CD-ROM drive or network connection) at a time when the user wishes to initiate interaction between the host computing device and the peripheral device. Additionally, when a peripheral device according to the invention is used with a host computing device which utilizes operating system software that supports the feature informally referred to as "plug and play", it is also possible to store the peripheral device driver in a memory device of the peripheral device and configure the peripheral device so that, when the peripheral device is connected for the first time to a particular host computing device, the host computing device automatically provides the user with the opportunity to instruct the host computing device to cause the peripheral device driver to be transferred from the peripheral device to the host computing device.

FIG. **7** is a flow chart of a method **700**, according to an embodiment of the invention, for using a peripheral device according to the invention. It is to be understood that the method **700** shown in FIG. **7** is not the only way to enable the aspects of use of a peripheral device according to the invention that are illustrated in FIG. **7**; as can be readily appreciated by those skilled in the art, such aspects can be implemented using any of a variety of other appropriate methods. Further, the use of a peripheral device according to the invention can include aspects not illustrated in FIG. **7**; likewise, such use may not include some of the aspects illustrated in FIG. **7**. The method **700** of FIG. **7** is shown merely to aid in the illustration of certain aspects of the invention, and should not be interpreted as restricting the manner in which a peripheral device according to the invention can be used.

To begin using a peripheral device according to the invention, a user instructs the host computing device to begin execution of the peripheral device driver, as shown by step **701** of the method **700**, the user having obtained knowledge of the appropriate command to begin execution of the peripheral device driver in any appropriate manner (e.g., from a user manual accompanying the peripheral device driver and/or the peripheral device). In general, the steps of the method **700** occur as a result of operation of a peripheral device driver; however, operation of the host driver may be necessary or desirable to enable some aspects of the method **700** (e.g., execution of a transaction, as in steps **708**, **712** and **715**).

As indicated above, a peripheral device according to the invention can be implemented so that the host driver cannot detect the presence of the security functionality of the peripheral device. In such case, the peripheral device driver enables the detection of the security functionality, as shown by step **702** of the method **700**. This can be accomplished by including instructions as part of the peripheral device driver that, when the peripheral device driver first begins executing, cause the peripheral device driver to access a predefined location of a memory device of the peripheral device (in FIG. **6**, the memory section **612***b*) for data that identifies whether the peripheral device is a device having security functionality that is compatible with the peripheral device driver. If the peripheral device is such a device, then the peripheral device driver can enable the user to make use of the security functionality of the peripheral device. Further, the peripheral device driver can be implemented, as shown in FIG. **7**, so that, if the proper security functionality is not detected, execution of the peripheral device driver terminates, preventing use of the peripheral device. Alternatively, the peripheral device driver can be implemented so that, if the proper security functionality is not detected, the target functionality of the peripheral device can be used without the security functionality of the peripheral device.

A peripheral device according to the invention can, in general, be operated in one of three modes: 1) a mode in which only the security functionality is used, 2) a mode in which both the security functionality and the target functionality are used, and 3) a mode in which only the target functionality is used. The user can be enabled to, via the peripheral device driver, select any one of the three modes of operation. However, in some applications, it may be desirable to inhibit operation in one or two of the modes. In particular, it may be desirable to prevent operation of the peripheral device in the last of the above-listed modes, i.e., a mode in which the security functionality is not used, if it is desired to ensure that use of the target functionality can only occur with the application of one or more security operations. This could be accomplished by implementing the peripheral device driver so that the option to operate in that mode is not presented to the user, or the peripheral device could be configured during manufacture to prohibit operation in that mode. For example, if the target functionality is embodied as a communications device or a memory device, it may be desirable to ensure that unencrypted data cannot be transferred via the communications device or stored in the memory device, whether done inadvertently or on purpose.

In the method **700**, all three of the above-listed modes are available for use. In the step **703** of the method **700**, a determination is made as to whether the security functionality is to be used. (As noted above, such use may be required.) If yes, the peripheral device is operated in one of the first two modes above (security functionality only, or security functionality plus peripheral functionality); if no, the third mode is used (peripheral functionality only).

The peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. In particular, it can be desirable to require an access code before enabling a user to use the security functionality, thus establishing a layer of security that protects the integrity of the security operations themselves. In the method **700**, as shown by the step **704**, an acceptable access code must be entered by the user before the security functionality of the peripheral device can be used. An access code can be entered, for example, by inputting the access code in a conventional manner using a user interface device (e.g., keyboard) of the host computing device. Or, an access code can be entered using particular embodiments of target functionality (such as a biometric device, discussed in more detail below) that is part of the peripheral device according to the invention.

Advantageously, an access code can be used not only to control access to the security (or other) functionality of the peripheral device, but also to identify a "personality" of the user. Each personality is represented by data that establishes certain characteristics of operation of the peripheral device, such as, for example, restrictions on operation of the peripheral device (e.g., limitations on the types of security operations that can be performed) or specification of operating parameters or characteristics (e.g., cryptographic keys or specification of a particular incarnation of a type of security algorithm, such as a particular encryption algorithm). A single user can have multiple personalities: each personality might, for example, correspond to a different capacity in which a user acts. Data representing personalities and corresponding user access codes can be stored in a memory device of the peripheral device.

Upon receipt of an acceptable access code, the peripheral device driver controls the host computing device to present a user interface that enables the user to effect desired control of the peripheral device, and, in particular, to use the peripheral device to perform security operations, as described below. (If access codes are also used to identify personalities, upon receipt of an acceptable access code, the peripheral device driver can also access and retrieve the data representing the corresponding personality, so that the operation of the peripheral device can be controlled accordingly.) The user interface for enabling a user to operate the peripheral device can be implemented in any of a variety of well known ways (e.g., as a graphical user interface) using methods and apparatus that are well known to those skilled in the art. Generally, the user interface enables the user to perform any functionality that is provided by the peripheral device, as described in more detail elsewhere herein.

As indicated above, a peripheral device according to the invention can be operated in any of three modes. Once an acceptable access code has been entered, the peripheral device driver can enable the user to select one of the three modes, as shown in step **705** of the method **700**. (Alternatively, as mentioned above, it may be desirable to present the user only with the option of choosing the security functionality only mode or the security functionality plus peripheral functionality mode, so as to eliminate the possibility that the user will effect an unsecured use of the target functionality.) If the security functionality only mode, or the security functionality plus peripheral functionality mode, is selected, then the user interface (and the underlying peripheral device driver) enables the user to input all desired or required instructions regarding the security operations to be performed for a particular "transaction" (e.g., a storage of data in a memory device, a transmission of data by a communications device, or an exchange of data with a smart card reader device), as shown by steps **706** and **710** of the method **700**. For example, the user interface can enable the user to select data to which security operations are to be performed, specify the application of particular security operations to data, or specify parameters or other information required for a particular security operation. If the security functionality plus peripheral functionality mode, or the peripheral functionality only mode, is selected, then the user interface and peripheral device driver enable the user to input all desired or required instructions regarding use of the target functionality for the transaction, as shown by steps **707** and **711** of the method **700**. For example, if the target functionality is embodied as a memory device, the user interface can enable the user to specify a name for the stored data. Or, for example, if the target functionality is embodied as a communications device, the user interface can enable the user to specify a destination (e.g., an electronic mail address) for the data.

Once the user has provided instructions in steps **706** and **707**, in step **710**, or in step **711**, the transaction is executed, as shown by step **708** or step **712** of the method **700**. After execution of the transaction, the user can be allowed to execute further transactions, as shown by step **709** of the method **700**. It is also possible for the user to begin using another personality (by entering an appropriate access code), as shown by step **709** of the method **700**. Eventually, use of the peripheral device ends, as shown by step **718** of the method **700**.

The peripheral device and associated peripheral device driver can be implemented so that it is possible to use only the security functionality of the peripheral device. The peripheral device can be used in this manner to, for example, encrypt or decrypt data stored on the host computing device by receiving the data from the host computing device, encrypting or decrypting the data as appropriate, then returning the encrypted or decrypted data to the host computing device.

As indicated above, the peripheral device and associated peripheral device driver can be implemented so that it is possible to use only the target functionality of the peripheral device, even without entering an appropriate access code. In the method **700**, such operation is shown by the steps **714**, **715** and **716**, which function in the same manner as steps **711**, **712** and **709**, described above. Using the peripheral device in this way can be useful, for example, when the target functionality is embodied as a biometric device, as described further below, that is used to perform user authentication. In particular, if the biometric device is to be used as the mechanism to enter the access code in step **704**, operation in this mode may be necessary (depending on the capabilities of the biometric device) to enable such use of the biometric device. (Of course, in this case, security functionality, i.e., user authentication, is used as part of the step **715**) The step **717** can also enable use of the security functionality to begin by causing a prompt for an appropriate access code to appear (step **704**). Again, eventually, use of the peripheral device ends (step **718**).

As described above, a peripheral device according to the invention that includes security functionality and target functionality can be implemented so that the host computing device is not aware of the presence of the security functionality. It may also be desirable to shield the user from knowledge of the presence of the security functionality and cause predetermined security operations to be performed automatically. This may be desirable so that, for example, it is not necessary for the user to provide input regarding the performance of security operations, thus eliminating the possibility that the user will neglect to provide such input, or will provide the input incorrectly or incompletely. Or, it may be desirable to make security operations transparent to users to enhance the security of those operations, since, if the performance of such operations is unknown, there will be no attempt to defeat the security provided by those operations. If such is the case, the peripheral device driver can be implemented so that the peripheral device can operate only in the security functionality plus peripheral functionality mode (steps **710**, **711**, **712**, **714**, **715**, **716** and **717** of the method **700** cannot be performed) and so that no indication (e.g., presentation of a user interface display that allows input of instructions regarding the performance of security operations, as in step **706** of the method **700**) is given of the presence of the security functionality of the peripheral device. Rather, the user would simply be presented with options regarding operation of the target functionality (step **707** of the method **700**). In such an implementation, the peripheral device driver can be implemented to automatically cause one or more predetermined security operations to be performed based upon a user-specified interaction with the target functionality, or the peripheral device can be configured to cause such security operations to be performed any time a specified interaction with the target functionality occurs.

A significant advantage of a peripheral device according to the invention is that the peripheral device can be implemented so that any of a variety of types of target functionality can be included as part of the peripheral device. In particular, as described in more detail below, the peripheral device includes an interface control device which enables and manages communications between and among the host computing device, a cryptographic processing device that is part of the peripheral device, and target functionality that is also part of the peripheral device. The interface control device can be adapted to provide an appropriate interface for each type of target functionality. Thus, in general, any desired target functionality can be used with a peripheral device according to the invention, so long as the target functionality is implemented so as to enable communication with an interface of the type presented. Those skilled in the art of data communications can readily understand how to implement such communication with target functionality in view of the detailed description below (see FIGS. **8**, **9**A and **9**B) of an embodiment of a peripheral device according to the invention, and, in particular, an interface control device of such a peripheral device.

For example, target functionality of a peripheral device according to the invention can be embodied as a memory device adapted to enable non-volatile storage of data. In general, any such memory device can be used to embody such target functionality. More particularly, a solid-state disk storage device (e.g., NAN flash memory device) can advantageously be used. Illustratively, a memory device that can be used to embody target functionality in a peripheral device according to the invention can be a compact flash memory device, such as an ATA format flash disk drive. Other solid-state disk storage devices, such as SCSI disks and IDE disks can be used. The construction and operation of memory devices in general, as well as those identified particularly above, is well understood by those skilled in that art, so that, together with an understanding of the required communication capability between the target functionality and the interface control device, a memory device for use with the invention can be easily constructed and operated. A peripheral device according to the invention that includes a memory device that embodies the target functionality can be used, for example, to securely store data in a manner that enables a user of the data to easily carry the data with them wherever they go.

Target functionality of a peripheral device according to the invention can also be embodied as a communications device adapted to enable communication between the host computing device and a remote device. In general, any such communications device can be used to embody target functionality. A communications device that can be used to embody target functionality in a peripheral device according to the invention can include, for example, a data communications modem (such as, for example, a conventional telephone line modem, an ISDN modem, a cable modem, or a wireless modem) or a LAN transceiver (either wired or wireless and, in the latter case, operating in, for example, the infrared or radiofrequency spectrum). The construction and operation of communication devices in general, as well as those identified particularly above, is well understood by those skilled in that art, so that, together with an understanding of the required communication capability between the target functionality and the interface control device, a communication device for use with the invention can be easily constructed and operated. A peripheral device according to the invention that includes a communications device that embodies target functionality can be used, for example, to encrypt electronic mail before transmission to an addressee. Or, such a peripheral device can be used, for example, to encrypt data files that a person wishes to securely transfer between a computing device at the person's place of work and a computing device at the person's home.

Target functionality of a peripheral device according to the invention can also be embodied as a biometric device, which is defined herein as any device that is adapted to receive input data regarding a physical characteristic of a person based upon a physical interaction of the person with the device. In general, any such biometric device can be used to embody target functionality. Biometric devices that can be used in a peripheral device according to the invention can include, for example, a fingerprint scanning device, a retinal scanning device or a faceprint scanning device.

In addition to conventional computational devices for storing and/or manipulating digital data, a biometric device includes a sensor for sensing the physical characteristic, and an analog-to-digital converter to transform the analog data representing the sensed characteristic into digital data. For example, a fingerprint scanning device includes a sensor upon which a person can place a finger, the sensor sensing the fingerprint of the finger, the content of the sensed fingerprint being converted into digital data by the device. Similarly, a retinal scanning device includes a sensor which can be placed proximate to a person's eye, the sensor sensing characteristics of the eye such as blood vessel pattern or iris pattern, the device translating the content of the sensed characteristics into digital data. The construction and operation of biometric devices in general, as well as those identified particularly above, is well understood by those skilled in that art, so that, together with an understanding of the required communication capability between the target functionality and the interface control device, a biometric device for use with the invention can be easily constructed and operated. Fingerprint scanning devices and retinal scanning devices that can readily be modified for use with the invention, i.e. to communicate with an interface control device according to the invention, are known to those skilled in that art. For example, fingerprint scanning devices such as those available from Identix Incorporated of Sunnyvale, Calif. can be used in a fingerprint scanning device for use with the invention.

A peripheral device according to the invention that includes a biometric device that embodies the target functionality can be used, for example, to enable user authentication to a host computing device before allowing access to particular data stored on the host computing device. Such user authentication can be accomplished by using a biometric device to obtain biometric data from a user and comparing the biometric data to an appropriate library of biometric data representing a predetermined group of people (e.g., authorized users). The library of data can be stored in a memory device of the peripheral device.

When a peripheral device including a fingerprint scanning device is embodied as a card adapted to be inserted into a slot of a host computing device (e.g., a slot conforming to a PCMCIA standard), it may be useful to make the peripheral device relatively long, so that a portion of the card on which the sensor is positioned can extend from the slot of the host computing device, thereby enabling fingerprints to be scanned while the peripheral device is inserted in the host computing device. Similarly, for a fingerprint scanning device, retinal scanning device or faceprint scanning device, it may be desirable to form the device so that the sensor is connected to the remainder of the device via an appropriate communication line, thus providing some range of movement of the sensor while the peripheral device is inserted in the host computing device, thereby facilitating use of the device.

A biometric device can be used in different ways with a system according to the invention, depending upon the capabilities of the biometric device. Using known apparatus and methods, a "smart" biometric device can be implemented with the capability to detect the presence of an input to the sensor, and, upon such detection, initiate acquisition of the biometric data and performance by the peripheral device of the appropriate data comparison. Such a biometric device can be used to perform user authentication as in step **704** of the method **700** above. Alternatively, the biometric device may be "stupid" and require that a user initiate the data acquisition and authentication process. Such a biometric device can be used to perform user authentication in a peripheral device that allows operation without entry of a proper access code, as in steps **714** and **715** of the method **700**.

Target functionality of a peripheral device according to the invention can also be embodied as a smart card reader device adapted to communicate with a smart card, such as, for example, a smart card compliant with the ISO 7816 standard. Such a device can be implemented by adapting a conventional smart card reader, the construction and operation of which is well known to those skilled in that art, to provide a communications interface that enables the smart card reader to communicate with the interface control device. A peripheral device according to the invention that includes a smart card reader device can be used to provide security features to a smart card reader, or add to existing security features of a smart card reader.

It is to be understood that the examples given above are merely illustrative, not exhaustive, of the ways in which a peripheral device according to the invention can be used. Many more possibilities exist.

FIG. **8** is a block diagram of a peripheral device **800** according to another embodiment of the invention. The peripheral device **800** includes a cryptographic processing device **801**, an interface control device **802**, a first memory device **803**, a second memory device **804**, a real-time clock **805**, a host computing device input/output (I/O) interface **806** and target functionality **807**.

The host computing device I/O interface **806** enables communications between the peripheral device **800** and a host computing device. The electrical and mechanical characteristics of the I/O interface **806**, as well as the protocol used to enable communication via the interface **806** are established in any manner that conforms to the industry standard specifications for an interface of that type. For example, a peripheral device according to the invention can be adapted for insertion into a PCMCIA slot of a host computing device. In such a peripheral device, the electrical and mechanical characteristics and communications protocol for the host computing device I/O interface **806** are established in conformance with the appropriate PCMCIA standards.

The cryptographic processing device **801** can be adapted to perform security operations. Generally, the cryptographic processing device **801** can be embodied by any processor capable of performing the cryptographic operations desired to be provided by the peripheral device **800**. In one embodiment of the peripheral device **800**, the cryptographic processing device **801** is a special purpose embedded processor, embodied on a single integrated chip and designated as MYK-82 (and also referred to by the name Capstone), which includes an ARM6™ processor core and several special purpose cryptographic processing elements that have been developed by the Department of Defense. The construction and operation of the Capstone chip is known by those skilled in the art of cryptographic processing.

The first memory device **803** can be a non-volatile data storage device which can be used to store computer programs and persistent data. The first memory device **803** can be implemented by any appropriate such device (of which there are many conventional, readily available incarnations), such as, for example, a conventional flash memory device.

The second memory device **804** can be a volatile data storage device that can also be a rapidly accessible data storage device in which frequently used data and program instructions can be stored during operation of the peripheral device **800**. The second memory device **804** can also be implemented by any appropriate such device (of which there are many conventional, readily available embodiments), such as, for example, a conventional random access memory (RAM) device.

The real-time clock **805** enables the creation of time stamps, which can be used in a number of security operations. Advantageously, the time stamps created by the real-time clock **805** are more secure than those that could otherwise be produced by the relatively insecure clock of a host computing device. The real-time clock **805** includes a conventional battery backup device that maintains power to the real-time clock **805** when the peripheral device **800** is not in use (i.e., when power is not supplied to the peripheral device **800**), so that the correct time is continuously preserved within the peripheral device **800**. The real-time clock **805** (including battery backup) can be embodied by any conventional such device, such as the DS1302 clock available from Dallas Semiconductor of Dallas, Texas.

In the peripheral device **800**, the interface control device **802** mediates the interaction between the host computing device, the target functionality **807** and the cryptographic processing device **801**. In one embodiment of the peripheral device **800**, the interface control device **802** is a conventional field-programmable gate array (FPGA) that is programmed to perform the functions that it is desired to implement with the interface control device **802**, as described in more detail below. The interface control device **802**, under control of the cryptographic processing device **801**, can be adapted to enable the peripheral device **800** to assume the identity of the target functionality **807**, as discussed above. The interface control device **802** also enables the in-line cryptography aspect of the invention, since the interface control device **802** controls the flow of data between the host computing device and the target functionality **807**.

FIG. **9A** is a block diagram illustrating the flow of data through the interface control device **802** of FIG. **8**. Data transferred from a host computing device enters the peripheral device **800** (not demarcated in FIG. **9A**) through the host computing device I/O interface **806**. The interface control device **802** presents the data to a cryptographic processing device interface **808** (not shown in FIG. **8**). Depending on the configuration of the interface control device **802**, as determined by operation of the peripheral device driver and/or by settings established during the manufacture of the peripheral device **800**, the data may or may not be processed by the cryptographic processing device **801** (FIG. **8**). Typically (or, in some cases, necessarily), as discussed in more detail above, cryptographic processing will occur. The interface control device **802** then causes the data to be transferred to the target functionality **807**. Data being transferred from the target functionality **807** to the host computing device follows a similar path in the reverse direction. When the target functionality **807** is not present or is not being used, data transferred from the host computing device, after being presented to the cryptographic processing device interface **808** and being processed by the cryptographic processing device **801**, is caused to be transferred back to the host computing device I/O interface **806** (and, from there, to the host computing device) by the interface control device **802**.

FIG. **9**B is a block diagram of a particular embodiment of an interface control device **910** for use in a peripheral device according to the invention. As shown in FIG. **9**B, the host computing device communicates via a PCMCIA interface and the target functionality is embodied by a compact flash memory device. Those skilled in the art will readily appreciate how the interface control device **910** can be modified for use with other host computing device interfaces and/or target functionalities.

The interface control device **910** includes sets of configuration registers **911**. The data stored in the configuration registers **911** establish operating characteristics of the interface control device: in particular, the content of the configuration registers enables the interface control device to present to the host computing device a desired identification of the peripheral device, and determines whether data passing through the peripheral device must be subjected to security operations.

A set of configuration registers is maintained for the host computing device I/O interface, the cryptographic processing device interface, and the target functionality interface. In particular, the content of the host computing device I/O interface configuration registers is such that the interaction of the host computing device with the peripheral device is the same as if the security functionality were not present (unless the data security system is operating in security functionality only mode). The content of the target functionality interface registers reflects the presence of the security functionality. The cryptographic processing device interface registers bridge the gap between the other two sets of registers.

The remainder of the functional blocks of the interface control device **910** shown in FIG. **9**B perform functions and operate in a manner that can readily be understood by those skilled in the art from the designation and interconnection of those blocks in FIG. **9**B.

In general, the security functionality of a peripheral device according to the invention can be configured to perform any cryptographic operation, as well as other, related mathematical operations. A configuration of the security functionality that enables a particular cryptographic or mathematical operation can be produced, for example, by using appropriate existing cryptographic software, application-specific hardware, or combination of the two, as known by those skilled in the art of producing cryptographic devices. Following is a description of exemplary cryptographic and mathematical operations that can be implemented as part of the security functionality of a peripheral device according to the invention. These cryptographic and mathematical operations are well-known and can readily be implemented in a peripheral device according to the invention by a person of skill in the art of cryptography.

For example, a peripheral device according to the invention can implement one or more cryptographic key exchange operations. Any key exchange operation can be implemented, such as, for example, the Department of Defense Standard, the RSA, the Diffie-Hellman, and the X9.42 (ANSI Banking Standard) key exchange algorithms.

A peripheral device according to the invention can also implement one or more hash operations. Any hash operation can be implemented, such as, for example, the FIPS 180-1 (SHA-1), the Message Digest 2 (RSA), and the Message Digest 5 (RSA) algorithms.

A peripheral device according to the invention can also implement one or more digital signature operations. Any digital signature operation can be implemented, such as, for example, the FIPS 186 (DSA—512, 1024) and the RSA Signature (512, 768, 1024, 2048) algorithms.

A peripheral device according to the invention can also implement one or more key wrapping operations for both symmetric and asymmetric keys. A key wrapping operation can ensure that plaintext keys are not accessible external to the peripheral device. Any key wrapping operation can be implemented.

A peripheral device according to the invention can also implement one or more symmetric encryption operations. Any symmetric encryption operation can be implemented, such as, for example, the FIPS 185 (implemented completely in hardware), the DES (including 3DES, EDE3, CBC and ECB), the RC-2 and the RC-4 algorithms.

A peripheral device according to the invention can also implement one or more asymmetric (public key) encryption operations. While asymmetric encryption operations underlie the key exchange operations described above, asymmetric key operations can also be used independently in a peripheral device according to the invention for bulk encryption. Any asymmetric encryption operation can be implemented, such as, for example, the RSA and Diffie-Hellman algorithms.

A peripheral device according to the invention can also implement one or more exponentiation operations, which are required in many cryptographic operations. Any exponentiation operation can be implemented. Since exponentiation requires a significant amount of processing time relative to other mathematical operations, it can be desirable to implement an exponentiation operation in dedicated hardware. In one embodiment of a peripheral device according to the invention, the security functionality of the peripheral device includes a full 1024 bit exponentiator implemented in hardware.

Various embodiments of the invention have been described. The descriptions are intended to be illustrative, not limitative. Thus, it will be apparent to one skilled in the art that certain modifications may be made to the invention as described above without departing from the scope of the claims set out below.

We claim:

1. A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device;

means for operably connecting the security means and/or the target means to the host computing device in response to an instruction from the host computing device; and means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means.

2. A peripheral device as in claim **1**, wherein the target means comprises means for non-volatilely storing data.

3. A peripheral device as in claim **1**, wherein the target means comprises means for enabling communication between the host computing device and a remote device.

4. A peripheral device as in claim **1**, wherein the target means comprises a biometric device.

5. A peripheral device as in claim **1**, wherein the target means comprises means for communicating with a smart card.

6. A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means,

means for enabling communication with a host computing device;

means for operably connecting the security means and/or the target means to the host computing device in response to an instruction from the host computing device; and

means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the target means.

7. A peripheral device as in claim **6**, wherein the target means comprises means for non-volatilely storing data.

8. A peripheral device as in claim **6**, wherein the target means comprises means for enabling communication between the host computing device and a remote device.

9. A peripheral device as in claim **6**, wherein the target means comprises a biometric device.

10. A peripheral device as in claim **6**, wherein the target means comprises means for communicating with a smart card.

11. A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device; and

means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means.

12. A peripheral device as in claim **11**, wherein the target means comprises means for non-volatilely storing data.

13. A peripheral device as in claim **12**, wherein the means for non-volatilely storing data further comprises a solid-state disk storage device.

14. A peripheral device as in claim **13**, wherein the solid-state disk storage device comprises an ATA format flash disk drive.

15. A peripheral device as in claim **11**, wherein the target means comprises means for enabling communication between the host computing device and a remote device.

16. A peripheral device as in claim **15**, wherein the means for enabling communication between the host computing device and a remote device further comprises wireless communication means.

17. A peripheral device as in claim **16**, wherein the wireless communication means comprises a wireless modem.

18. A peripheral device as in claim **16**, wherein the wireless communication means comprises a wireless LAN transceiver.

19. A peripheral device as in claim **11**, wherein the target means comprises a biometric device.

20. A peripheral device as in claim **19**, wherein the biometric device comprises a fingerprint scanning device.

21. A peripheral device as in claim **19**, wherein the biometric device comprises a retinal scanning device.

22. A peripheral device as in claim **11**, wherein the target means comprises means for communicating with a smart card.

23. A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device;

means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means; and

means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the target means.

24. A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device; and

means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the target.

25. A peripheral device as in claim **24**, wherein the target means comprises means for non-volatilely storing data.

26. A peripheral device as in claim **25**, wherein the means for non-volatilely storing data further comprises a solid-state disk storage device.

27. A peripheral device as in claim **26**, wherein the solid-state disk storage device comprises an ATA format flash disk drive.

28. A peripheral device as in claim **24**, wherein the target means comprises means for enabling communication between the host computing device and a remote device.

29. A peripheral device as in claim **28**, wherein the means for enabling communication between the host computing device and a remote device further comprises wireless communication means.

30. A peripheral device as in claim **29**, wherein the wireless communication means comprises a wireless modem.

31. A peripheral device as in claim **29**, wherein the wireless communication means comprises a wireless LAN transceiver.

32. A peripheral device as in claim **24**, wherein the target means comprises a biometric device.

33. A peripheral device as in claim **32**, wherein the biometric device comprises a fingerprint scanning device.

34. A peripheral device as in claim **32**, wherein the biometric device comprises a retinal scanning device.

35. A peripheral device as in claim **24**, wherein the target means comprises means for communicating with a smart card.

36. A data security system, comprising:

a host computing device including one or more device interfaces adapted to enable communication with another device;

a peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device; and

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device; and

means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means.

37. A data security system, comprising:

a host computing device including one or more device interfaces adapted to enable communication with another device;

a peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device; and

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device; and

means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the target means.

38. For use in a peripheral device adapted for communication with a host computing device, performance of one or more security operations on data, and interaction with a host computing device in a defined way, a method comprising the steps of:

receiving a request from a host computing device for information regarding the type of the peripheral device; and

providing to the host computing device, in response to the request, information regarding the type of the defined interaction.

39. For use in a peripheral device adapted for communication with a host computing device, performance of one or more security operations on data, and interaction with a host computing device in a defined way, a method comprising the steps of:

communicating with the host computing device to exchange data between the host computing device and the peripheral device;

performing one or more security operations and the defined interaction on the exchanged data; and

mediating communication of the exchanged data between the host computing device and the peripheral device so that the exchanged data must first sass through means for performing the one or more security operations.

* * * * *

#7

A/No Fee

Attorney Docket No.: SPY-004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

June 4, 1997

Assistant Commissioner for Patents
Washington, D. C. 20231
ATTN: BOX PATENT APPLICATION

Transmitted herewith for filing is a patent application, as follows:

Inventors: William P. Bialick, Mark J. Sutherland, Janet L. Dolphin-Peterson, Thomas K. Rowland, Kirk W. Skeba and Russell D. Housley
Title: PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY

Enclosed with this transmittal letter are:

42 pages of specification, claims and abstract
7 sheets of drawings: ___ (Formal) _X_ (Informal)
3 pages of Declaration and Power of Attorney (Unexecuted)
___ Power of Attorney
___ Assignment of invention to Spyrus, Inc.
___ Small Entity Declaration
___ Independent Inventor's Declaration
___ PTO Form-1449
___ Preliminary amendment

The filing fee is calculated as follows (small entity status is claimed):

CLAIMS AS FILED (fees computed under §1.9(f))

	Number Filed		Number Extra		Rate		Fee
Basic Filing Fee:							$ 385.00
Total Claims:	32	- 20 =	12	X	$11	=	$ 132.00
Independent Claims:	12	- 3 =	9	X	$40	=	$ 360.00
___ Application contains one or more multiple dependent claims ($260 total fee)							$ 0.00
TOTAL FILING FEE:							**$ 877.00**

A Return Post Card and this sheet in duplicate are also enclosed.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C., 20231, on June 4, 1997. Express Mail Receipt No. EF 557 934 406 US

David R. Graham 6-4-97
David R. Graham Date

Respectfully submitted,

David R. Graham
David R. Graham
Reg. No. 36,150
Attorney for Applicants

PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY

William P. Bialick
Mark J. Sutherland
Janet L. Dolphin-Peterson
Thomas K. Rowland
Kirk W. Skeba
Russell D. Housley

CROSS-REFERENCE TO RELATED APPLICATION

This application is related to the commonly owned, co-pending United States Patent Application entitled "Modular Security Device," by William P. Bialick, Mark J. Sutherland, Janet L. Dolphin-Peterson, Thomas K. Rowland, Kirk W. Skeba and Russell D. Housley, filed on the same date as the present application and having Attorney Docket No. SPY-003, the disclosure of which is incorporated by reference herein.

8/869,120

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to a peripheral, often portable, device (as well as the methods employed by such a peripheral device, and systems including such a peripheral device and a host computing device with which the peripheral device communicates) that can communicate with a host computing device to enable one or more security operations to be performed by the peripheral device on data stored within the host computing device, data provided from the host computing device to the peripheral device, or data retrieved by the host computing device from the peripheral device.

2. Related Art

Computing capability is becoming increasingly portable. In particular, there are more and more portable peripheral devices that are adapted for communication with a host computing device (e.g., desktop computer, notebook computer or personal digital assistant) to enable particular functionality to be achieved. These portable peripheral devices can take a variety of physical forms (e.g., PCMCIA cards, smart cards, CD-ROMs) and can perform an assortment of functions (e.g., storage, communications and cryptography).

However, while portable computing affords a number of advantages, it has a significant disadvantage in that the computational environment (including the portable peripheral devices, the host computing devices in which they are used, and any other computational devices that communicate with those devices) is more susceptible to security breaches, i.e., unauthorized access to, or modification of, programs and/or data resident within the environment. Consequently, cryptographic devices and methods have been developed for use with such computational environments (as well as other computational environments) to enable increased levels of environment security to be obtained.

FIG. 1 is a block diagram of a prior art system for enabling a host computing device to provide secured data to, and retrieve secured data from, a portable device. In FIG. 1, a system 100 includes a host computing device 101 and a portable device 102. The host computing device 101 and portable device 102 are adapted to enable communication between the devices 101 and 102. The host computing device 101 includes a security mechanism 101a (which can be embodied by appropriately configured hardware, software and/or firmware, such as, for example, a general purpose microprocessor operating in accordance with instructions of one or more computer programs stored in a data storage device such as a hard disk) which can be directed to perform one or more cryptographic operations.

In the system 100, if it is desired to provide secured data from the host computing device 101 to the portable device 102, the host computing device 101 causes the security mechanism 101a to perform appropriate cryptographic operations on data before the data is transferred to the portable device 102. Similarly, the host computing device 101 can receive secured data from the portable device 102 and perform appropriate cryptographic operations on the data to convert the data into a form that enables the data to be accessed and/or modified by a person who is authorized to do so.

A significant deficiency of the system 100 is that the security mechanism 101a is itself typically not adequately secure. It is commonly accepted that the components (including hardware, software and/or firmware) of most host computing devices are inherently insecure. This is because the system design of host computing devices is, typically, intentionally made open so that components made by different manufacturers can work together seamlessly. Thus, an unauthorized person may obtain knowledge of the operation of the security mechanism 101a (e.g., identify a cryptographic key), thereby enabling that person to gain access to, and/or modify, the (thought to be secured) data.

FIG. 2 is a block diagram of another prior art system for enabling a host computing device to provide secured data to, and retrieve secured data from, a portable device. In FIG. 2, a system 200 includes a host computing device 201, a portable device 202 and a security device 203. The host computing device 201, the portable device 202 and security device 203 are adapted to enable communication between the devices 201 and 202, and between the devices 201 and 203. The security device 203 includes appropriately configured hardware, software and/or firmware which can be directed to perform one or more cryptographic operations.

In the system 200, if it is desired to provide secured data from the host computing device 201 to the portable device 202, the host computing device 201 first causes data to be transferred to the security device 203, where appropriate cryptographic operations are performed on the data. The secured data is then transferred back to the host computing device 201, which, in turn, transfers the secured data to the portable device 202. Similarly, the host computing device 201 can receive secured data from the portable device 202 by, upon receipt of secured data, transferring the secured data to the security device 203, which performs appropriate cryptographic operations on the data to convert the data into a form that enables the data to be accessed and/or modified by a person who is authorized to do so, then transfers the unsecured data back to the host computing device 201.

The system 200 can overcome the problem with the system 100 identified above. The security device 203 can be constructed so that the cryptographic functionality of the device 203 can itself be made secure. (Such a security device is often referred to as a security "token.") An unauthorized person can therefore be prevented (or, at least, significantly deterred) from obtaining knowledge of the operation of the security device 203, thereby preventing (or significantly deterring) that person from gaining access to, and/or modifying, the secured data.

However, the system 200 may still not always ensure adequately secured data. In particular, unsecured data may be provided by the host computing device 201 to the portable device 202 if the host computing device 201 - whether through inadvertent error or deliberate attack by a user of the host computing device 201, or through malfunction of the host computing device 201 - fails to first transfer data to the security device 203 for appropriate cryptographic treatment before providing the data to the portable device 202.

Additionally, the system 200 requires the use of two separate peripheral devices (portable device 202 and security device 203) to enable the host computing device 201 to exchange secured data with the portable device 202. For several reasons, this may be inconvenient. First, both devices 202 and 203 may not be available at the time that it is desired to perform a secure data exchange (e.g., one may have been forgotten or misplaced). Second, even if both devices 202 and 203 are available, it may not be possible to connect both devices 202 and 203 at the same time to the host computing device 201, making use of the devices 202 and 203 cumbersome and increasing the likelihood that unsecured data is provided by the host computing device 201 to the portable device 202.

SUMMARY OF THE INVENTION

A peripheral device according to the invention can be used to communicate with a host computing device to enable one or more security operations to be performed by the peripheral device on data stored within the host computing device, data provided from the host computing device to the peripheral device (which can then be, for example, stored in the peripheral device or transmitted to yet another device), or data retrieved by the host computing device from the peripheral device (e.g., data that has been stored in the peripheral device, ~~or~~ a' transmitted to the peripheral device from another device a'). In particular, the peripheral device can be adapted to enable, in a single integral peripheral device, performance of one or more security operations on data, and a defined interaction with a host computing device that has not previously been integrated with security operations in a single integral device. The defined interactions can provide a variety of types of functionality (e.g., data storage, data communication, data input and output, user identification), as described further below. The peripheral device can be implemented so that the peripheral device can be operated in any one of multiple user-selectable modes: a security functionality only mode, a target functionality mode, and a combined security and target functionality mode. The peripheral device can also be implemented so that the security operations are performed in-

a Ins a'

line, i.e., the security operations are performed between the communication of data to or from the host computing device and the performance of the defined interaction. Moreover, the peripheral device can be implemented so that the security functionality of the peripheral device is transparent to the host computing device.

A peripheral device according to the invention can advantageously enable application of security operations to a wide variety of interactions with a host computing device. In particular, a peripheral device according to the invention can accomplish this without necessity to use two peripheral devices: one that performs the security operations and one that performs the defined interaction. This can, for example, minimize the possibility that the device adapted to perform the defined interaction will be used with the host computing system without proper application of security operations to that interaction. Moreover, the provision of in-line security in a peripheral device according to the invention enables a more secure exchange of data between a host computing device and the peripheral device, overcoming the problems identified above in previous systems for performing security operations on data exchanged between such devices. Additionally, implementing a modular device according to the invention so that the performance of security operations by the modular device is transparent can reduce or eliminate the need to modify aspects of the operation of the host computing device (e.g., device drivers of the host computing device), making implementation and use of a data security system including the modular device simpler and easier. Thus, the possibility that a user will use the system incorrectly (e.g., fail to apply security operations to an interaction with the host computing device, or apply the security operations incorrectly or incompletely) is reduced. Making the security operations transparent can also enhance the security of those operations.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a prior art system for enabling a host computing device to provide secured data to, and retrieve secured data from, a portable device.

FIG. 2 is a block diagram of another prior art system for enabling a host computing device to provide secured data to, and retrieve secured data from, a portable device.

FIG. 3A is a block diagram of a system according to the invention.

FIG. 3B is a perspective view of a physical implementation of the system of FIG. 3A according to one embodiment of the invention.

FIG. 4 is a block diagram of a peripheral device according to an embodiment of the invention.

FIG. 5 is a flow chart of a method, according to an embodiment of the invention, for initiating use of a system according to the invention.

FIG. 6 is a block diagram of a system, according to an embodiment of the invention, illustrating operation of the system during a method according to the invention as in FIG. 5.

FIG. 7 is a flow chart of a method, according to an embodiment of the invention, for using a peripheral device according to the invention.

FIG. 8 is a block diagram of a peripheral device according to another embodiment of the invention.

FIG. 9A is a block diagram illustrating the flow of data through the interface control device of FIG. 8.

FIG. 9B is a block diagram of a particular embodiment of an interface control device for use in a peripheral device according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 3A is a block diagram of a system 300 according to the invention. The system 300 includes a host computing device 301 and a peripheral device 302 that communicate via a communications interface 303. Herein, "peripheral device" can refer to any device that operates outside of a host ~~computational~~ computing device and that is connected to the host ~~computational~~ computing device. The peripheral device 302 includes a security mechanism 302a that enables security operations (examples of which are described in more detail below) to be performed on data that is stored within the host computing device 301, data that is transmitted from the host computing device 301 to ~~another~~ the peripheral device 302, or data that is transmitted from ~~another~~ the peripheral device to the host computing device 301. As explained in more detail below, the peripheral device 302 also provides additional functionality (referred to herein as "target functionality") to the system 300, such as, for example, the capability to store data in a solid-state disk storage device, the capability to enable communications from the host computing device 301 to another device, the capability to accept biometric input to enable user authentication to the host computing device 301, and the capability to receive and read a smart card inserted into the peripheral device 302.

Generally, the communications interface 303 can be any embodied by any of a variety of communication interfaces, such as a wireless communications interface, a PCMCIA interface, a smart card interface, a serial interface (such as an RS-232 interface), a parallel interface, a SCSI interface or an IDE interface. Each embodiment of the communications interface 303 includes hardware present in each of the host computing device 301 and peripheral device 302 that operates in accordance with a communications protocol (which can be embodied, for example, by software stored in a memory device and/or firmware that is present in the host computing device 301 and/or peripheral device 302) appropriate for that type of communications interface, as known to those skilled in the art. Each embodiment of the communications interface 303 also includes mechanisms to enable physical engagement, if any, between the host computing device 301 and peripheral device 302.

Generally, the security mechanism 302a can be configured to perform any electronic data security operation (herein, referred to simply as "security operation") including, for example, operations that provide one or more of the basic cryptographic functions, such as maintenance of data confidentiality, verification of data integrity, user authentication and user non-repudiation. Particular security operations that can be implemented in a peripheral device according to the invention are described in more detail below.

The security mechanism 302a can be, for example, embodied as a security token. Herein, "security token" refers to a device that performs security operations and that includes one or more mechanisms (such as, for example, use of a hardware random number generator and/or protected memory) to provide security for the content of those operations.

FIG. 3B is a perspective view of a physical implementation of the system 300 of FIG. 3A, according to one embodiment of the invention. In FIG. ~~3A~~ 3B, the peripheral device 302 is embodied as a card 312 that can be inserted into a corresponding slot 313 formed in a portable computer 311 that, in FIG. 3B, embodies the host computing device 301. Often a peripheral device according to the invention is a portable device, such as the card 312 shown in FIG. 3B. Herein, "portable device" can refer generally to any device that is capable of being easily carried by hand.

FIG. 4 is a block diagram of a peripheral device 400 according to an embodiment of the invention. The peripheral device 400 includes security functionality 401, target functionality 402 and a host interface 403 that are formed together as part of a single physical device. For example, the security functionality 401 and target functionality 402 can be enclosed in a single, card-like housing (designated in FIG. 4 by the numeral 404) conforming to a PCMCIA card or smart card standard.

The peripheral device 400 can have a number of advantageous characteristics. The peripheral device 400 can be implemented in a manner that enables the security operations of the security functionality 401 to be performed in a manner that is transparent to a host computing device (and, depending upon the particular implementation of the peripheral device 400, to a user of a system including the peripheral device 400) of a system according to the invention, so that the host computing device (and, perhaps, user) is aware only of the presence of the target functionality 402. Additionally, the peripheral device 400 can be implemented so that security operations are performed "in-line," i.e., the security operations are performed between the communication of data to or from the host computing device and the performance of the target functionality provided by the peripheral device. Further, the peripheral device 400 enables a wide variety of secure target functionality to be easily provided to a host computing device.

FIG. 5 is a flow chart of a method 500, according to an embodiment of the invention, for initiating use of a system according to the invention. The method 500 enables an aspect of the invention in which the presence of security functionality as part of a peripheral device is not detected by a host computing device, thus making the security functionality transparent to the host computing device and, depending upon the particular manner in which the security functionality is implemented, to a user of the system.

FIG. 6 is a block diagram of a system 600, according to an embodiment of the invention, illustrating operation of the system 600 during a method according to the invention such as the method 500 of FIG. 5. The system 600 includes a host computing device 601 and a peripheral device 602. The host computing device 601 includes a display device 603a (e.g., a conventional computer display monitor) and user input device 603b (e.g., a keyboard, mouse, trackball, joystick or other appropriate device), referred to collectively hereinafter as user interface device 603. The host computing device 601 also includes, mounted within a housing 604, a processing device 605, a memory device 606, an input/output (I/O) device 607 for enabling communication with the user interface device 603, and an input/output (I/O) device 608 for enabling communication with peripheral device 602. The devices 605, 606, 607 and 608 can each be implemented by conventional such devices and can communicate with each other via a conventional computer bus 609, as is well known and understood. The peripheral device 602 includes security functionality 611, a memory device 612, an input/output (I/O) device 613 for enabling communication with the host computing device 601 and target functionality 614. The security functionality 611, memory device 612, I/O device 613 and target functionality 614 can each be implemented by conventional devices and can communicate with each other via a conventional computer bus 615, as is well known and understood. The host computing device 601 and the peripheral device 602 are shown in simplified form in FIG. 6 to facilitate clarity in illustration of this aspect of the invention; as described in more detail below and as understood by those skilled in the art, the host computing device 601 and the peripheral device 602 can - and typically will - include other devices not shown in FIG. 6.

Returning to FIG. 5, use of a system according to the invention begins when, as shown by step 501, a user of the system connects a peripheral device according to the invention to a host computing device. Such connection can occur in any manner that enables the peripheral device to communicate with the host computing device. Frequently, this will occur as a result of a physical connection of the peripheral device to the host computing device. (In general, such physical connection can occur either before or after the host computing device begins operating; however, in the former case, subsequent steps of the method 500 - with the exception of, depending upon the implementation of the peripheral device, the step 503 - cannot be performed until the host computing device begins operating.) For example, the peripheral device can be embodied in a card or disk (e.g., a card conforming to a PCMCIA form factor as established by the appropriate standard) that is inserted into a corresponding socket formed in the host computing device. Or, the peripheral device can be embodied in a housing from which a cord extends, a plug of the cord being inserted into a mating receptacle formed in the host computing device. However, such physical connection need not necessarily occur; the peripheral device can also be connected to the host computing device by any type of wireless communication for which the host computing device contains an appropriate interface.

Once connection between the peripheral device and the host computing device is made, the host computing device detects the presence of the peripheral device, as shown by step 502. Such detection of the presence of a peripheral device is typically enabled as a standard aspect of the operating system software of the host computing device.

Typically, once the presence of a new peripheral device is detected by the operating system software of the host computing device, the operating system software (or companion software program) also identifies the type of the peripheral device. This can be accomplished, for example, by a standard software device driver (hereinafter, "host driver") for devices of the type that use the host computing device interface that is being used by the peripheral device 602. In FIG. 6, the host driver is shown stored in the memory section 606a of the memory device 606 of the host computing device 601. (The Card Services or Socket Services programs that often are bundled with the Windows95^{TM} operating system software for use in performing various "housekeeping" functions associated with a PCMCIA interface are ~~an~~ examples of such drivers.) However, in the method 500, before the operating system software can perform such identification, the peripheral device according to the invention suspends operation of this aspect of the operating system software, so that the peripheral device can establish its identity, as shown by step 503, and explained further below. As will be apparent from that explanation, performance of the step 503 advantageously enables the peripheral device to assume the identity of the target functionality that is part of the peripheral device. Since, as described elsewhere herein, a peripheral device according to the invention can include a variety of types of target functionality, the peripheral device can take a variety of identities.

The particular manner in which operation of the operating system software is suspended so that the peripheral device can establish its identity can depend on the characteristics of the operating system software and/or the device interface. However, for many combinations of operating system software and device interface, the operating system software waits for confirmation that the device connected to the device interface is ready for further interaction with the operating system software before the operating system software seeks to identify the type of the device connected to the interface (the standard for PCMCIA interfaces, for example, specifies such operation). In such cases, the peripheral device can be configured to delay informing the operating system software that the peripheral device is ready for further interaction until the peripheral device has established its identity.

The following description of one way in which the step 503 can be implemented can best be understood by reference to the system 600 shown in FIG. 6. One way in which the operating system software of a host computing device can identify the type of a peripheral device is to access a known memory section of a memory device of the peripheral device, as established by an interface standard developed for that type of peripheral device, that stores data representing the type of the peripheral device. This is true for a variety of types of peripheral devices, such as, for example, peripheral devices that conform to the PCMCIA standard. (The PCMCIA standard, for example, includes a specification, called the Card Information Structure, that defines, among other things, a location in a portion of memory of a PCMCIA card, denoted as "attribute memory", that stores data identifying the type of the PCMCIA card.) In the system 600, the peripheral device 602 is such a device. The memory section of the memory device 612 of the peripheral device 602 which the host computing device 601 seeks to access is shown in FIG. 6 as the memory section 612a, and the data stored therein is referred to herein as "peripheral device identification data."

The peripheral device 602 can be implemented so that the peripheral device 602 assumes the identity of the target functionality 614 (whether or not the security functionality of the peripheral device is also being used). This enables the host computing device 601 to interact with the peripheral device 602 as though the peripheral device 602 were a device of the type of the target functionality 614, without recognizing that security functionality 611 is present that may be performing security operations. Thus, the need to modify aspects of the operation of the host computing device (e.g., the host device driver) a2 is reduced or eliminated, making implementation and use of a data security system including the peripheral device 602 simpler and easier. Since use of the data security system is easier (e.g., a user

Ins a1 a2

need not provide input to cause the host driver to be appropriately tailored to enable desired interaction with a security device), the possibility that a user will use the system incorrectly (e.g., fail to apply security operations to an interaction with the host computing device, or apply the security operations incorrectly or incompletely) is reduced.

Though, as shown in FIG. 6, the peripheral device 602 includes security functionality 611 and target functionality 614, the system 600 can be operated so that only the security functionality 611 is used. The peripheral device 602 and peripheral device driver (discussed below) can be implemented so that, when the peripheral device 602 is operated in that way, the peripheral device identification data stored in the memory location 612a identifies the peripheral device 602 as a security device.

Returning to FIG. 5, after the peripheral device has established its identity, the host computing device identifies the peripheral device, as shown by step 504. This can be implemented as part of the host driver, as indicated above.

Once the host computing device has identified the peripheral device (and other host computing device operating system software operations concluded, if applicable), the user can begin using the peripheral device (in particular, the security functionality of the peripheral device), as shown by step 505 of the method 500. Such use can be enabled by one or more software programs (referred to collectively hereinafter as a "peripheral device driver," though such programs can include programs in addition to those conventionally termed "drivers," such as programs conventionally termed "applications") that are executed by the host computing device.

The use of a separate driver to control and interact with the security functionality of a peripheral device according to the invention can be advantageous because it reduces or eliminates the need to modify the host driver. As a practical matter, such modification of the host driver can likely only be accomplished by requiring a user to interact with a standard host driver to appropriately modify the standard host driver. This is undesirable because the user may forget to modify the driver or modify the driver incorrectly or incompletely.

The peripheral device driver can have previously been installed on a data storage device (e.g., hard disk) of the host computing device (in FIG. 6, the peripheral device driver is shown stored in the memory section 606b of the memory device 606 of the host computing device 601), or can be made accessible to the host computing device via an appropriate interface (such as a floppy disk drive, CD-ROM drive or network connection) at a time when the user wishes to initiate interaction between the host computing device and the peripheral device. Additionally, when a peripheral device according to the invention is used with a host computing device which utilizes operating system software that supports the feature informally ~~colloquially~~ referred to as "plug and play", it is also possible to store the peripheral device driver in a memory device of the peripheral device and configure the peripheral device so that, when the peripheral device is connected for the first time to a particular host computing device, the host computing device automatically provides the user with the opportunity to instruct the host computing device to cause the peripheral device driver to be transferred from the peripheral device to the host computing device.

FIG. 7 is a flow chart of a method 700, according to an embodiment of the invention, for using a peripheral device according to the invention. It is to be understood that the method 700 shown in FIG. 7 is not the only way to enable the aspects of use of a peripheral device according to the invention that are illustrated in FIG. 7; as can be readily appreciated by those skilled in the art, such aspects can be implemented using any of a variety of other appropriate methods. Further, the use of a peripheral device according to the invention can include aspects not illustrated in FIG. 7; likewise, such use may not include some of the aspects illustrated in FIG. 7. The method 700 of FIG. 7 is shown merely to aid in the illustration of certain aspects of the invention, and should not be interpreted as restricting the manner in which a peripheral device according to the invention can be used.

To begin using a peripheral device according to the invention, a user instructs the host computing device to begin execution of the peripheral device driver, as shown by step 701 of the method 700, the user having obtained knowledge of the appropriate command to begin execution of the peripheral device driver in any appropriate manner (e.g., from a user manual accompanying the peripheral device driver and/or the peripheral device). In general, the steps of the method 700 occur as a result of operation of a peripheral device driver; however, operation of the host driver may be necessary or desirable to enable some aspects of the method 700 (e.g., execution of a transaction, as in steps 708, 712 and 715).

As indicated above, a peripheral device according to the invention can be implemented so that the host driver cannot detect the presence of the security functionality of the peripheral device. In such case, the peripheral device driver enables the detection of the security functionality, as shown by step 702 of the method 700. This can be accomplished by including instructions as part of the peripheral device driver that, when the peripheral device driver first begins executing, cause the peripheral device driver to access a predefined location of a memory device of the peripheral device (in FIG. 6, the memory section 612b) for data that identifies whether the peripheral device is a device having security functionality that is compatible with the peripheral device driver. If the peripheral device is such a device, then the peripheral device driver can enable the user to make use of the security functionality of the peripheral device. Further, the peripheral device driver can be implemented, as shown in FIG. 7, so that, if the proper security functionality is not detected, execution of the peripheral device driver terminates, preventing use of the peripheral device. Alternatively, the peripheral device driver can be implemented so that, if the proper security functionality is not detected, the target functionality of the peripheral device can be used without the security functionality of the peripheral device.

A peripheral device according to the invention can, in general, be operated in one of three modes: 1) a mode in which only the security functionality is used, 2) a mode in which both the security functionality and the target functionality are used, and 3) a mode in which only the target functionality is used. The user can be enabled to, via the peripheral device driver, select any one of the three modes of operation. However, in some applications, it may be desirable to inhibit operation in one or two of the modes. In particular, it may be desirable to prevent operation of the peripheral device in the last of the above-listed modes, i.e., a mode in which the security functionality is not used, if it is desired to ensure that use of the target functionality can only occur with the application of one or more security operations. This could be accomplished by implementing the peripheral device driver so that the option to operate in that mode is not presented to the user, or the peripheral device could be configured during manufacture to prohibit operation in that mode. For example, if the target functionality is embodied as a communications device or a memory device, it may be desirable to ensure that unencrypted data cannot be transferred via the communications device or stored in the memory device, whether done inadvertently or on purpose.

In the method 700, all three of the above-listed modes are available for use. In the step 703 of the method 700, a determination is made as to whether the security functionality is to be used. (As noted above, such use may be required.) If yes, the peripheral device is operated in one of the first two modes above (security functionality only, or security functionality plus peripheral functionality); if no, the third mode is used (peripheral functionality only).

The peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. In particular, it can be desirable to require an access code before enabling a user to use the security functionality, thus establishing a layer of security that protects the integrity of the security operations themselves. In the method 700, as shown by the step 704, an acceptable access code must be entered by the user before the security functionality of the peripheral device can be used. An access code can be entered, for example, by inputting the access code in a conventional manner using a user interface device (e.g., keyboard) of the host computing device. Or, an access code can be entered using particular embodiments of target functionality (such as a biometric device, discussed in more detail below) that is part of the peripheral device according to the invention.

Advantageously, an access code can be used not only to control access to the security (or other) functionality of the peripheral device, but also to identify a "personality" of the user. Each personality is represented by data that establishes certain characteristics of operation of the peripheral device, such as, for example, restrictions on operation of the peripheral device (e.g., limitations on the types of security operations that can be performed) or specification of operating parameters or characteristics (e.g., cryptographic keys or specification of a particular incarnation of a type of security algorithm, such as a particular encryption algorithm). A single user can have multiple personalities: each personality might, for example, correspond to a different capacity in which a user acts. Data representing personalities and corresponding user access codes can be stored in a memory device of the peripheral device.

Upon receipt of an acceptable access code, the peripheral device driver controls the host computing device to present a user interface that enables the user to effect desired control of the peripheral device, and, in particular, to use the peripheral device to perform security operations, as described below. (If access codes are also used to identify personalities, upon receipt of an acceptable access code, the peripheral device driver can also access and retrieve the data representing the corresponding personality, so that the operation of the peripheral device can be controlled accordingly.) The user interface for enabling a user to operate the peripheral device can be implemented in any of a variety of well known ways (e.g., as a graphical user interface) using methods and apparatus that are well known to those skilled in the art. Generally, the user interface enables the user to perform any functionality that is provided by the peripheral device, as described in more detail elsewhere herein.

As indicated above, a peripheral device according to the invention can be operated ~~implemented~~ in any of three modes. Once an acceptable access code has been entered, the peripheral device driver can enable the user to select one of the three modes, as shown in step 705 of the method 700. (Alternatively, as mentioned above, it may be desirable to present the user only with the option of choosing the security functionality only mode or the security functionality plus peripheral functionality mode, so as to eliminate the possibility that the user will effect an unsecured use of the target functionality.) If the security functionality only mode, or the security functionality plus peripheral functionality mode, is selected, then the user interface (and the underlying peripheral device driver) enables the user to input all desired or required instructions regarding the security operations to be performed for a particular "transaction" (e.g., a storage of data in a memory device, a transmission of data by a communications device, or an exchange of data with a smart card reader device), as shown by steps 706 and 710 of the method 700. For example, the user interface can enable the user to select data to which security operations are to be performed, specify the application of particular security operations to data, or specify parameters or other information required for a particular security operation. If the security functionality plus peripheral functionality mode, or the peripheral functionality only mode, is selected, then the user interface and peripheral device driver enable the user to input all desired or required instructions regarding use of the target functionality for the transaction, as shown by steps 707 and 711 of the method 700. For example, if the target functionality is embodied as a memory device, the user interface can enable the user to specify a name for the stored data. Or, for example, if the target functionality is embodied as a communications device, the user interface can enable the user to specify a destination (e.g., an electronic mail address) for the data.

Once the user has provided instructions in steps 706 and 707, in step 710, or in step 711, the transaction is executed, as shown by step 708 or step 712 of the method 700. After execution of the transaction, the user can be allowed to execute further transactions, as shown by step 709 of the method 700. It is also possible for the user to begin using another personality (by entering an appropriate access code), as shown by step 709 of the method 700. Eventually, use of the peripheral device ends, as shown by step 718 of the method 700.

a

The peripheral device and associated peripheral device driver can be implemented so that it is possible to use only the security functionality of the peripheral device. ~~This~~ the peripheral device can be used in this manner to, for example, encrypt or decrypt data stored on the host computing device by receiving the data from the host computing device, encrypting or decrypting the data as appropriate, then returning the encrypted or decrypted data to the host computing device.

a

As indicated above, the peripheral device and associated peripheral device driver can be implemented so that it is possible to use only the ~~peripheral~~ target functionality of the peripheral device, even without entering an appropriate access code. In the method 700, such operation is shown by the steps 714, 715 and 716, which function in the same manner as steps 711, 712 and 709, described above. Using the peripheral device in this way can be useful, for example, when the target functionality is embodied as a biometric device, as described further below, that is used to perform user authentication. In particular, if the biometric device is to be used as the mechanism to enter the access code in step 704, operation in this mode may be necessary (depending on the capabilities of the biometric device) to enable such use of the biometric device. a³ The step 717 can also enable use of the security functionality to begin by causing a prompt for an appropriate access code to appear (step 704). Again, eventually, use of the peripheral device ends (step 718).

Ins a³

As described above, a peripheral device according to the invention that includes security functionality and target functionality can be implemented so that the host computing device is not aware of the presence of the security functionality. It may also be desirable to shield the user from knowledge of the presence of the security functionality and cause predetermined security operations to be performed automatically. This may be desirable so that, for example, it is not necessary for the user to provide input regarding the performance of security operations, thus eliminating the possibility that the user will neglect to provide such input, or will provide the input incorrectly or incompletely. Or, it may be desirable to make security operations transparent to users to enhance the security of those operations, since, if the performance of such operations is unknown, there will be no attempt to defeat the security provided by those operations. If such is the case, the peripheral device driver can be implemented so that the peripheral device can operate only in the security functionality plus peripheral functionality mode (steps 710, 711, 712, 714, 715, 716 and 717 of the method 700 cannot be performed) and so that no indication (e.g., presentation of a user interface display that allows input of instructions regarding the performance of security operations, as in step 706 of the method 700) is given of the presence of the security functionality of the peripheral device. Rather, the user would simply be presented with options regarding operation of the target functionality (step 707 of the method 700). In such an implementation, the peripheral device driver can be implemented to automatically cause one or more predetermined security operations to be performed based upon a user-specified interaction with the target functionality, or the peripheral device can be configured to cause such security operations to be performed any time a specified interaction with the target functionality occurs.

A significant advantage of a peripheral device according to the invention is that the peripheral device can be implemented so that any of a variety of types of target functionality can be included as part of the peripheral device. In particular, as described in more detail below, the peripheral device includes an interface control device which enables and manages communications between and among the host computing device, a cryptographic processing device that is part of the peripheral device, and target functionality that is also part of the peripheral device. The interface control device can be adapted to provide an appropriate interface for each type of target functionality. Thus, in general, any desired target functionality can be used with a peripheral device according to the invention, so long as the target functionality is implemented so as to enable communication with an interface of the type presented. Those skilled in the art of data communications can readily understand how to implement such communication with target functionality in view of the detailed description below (see FIGS. 8, 9A and 9B) of an embodiment of a peripheral device according to the invention, and, in particular, an interface control device of such a peripheral device.

For example, target functionality of a peripheral device according to the invention can be embodied as a memory device adapted to enable non-volatile storage of data. In general, any such memory device can be used to embody such target functionality. More particularly, a solid-state disk storage device (e.g., NAN flash memory device) can advantageously be used. Illustratively, a memory device that can be used to embody target functionality in a peripheral device according to the invention can be a compact flash memory device, such as an ATA format flash disk drive. Other solid-state disk storage devices, such as SCSI disks and IDE disks can be used. The construction and operation of memory devices in general, as well as those identified particularly above, is well understood by those skilled in that art, so that, together with an understanding of the required communication capability between the target functionality and the interface control device, a memory device for use with the invention can be easily constructed and operated. A peripheral device according to the invention that includes a memory device that embodies the target functionality can be used, for example, to securely store data in a manner that enables a user of the data to easily carry the data with them wherever they go.

Target functionality of a peripheral device according to the invention can also be embodied as a communications device adapted to enable communication between the host computing device and a remote device. In general, any such communications device can be used to embody target functionality. A communications device that can be used to embody target functionality in a peripheral device according to the invention can include, for example, a data communications modem (such as, for example, a conventional telephone line modem, an ISDN modem, a cable modem, or a wireless modem) or a LAN transceiver (either wired or wireless and, in the latter case, operating in, for example, the infrared or radiofrequency spectrum). The construction and operation of communication devices in general, as well as those identified particularly above, is well understood by those skilled in that art, so that, together with an understanding of the required communication capability between the target functionality and the interface control device, a communication device for use with the invention can be easily constructed and operated. A peripheral device according to the invention that includes a communications device that embodies target functionality can be used, for example, to encrypt electronic mail before transmission to an addressee. Or, such a peripheral device can be used, for example, to encrypt data files that a person wishes to securely transfer between a computing device at the person's place of work and a computing device at the person's home.

Target functionality of a peripheral device according to the invention can also be embodied as a biometric device, which is defined herein as any device that is adapted to receive input data regarding a physical characteristic of a person based upon a physical interaction of the person with the device. In general, any such biometric device can be used to embody target functionality. Biometric devices that can be used in a peripheral device according to the invention can include, for example, a fingerprint scanning device, a retinal scanning device or a faceprint scanning device.

In addition to conventional computational devices for storing and/or manipulating digital data, a biometric device includes a sensor for sensing the physical characteristic, and an analog-to-digital converter to transform the analog data representing the sensed characteristic into digital data. For example, a fingerprint scanning device includes a sensor upon which a person can place a finger, the sensor sensing the fingerprint of the finger, the content of the sensed fingerprint being converted into digital data by the device. Similarly, a retinal scanning device includes a sensor which can be placed proximate to a person's eye, the sensor sensing characteristics of the eye such as blood vessel pattern or iris pattern, the device translating the content of the sensed characteristics into digital data. The construction and operation of biometric devices in general, as well as those identified particularly above, is well understood by those skilled in that art, so that, together with an understanding of the required communication capability between the target functionality and the interface control device, a biometric device for use with the invention can be easily constructed and operated. Fingerprint scanning devices and retinal scanning devices that can readily be modified for use with the invention, i.e. to communicate with an interface control device according to the invention, are known to those skilled in that art. For example, fingerprint scanning devices such as those available from Identix Incorporated of Sunnyvale, California can be used in a fingerprint scanning device for use with the invention.

A peripheral device according to the invention that includes a biometric device that embodies the target functionality can be used, for example, to enable user authentication to a host computing device before allowing access to particular data stored on the host computing device. Such user authentication can be accomplished by using a biometric device to obtain biometric data from a user and comparing the biometric data to an appropriate library of biometric data representing a predetermined group of people (e.g., authorized users). The library of data can be stored in a memory device of the peripheral device.

When a peripheral device including a fingerprint scanning device is embodied as a card adapted to be inserted into a slot of a host computing device (e.g., a slot conforming to a PCMCIA standard), it may be useful to make the peripheral device relatively long, so that a portion of the card on which the sensor is positioned can extend from the slot of the host computing device, thereby enabling fingerprints to be scanned while the peripheral device is inserted in the host computing device. Similarly, for a fingerprint scanning device, retinal scanning device or faceprint scanning device, it may be desirable to form the device so that the sensor is connected to the remainder of the device via an appropriate communication line, thus providing some range of movement of the sensor while the peripheral device is inserted in the host computing device, thereby facilitating use of the device.

A biometric device can be used in different ways with a system according to the invention, depending upon the capabilities of the biometric device. Using known apparatus and methods, a "smart" biometric device can be implemented with the capability to detect the presence of an input to the sensor, and, upon such detection, initiate acquisition of the biometric data and performance by the peripheral device of the appropriate data comparison. Such a biometric device can be used to perform user authentication as in step 704 of the method 700 above. Alternatively, the biometric device may be "stupid" and require that a user initiate the data acquisition and authentication process. Such a biometric device can be used to perform user authentication in a peripheral device that allows operation without entry of a proper access code, as in steps 714 and 715 of the method 700.

Target functionality of a peripheral device according to the invention can ~~be~~ also be embodied as a smart card reader device adapted to communicate with a smart card, such as, for example, a smart card compliant with the ISO 7816 standard. Such a device can be implemented by adapting a conventional smart card reader, the construction and operation of which is well known to those skilled in that art, ~~with~~ to provide a communications interface that enables the smart card reader to communicate with the interface control device. A peripheral device according to the invention that includes a smart card reader device can be used to provide security features to a smart card reader, or add to existing security features of a smart card reader.

It is to be understood that the examples given above are merely illustrative, not exhaustive, of the ways in which a peripheral device according to the invention can be used. Many more possibilities exist.

FIG. 8 is a block diagram of a peripheral device 800 according to another embodiment of the invention. The peripheral device 800 includes a cryptographic processing device 801, an interface control device 802, a first memory device 803, a second memory device 804, a real-time clock 805, a host computing device input/output (I/O) interface 806 and target functionality 807.

The host computing device I/O interface 806 enables communications between the peripheral device 800 and a host computing device. The electrical and mechanical characteristics of the I/O interface 806, as well as the protocol used to enable communication via the interface 806, are established in any manner that conforms to the industry standard specifications for an interface of that type. For example, a peripheral device according to the invention can be adapted for insertion into a PCMCIA slot of a host computing device. In such a peripheral device, the electrical and mechanical characteristics and communications protocol for the host computing device I/O interface 806 are established in conformance with the appropriate PCMCIA standards.

The cryptographic processing device 801 can be adapted to perform security operations. Generally, the cryptographic processing device 801 can be embodied by any processor capable of performing the cryptographic operations desired to be provided by the peripheral device 800. In one embodiment of the peripheral device 800, the cryptographic processing device 801 is a special purpose embedded processor, embodied on a single integrated chip and designated as MYK-82 (and also referred to by the name Capstone), which includes an ARM6^{TM} processor core and several special purpose cryptographic processing elements that have been developed by the Department of Defense. The construction and operation of the Capstone chip is known by those skilled in the art of cryptographic processing.

The first memory device 803 can be a non-volatile data storage device which can be used to store computer programs and persistent data. The first memory device 803 can be implemented by any appropriate such device (of which there are many conventional, readily available incarnations), such as, for example, a conventional flash memory device.

The second memory device 804 can be a volatile data storage device that can also be a rapidly accessible data storage device in which frequently used data and program instructions can be stored during operation of the peripheral device 800. The second memory device 804 can also be implemented by any appropriate such device (of which there are many conventional, readily available embodiments), such as, for example, a conventional random access memory (RAM) device.

The real-time clock 805 enables the creation of time stamps, which can be used in a number of security operations. Advantageously, the time stamps created by the real-time clock 805 are more secure than those that could otherwise be produced by the relatively insecure clock of a host computing device. The real-time clock 805 includes a conventional battery backup device that maintains power to the real-time clock 805 when the peripheral device 800 is not in use (i.e., when power is not supplied to the peripheral device 800), so that the correct time is continuously preserved within the peripheral device 800. The real-time clock 805 (including battery backup) can be embodied by any conventional such device, such as the DS1302 clock available from Dallas Semiconductor of Dallas, Texas.

In the peripheral device 800, the interface control device 802 mediates the interaction between the host computing device, the target functionality 807 and the cryptographic processing device 801. In one embodiment of the peripheral device 800, the interface control device 802 is a conventional field-programmable gate array (FPGA) that is programmed to perform the functions that it is desired to implement with the interface control device 802, as described in more detail below. The interface control device 802, under control of the cryptographic processing device 801, can be adapted to enable the peripheral device 800 to assume the identity of the target functionality 807, as discussed above. The interface control device 802 also enables the in-line cryptography aspect of the invention, since the interface control device 802 controls the flow of data between the host computing device and the target functionality 807.

FIG. 9A is a block diagram illustrating the flow of data through the interface control device 802 of FIG. 8. Data transferred from a host computing device enters the peripheral device 800 (not demarcated in FIG. 9A) through the host computing device I/O interface 806. The interface control device 802 presents the data to a cryptographic processing device interface 808 (not shown in FIG. 8). Depending on the configuration of the interface control device 802, as determined by operation of the peripheral device driver and/or by settings established during the manufacture of the peripheral device 800, the data may or may not be processed by the cryptographic processing device 801 (FIG. 8). Typically (or, in some cases, necessarily), as discussed in more detail above, cryptographic processing will occur. The interface control device 802 then causes the data to be transferred to the target functionality 807. Data being transferred from the target functionality 807 to the host computing device follows a similar path in the reverse direction. When the target functionality 807 is not present or is not being used, data transferred from the host computing device, after being presented to the cryptographic processing device interface 808 and being processed by the cryptographic processing device 801, is caused to be transferred back to the host computing device I/O interface 806 (and, from there, to the host computing device) by the interface control device 802.

FIG. 9B is a block diagram of a particular embodiment of an interface control device 910 for use in a peripheral device according to the invention. As shown in FIG. 9B, the host computing device communicates via a PCMCIA interface and the target functionality is embodied by a compact flash memory device. Those skilled in the art will readily appreciate how the interface control device 910 can be modified for use with other host computing device interfaces and/or target functionalities.

The interface control device 910 includes sets of configuration registers 911. The data stored in the configuration registers 911 establish operating characteristics of the interface control device: in particular, the content of the configuration registers enables the interface control device to present to the host computing device a desired identification of the peripheral device, and determines whether data passing through the peripheral device must be subjected to security operations.

A set of configuration registers is maintained for the host computing device I/O interface, the cryptographic processing device interface, and the target functionality interface. In particular, the content of the host computing device I/O interface configuration registers is such that the interaction of the host computing device with the peripheral device is the same as if the security functionality were not present (unless the data security system is operating in security functionality only mode). The content of the target functionality interface registers reflects the presence of the security functionality. The cryptographic processing device interface registers bridge the gap between the other two sets of registers.

The remainder of the functional blocks of the interface control device 910 shown in FIG. 9B perform functions and operate in a manner that can readily be understood by those skilled in the art from the designation and interconnection of those blocks in FIG. 9B.

In general, the security functionality of a peripheral device according to the invention can be configured to perform any cryptographic operation, as well as other, related mathematical operations. A configuration of the security functionality that enables a particular cryptographic or mathematical operation can be produced, for example, by using appropriate existing cryptographic software, application-specific hardware, or combination of the two, as known by those skilled in the art of producing cryptographic devices. Following is a description of exemplary cryptographic and mathematical operations that can be implemented as part of ~~a~~ the security functionality of a peripheral device according to the invention. These cryptographic and mathematical operations are well-known and can readily be implemented in a peripheral device according to the invention by a person of skill in the art of cryptography.

For example, a peripheral device according to the invention can implement one or more cryptographic key exchange operations. Any key exchange operation can be implemented, such as, for example, the Department of Defense Standard, the RSA, the Diffie-Hellman, and the X9.42 (ANSI Banking Standard) key exchange algorithms.

A peripheral device according to the invention can also implement one or more hash operations. Any hash operation can be implemented, such as, for example, the FIPS 180-1 (SHA-1), the Message Digest 2 (RSA), and the Message Digest 5 (RSA) algorithms.

A peripheral device according to the invention can also implement one or more digital signature operations. Any digital signature operation can be implemented, such as, for example, the FIPS 186 (DSA - 512, 1024) and the RSA Signature (512, 768, 1024, 2048) algorithms.

A peripheral device according to the invention can also implement one or more key wrapping operations for both symmetric and asymmetric keys. A key wrapping operation can ensure that plaintext keys are not accessible external to the peripheral device. Any key wrapping operation can be implemented.

A peripheral device according to the invention can also implement one or more symmetric encryption operations. Any symmetric encryption operation can be implemented, such as, for example, the FIPS 185 (implemented completely in hardware), the DES (including 3DES, EDE3, CBC and ECB), the RC-2 and the RC-4 algorithms.

A peripheral device according to the invention can also implement one or more asymmetric (public key) encryption operations. While asymmetric encryption operations underlie the key exchange operations described above, asymmetric key operations can also be used independently in a peripheral device according to the invention for bulk encryption. Any asymmetric encryption operation can be implemented, such as, for example, the RSA and Diffie-Hellman algorithms.

A peripheral device according to the invention can also implement one or more exponentiation operations, which are required in many cryptographic operations. Any exponentiation operation can be implemented. Since a ~~peripheral~~ exponentiation requires a significant amount of processing time relative to other mathematical operations, it can be desirable to implement an exponentiation operation in dedicated hardware. In one embodiment of a peripheral device according to the invention, the security functionality of the peripheral device includes a full 1024 bit exponentiator implemented in hardware.

Various embodiments of the invention have been described. The descriptions are intended to be illustrative, not limitative. Thus, it will be apparent to one skilled in the art that certain modifications may be made to the invention as described above without departing from the scope of the claims set out below.

We claim:

~~1. A peripheral device, comprising:~~

~~security means for enabling one or more security operations to be performed on data;~~

~~target means for enabling a defined interaction with a host computing device;~~

~~means for enabling communication between the security means and the target means;~~

~~means for enabling communication with a host computing device; and~~

~~means for operably connecting the security means and/or the target means to the host computing device in response to an instruction from the host computing device.~~

Sub a4

~~2. A peripheral device as in Claim 1, wherein the target means comprises means for non-volatilely storing data.~~

~~3. A peripheral device as in Claim 1, wherein the target means comprises means for enabling communication between the host computing device and a remote device.~~

~~4. A peripheral device as in Claim 1, wherein the target means comprises a biometric device.~~

~~5. A peripheral device as in Claim 1, wherein the target means comprises means for communicating with a smart card.~~

~~6. A peripheral device as in Claim 1, further comprising means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means.~~

~~7. A peripheral device as in Claim 1, further~~

comprising means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the means for enabling ~~a defined interaction with a host computing device.~~

11 ~~8~~. A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device; and

means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means.

12 ~~9~~. A peripheral device as in Claim 11 ~~8~~, wherein the target means comprises means for non-volatilely storing data.

15 ~~10~~. A peripheral device as in Claim 11 ~~8~~, wherein the target means comprises means for enabling communication between the host computing device and a remote device.

19 ~~11~~. A peripheral device as in Claim 11 ~~8~~, wherein the target means comprises a biometric device.

22 ~~12~~. A peripheral device as in Claim 11 ~~8~~, wherein the target means comprises means for communicating with a smart card.

Sub A5 13. A peripheral device as in Claim 8, further

~~comprising means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the means for enabling a defined interaction with a host computing device.~~

~~14. A peripheral device, comprising:~~

~~security means for enabling one or more security operations to be performed on data;~~

~~target means for enabling a defined interaction with a host computing device;~~

~~means for enabling communication between the security means and the target means;~~

~~means for enabling communication with a host computing device; and~~

~~means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the means for enabling a defined interaction with a host computing device.~~

25 ~~15~~. A peripheral device as in Claim 24 ~~14~~, wherein the target means comprises means for non-volatilely storing data.

28 ~~16~~. A peripheral device as in Claim 24 ~~14~~, wherein the target means comprises means for enabling communication between the host computing device and a remote device.

32 ~~17~~. A peripheral device as in Claim 24 ~~14~~, wherein the target means comprises a biometric device.

35 ~~18~~. A peripheral device as in Claim 24 ~~14~~, wherein the target means comprises means for communicating with a smart card.

19. A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

a solid-state disk storage device for storing data;

means for enabling communication between the security means and the solid-state disk storage device; and

means for enabling communication with a host ~~computing device.~~

Sub a6

20. A peripheral device ~~as in~~ Claim 1, wherein the solid-state disk storage device comprises an ATA format flash disk drive.

21. A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

means for wirelessly communicating with a remote device;

means for enabling communication between the security means and the wireless communication means; and

means for enabling communication with a host ~~computing device.~~

Sub a7

22. A peripheral device as in Claim 21, wherein the wireless communication means comprises a wireless modem.

23. A peripheral device as in Claim 21, wherein the wireless communication means comprises a wireless LAN t~~ransceiver~~.

24. A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

a biometric device for receiving input data regarding a physical characteristic of a person based upon a physical interaction of the person with the peripheral device;

means for enabling communication between the security means and the biometric device; and

means for enabling communication with a host ~~computing device.~~

Sub A8

25. A peripheral device as in Claim 24, wherein the biometric device comprises a fingerprint scanning device.

26. A peripheral device as in Claim 24, wherein the biometric device comprises a retinal scanning device.

27. A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

means for communicating with a smart card;

means for enabling communication between the security means and the smart card communication means; and

means for enabling communication with a host computing device.

28. A data security system, comprising:

a host computing device including one or more device interfaces adapted to enable communication with another device;

a peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device; and

means for operably connecting the security means and/or the target means to the host computing device in response to an instruction from the host ~~computing device.~~

36

~~29~~. A data security system, comprising:

a host computing device including one or more device interfaces adapted to enable communication with another device;

a peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device; and

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device; and

means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means.

Sub A9

30. A data security system, comprising:

a host computing device including one or more device interfaces adapted to enable communication with another device;

a peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device; and

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device; and

means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the means for enabling a defined ~~interaction with a host computing device.~~

~~31~~ 38. For use in a peripheral device adapted for communication with a host computing device, performance of one or more security operations on data, and interaction with a host computing device in a defined way, a method comprising the steps of:

receiving a request from a host computing device for information regarding the type of the peripheral device; and

providing to the host computing device, in response to the request, information regarding the type of the defined interaction.

Sub a 10

32. For use in a peripheral device adapted for communication with a host computing device, performance of one or more security operations on data, and interaction with a host computing device in a defined way, a method comprising the steps of:

receiving an instruction from a host computing device regarding operation of the peripheral device; and

performmg security operations and/or the defined interaction in response to the instruction from the host computing device.

Add A11

PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY

William P. Bialick
Mark J. Sutherland
Janet L. Dolphin-Peterson
Thomas K. Rowland
Kirk W. Skeba
Russell D. Housley

ABSTRACT

The invention enables a peripheral device to communicate with a host computing device to enable one or more security operations to be performed by the peripheral device on data stored within the host computing device, data provided from the host computing device to the peripheral device (which can then be, for example, stored in the peripheral device or transmitted to yet another device), or data retrieved by the host computing device from the peripheral device (e.g., data that has been stored in the peripheral device, ~~or~~ and/or transmitted to the peripheral device from another device). In particular, the peripheral device can be adapted to enable, in a single integral peripheral device, performance of one or more security operations on data, and a defined interaction with a host computing device that has not previously been integrated with security operations in a single integral device. The defined interactions can provide a variety of types of functionality (e.g., data storage, data communication, data input and output, user identification)~~, as described further below~~. The peripheral device can also be implemented so that the security operations are performed in-line, i.e., the security operations are performed between the communication of data to or from the host computing device and the performance of the defined interaction. Moreover, the peripheral device can be implemented so that the security functionality of the peripheral device is transparent to the host computing device.

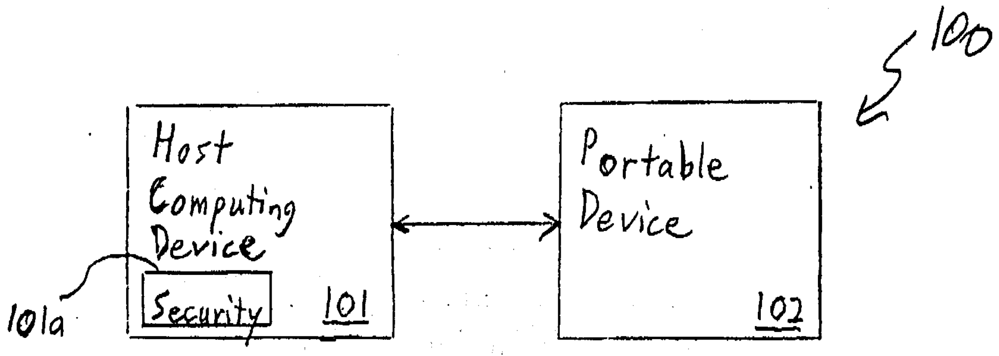


FIG. 1
(Prior Art)

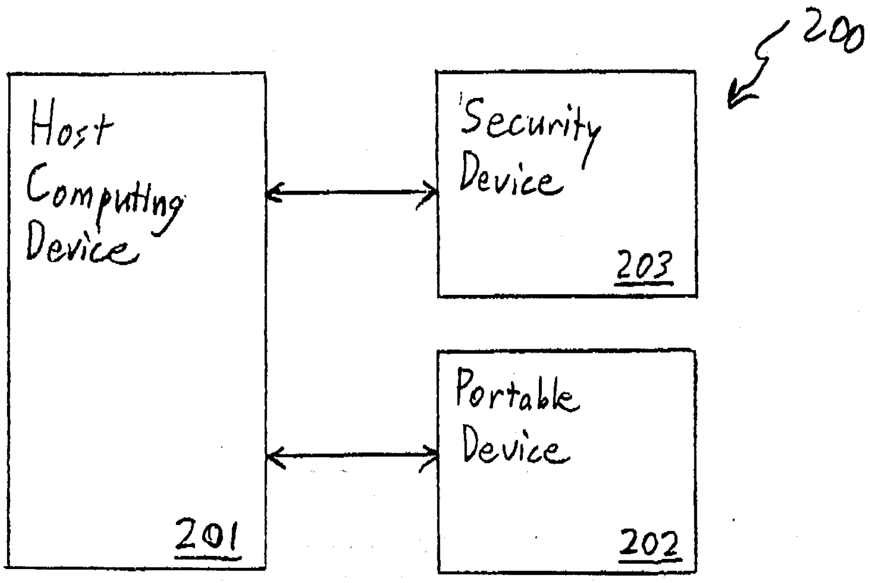


FIG. 2
(Prior Art)

11

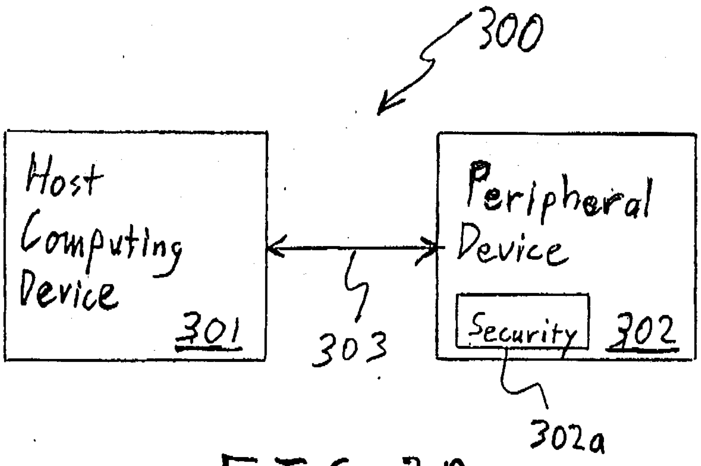

300
Host Computing Device 301
303
Peripheral Device
Security
302
302a

FIG. 3A

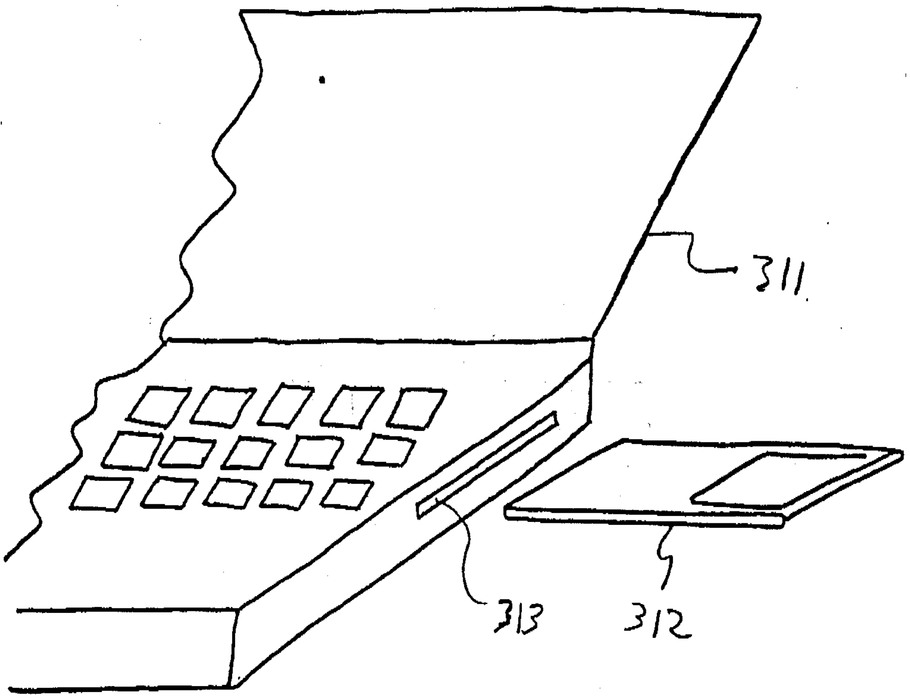

311
313
312

FIG. 3B

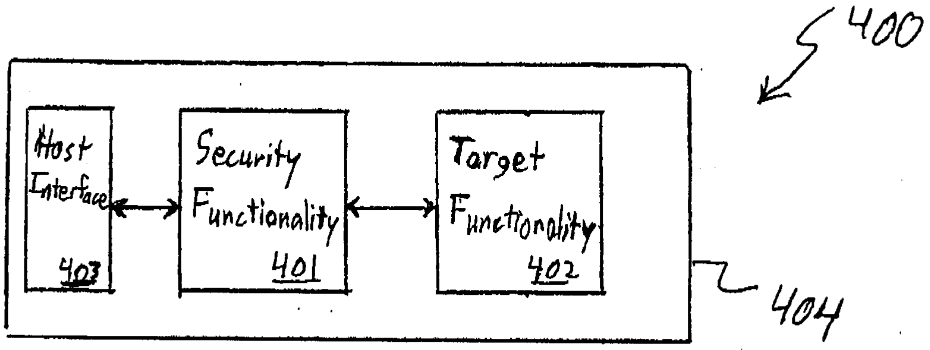

400
Host Interface
403
Security Functionality
401
Target Functionality
402
404

FIG. 4

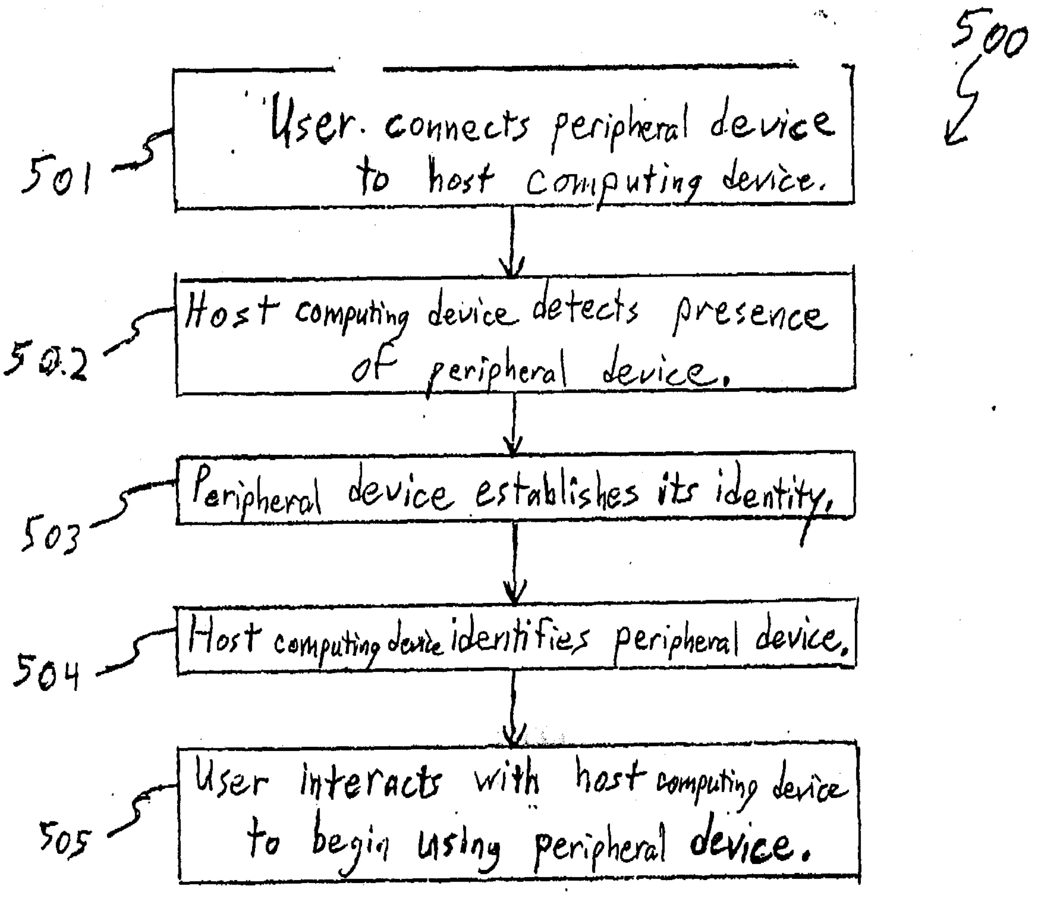

500
501
User connects peripheral device to host computing device.
502
Host computing device detects presence of peripheral device.
503
Peripheral device establishes its identity.
504
Host computing device identifies peripheral device.
505
User interacts with host computing device to begin using peripheral device.

FIG. 5

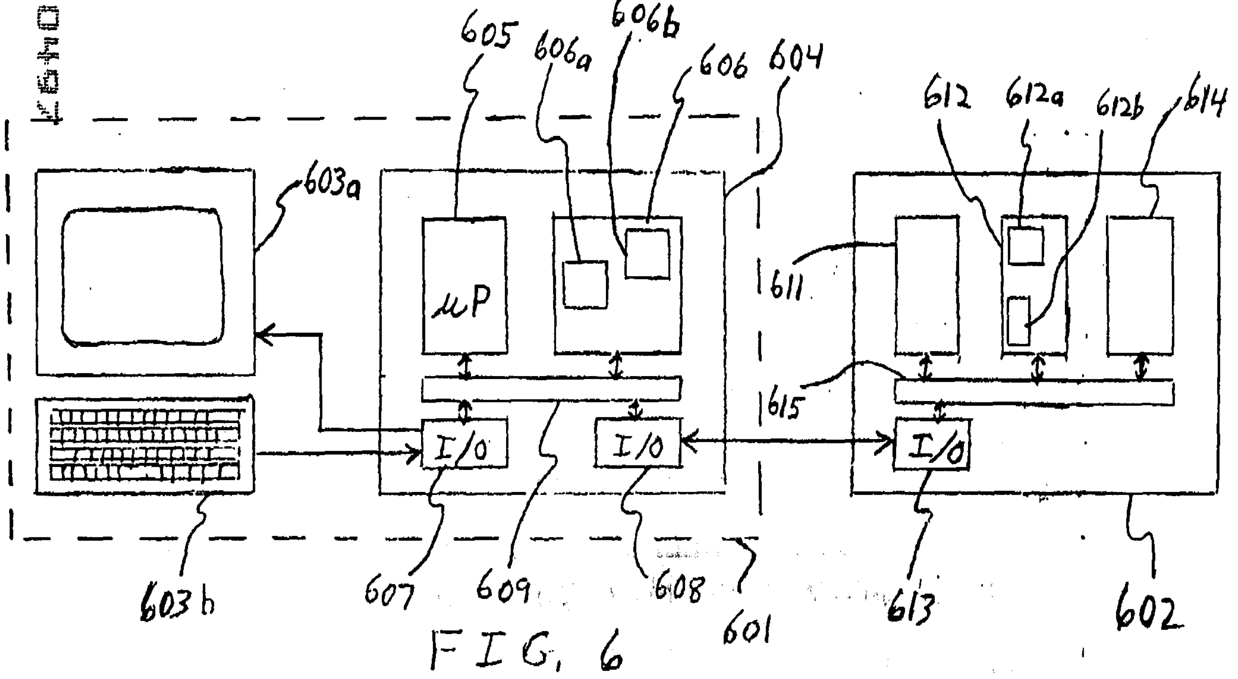

605
606a
606b
606
604
612
612a
612b
614
603a
μP
611
615
I/O
I/O
I/O
603b
607
609
608
601
613
602

FIG. 6

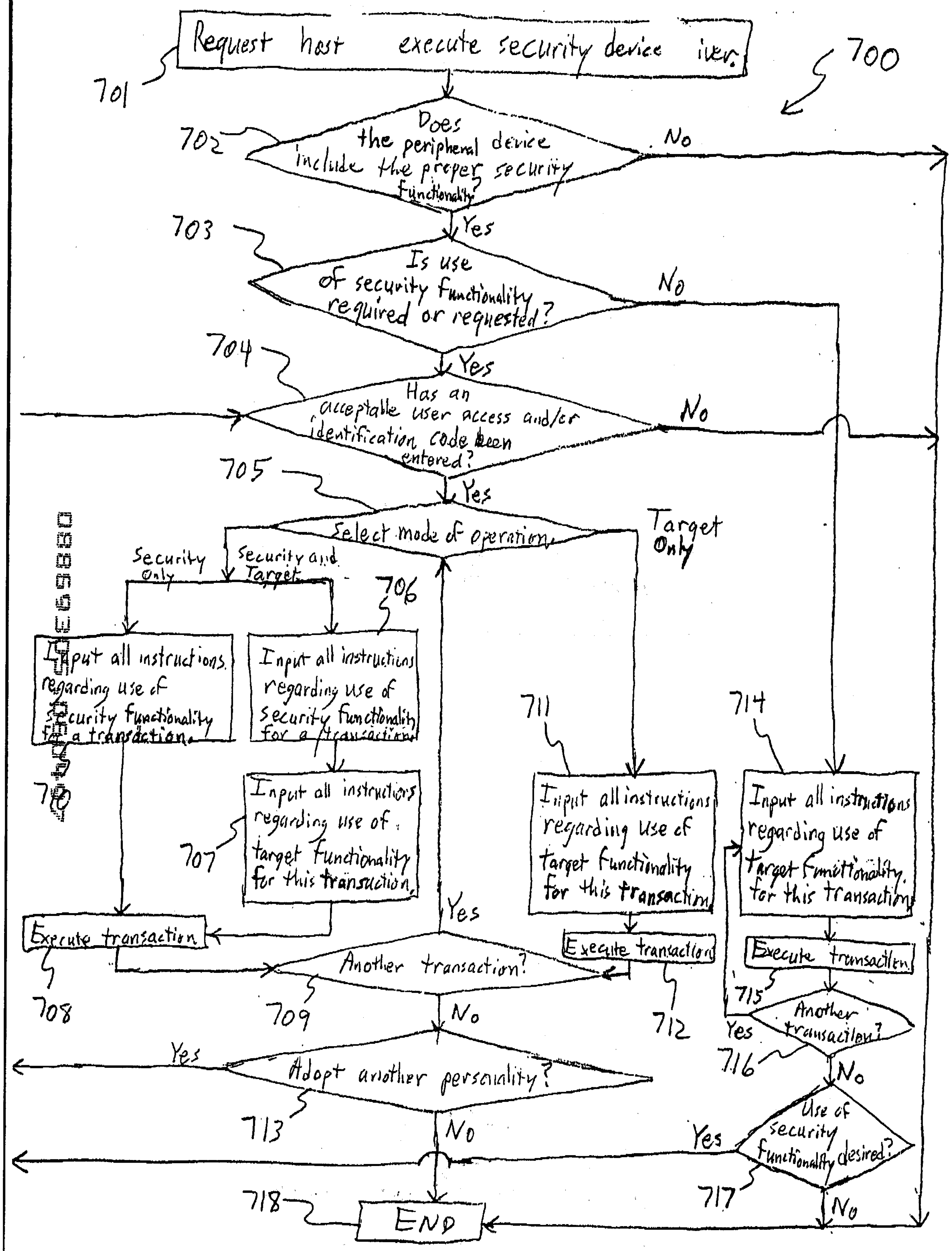

700
701
Request host execute security device iter.
702
Does the peripheral device include the proper security functionality?
No
Yes
703
Is use of security functionality required or requested?
No
Yes
704
Has an acceptable user access and/or identification code been entered?
No
Yes
705
Select mode of operation
Security Only
Security and Target
Target Only
706
Input all instructions regarding use of security functionality for a transaction.
Input all instructions regarding use of security functionality for a transaction
710
707
Input all instructions regarding use of target functionality for this transaction.
711
Input all instructions regarding use of target functionality for this transaction
714
Input all instructions regarding use of target functionality, for this transaction
Execute transaction
708
Yes
Another transaction?
709
Execute transaction
712
Execute transaction
715
Another transaction?
Yes
716
No
No
Yes
Adopt another personality?
713
No
Use of security functionality desired?
Yes
717
No
718
END

FIG. 7

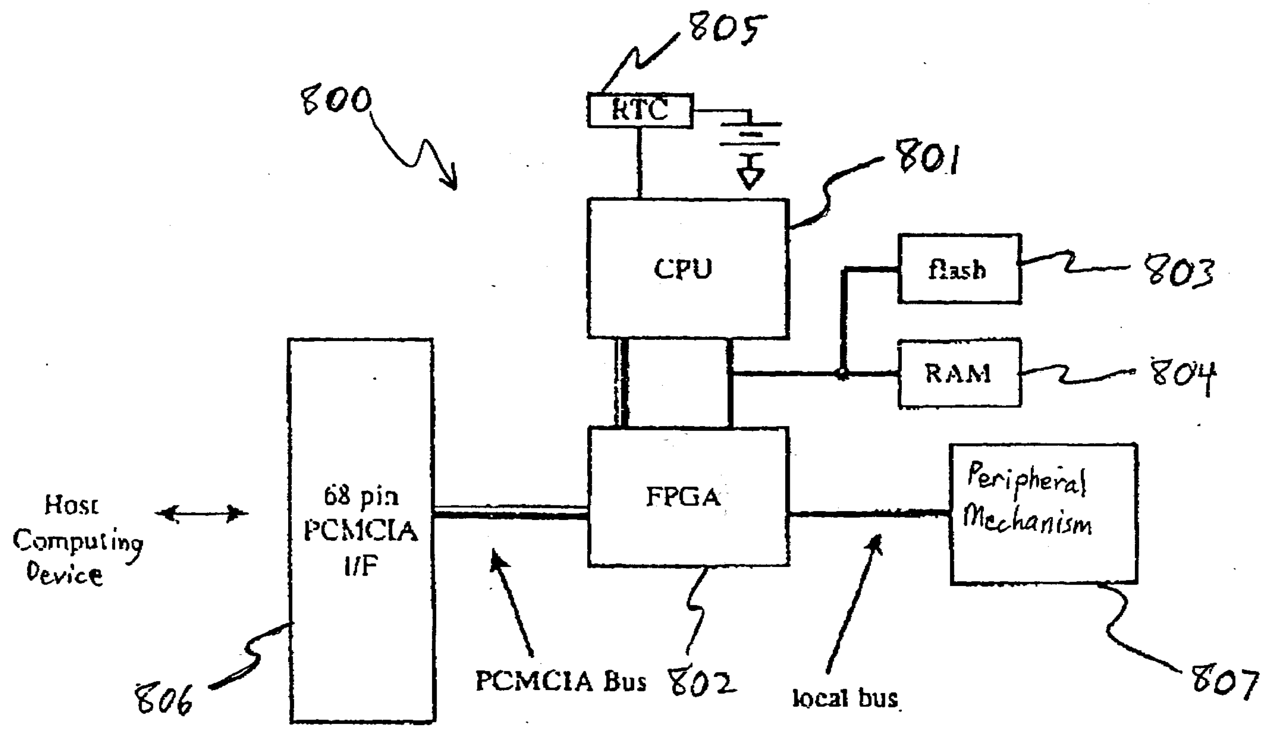

800
805
RTC
801
CPU
flash
803
RAM
804
FPGA
Peripheral Mechanism
807
Host Computing Device
68 pin PCMCIA I/F
806
PCMCIA Bus
802
local bus

FIG. 8

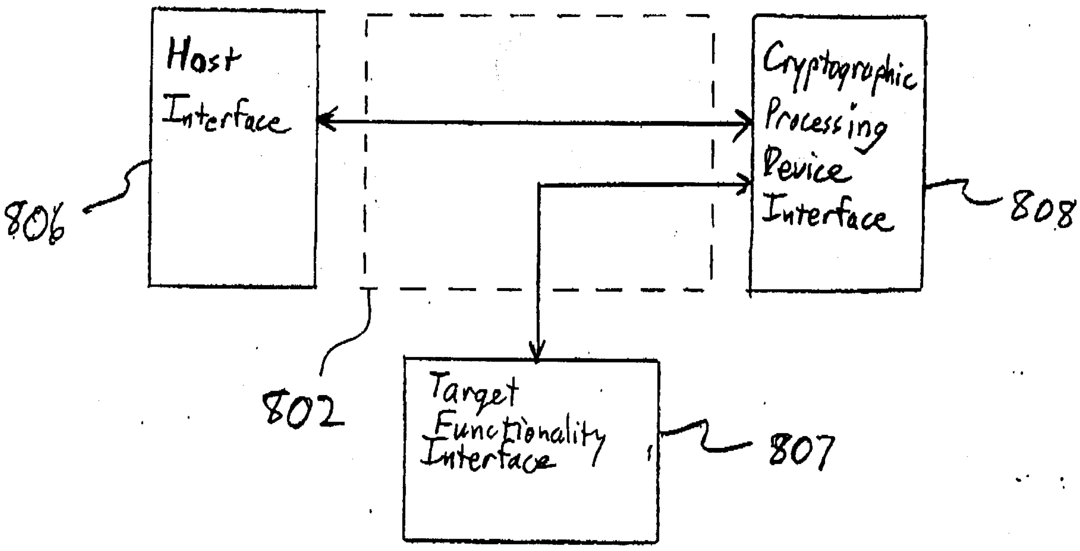

Host Interface
806
Cryptographic Processing Device Interface
808
802
Target Functionality Interface
807

FIG. 9A

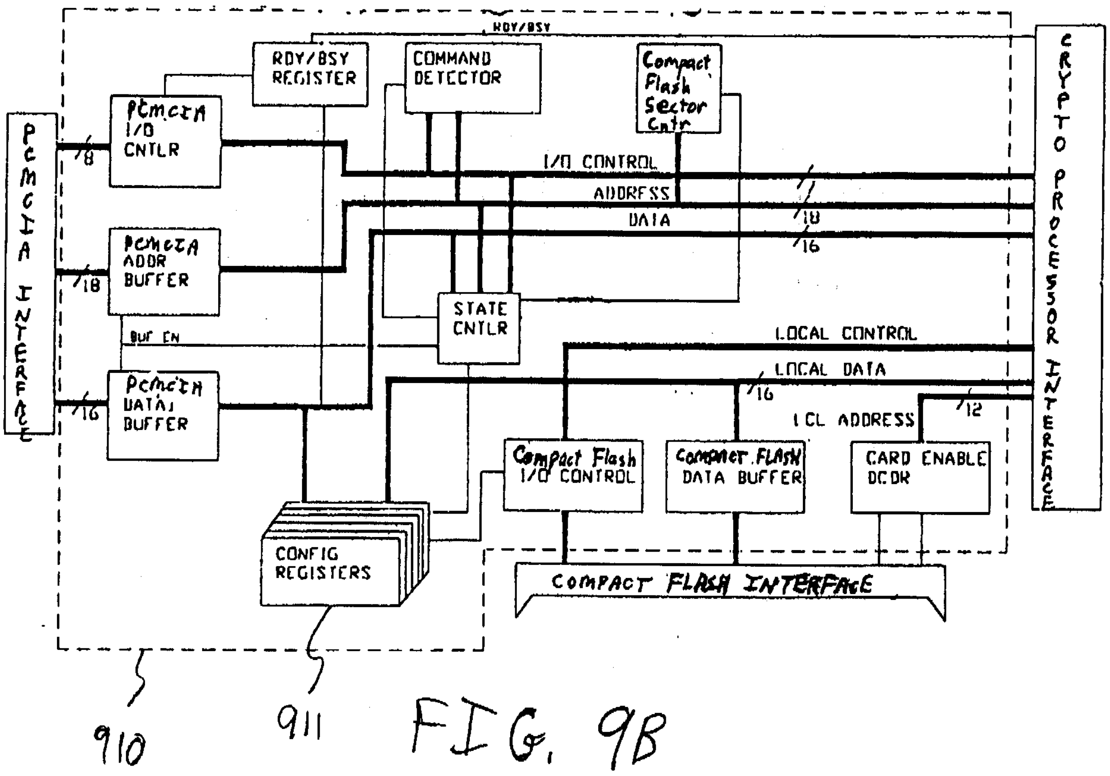

RDY/BSY
RDY/BSY REGISTER
COMMAND DETECTOR
Compact Flash Sector Cntr
PCMCIA INTERFACE
PCMCIA I/O CNTLR
8
I/O CONTROL
ADDRESS
DATA
18
16
PCMCIA ADDR BUFFER
18
BUF EN
STATE CNTLR
PCMCIA DATA BUFFER
16
LOCAL CONTROL
LOCAL DATA
16
LCL ADDRESS
12
Compact Flash I/O CONTROL
Compact FLASH DATA BUFFER
CARD ENABLE DCDR
CRYPTO PROCESSOR INTERFACE
CONFIG REGISTERS
COMPACT FLASH INTERFACE
910
911

FIG. 9B

DECLARATION AN' OWER OF ATTORNEY FOR PATT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below adjacent to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of subject matter (process, machine, manufacture, or composition of matter, or an improvement thereof) which is claimed and for which a patent is sought by way of the application entitled: <u>Peripheral Device With Integrated Security Functionality</u>

which (check) [X] is attached hereto.
[ ] and is amended by the Preliminary Amendment attached hereto.
[ ] was filed on ____________ as Application Serial No. ______________.
[ ] and was amended on ___________ (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified application, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office information known to me to be material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim the priority benefit under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate for the same invention having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s) Priority Claimed

N/A__________ ______________ ____________________ Yes No
(Number) (Country) (Date Filed)

______________ ______________ ____________________ Yes No
(Number) (Country) (Date Filed)

I hereby claim the priority benefit under Title 35, United States Code, §§ 119 and 365(a) of any international patent application(s), listed below, that do not designate the United States, but do designate at least one country other than the United States, and have also identified below any such international application for the same invention having a filing date before that of the application on which priority is claimed:

Prior International Application(s) Priority Claimed

N/A____________________ ____________________ Yes No
(Number) (Date Filed)

______________________ ____________________ Yes No
(Number) (Date Filed)

I hereby claim the priority benefit under Title 35, United States Code, § 119(e) of the United States provisional patent application(s) listed below and, insofar as any subject matter of the claims of this application is not disclosed in such prior United States provisional application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which became available between the filing date of the prior provisional application(s) and the national or PCT international filing date of this application:

N/A
(Appl. Ser. No.) (Date Filed) (Status-patented, pending, abandoned)

(Appl. Ser. No.) (Date Filed) (Status-patented, pending, abandoned)

I hereby claim the priority benefit under Title 35, United States Code, § 120 of the United States patent application(s) listed below and, insofar as any subject matter of the claims of this application is not disclosed in such prior United States application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

N/A
(Appl. Ser. No.) (Date Filed) (Status-patented, pending, abandoned)

(Appl. Ser. No.) (Date Filed) (Status-patented, pending, abandoned)

I hereby claim the priority benefit under Title 35, United States Code, §§ 120 and 365(c) of any international patent application(s), listed below, that designate the United States and have also identified below any such international application for the same invention having a filing date before that of the application(s) on which priority is claimed, and, insofar as any subject matter of the claims of this application is not disclosed in such prior international application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which became available between the filing date of the prior international application(s) and the national or PCT international filing date of this application:

Prior International Application(s) Priority Claimed

N/A
(Number) (Date Filed) Yes No

(Number) (Date Filed) Yes No

I hereby appoint the fol ·ing attorney, with full , ɜr of substitution, to prosecute this applic..ion and to transact all bu..ness in the United States Patent and Trademark Office connected therewith: David R. Graham, Reg. No. 36,150.

Please address all correspondence regarding this application to David R. Graham, 1337 Chewpon Avenue, Milpitas, California 95035.

Please direct all telephone calls regarding this application to David R. Graham at telephone number (408) 945-9912.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made herein on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor's signature ____________ Date ________
Full name of inventor William P. Bialick
Residence Clarksville, Maryland Citizenship US
Post Office Address 7150 Moorland Drive
Clarksville, Maryland 21029-1735

Inventor's signature ____________ Date ________
Full name of inventor Mark J. Sutherland
Residence Milpitas, California Citizenship US
Post Office Address 1209 Eagle Ridge Way
Milpitas, Califonia 95035-7817

Inventor's signature ____________ Date ________
Full name of inventor Janet L. Dolphin-Peterson
Residence Belvedere, California Citizenship US
Post Office Address 296 Beach Road
Belvedere, California 94920-2472

Inventor's signature ____________ Date ________
Full name of inventor Thomas K. Rowland
Residence Los Gatos, California Citizenship US
Post Office Address P.O. Box 33157
Los Gatos, California 95031-3157

Inventor's signature ____________ Date ________
Full name of inventor Kirk W. Skeba
Residence Fremont, Califonia Citizenship US
Post Office Address 400 Calistoga Circle
Fremont, California 94536-7620

Inventor's signature ____________ Date ________
Full name of inventor Russell D. Housley
Residence Herndon, Virginia Citizenship US
Post Office Address 918 Spring Knoll Drive
Herndon, Virginia

~~0260~~
0300

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#5

Applicants: William P. Bialick et al.

Assignee: Spyrus, Inc.

Title: Peripheral Device With Integrated Security Functionality

Serial No.: 08/869,305 Filed: June 4, 1997

Examiner: Unknown Group Art Unit: Unknown

Attorney Docket No.: SPY-004

Milpitas, California
August 11, 1997

Assistant Commissioner for Patents
Washington, D. C. 20231

INFORMATION DISCLOSURE STATEMENT

Sir:

Pursuant to 37 C.F.R. § 1.56, § 1.97 and § 1.98, Applicants bring the documents (copy of the U.S. Patent enclosed) listed on the enclosed Form PTO-1449 to the Examiner's attention in the above-identified application. Citation of these documents shall not be construed as an admission that the documents are necessarily prior art with respect to the instant invention. Also, citation of these documents shall not be construed as an admission that the information disclosed therein is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on August 11, 1997.

8-11-97 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants

part of #5

1 OF 1

U.S. DEPT OF COMMERCE - PATENT AND TRADEMARK OFFICE INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	ATTORNEY DOCKET NO.: SPY-004 SERIAL NO.: 08/869,305 APPLICANTS: William P. Bialick et al. FILING DATE: June 4, 1997 GROUP ART UNIT: Unknown

U.S. PATENTS

EXAMINER'S INITIALS	PATENT NUMBER	ISSUE DATE	INVENTOR(S)	CLASS	SUB-CLASS	FILING DATE
LVH	5,546,[illegible]	8/13/96	Caputo et al.	380	26	7/12/94

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	DOCUMENT NUMBER	PUBLICATION DATE	NAME(S)	COUNTRY	TRANSLATION?	
					YES	NO

COMMONLY OWNED, CO-PENDING U.S. PATENT APPLICATIONS

EXAMINER'S INITIALS	SERIAL NUMBER	ATTORNEY DOCKET NO.	APPLICANT(S)	CLASS	SUB-CLASS	FILING DATE
LVH	08/869,120	SPY-003	William P. Bialick et al.	—	—	6/4/97

OTHER DOCUMENTS

EXAMINER'S INITIALS	AUTHOR(S), TITLE, DATE, PERTINENT PAGES, ETC.

EXAMINER: Ly V. Hua   DATE CONSIDERED: 11/23/98

Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

Other Prior Art

According to the information contained in form PTO-1449 or PTO-892, there are one or more other prior art/non-patent literature documents missing from the original file history record obtained from the United States Patent and Trademark Office. Upon your request we will attempt to obtain these documents from alternative resources. Please note that additional charges will apply for this service.

Transaction History Date 1997-11-04
Date information retrieved from USPTO Patent
Application Information Retrieval (PAIR)
system records at www.uspto.gov

BEST COPY

UNITED STAT__ DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO./TITLE
08/869,305	06/04/97	BIALICK	W SPY-004

0292/1104

DAVID R GRAHAM
1337 CHEWPON AVENUE
MILPITAS CA 95035

NOT ASSIGNED

2202

DATE MAILED: 11/04/97

NOTICE TO FILE MISSING PARTS OF APPLICATION
Filing Date Granted

An Application Number and Filing Date have been assigned to this application. However, the items indicated below are missing. The required items and fees identified below must be timely submitted ALONG WITH THE PAYMENT OF A SURCHARGE for items 1 and 3-6 only of $ 130 for a ☐ large entity ☐ small entity in compliance with 37 CFR 1.27. The surcharge is set forth in 37 CFR 1.16(e). Applicant is given TWO MONTHS FROM THE DATE OF THIS NOTICE within which to file all required items and pay any fees required above to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

If all required items on this form are filed within the period set above, the total amount owed by applicant as a ☑ large entity ☐ small entity (verified statement filed), is $ [illegible].

☑ 1. The statutory basic filing fee is:
- ☑ missing.
- ☐ insufficient.

Applicant must submit $ 790 to complete the basic filing fee and/or file a verified small entity statement claiming such status (37 CFR 1.27).

☑ 2. Additional claim fees of $ [illegible], including any multiple dependent claim fees, are required. *Applicant must either submit the additional claim fees or cancel additional claims for which fees are due.*

☐ 3. The oath or declaration:
- ☐ is missing.
- ☐ does not cover the newly submitted items.
- ☐ does not identify the application to which it applies.
- ☐ does not include the city and state or foreign country of applicant's residence.

An oath or declaration in compliance with 37 CFR 1. 63, including residence information and identifying the application by the above Application Number and Filing Date is required.

☑ 4. The signature(s) to the oath or declaration is/are:
- ☑ missing.
- ☐ by a person other than inventor or person qualified under 37 CFR 1.42, 1.43, or 1.47.

A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.

☐ 5. The signature of the following joint inventor(s) is missing from the oath or declaration:

____

An oath or declaration listing the names of all inventors and signed by the omitted inventor(s), identifying this application by the above Application Number and Filing Date, is required.

☐ 6. A $__________ processing fee is required since your check was returned without payment (37 CFR 1.21(m)).

☐ 7. Your filing receipt was mailed in error because your check was returned without payment.

☐ 8. The application does not comply with the Sequence Rules. *See attached "Notice to Comply with Sequence Rules 37 CFR 1.821-1.825."*

☐ 9. OTHER:

Direct the response and any questions about this notice to "Attention: Box Missing Parts."

A copy of this notice MUST be returned with the response.

Customer Service Center
Initial Patent Examination Division (703) 308-1202

Sector #

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: William P. Bialick et al.

Assignee: Spyrus, Inc.

Title: Peripheral Device With Integrated Security Functionality 3

Serial No.: 08/869,305 Filed: June 4, 1997

Examiner: Unknown Group Art Unit: 2202

Attorney Docket No.: SPY-004

Milpitas, California
January 5, 1998

Box Missing Parts
Assistant Commissioner for Patents
Washington, D. C. 20231

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION - FILING DATE GRANTED

Sir:

In response to the "Notice to File Missing Parts of Application - Filing Date Granted" mailed by the United States Patent and Trademark Office on November 4, 1997, the following documents are enclosed to complete the filing of the above-referenced patent application:

1. Declaration and Power of Attorney for Patent Application, signed in counterpart by the inventors in compliance with 37 CFR 1.63;
2. Copy of Notice to File Missing Parts of Application - Filing Date Granted; and
3. Verified Statement Under 37 CFR 1.9(f) and 1.27(c) Claiming Small Entity Status by Assignee.

Enclosed is a check (Check No. 1155) in the amount of $961.00 for:

1. Statutory basic filing fee - $395.00;
2. Additional claim fees - $501.00; and
3. Surcharge for filing declaration on a date later than the filing date of the application - $65.00.

It is hereby submitted that the enclosed documents complete the filing of the above-referenced patent application and justify the filing date of June 4, 1997. This document is being submitted in duplicate. If there are any questions regarding this Response, please telephone Applicants' undersigned attorney at (408) 945-9912.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on January 5, 1998.

1-5-98 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

#3

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below adjacent to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of subject matter (process, machine, manufacture, or composition of matter, or an improvement thereof) which is claimed and for which a patent is sought by way of the application entitled: Peripheral Device With Integrated Security Functionality

which (check) [ ] is attached hereto.
[ ] and is amended by the Preliminary Amendment attached hereto.
[X] was filed on June 4, 1997, as Application Serial No. 08/869,305.
[ ] and was amended on ___________ (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified application, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office information known to me to be material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim the priority benefit under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate for the same invention having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s) Priority Claimed

N/A (Number)	(Country)	(Date Filed)	Yes	No
(Number)	(Country)	(Date Filed)	Yes	No

I hereby claim the priority benefit under Title 35, United States Code, §§ 119 and 365(a) of any international patent application(s), listed below, that do not designate the United States, but do designate at least one country other than the United States, and have also identified below any such international application for the same invention having a filing date before that of the application on which priority is claimed:

Prior International Application(s) Priority Claimed

N/A (Number)	(Date Filed)	Yes	No
(Number)	(Date Filed)	Yes	No

hereby claim the priority benefit under Title 35, United States Code, 19(e) of the United States provisional patent application(s) listed low and, insofar as any subject matter of the claims of this application not disclosed in such prior United States provisional application(s) in manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which became available between the filing date of the prior provisional application(s) and the national or PCT international filing date of this application:

N/A
(Appl. Ser. No.) (Date Filed) (Status-patented, pending, abandoned)

(Appl. Ser. No.) (Date Filed) (Status-patented, pending, abandoned)

I hereby claim the priority benefit under Title 35, United States Code, § 120 of the United States patent application(s) listed below and, insofar as any subject matter of the claims of this application is not disclosed in such prior United States application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

N/A
(Appl. Ser. No.) (Date Filed) (Status-patented, pending, abandoned)

(Appl. Ser. No.) (Date Filed) (Status-patented, pending, abandoned)

I hereby claim the priority benefit under Title 35, United States Code, §§ 120 and 365(c) of any international patent application(s), listed below, that designate the United States and have also identified below any such international application for the same invention having a filing date before that of the application(s) on which priority is claimed, and, insofar as any subject matter of the claims of this application is not disclosed in such prior international application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which became available between the filing date of the prior international application(s) and the national or PCT international filing date of this application:

Prior International Application(s) Priority Claimed

N/A
(Number) (Date Filed) Yes No

(Number) (Date Filed) Yes No

I hereby appoint the following attorney, with full power of substitution, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith: David R. Graham, Reg. No. 36,150.

Please address all correspondence regarding this application to David R. Graham, 1337 Chewpon Avenue, Milpitas, California 95035.

Please direct all telephone calls regarding this application to David R. Graham at telephone number (408) 945-9912.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made herein on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor's signature ______ Date ______
Full name of inventor William P. Bialick
Residence Clarksville, Maryland Citizenship US
Post Office Address 7150 Moorland Drive
Clarksville, Maryland 21029-1735

Inventor's signature ______ Date 18 Dec 97
Full name of inventor Mark J. Sutherland
Residence Milpitas, California Citizenship US
Post Office Address 1209 Eagle Ridge Way
Milpitas, Califonia 95035-7817

Inventor's signature ______ Date ______
Full name of inventor Janet L. Dolphin-Peterson
Residence Belvedere, California Citizenship US
Post Office Address 296 Beach Road
Belvedere, California 94920-2472

Inventor's signature ______ Date 12-18-97
Full name of inventor Thomas K. Rowland
Residence Los Gatos, California Citizenship US
Post Office Address P.O. Box 33157
Los Gatos, California 95031-3157

Inventor's signature ______ Date ______
Full name of inventor Kirk W. Skeba
Residence Fremont, Califonia Citizenship US
Post Office Address 400 Calistoga Circle
Fremont, California 94536-7620

Inventor's signature Russell Housley Date 20 Aug 1997
Full name of inventor Russell D. Housley
Residence Herndon, Virginia Citizenship US
Post Office Address 918 Spring Knoll Drive
Herndon, Virginia

I hereby appoint the following attorney, with full power of substitution, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith: David R. Graham, Reg. No. 36,150.

Please address all correspondence regarding this application to David R. Graham, 1337 Chewpon Avenue, Milpitas, California 95035.

Please direct all telephone calls regarding this application to David R. Graham at telephone number (408) 945-9912.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made herein on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor's signature William P. Bialick Date 12/19/97
Full name of inventor William P. Bialick
Residence Clarksville, Maryland Citizenship US
Post Office Address 7150 Moorland Drive
Clarksville, Maryland 21029-1735

Inventor's signature Date 18 Dec 97
Full name of inventor Mark J. Sutherland
Residence Milpitas, California Citizenship US
Post Office Address 1209 Eagle Ridge Way
Milpitas, Califonia 95035-7817

Inventor's signature Date
Full name of inventor Janet L. Dolphin-Peterson
Residence Belvedere, California Citizenship US
Post Office Address 296 Beach Road
Belvedere, California 94920-2472

Inventor's signature Date 12-18-97
Full name of inventor Thomas K. Rowland
Residence Los Gatos, California Citizenship US
Post Office Address P.O. Box 33157
Los Gatos, California 95031-3157

Inventor's signature Kirk W. Skeba Date 12/23/97
Full name of inventor Kirk W. Skeba
Residence Fremont, Califonia Citizenship US
Post Office Address 400 Calistoga Circle
Fremont, California 94536-7620

Inventor's signature Russell Housley Date 20 Aug 1997
Full name of inventor Russell D. Housley
Residence Herndon, Virginia Citizenship US
Post Office Address 918 Spring Knoll Drive
Herndon, Virginia

I hereby appoint the following attorney, with full power of substitution, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith: David R. Graham, Reg. No. 36,150.

Please address all correspondence regarding this application to David R. Graham, 1337 Chewpon Avenue, Milpitas, California 95035.

Please direct all telephone calls regarding this application to David R. Graham at telephone number (408) 945-9912.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made herein on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor's signature ____________ Date ________
Full name of inventor William P. Bialick
Residence Clarksville, Maryland Citizenship US
Post Office Address 7150 Moorland Drive
Clarksville, Maryland 21029-1735

Inventor's signature ____________ Date 18 Dec 97
Full name of inventor Mark J. Sutherland
Residence Milpitas, California Citizenship US
Post Office Address 1209 Eagle Ridge Way
Milpitas, Califonia 95035-7817

Inventor's signature ____________ Date 20-DEC-97
Full name of inventor Janet L. Dolphin-Peterson
Residence Belvedere, California Citizenship US
Post Office Address 296 Beach Road
Belvedere, California 94920-2472

Inventor's signature ____________ Date 12-18-97
Full name of inventor Thomas K. Rowland
Residence Los Gatos, California Citizenship US
Post Office Address P.O. Box 33157
Los Gatos, California 95031-3157

Inventor's signature ____________ Date ________
Full name of inventor Kirk W. Skeba
Residence Fremont, Califonia Citizenship US
Post Office Address 400 Calistoga Circle
Fremont, California 94536-7620

Inventor's signature Russell Housley Date 20 Aug 1997
Full name of inventor Russell D. Housley
Residence Herndon, Virginia Citizenship US
Post Office Address 918 Spring Knoll Drive
Herndon, Virginia

BEST COPY

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO./TITLE
08/869,305	06/04/97	BIHLICK	W SPY-004

0292/1104

DAVID K GRAHAM
1337 CHEWPON AVENUE
MILPITAS CA 95035

NOT ASSIGNED

2202

DAVID MAILED:

DATE MAILED: 11/04/97

NOTICE TO FILE MISSING PARTS OF APPLICATION

Filing Date Granted

An Application Number and Filing Date have been assigned to this application. However, the items indicated below are missing. The required items and fees identified below must be timely submitted ALONG WITH THE PAYMENT OF A SURCHARGE for items 1 and 3-6 only of $ 130 for a ☐ large entity ☐ small entity in compliance with 37 CFR 1.27. The surcharge is set forth in 37 CFR 1.16(e). Applicant is given TWO MONTHS FROM THE DATE OF THIS NOTICE within which to file all required items and pay any fees required above to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

If all required items on this form are filed within the period set above, the total amount owed by applicant as a ☒ large entity ☐ small entity (verified statement filed), is $ 1922.

☒ 1. The statutory basic filing fee is:
☒ missing.
☐ insufficient.
Applicant must submit $ 790 to complete the basic filing fee and/or file a verified small entity statement claiming such status (37 CFR 1.27).

☒ 2. Additional claim fees of $ 1002, including any multiple dependent claim fees, are required.
Applicant must either submit the additional claim fees or cancel additional claims for which fees are due.

☐ 3. The oath or declaration:
☐ is missing.
☐ does not cover the newly submitted items.
☐ does not identify the application to which it applies.
☐ does not include the city and state or foreign country of applicant's residence.
An oath or declaration in compliance with 37 CFR 1.63, including residence information and identifying the application by the above Application Number and Filing Date is required.

☒ 4. The signature(s) to the oath or declaration is/are:
☒ missing.
☐ by a person other than inventor or person qualified under 37 CFR 1.42, 1.43, or 1.47.
A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.

☐ 5. The signature of the following joint inventor(s) is missing from the oath or declaration:

An oath or declaration listing the names of all inventors and signed by the omitted inventor(s), identifying this application by the above Application Number and Filing Date, is required.

☐ 6. A $______ processing fee is required since your check was returned without payment (37 CFR 1.21(m)).

☐ 7. Your filing receipt was mailed in error because your check was returned without payment.

☐ 8. The application does not comply with the Sequence Rules.
See attached "Notice to Comply with Sequence Rules 37 CFR 1.821-1.825."

☐ 9. OTHER:

Direct the response and any questions about this notice to "Attention: Box Missing Parts."

A copy of this notice MUST be returned with the response.

Customer Service Center
Initial Patent Examination Division (703) 308-1202

PART 2 - COPY TO BE RETURNED WITH RESPONSE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	William P. Bialick et al.		
Assignee:	Spyrus, Inc.		
Title:	Peripheral Device With Integrated Security Functionality		
Serial No.:	08/869,305	Filed:	June 4, 1997
Examiner:	Unknown	Group Art Unit:	Unknown

Attorney Docket No.: SPY-004

San Jose, California

Assistant Commissioner for Patents
Washington, D. C. 20231

VERIFIED STATEMENT UNDER 37 CFR 1.9(f) AND 1.27(c)
CLAIMING SMALL ENTITY STATUS BY ASSIGNEE

Sir:

I declare that I am an official empowered to act on behalf of the concern identified above as assignee.

Exclusive rights to the above invention as described in U.S. patent application Serial No. 08/869,305, filed June 4, 1995 have been conveyed to and remain with the above concern.

For purposes of paying reduced fees under Section 41 of Title 35 of the United States Code with regard to this invention, I declare that the above concern qualifies as a small business concern as defined in 13 CFR 121.12 and reproduced in 37 CFR 1.9(d), namely, the concern's number of employees, including those of its affiliates, does not exceed 500 persons and the concern has not assigned, granted, conveyed, or licensed, and is under no obligation under contract or law to assign, grant, convey or license, any rights in the invention to any person who could not be classified as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

I acknowledge my duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate per 37 CFR 1.28(b).

I further declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of this application, or any patent issued thereon.

Signature: ______________ Date: November 25, 1997
Official's Name: Kevin O'Neill, Esq.
Official's Title: Corporate Secretary
Concern's Name: Spyrus, Inc.
Concern's Address: 2460 North First Street, Suite 100
San Jose, CA 95131

GP2202

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

11·23·98

Applicants:	William P. Bialick et al.		
Assignee:	Spyrus, Inc.		
Title:	Peripheral Device With Integrated Security Functionality		
Serial No.:	08/869,305	Filed:	June 4, 1997
Examiner:	Unknown	Group Art Unit:	2202
Attorney Docket No.:	SPY-004		

Milpitas, California
October 6, 1998

Assistant Commissioner for Patents
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT
WITH CERTIFICATION UNDER 37 C.F.R. §1.97(e)(1)

Sir:

Pursuant to 37 C.F.R. § 1.56, § 1.97 and § 1.98, Applicants bring the documents (copies enclosed) listed on the enclosed Form PTO-1449 to the Examiner's attention in the above-identified application. These documents were cited by the European Patent Office in the International Search Report (copy enclosed) for the corresponding PCT Application No. PCT/US98/11052.

Citation of these documents shall not be construed as an admission that the documents are necessarily prior art with respect to the instant invention. Also, citation of these documents shall not be construed as an admission that the information disclosed therein is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

The undersigned hereby certifies in accordance with 37 C.F.R. §1.97(e)(1) that each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this information disclosure statement.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on October 6, 1998.

10-6-98 David R. Graham
Date Signature

Respectfully submitted
and certified by,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants

part of # 4

SHEET 1 OF 1

U.S. DEPT OF COMMERCE - PATENT AND TRADEMARK OFFICE INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	ATTORNEY DOCKET NO.: SPY-004 / SERIAL NO.: 08/869,305 APPLICANTS: William P. Bialick et al. FILING DATE: June 4, 1997 / GROUP ART UNIT: 2202

U.S. PATENTS

EXAMINER'S INITIALS	PATENT NUMBER	ISSUE DATE	INVENTOR(S)	CLASS	SUB-CLASS	FILING DATE
LVH	5,548,721	8/20/96	Denslow	395	187.01	4/28/94
LVH	5,457,590	10/10/95	Barrett et al.	360	133	6/11/91
LVH	5,630,174	5/13/97	Stone, III et al.	395	883	2/3/95
LVH	4,910,776	3/20/90	Dyke	380	25	2/24/89

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	DOCUMENT NUMBER	PUBLICATION DATE	NAME(S)	COUNTRY	TRANSLATION? YES	TRANSLATION? NO
LVH	WO 97/29416	8/14/97	Mooney et al.	PCT	X	
LVH	WO 82/03286	9/30/82	Lofberg	PCT	X	

COMMONLY OWNED, CO-PENDING U.S. PATENT APPLICATIONS

EXAMINER'S INITIALS	SERIAL NUMBER	ATTORNEY DOCKET NO.	APPLICANT(S)	CLASS	SUB-CLASS	FILING DATE

OTHER DOCUMENTS

EXAMINER'S INITIALS	AUTHOR(S), TITLE, DATE, PERTINENT PAGES, ETC.

EXAMINER: Ly V. Hua

DATE CONSIDERED: 11/23/98

Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

Transaction History Date 1998-12-11
Date information retrieved from USPTO Patent
Application Information Retrieval (PAIR)
system records at www.uspto.gov

BEST COPY

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
[illegible]	[illegible]	[illegible]	[illegible]

[illegible]

DAVID R GRAHAM
1337 CHEWPON AVENUE
MILPITAS CA 95035

EXAMINER	
HUA,L	
ART UNIT	PAPER NUMBER
2765	6

DATE MAILED: 12/11/98

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

Commissioner of Patents and Trademarks

08/869,305

	Application No.	Applicant(s)	
Office Action Summary	Examiner	Group Art Unit	

—The MAILING DATE of this communication appears on the cover sheet beneath the correspondence address—

Period for Response

A SHORTENED STATUTORY PERIOD FOR RESPONSE IS SET TO EXPIRE three MONTH(S) 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 response be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for response is specified above, such period shall, by default, expire SIX (6) MONTHS from the mailing date of this communication .
- Failure to respond within the set or extended period for response will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

☑ Responsive to communication(s) filed on October 8, 1998.

□ This action is **FINAL.**

□ 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. 1 1; 453 O.G. 213.

Disposition of Claims

☑ Claim(s) 1-32 is/are pending in the application.

Of the above claim(s) ______ is/are withdrawn from consideration.

□ Claim(s) ______ is/are allowed.

□ Claim(s) 1, 8, 14, 4, 11, 17, 32, 31, 28, 29, 30 and 24-26 is/are rejected.

□ Claim(s) 6, 7 and 13 is/are objected to.

☑ Claim(s) 2, 3, 5, 20, 9, 10, 12, 15, 16, 18, 19, 21-23 and 27 are subject to restriction or election requirement.

Application Papers

□ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

□ The proposed drawing correction, filed on ______ is □ approved □ disapproved.

□ The drawing(s) filed on ______ is/are objected to by the Examiner.

□ The specification is objected to by the Examiner.

□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119 (a)-(d)

□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 11 9(a)-(d).

□ All □ Some* □ None of the CERTIFIED copies of the priority documents have been

□ received.

□ received in Application No. (Series Code/Serial Number) ______.

□ received in this national stage application from the International Bureau (PCT Rule 1 7.2(a)).

*Certified copies not received: ______.

Attachment(s)

☑ Information Disclosure Statement(s), PTO-1449, Paper No(s). 5 and 4 □ Interview Summary, PTO-413

☑ Notice of References Cited, PTO-892 □ Notice of Informal Patent Application, PTO-152

□ Notice of Draftsperson's Patent Drawing Review, PTO-948 □ Other ______

Office Action Summary

1. This application contains claims directed to the following patentably distinct species of the claimed invention: first, second, third, fourth species of target means.

Applicant is required under 35 U.S.C. 121 to elect a single disclosed species for prosecution on the merits to which the claims shall be restricted if no generic claim is finally held to be allowable. Currently, the target means is generic.

Applicant is advised that a response to this requirement must include an identification of the species that is elected consonant with this requirement, and a listing of all claims readable thereon, including any claims subsequently added. An argument that a claim is allowable or that all claims are generic is considered nonresponsive unless accompanied by an election.

Upon the allowance of a generic claim, applicant will be entitled to consideration of claims to additional species which are written in dependent form or otherwise include all the limitations of an allowed generic claim as provided by 37 CFR 1.141. If claims are added after the election, applicant must indicate which are readable upon the elected species. MPEP § 809.02(a).

Should applicant traverse on the ground that the species are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the species to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.

2. During a telephone conversation with Mr. Vavid R. Graham (Reg. No. 36160) on November 6, 1998, a provisional election was made with traverse to prosecute the invention of the first species, claims 1, 4, 6, 7, 8, 11, 13, 14, 17, 24-26, 28, 29, 30, 31 and 32. Affirmation of this election must be made by applicant in responding to this Office action. Claims 2, 3, 5, 20, 9, 10, 12, 15, 16, 18, 19-20, 21-

23 and 27 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

3. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a diligently-filed petition under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(h).

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

5. Claims 24-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Novis et al (5,770,849 hereinafter Novis).

a. <u>As per claim 24</u>:

Novis teaches a peripheral device [10], comprising:

(1) security means [86] ~~for enabling one or more security operations to be performed on data~~ ;

(2) a biometric device [14 (col. 3, lines 36-44; col. 9, lines 28-3~~0)]~~ for ~~receiving input data regarding a physical characteristic of a person based upon a physical interaction of the person with the peripheral device~~;

(3) means [16] for enabling communication between

(a) the security means [86] and

(b) the biometric device [14],

[which communication is for transferring captured user characteristic from biometric 14 to the security means 86 for authentication thereat (col. 9, lines 26-37] ; and

(4) means [95] for enabling communication with a host computing device [96].

b. As per claim 25 or 26:

Novis teaches that his biometric device comprises either:

(1) a fingerprint scanning device [in order to input biometric identifier such as a finger print (col. 3, lines 37-40)] or

(2) a retinal scanning device [in order to input biometric identifier such as a retinal scan (col. 3, lines 37-40)].

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary.

Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(f) or (g) prior art under 35 U.S.C. 103(a).

8. Claims 1, 8, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Novis et al (5,770,849 her

a. As per claims 1, 8, and 14:

i. Novis teaches a peripheral device, comprising:

(1) security means [86] for enabling one or more security operations to be performed on data;

(2) target means [14 (col. 3, lines 36-44, col. 9, lines 28-30) for capturing biometric input] for enabling a defined interaction with a host computing device;

(3) means [16] for enabling communication between

(a) the security means and

(b) the target means ,

[which communication is for transferring captured user characteristic from biometric 14 to the security means 86 for authentication thereat (col. 9, lines 26-37];

(4) means [95] for enabling communication with a host computing device [96].

ii. Applican't s admitted prior art teaches:

(1) means [inherent in the host computing device 201 of Fig. 2] for operably connecting

(a) [either] the security means [86] **and/or** the target means [14] to

(b) the host computing device [96]

in response to an instruction from the host computing device.

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to maitain, (even when the security device 203 and the target device 202 of applican't admitted art are implemented in a single unit), the means [inherent in the host computing device 201 of Fig. 2] for operably connecting

(a) [either] the security means [86] **and/or** the target means [14] to

(b) the host computing device [96]

in response to an instruction from the host computing device.

iv. This is because the admitted prior works fine.

b. <u>As per claim 4, 11 or 17</u>:

Novis teaches that his target means 14 comprises a biometric device [col. 3, lines 41-44].

c. <u>As per claims 32 and 31</u>:

These claims do not teach or cover more than those which are covered by claims 1, 8 and 14 and thus are similarly rejected with the same rationale applied thereto.

d. <u>As per laims 28, 29 and 30</u>:

Using the above rejected claims 1, 8 and 14 with a host computer device would have been obvious to a person of ordinary skill in the art. This is because peripheral devices are to be use with host device.

9. Claims 6, 7, and 13 are objected to as they depend on rejected claims.

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

11. **Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks
Washington, D.C. 20231

or faxed to:

(703) 308-9051, (for formal communications intended for entry)

Or:

(703)305-9724 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington. VA., Sixth Floor (Receptionist).

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Ly Hua whose telephone number is (703) 305-9684. The examiner can normally be reached on Monday to Friday from 9:30 AM to 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Mr. Robert W. Beausoliel, Jr., can be reached on (703) 305-9713. The fax phone number for this Group is (703) 305-9724.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

LY V. HUA
PATENT EXAMINER
ART UNIT 2785

L. Hua
November 20, 1998

Notice of References Cited	Application No. 08/869,305	Applicant(s) BIALICK ET AL
	Examiner Ly Hua	Group Art Unit 2785 · Page 1 of 1

U.S. PATENT DOCUMENTS

*		DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS
	A	5,770,849	6/98	NOVIS ET AL.	235	492
	B	5,473,692	12/95	DAVIS	380	25
	C	5,546,463	8/96	CAPUTO ET AL.	380	25
	D	5,282,247	1/94	MCLEAN ET AL.	380	4
	E	5,191,611	3/93	LANG	380	25
	F	5,537,544	7/96	MORISAWA ET AL.	395	188.01
	G	5,742,683	4/98	LEE ET AL.	380	23
	H	5,491,827	2/96	HOLTEY	395	800
	I	5,442,704	8/95	HOLTEY	380	23
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		DOCUMENT NO.	DATE	COUNTRY	NAME	CLASS	SUBCLASS
	N						
	O						
	P						
	Q						
	R						
	S						
	T						

NON-PATENT DOCUMENTS

*		DOCUMENT (Including Author, Title, Source, and Pertinent Pages)	DATE
	U		
	V		
	W		
	X		

* A copy of this reference is not being funished with this Office action.
(See Manual of Patent Examining Procedure, Section 707.05(a).)

U.S. Patent and Trademark Office

Part of Paper No. 6

GAU 2785

Attorney Docket No.: SPY-004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

March 11, 1999

Assistant Commissioner for Patents
Washington, D.C. 20231

Re: Applicants: William P. Bialick et al.
Assignee: Spyrus, Inc.
Title: Peripheral Device With Integrated Security Functionality
Serial No.: 08/869,305
Filed: June 4, 1997
Examiner: L. Hua
Group Art Unit: 2785

Transmitted herewith are the following documents in the above-identified application:

(1) Response to Office Action (16 pages);
(2) Check for $63.00 (Check No. 1385);
(3) Return receipt postcard; and
(4) This sheet in duplicate.

The fee is calculated as follows (small entity status is claimed):

CLAIMS AS AMENDED

	Claims After Amendment		Highest Number Paid For		Additional Claims		Rate		Fee
Total Claims:	39	-	32	=	7	X	$9	= $	63.00
Independent Claims:	8	-	12	=	0	X	$38	= $	0.00
____ First filing of one or more multiple dependent claims ($270 total fee)								$	0.00
____ Fee for Petition for Extension of Time (____ months)								$	0.00
TOTAL FEE:								**$**	**63.00**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on March 11, 1999.

3-11-99 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants
1337 Chewpon Ave.
Milpitas, CA 95035
Tel. No.: (408) 945-9912

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#7/A

Applicants: William P. Bialick et al.

Assignee: Spyrus, Inc.

Title: Peripheral Device With Integrated Security Functionality

Serial No.: 08/869,305 Filed: June 4, 1997

Examiner: L. Hua Group Art Unit: 2785

Attorney Docket No.: SPY-004

3/25/99

Milpitas, California
March 11, 1999

Assistant Commissioner for Patents
Washington, D.C. 20231

RESPONSE TO OFFICE ACTION

3/26/99

Sir:

Please enter the following response to the Office Action dated December 11, 1998, in the above-identified application.

IN THE SPECIFICATION

At page 5, line 19, delete "or" and substitute --,--;

line 20, after "device" (first occurrence), insert --or input to the peripheral device by a person--.

A1

At page 8, line 4, delete "computational" and substitute --computing--;

line 5, delete "computational" and substitute --computing--.;

line 10, delete "another" and substitute --the peripheral--;

after "device" (second occurrence), insert --302--;

line 11, delete "another" and substitute --the peripheral--;

after "device" (first occurrence), insert --302--.

At page 9, line 22, delete "3A" and substitute --3B--.

At page 13, line 5, delete "an".

At page 14, line 32, after ")", insert --to enable performance of security operations--.

A2

At page 16, line 21, delete "colloquially" and substitute --informally--.

At page 20, line 31, delete "implemented" and substitute --operated--.

At page 22, line 9, delete "This" and substitute --The--;

line 18, delete "peripheral" and substitute --target--;

line 30, after "device.", insert --(Of course, in this case, security functionality, i.e., user authentication, is used as part of the step 715)--.

A3

At page 24, line 18, after "below", insert --(see FIGS. 8, 9A and 9B)--.

At page 28, line 13, delete "be";

after "also", insert --be--;

line 18, delete "with" and substitute

--to provide--.

At page 29, line 5, after "806", insert --,--.

At page 33, line 7, delete "a" (first occurrence) and

substitute --the--.

At page 34, line 18, delete "peripheral".

IN THE CLAIMS

Please cancel Claims 1, 19, 21, 24, 27 and 28.

Please amend the claims as follows:

2. (Amended) A peripheral device as in Claim [1] ~~6~~ 1, wherein the target means comprises means for non-volatilely storing data.

A4

3. (Amended) A peripheral device as in Claim [1] ~~6~~ 1, wherein the target means comprises means for enabling communication between the host computing device and a remote device.

4. (Amended) A peripheral device as in Claim [1] ~~6~~ 1, wherein the target means comprises a biometric device.

5. (Amended) A peripheral device as in Claim [1] ~~6~~ 1, wherein the target means comprises means for communicating with a smart card.

1 ~~6~~. (Amended) A peripheral device [as in Claim 1], [further] comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means;

A4

means for enabling communication with a host computing device;

means for operably connecting the security means and/or the target means to the host computing device in response to an instruction from the host computing device; and

means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means.

6 ~~7~~. (Amended) A peripheral device [as in Claim 1], [further] comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device;

A4 means for operably connecting the security means and/or the target means to the host computing device in response to an instruction from the host computing device; and

means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the target means [for enabling a defined interaction with a host computing device].

Sub B' A5

~~13. (Amended) A peripheral device as in Claim 8, further comprising means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the target means [for enabling a defined interaction with a host computing device].~~

24~~14~~. (Amended) A peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

45

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device; and

A5

means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the target means [for enabling a defined interaction with a host computing device].

A6

14 ~~20~~. (Amended) A peripheral device as in Claim [1] 13 ~~37~~, wherein the solid-state disk storage device comprises an ATA format flash disk drive.

A7

17 ~~22~~. (Amended) A peripheral device as in Claim [21] ~~36~~ 16 ~~38~~, wherein the wireless communication means comprises a wireless modem.

18 ~~23~~. (Amended) A peripheral device as in Claim [21] 16 ~~28~~, wherein the wireless communication means comprises a wireless LAN transceiver.

117

20~~25~~. (Amended) A peripheral device as in Claim [24]19~~11~~, wherein the biometric device comprises a fingerprint scanning device.

A8

21~~26~~. (Amended) A peripheral device as in Claim [24] 19 ~~11~~, wherein the biometric device comprises a retinal scanning device.

37 ~~30~~. (Amended) A data security system, comprising:

a host computing device including one or more device interfaces adapted to enable communication with another device;

a peripheral device, comprising:

security means for enabling one or more security operations to be performed on data;

target means for enabling a defined interaction with a host computing device; and

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device; and

means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the target means [for enabling a defined interaction with a host computing device].

A9

39 ~~32~~. (Amended) For use in a peripheral device adapted for communication with a host computing device, performance of one or more security operations on data, and interaction with a host computing device in a defined way, a method comprising the steps of:

A10

communicating with the [receiving an instruction from a] host computing device to exchange data between the host computing device and [regarding operation of] the peripheral device; [and]

[performng] performing one or more security operations and the defined interaction [in response to the instruction from the host computing device] on the exchanged data; and

mediating communication of the exchanged data between the host computing device and the peripheral device so that the exchanged data must first pass through means for performing the one or more security operations.

Please enter the following new claims:

7 ~~33~~. (New) A peripheral device as in Claim 6 ~~7~~, wherein the target means comprises means for non-volatilely storing data.

A11

8 ~~34~~. (New) A peripheral device as in Claim 6 ~~7~~, wherein the target means comprises means for enabling communication between the host computing device and a remote device.

9 ~~35~~. (New) A peripheral device as in Claim 6 ~~7~~, wherein the target means comprises a biometric device.

10 ~~36~~. (New) A peripheral device as in Claim 6 ~~7~~, wherein the target means comprises means for communicating with a smart card.

13 ~~37~~. (New) A peripheral device as in Claim 12 ~~8~~, wherein the means for non-volatilely storing data further comprises a solid-state disk storage device.

16 ~~38~~. (New) A peripheral device as in Claim 15 ~~10~~, wherein the means for enabling communication between the host computing device and a remote device further comprises wireless communication means.

26 ~~39~~. (New) A peripheral device as in Claim 25 ~~15~~, wherein the means for non-volatilely storing data further comprises a solid-state disk storage device.

27 ~~40~~. (New) A peripheral device as in Claim 26 ~~39~~, wherein the solid-state disk storage device comprises an ATA format flash disk drive.

29 ~~41~~. (New) A peripheral device as in Claim 28 ~~16~~, wherein the means for enabling communication between the host computing device and a remote device further comprises wireless communication means.

30 ~~42~~. (New) A peripheral device as in Claim 29 ~~41~~, wherein the wireless communication means comprises a wireless modem.

31 ~~43~~. (New) A peripheral device as in Claim 29 ~~41~~, wherein the wireless communication means comprises a wireless LAN transceiver.

A11

33 ~~44~~. (New) A peripheral device as in Claim 32 ~~17~~, wherein the biometric device comprises a fingerprint scanning device.

34 ~~45~~. (New) A peripheral device as in Claim 32 ~~17~~, wherein the biometric device comprises a retinal scanning device.

IN THE ABSTRACT

Line 17, delete "or" and substitute --,--.

Line 18, after "device" (second occurrence), insert --for input to the peripheral device by a person--.

A12

Line 26, delete "," (third occurrence).

Line 27, delete "as described further below".

REMARKS

Claims 1-32 were filed and are pending. Claims 2, 3, 5, 9, 10, 12, 15, 16, 18-23 and 27 were not examined, since directed to species that were not provisionally elected for examination by the Examiner. Claims 24-26 were rejected under 35 U.S.C. § 102. Claims 1, 4, 8, 11, 14, 17 and 28-32 were rejected under 35 U.S.C. § 103. Claims 6, 7 and 13 were objected to as dependent on a rejected claim. Claims 1, 19, 21, 24, 27 and 28 have been canceled. Claims 2-7, 13, 14, 20, 22, 23, 25, 26, 30 and 32 have been amended. Claims 33-45 have been added.

Reconsideration and allowance of Claims 2-18, 20, 22, 23, 25, 26, 29-32, and allowance of Claims 33-45 is requested.

In the Office Action, the Examiner stated:

> This application contains claims directed to the following patentably distinct species of the claimed invention: <u>first, second, third, fourth species of target means</u>.
>
> Applicant is required under 35 U.S.C. 121 to elect a single disclosed species for prosecution on the merits to which the claims shall be restricted if no generic claim is finally held to be allowable. Currently, <u>the target means</u> is generic.
>
> Applicant is advised that a response to this requirement must include an identification of the species that is elected consonant with this requirement, and a listing of all claims readable thereon, including any claims subsequently added. An argument that a claim is allowable or that all claims are generic is considered nonresponsive unless accompanied by an election.
>
> Upon the allowance of a generic claim, applicant will be entitled to consideration of claims to additional species which are written in dependent form or otherwise include all the limitations of an allowed generic claim as provided by 37 CFR 1.141. If claims are added after the election, applicant must indicate which are readable upon the elected species. MPEP § 809.02(a).
>
> Should applicant traverse on the ground that the species are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the species to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.
>
> During a telephone conversation with Mr. [D]avid R. Graham (Reg. No. 36,160 [sic]) on November 6, 1998, a provisional election was made with traverse to prosecute the invention of the first species, claims, 1, 4, 6, 7, 8, 11, 13, 14, 17, 24-26, 28, 29, 30, 31 and 32. Affirmation of this election must be made by applicant in responding to this Office action. Claims 2, 3, 5, 20, 9, 10, 12, 15, 16, 18, 19-20, 21-23 and 27

> are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Applicants confirm the provisional election to prosecute the invention of the first species (i.e., the species in which the target means can be embodied by a biometric device), originally pending claims 1, 4, 6-8, 11, 13, 14, 17, 24-26 and 28-32 readable thereon. Applicants have added Claims 33-45. Claims 35, 44 and 45 are also readable on the invention of the elected first species. Claims 33, 37, 39 and 40 are readable on the invention of the species in which the target means can be embodied by means for non-volatilely storing data. Claims 34, 38 and 41-43 are readable on the invention of the species in which the target means can be embodied by means for enabling communication between the host computing device and a remote device. Claim 36 is readable on the invention of the species in which the target means can be embodied by means for communicating with a smart card.

However, in view of the above amendments and the remarks below, Applicants contend that all pending claims, including those readable on non-elected species, are either an allowable generic claim (i.e., Claims 6, 7, 8, 13, 14 and 29-32) or are dependent on an allowable generic claim (i.e., Claims 2-5, 9-12, 15-18, 20, 22, 23, 25, 26 and 33-45).

The Examiner further stated in the Office Action that "Claims 6, 7, and 13 are objected to as they depend on rejected claims," i.e., Claims 6, 7 and 13 would be allowable if rewritten in independent form to include the limitations of the base claim and any intervening claims. Claims 6, 7 and 13 have been rewritten in this manner and are therefore in condition for allowance. (Claims 7 and 13 have also been amended to simplify a recitation of the target means.) Further, Claims 2-5 have each been amended to depend upon Claim 6 and are therefore allowable as dependent on an allowable claim. Additionally, new Claims 33-36 each depend upon Claim 7 and are therefore allowable as dependent on an allowable claim.

Before amendment, Claim 6 recited "[a] peripheral device as in Claim 1, further comprising means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means" (emphasis added). Since Claim 1 was rejected under 35 U.S.C. § 103 as unpatentable over Novis et al., the above-emphasized recitation in Claim 6 is apparently the basis for allowability of Claim 6. Claims 8 and 29 were also rejected under 35 U.S.C. § 103 as unpatentable over Novis et al. However, Claims 8 and 29, like Claim 6, recite "means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means." Therefore, Applicants submit that Claims 8 and 29, like Claim 6, are allowable. Further, Claims 9-12, which each depend upon Claim 8, are therefore allowable as dependent on an allowable claim. Additionally, Claims 20, 22, 23, 25 and 26, which have been amended so that each depends either directly or indirectly upon one of Claims 9-11, are also allowable as dependent on an allowable claim. Similarly, new

Claims 37 and 38, which depend upon Claims 9 and 10, respectively, are allowable as dependent on an allowable claim.

Before amendment, Claim 7 recited "[a] peripheral device as in Claim 1, further comprising means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the means for enabling a defined interaction with a host computing device" (emphasis added). Since Claim 1 was rejected under 35 U.S.C. § 103 as unpatentable over Novis et al., the above-emphasized recitation in Claim 7 is apparently the basis for allowability of Claim 7. Claims 14 and 30 were also rejected under 35 U.S.C. § 103 as unpatentable over Novis et al. However, before amendment, Claims 14 and 30, like Claim 7, recited "means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the means for enabling a defined interaction with a host computing device." (Claims 14 and 30 have been amended, like Claim 7, to simplify a recitation of the target means.) Therefore, Applicants submit that Claims 14 and 30, like Claim 7, are allowable. Further, Claims 15-18, which each depend upon Claim 14, are therefore allowable as dependent on an allowable claim. Additionally, new Claims 39-45, which each depend upon one of Claims 15-17 either directly or indirectly, are also allowable as dependent on an allowable claim.

Claim 31 recites "[f]or use in a peripheral device adapted for communication with a host computing device, performance of one or more security operations on data, and interaction with a host computing device in a defined way, a method comprising the steps of: receiving a request from a host computing device for information regarding the type of the peripheral device; and providing to the host computing device, in response to the request, information regarding the type of the defined interaction (emphasis added). The above-emphasized part of Claim 31 recites functionality similar to that of allowable Claims 7, 13, 14 and 30. Therefore, Applicants submit that Claim 31 is allowable.

As amended, Claim 32 recites "[f]or use in a peripheral device adapted for communication with a host computing device, performance of one or more security operations on data, and interaction with a host computing device in a defined way, a method comprising the steps of: communicating with the host computing device to exchange data between the host computing device and the peripheral device; performing one or more security operations and the defined interaction on the exchanged data; and mediating communication of the exchanged data between the host computing device and the peripheral device so that the exchanged data must first pass through means for performing the one or more security operations" (emphasis added). The above-emphasized part of Claim 32 recites functionality similar to that of allowable Claims 6, 8 and 29. Therefore, Applicants submit that Claim 32 is allowable.

Claims 1, 19, 21, 24, 27 and 28 have been canceled, thereby obviating the rejections of those claims.

In view of the foregoing, Applicants submit that Claims 2-18, 20, 22, 23, 25, 26 and 29-41 are in condition for allowance.

CONCLUSION

Claims 1-32 were pending. Claims 2, 3, 5, 9, 10, 12, 15, 16, 18-23 and 27 were not examined, since directed to species that were not provisionally elected for examination by the Examiner. Claims 1, 4, 8, 11, 14, 17, 24-26 and 28-32 were rejected. Claims 6, 7 and 13 were objected to. Claims 1, 19, 21, 24, 27 and 28 have been canceled. Claims 2-7, 13, 14, 20, 22, 23, 25, 26, 30 and 32 have been amended. Claims 33-45 have been added. In view of the foregoing, it is requested that Claims 2-18, 20, 22, 23, 25, 26 and 29-45 be allowed. If the Examiner wishes to discuss any aspect of this application, the Examiner is invited to telephone Applicants' undersigned attorney at (408) 945-9912.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on March 11, 1999.

3-11-99 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants

Hua 8/869,305 GAU2785

Attorney Docket No.: SPY-004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

March 12, 1999

Assistant Commissioner for Patents
Washington, D.C. 20231

Re: Applicants: William P. Bialick et al.
Assignee: Spyrus, Inc.
Title: Peripheral Device With Integrated Security Functionality
Serial No.: 08/869,305
Filed: June 4, 1997
Examiner: L. Hua
Group Art Unit: 2785

A

Transmitted herewith are the following documents in the above-identified application:

(1) Supplemental Response to Office Action (3 pages); and
(2) Return receipt postcard.

The fee is calculated as follows (small entity status is claimed):

CLAIMS AS AMENDED

	Claims After Amendment		Highest Number Paid For		Additional Claims		Rate		Fee
Total Claims:	39	-	39	=	0	X	$9	=	$ 0.00
Independent Claims:	9	-	12	=	0	X	$38	=	$ 0.00
___ First filing of one or more multiple dependent claims ($270 total fee)									$ 0.00
___ Fee for Petition for Extension of Time (___ months)									$ 0.00
TOTAL FEE:									**$ 0.00**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on March 12, 1999.

3-12-99 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants
1337 Chewpon Ave.
Milpitas, CA 95035
Tel. No.: (408) 945-9912

#8/B

4/1/99

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: William P. Bialick et al.

Assignee: Spyrus, Inc.

Title: Peripheral Device With Integrated Security Functionality

Serial No.: 08/869,305 Filed: June 4, 1997

Examiner: L. Hua Group Art Unit: 2785

Attorney Docket No.: SPY-004

Milpitas, California
March 12, 1999

Assistant Commissioner for Patents
Washington, D.C. 20231

SUPPLEMENTAL RESPONSE TO OFFICE ACTION

Sir:

Please enter the following supplemental response to the Office Action dated December 11, 1998, in the above-identified application. A Response to Office Action was previously submitted by Applicants on March 11, 1999 (hereinafter, the "previous Office Action response"), responding to that Office Action.

IN THE CLAIMS

Please amend the claims as follows:

B1

23~~13~~. (Twice Amended) A peripheral device [as in Claim 8], [further] comprising:

security means for enabling one or more security operations to be performed on data;

B1

target means for enabling a defined interaction with a host computing device;

means for enabling communication between the security means and the target means;

means for enabling communication with a host computing device;

means for mediating communication of data between the host computing device and the target means so that the communicated data must first pass through the security means; and

means for providing to a host computing device, in response to a request from the host computing device for information regarding the type of the peripheral device, information regarding the function of the target means.

REMARKS

In the previous Office Action response, Applicants stated that Claim 13 had been rewritten in independent form to include the limitations of the base claim and any intervening claims and was, therefore, in condition for allowance. However, Claim 13 was inadvertently not amended in that way in the previous Office Action response. Claim 13 has been amended herein as indicated above.

Claims 2-18, 20, 22, 23, 25, 26 and 29-45 are pending. Allowance of Claims 2-18, 20, 22, 23, 25, 26 and 29-45 is requested. If the Examiner wishes to discuss any aspect of this application, the Examiner is invited to telephone Applicants' undersigned attorney at (408) 945-9912.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on March 12, 1999.

3-12-99 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants

GAU 2785

#9

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: William P. Bialick et al.

Assignee: Spyrus, Inc.

Title: Peripheral Device With Integrated Security Functionality

Serial No.: 08/869,305 Filed: June 4, 1997

Examiner: L. Hua Group Art Unit: 2785

Attorney Docket No.: SPY-004

Milpitas, California
March 24, 1999

Assistant Commissioner for Patents
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT
WITH CERTIFICATION UNDER 37 C.F.R. §1.97(e)(2)

Sir:

Pursuant to 37 C.F.R. § 1.56, § 1.97 and § 1.98, Applicants bring the documents (copies enclosed) listed on the enclosed Form PTO-1449 to the Examiner's attention in the above-identified application. Citation of these documents shall not be construed as an admission that the documents are necessarily prior art with respect to the instant invention. Also, citation of these documents shall not be construed as an admission that the information disclosed therein is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

The undersigned hereby certifies in accordance with 37 CFR §1.97(e)(2) that no item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to the knowledge of the person signing the certification after making reasonable inquiry, was known to any individual designated in §1.56(c) more than three months prior to the filing of this information disclosure statement.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on March 24, 1999.

3-24-99 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants

part of #9

SHEET 1 OF 1

U.S. DEPT OF COMMERCE - PATENT AND TRADEMARK OFFICE INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	ATTORNEY DOCKET NO.: SPY-004 | SERIAL NO.: 08/869,305 APPLICANTS: William P. Bialick et al. FILING DATE: June 4, 1997 | GROUP ART UNIT: 2785

U.S. PATENTS

EXAMINER'S INITIALS	PATENT NUMBER	ISSUE DATE	INVENTOR(S)	CLASS	SUB-CLASS	FILING DATE
LVH	5,694,335	12/2/97	Hollenberg	364	514	3/12/96
LVH	5,297,206	3/22/94	Orton	380	30	10/7/92

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	DOCUMENT NUMBER	PUBLICATION DATE	NAME(S)	COUNTRY	TRANSLATION? YES	TRANSLATION? NO

COMMONLY OWNED, CO-PENDING U.S. PATENT APPLICATIONS

EXAMINER'S INITIALS	SERIAL NUMBER	ATTORNEY DOCKET NO.	APPLICANT(S)	CLASS	SUB-CLASS	FILING DATE

OTHER DOCUMENTS

EXAMINER'S INITIALS	AUTHOR(S), TITLE, DATE, PERTINENT PAGES, ETC.

EXAMINER: Ly V. Hua

DATE CONSIDERED: 6/2/1999

Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

BEST COPY

08/869,305

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
08/869,305	06/04/97	BIALICK	

EXAMINER
SPY-004

LM21/0607

DAVID R GRAHAM
1337 CHEWPON AVENUE
MILPITAS CA 95035

ART UNIT	PAPER NUMBER
HUA, L	10

DATE MAILED: 2785

06/07/99

This is a communication from the examiner in charge of your application.
COMMISSIONER OF PATENTS AND TRADEMARKS

NOTICE OF ALLOWABILITY

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance and Issue Fee Due or other appropriate communication will be mailed in due course.

☑ This communication is responsive to Applicant's correspondence filed on March 15, 18, 3 1999.

☑ The allowed claim(s) is/are 2-18, 20, 22, 23, 25, 26, and 29-45.

□ The drawings filed on ______________ are acceptable.

□ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

□ All □ Some* □ None of the CERTIFIED copies of the priority documents have been

□ received.

□ received in Application No. (Series Code/Serial Number) ______________.

□ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______________.

□ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

A SHORTENED STATUTORY PERIOD FOR RESPONSE to comply with the requirements noted below is set to EXPIRE THREE MONTHS FROM THE "DATE MAILED" of this Office action. Failure to timely comply will result in ABANDONMENT of this application. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

□ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION, PTO-152, which discloses that the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.

☑ Applicant MUST submit NEW FORMAL DRAWINGS

☑ because the originally filed drawings were declared by applicant to be informal.

□ including changes required by the Notice of Draftperson's Patent Drawing Review, PTO-948, attached hereto or to Paper No. ____.

□ including changes required by the proposed drawing correction filed on ______________, which has been approved by the examiner.

□ including changes required by the attached Examiner's Amendment/Comment.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the reverse side of the drawings. The drawings should be filed as a separate paper with a transmittal letter addressed to the Official Draftperson.

□ Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Any response to this letter should include, in the upper right hand corner, the APPLICATION NUMBER (SERIES CODE/SERIAL NUMBER). If applicant has received a Notice of Allowance and Issue Fee Due, the ISSUE BATCH NUMBER and DATE of the NOTICE OF ALLOWANCE should also be included.

Attachment(s)

□ Notice of References Cited, PTO-892

☑ Information Disclosure Statement(s), PTO-1449, Paper No(s). 9

□ Notice of Draftsperson's Patent Drawing Review, PTO-948

□ Notice of Informal Patent Application, PTO-152

□ Interview Summary, PTO-413

□ Examiner's Amendment/Comment

□ Examiner's Comment Regarding Requirement for Deposit of Biological Material

Examiner's Statement of Reasons for Allowance

LY V. HUA
PRIMARY EXAMINER

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

NOTICE OF ALLOWANCE AND ISSUE FEE DUE

[illegible]

[illegible]
[illegible]
[illegible]

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT		DATE MAILED
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
First Named Applicant	[illegible]		[illegible]		

TITLE OF INVENTION [illegible]

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
[illegible]	[illegible]	[illegible]	[illegible]	YES	$605.00	[illegible]

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED.

THE ISSUE FEE MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED.

HOW TO RESPOND TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.
If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is changed, pay twice the amount of the FEE DUE shown above and notify the Patent and Trademark Office of the change in status, or

B. If the status is the same, pay the FEE DUE shown above.

If the SMALL ENTITY is shown as NO:

A. Pay FEE DUE shown above, or

B. File verified statement of Small Entity Status before, or with, payment of 1/2 the FEE DUE shown above.

II. Part B-Issue Fee Transmittal should be completed and returned to the Patent and Trademark Office (PTO) with your ISSUE FEE. Even if the ISSUE FEE has already been paid by charge to deposit account, Part B Issue Fee Transmittal should be completed and returned. If you are charging the ISSUE FEE to your deposit account, section "4b" of Part B-Issue Fee Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give application number and batch number. Please direct all communications prior to issuance to Box ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PATENT AND TRADEMARK OFFICE COPY

2160
2785

B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: William P. Bialick et al.

Assignee: Spyrus, Inc.

Title: Peripheral Device With Integrated Security Functionality

Serial No.: 08/869,305 Filed: June 4, 1997

Examiner: L. Hua Group Art Unit: 2785

Batch No.: U04 Allowed: June 7, 1999

Attorney Docket No.: SPY-004

Milpitas, California
June 16, 1999

Box Issue Fee
Assistant Commissioner for Patents
Washington, D.C. 20231

SUBMISSION OF FORMAL DRAWINGS

Sir:

In a Notice of Allowability dated June 7, 1999, in the above-identified application, Applicants were required to submit formal drawings. Applicants submit herewith nine (9) sheets of formal drawings consisting of FIGS. 1, 2, 3A, 3B, 4, 5, 6, 7, 8, 9A and 9B. The Official Draftsperson is requested to telephone Applicants' undersigned attorney at (408) 945-9912 if there are any questions or problems with the enclosed formal drawings.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on June 16, 1999.

6-16-99 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants

6088802

1/9

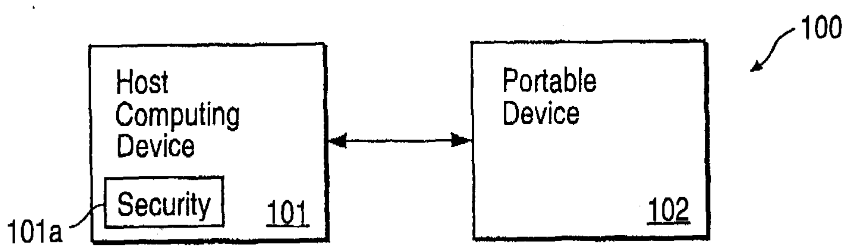


FIG. 1
(PRIOR ART)

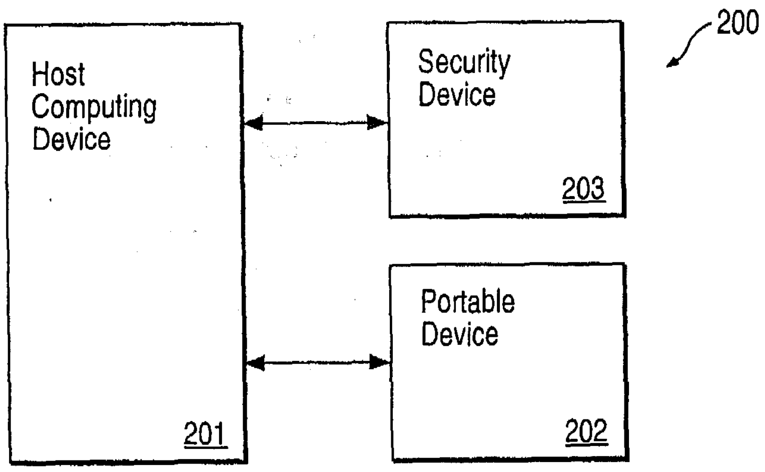


FIG. 2
(PRIOR ART)

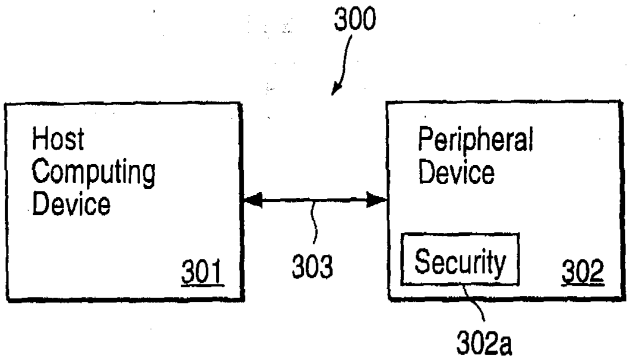

300
Host Computing Device
301
303
Peripheral Device
Security
302
302a

FIG. 3A

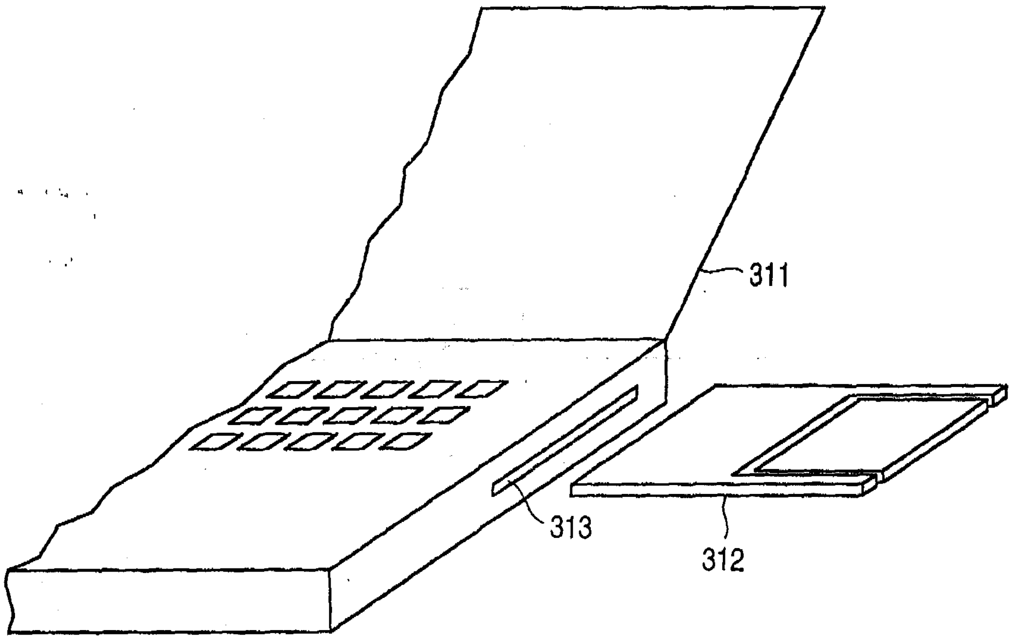

311
313
312

FIG. 3B

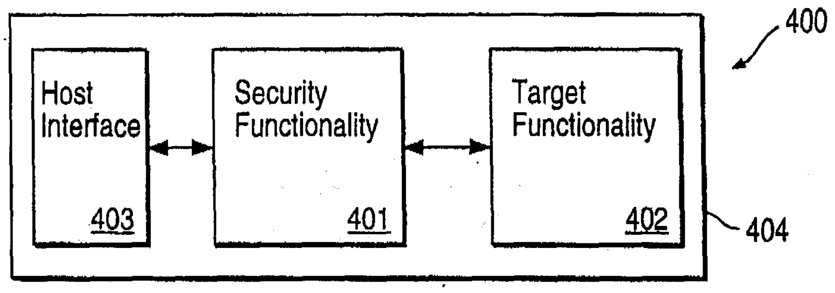

400
Host Interface
403
Security Functionality
401
Target Functionality
402
404

FIG. 4

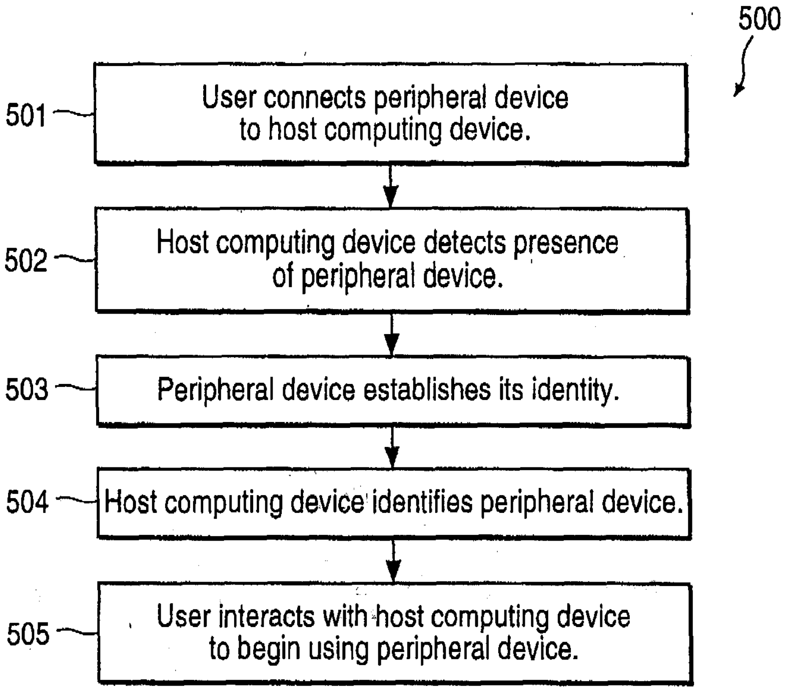

500
501
User connects peripheral device to host computing device.
502
Host computing device detects presence of peripheral device.
503
Peripheral device establishes its identity.
504
Host computing device identifies peripheral device.
505
User interacts with host computing device to begin using peripheral device.

FIG. 5

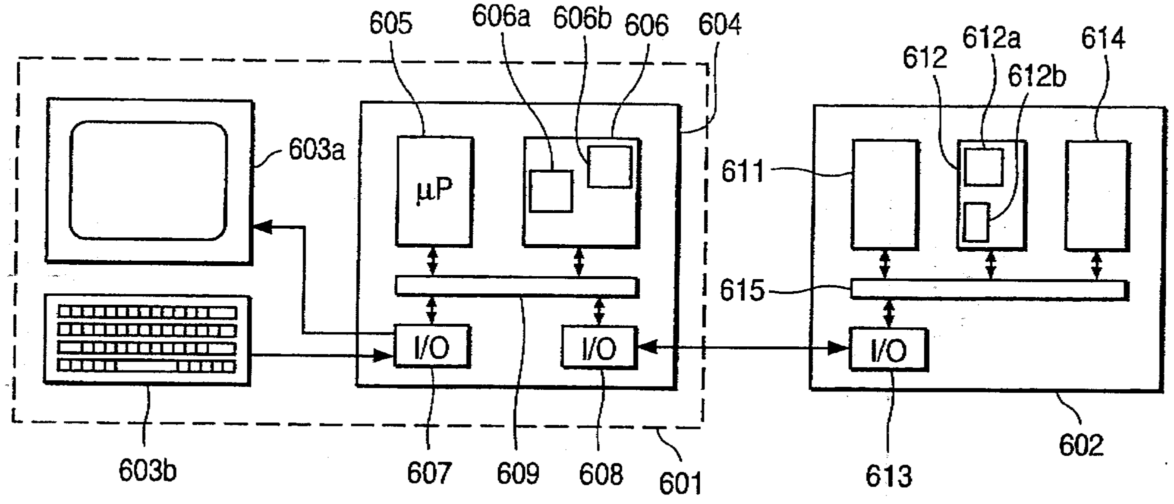

605
606a
606b
606
604
603a
µP
I/O
I/O
603b
607
609
608
601
612
612a
612b
614
611
615
I/O
602
613

FIG. 6

FIG. 7

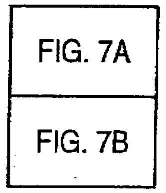
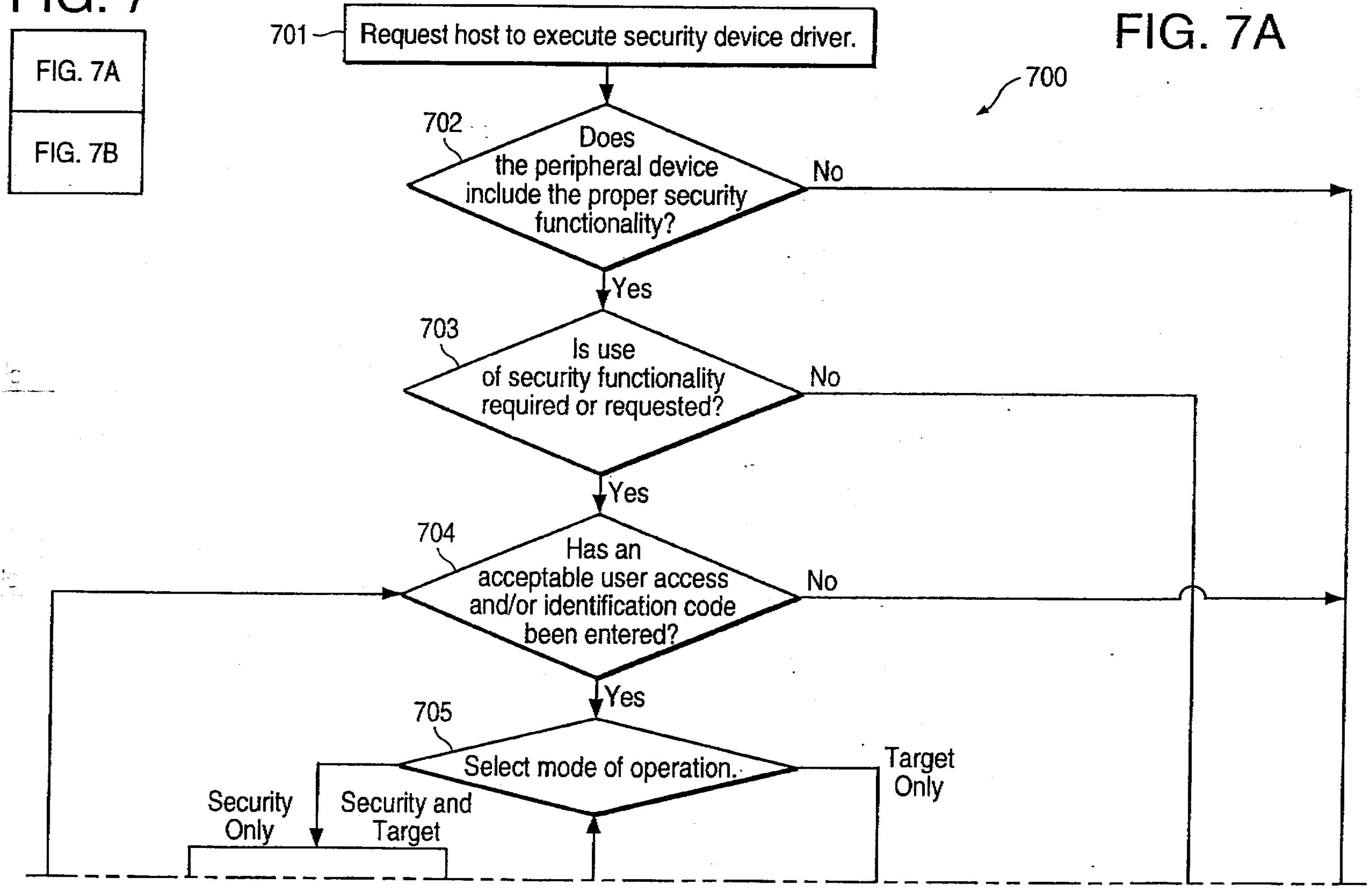


FIG. 7A
FIG. 7B

FIG. 7A


700
701
Request host to execute security device driver.
702
Does the peripheral device include the proper security functionality?
No
Yes
703
Is use of security functionality required or requested?
No
Yes
704
Has an acceptable user access and/or identification code been entered?
No
Yes
705
Select mode of operation.
Target Only
Security and Target
Security Only

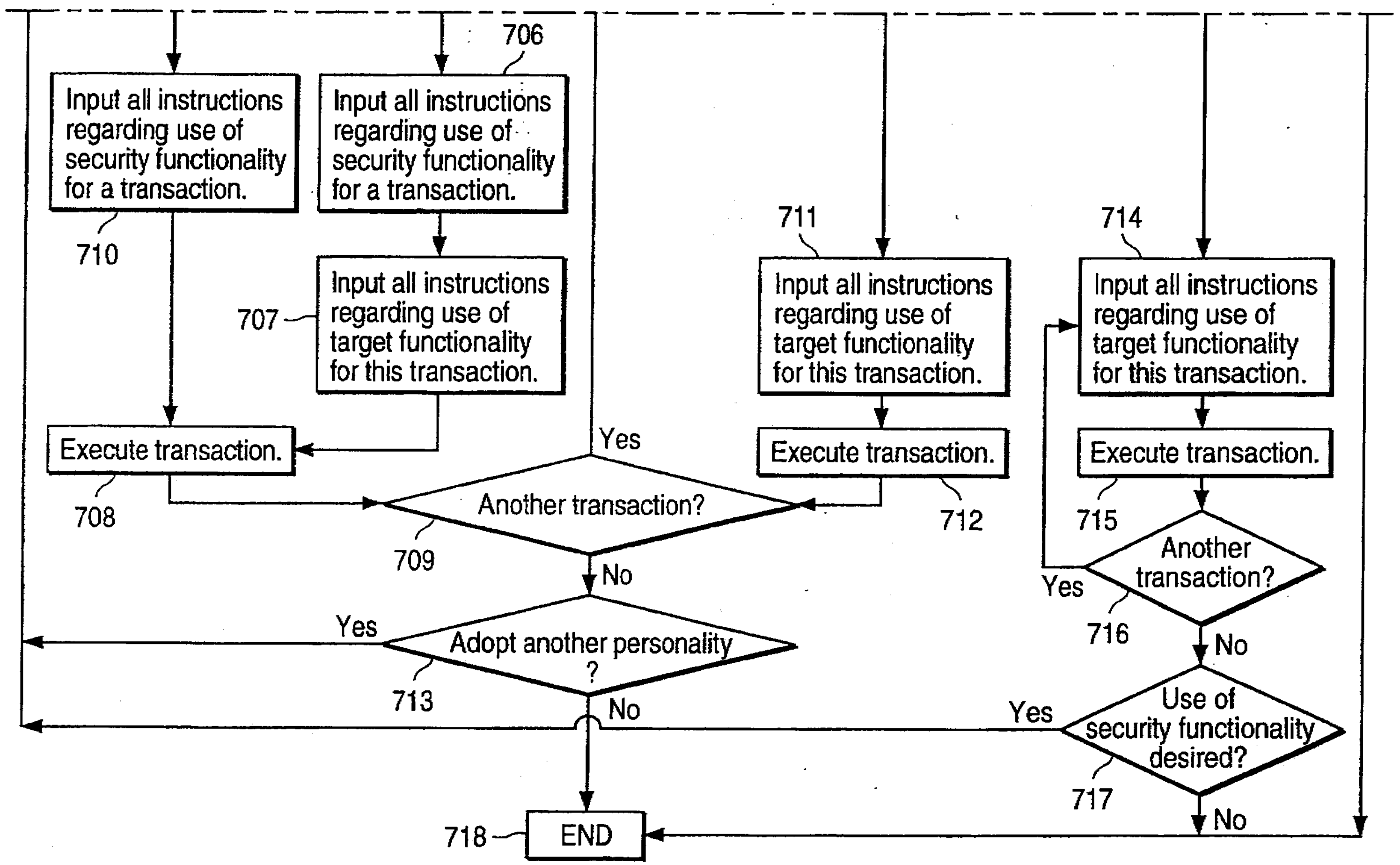

706
Input all instructions regarding use of security functionality for a transaction.
707
Input all instructions regarding use of target functionality for this transaction.
710
Input all instructions regarding use of security functionality for a transaction.
708
Execute transaction.
709
Another transaction?
Yes
No
713
Adopt another personality ?
Yes
No
711
Input all instructions regarding use of target functionality for this transaction.
712
Execute transaction.
714
Input all instructions regarding use of target functionality for this transaction.
715
Execute transaction.
716
Another transaction?
Yes
No
717
Use of security functionality desired?
Yes
No
718
END

FIG. 7B

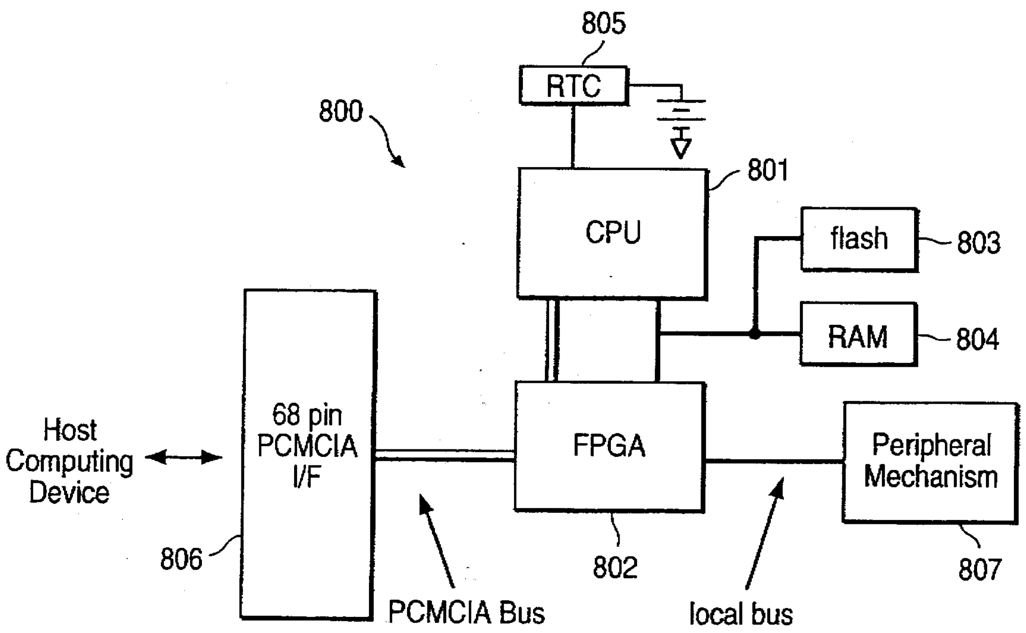

805
RTC
800
801
CPU
flash
803
RAM
804
Host
Computing
Device
68 pin
PCMCIA
I/F
FPGA
Peripheral
Mechanism
806
PCMCIA Bus
802
local bus
807

FIG. 8

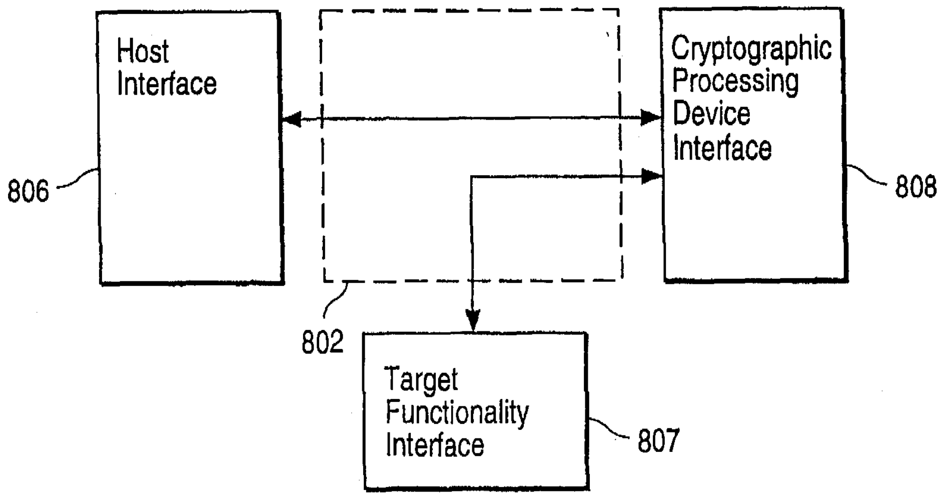

Host Interface
806
Cryptographic Processing Device Interface
808
802
Target Functionality Interface
807

FIG. 9A

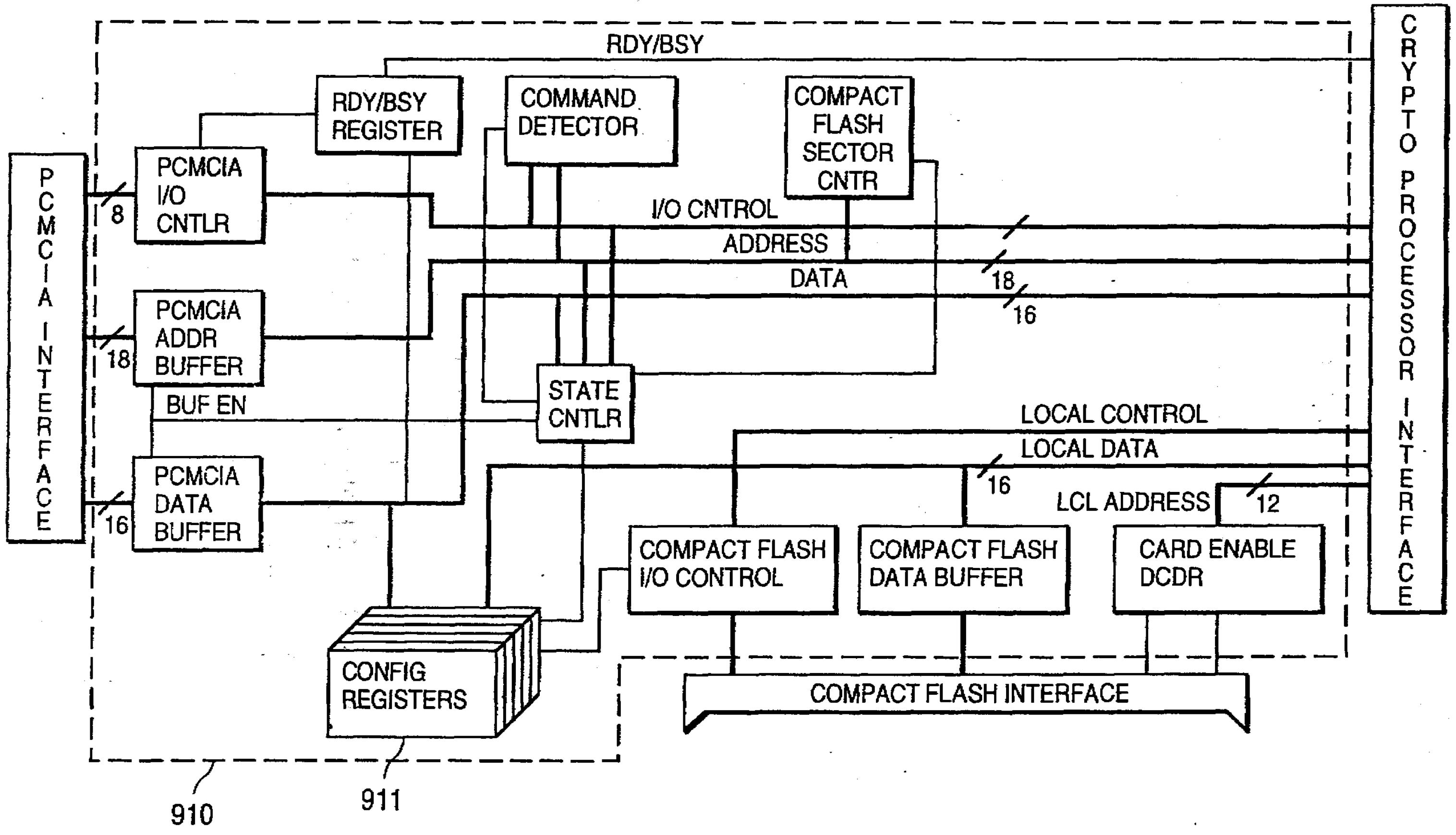

RDY/BSY
RDY/BSY REGISTER
COMMAND DETECTOR
COMPACT FLASH SECTOR CNTR
PCMCIA INTERFACE
PCMCIA I/O CNTLR
PCMCIA ADDR BUFFER
BUF EN
PCMCIA DATA BUFFER
8
18
16
I/O CNTROL
ADDRESS
DATA
18
16
STATE CNTLR
LOCAL CONTROL
LOCAL DATA
16
LCL ADDRESS
12
CRYPTO PROCESSOR INTERFACE
COMPACT FLASH I/O CONTROL
COMPACT FLASH DATA BUFFER
CARD ENABLE DCDR
CONFIG REGISTERS
COMPACT FLASH INTERFACE
910
911

FIG. 9B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	William P. Bialick et al.		
Assignee:	Spyrus, Inc.		
Title:	Peripheral Device With Integrated Security Functionality		
Serial No.:	08/869,305	Filed:	June 4, 1997
Examiner:	L. Hua	Group Art Unit:	2785
Batch No.:	U04	Allowed:	June 7, 1999
Attorney Docket No.:	SPY-004		

Milpitas, California
September 7, 1999

Box Issue Fee
Assistant Commissioner for Patents
Washington, D.C. 20231

PETITION UNDER 37 C.F.R. § 1.97(d)(2)

Sir:

In view of the allowed status of the above-referenced application, pursuant to 37 C.F.R. § 1.97(d)(2), Applicants hereby request consideration of the accompanying Information Disclosure Statement. Enclosed is a check (Check No. 1461) for $130.00 for the petition fee under 37 C.F.R. § 1.17(i). This Petition is being submitted in duplicate.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on September 7, 1999.

9-7-99 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants

B#

#11

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	William P. Bialick et al.		
Assignee:	Spyrus, Inc.		
Title:	Peripheral Device With Integrated Security Functionality		
Serial No.:	08/869,305	Filed:	June 4, 1997
Examiner:	L. Hua	Group Art Unit:	2785
Batch No.:	U04	Allowed:	June 7, 1999
Attorney Docket No.:	SPY-004		

Milpitas, California
September 7, 1999

Box Issue Fee
Assistant Commissioner for Patents
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT
WITH CERTIFICATION UNDER 37 C.F.R. §1.97(e)(2)

Sir:

Pursuant to 37 C.F.R. § 1.56, § 1.97 and § 1.98, Applicants bring the documents (copies enclosed) listed on the enclosed Form PTO-1449 to the Examiner's attention in the above-identified application. Citation of these documents shall not be construed as an admission that the documents are necessarily prior art with respect to the instant invention. Also, citation of these documents shall not be construed as an admission that the information disclosed therein is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

The undersigned hereby certifies in accordance with 37 CFR §1.97(e)(2) that no item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to the knowledge of the person signing the certification after making reasonable inquiry, was known to any individual designated in §1.56(c) more than three months prior to the filing of this information disclosure statement, except for U.S. Patent No. 4,709,136 to Watanabe.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on September 7, 1999.

9-7-99 David R. Graham
Date Signature

Respectfully submitted
and certified by,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants

1 OF 1

U.S. DEPT OF COMMERCE - PATENT AND TRADEMARK OFFICE INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	ATTORNEY DOCKET NO.: SPY-004	SERIAL NO.: 08/869,305
	APPLICANTS: William P. Bialick et al.	
	FILING DATE: June 4, 1997	GROUP ART UNIT: 2785

U.S. PATENTS

EXAMINER'S INITIALS	PATENT NUMBER	ISSUE DATE	INVENTOR(S)	CLASS	SUB-CLASS	FILING DATE
LVH	4,709,136	11/24/87	Watanabe	235	379	06/03/86
LVH	5,878,142	3/2/99	Caputo et al.	380	25	6/10/96
LVH	5,790,674	8/4/98	Houvener et al.	380	23	7/19/96
LVH	5,610,981	3/11/97	Mooney et al.	380	25	2/28/95
LVH	5,524,134	6/4/96	Gustafson et al.	379	58	4/28/94
LVH	5,828,832	10/27/98	Holden et al.	395	187.01	7/30/96
LVH	5,640,302	6/17/97	Kikinis	361	687	3/11/96

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	DOCUMENT NUMBER	PUBLICATION DATE	NAME(S)	JURISDICTION	TRANSLATION? YES	TRANSLATION? NO

OTHER DOCUMENTS

EXAMINER'S INITIALS	AUTHOR(S), TITLE, PUBLICATION, DATE, PERTINENT PAGES, ETC.

EXAMINER: Ly V. Hua

DATE CONSIDERED: 12/14/99

Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

BEST COPY

PART B—ISSUE FEE TRANSMI

Complete and mail this form, together wi.. applicable fees, to:

Box ISSUE FEE
Assistant Commissioner for Patents
Washington, D.C. 20231

B8

MAILING INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE. Blocks 1 through 4 should be completed where appropriate. All further correspondence including the Issue Fee Receipt, the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Legibly mark-up with any corrections or use Block 1)

LM21/0607

DAVID R GRAHAM
1337 CHEWPON AVENUE
MILPITAS CA 95035

Note: The certificate of mailing below can only be used for domestic mailings of the Issue Fee Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing.

Certificate of Mailing

I hereby certify that this Issue Fee Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Box Issue Fee address above on the date indicated below.

David R. Graham (Depositor's name)
David R. Graham (Signature)
September 7, 1999 (Date)

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT		DATE MAILED
08/869,305	06/04/97	039	HUA, L	2785	06/07/99

First Named Applicant: BIALICK, 35 USC 154(b) term ext. = 0 Days.

TITLE OF INVENTION: PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2 SPY-004	713-200.000	U04	UTILITY	YES	$605.00	09/07/99

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363). Use of PTO form(s) and Customer Number are recommended, but not required.

   □ Change of correspondence address (or Change of Correspondance Address form PTO/SB/122) attached.

   □ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47) attached.

2. For printing on the patent front page, list (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

   1 David R.Graham
   2 ____________
   3 ____________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)
   PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. Inclusion of assignee data is only appropiate when an assignment has been previously submitted to the PTO or is being submitted under separate cover. Completion of this form is NOT a subsititue for filing an assignment.

   (A) NAME OF ASSIGNEE Spyrus, Inc.

   (B) RESIDENCE: (CITY & STATE OR COUNTRY) Santa Clara, California

   Please check the appropriate assignee category indicated below (will not be printed on the patent)
   □ individual ☒ corporation or other private group entity □ government

4a. The following fees are enclosed (make check payable to Commissioner of Patents and Trademarks):
   ☒ Issue Fee
   ☒ Advance Order - # of Copies 10

4b. The following fees or deficiency in these fees should be charged to:
   DEPOSIT ACCOUNT NUMBER 50-0840
   (ENCLOSE AN EXTRA COPY OF THIS FORM)
   □ Issue Fee
   □ Advance Order - # of Copies ____________

The COMMISSIONER OF PATENTS AND TRADEMARKS IS requested to apply the Issue Fee to the application identified above.

(Authorized Signature) David R. Graham (Date) 9-7-99

NOTE: The Issue Fee will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the Patent and Trademark Office.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending on the needs of the individual case. Any comments on the amount of time required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND FEES AND THIS FORM TO: Box Issue Fee, Assistant Commissioner for Patents, Washington D.C. 20231

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES L /ARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/869,305	06/04/97	BIALICK W	SPY-004

LM21/1216

DAVID R GRAHAM
1337 CHEWPON AVENUE
MILPITAS CA 95035

EXAMINER	
HUA,L	
ART UNIT	PAPER NUMBER
2785	12

DATE MAILED: 12/16/99

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

Commissioner of Patents and Trademarks

08/869,305

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR		ATTORNEY DOCKET NO.
08/869,305	06/04/97	BIALICK	W	SPY-004

LM21/1216

DAVID R GRAHAM
1337 CHEWPON AVENUE
MILPITAS CA 95035

EXAMINER	
HUA, L	
ART UNIT	PAPER NUMBER
2785	12

DATE MAILED: 12/16/99

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

Commissioner of Patents and Trademarks

The Examiner hereby informs the Applicant(s) that the Information Disclosure Statement Under 37 C.F.R. 1.97(c) (1) filed on September 13, 1999, has been received, (i) matched up with its associated Application No. 08/869,305 after the Notice of Allowance (mailed on June 7, 1999, and (ii) entered. The references have been considered by the Examiner as indicated in the copy of initialed Form PTO-1449 attached herewith.

Attachement: **Form PTO-1449**

Ly V. Hua
Patent Examiner
Art Unit 2785

L. Hua
December 14, 1999

File History Content Report

The following content is missing from the original file history record obtained from the United States Patent and Trademark Office. No additional information is available.

Document Date - 1999-12-16

Document Title - List of References cited by applicant and considered by examiner

File History Content Report

The following content is missing from the original file history record obtained from the United States Patent and Trademark Office. No additional information is available.

Document Date - 2000-07-11

Document Title - USPTO Grant

Electronic Acknowledgement Receipt

EFS ID:	21563316
Application Number:	08869305
International Application Number:	
Confirmation Number:	5587
Title of Invention:	PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY
First Named Inventor/Applicant Name:	WILLIAM P. BIALICK
Customer Number:	23676
Filer:	Robert Rose
Filer Authorized By:	
Attorney Docket Number:	18835
Receipt Date:	21-FEB-2015
Filing Date:	04-JUN-1997
Time Stamp:	15:22:00
Application Type:	Utility under 35 USC 111(a)

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	Assignee showing of ownership per 37 CFR 3.73.	373-6088802.pdf	1224058 43a925d4522ebef618113b2d070fd0a12267fd59	no	1

Warnings:

Information:

2	Power of Attorney	SPEX-SB80.pdf	902057 bafb837024dda0592e2767f220b33bdc7463ed4f	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	2126115		

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.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: SPEX TECHNOLOGIES

Application No./Patent No.: 6088802 Filed/Issue Date: 07/11/2000

Titled: PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY

SPEX Techologies, Inc.. , a corporation
(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: BIALICK, et al. To: Spyrus, Inc.
The document was recorded in the United States Patent and Trademark Office at
Reel 008942 , Frame 0204 , or for which a copy thereof is attached.

2. From: Spyrus, Inc. To: SPEX Technologies, Inc.
The document was recorded in the United States Patent and Trademark Office at
Reel 034971 , Frame 0298 , or for which a copy thereof is attached.

3. From: ____________ To: ____________
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.

Robert Rose
Signature

02/19/2015
Date

Robert Rose
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.

PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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: 103677

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: 103677

OR

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

Assignee Name and Address:

SPEX Technologies, Inc.
1860 HARTOG DRIVE
SAN JOSE CA 95131

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	2/19/2015
Name	Tom Hakel	Telephone	(408) 392-9131
Title	President		

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 1.11 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.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
PO Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
08/869,305	06/04/1997	WILLIAM P. BIALICK	

CONFIRMATION NO. 5587

POA ACCEPTANCE LETTER

OC000000073704553

103677
Law Office of Robert J. Rose
PO Box 4341
Diamond Bar, CA 91765

Date Mailed: 03/02/2015

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

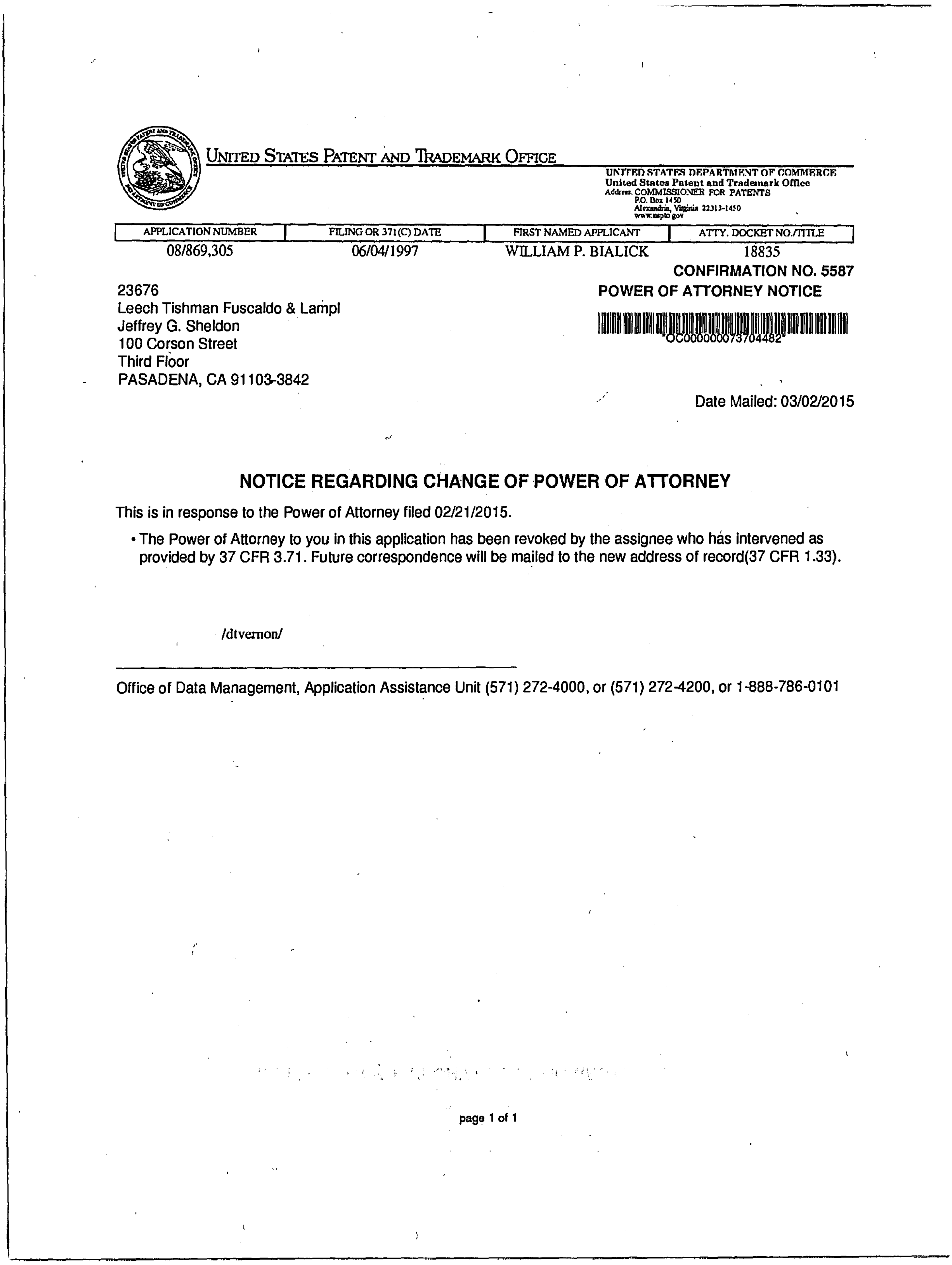
This is in response to the Power of Attorney filed 02/21/2015.

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.

/dtvernon/

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

page 1 of 1



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
08/869,305	06/04/1997	WILLIAM P. BIALICK	18835

CONFIRMATION NO. 5587

POWER OF ATTORNEY NOTICE

OC000000073704482

23676
Leech Tishman Fuscaldo & Lampl
Jeffrey G. Sheldon
100 Corson Street
Third Floor
PASADENA, CA 91103-3842

Date Mailed: 03/02/2015

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/21/2015.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/dtvernon/

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

page 1 of 1

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE** **FILING OR DETERMINATION OF AN** **ACTION REGARDING A PATENT OR** **TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Central District of California on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 8:16-cv-01790	DATE FILED 9/27/2016	U.S. DISTRICT COURT Central District of California
PLAINTIFF SPEX Technologies, Inc.		DEFENDANT Kingston Technology Corporation, et al.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,088,802	7/11/2000	SPEX Technologies, Inc.
2 6,003,135	12/14/1999	SPEX Technologies, Inc.
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

BEST COPY

7 sheets

PATENT APPLICATION FEE DETERMINATION RECORD Effective October 1, 1997	Application or Docket Number

CLAIMS AS FILED - PART I

FOR	(Column 1) NUMBER FILED		(Column 2) NUMBER EXTRA	SMALL ENTITY TYPE □ RATE	FEE	OR	OTHER THAN SMALL ENTITY RATE	FEE
BASIC FEE					395.00	OR		790.00
TOTAL CLAIMS	32	minus 20 =	* 12	x$11=		OR	x$22=	264
INDEPENDENT CLAIMS	12	minus 3 =	* 9	x41=		OR	x82=	738
MULTIPLE DEPENDENT CLAIM PRESENT				+135=		OR	+270=	
				TOTAL		OR	TOTAL	1792

* If the difference in column 1 is less than zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

AMENDMENT A	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE	ADDITIONAL FEE	OR	OTHER THAN SMALL ENTITY RATE	ADDITIONAL FEE
Total	* 39	Minus	** 32	= 7	x$~~11~~9=	63	OR	x$22=	
Independent	* 8	Minus	***	=	x41=		OR	x82=	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+135=		OR	+270=	
					TOTAL ADDIT. FEE	63	OR	TOTAL ADDIT. FEE	

AMENDMENT B	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
Total	* 39	Minus	**	=	x$11=		OR	x$22=	
Independent	* 9	Minus	*** 12	= /	x41=		OR	x82=	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+135=		OR	+270=	
					TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
Total	*	Minus	**	=	x$11=		OR	x$22=	
Independent	*	Minus	***	=	x41=		OR	x82=	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+135=		OR	+270=	
					TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

THOMSON INNOVATION

Thomson Innovation Patent Export, 2016-10-03 04:50:04 -0500

Table of Contents

Family 1/1

4 record(s) per family

Record 1/4 WO1998055911A1 PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY | DISPOSITIF PERIPHERIQUE A FONCTIONS DE SECURITE INTEGREES

Publication Number: WO1998055911A1 19981210

Title: PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY | DISPOSITIF PERIPHERIQUE A FONCTIONS DE SECURITE INTEGREES

Title - DWPI: Peripheral device with integrated security functionality in which portable computing module communicates with host device, and includes security functionality which enables security operations to be performed on data stored in host computer

Priority Number: US1997869305A

Priority Date: 1997-06-04

Application Number: WO1998US11052A

Application Date: 1998-06-01

Publication Date: 1998-12-10

IPC Class Table:

IPC	Section	Class	Subclass	Class Group	Subgroup
G06F002100	G	G06	G06F	G06F0021	G06F002100

IPC Class Table - DWPI:

IPC - DWPI	Section - DWPI	Class - DWPI	Subclass - DWPI	Class Group - DWPI	Subgroup - DWPI
G06F000100	G	G06	G06F	G06F0001	G06F000100
G06K001467	G	G06	G06K	G06K0014	G06K001467

Assignee/Applicant: SPYRUS INC.,US

JP F Terms:

JP FI Codes:

Assignee - Original: SPYRUS INC.

Any CPC Table:

Type	Invention	Additional	Version	Office
Current	**G06F 21/34**	-	20130101	EP

ECLA: G06F002134

Abstract:

The invention enables a peripheral device to communicate with a host computing device to enable one or more security operations to be performed by the peripheral device on data stored within the host computing device, data provided from the host computing device to the peripheral device (which can then be, for example, stored in the peripheral device or transmitted to yet another device), or data retrieved by the host computing device from the peripheral device (e.g., data that has been stored in the peripheral device or transmitted to the peripheral device from another device). In particular, the peripheral device can be adapted to enable, in a single integral peripheral device, performance of one or more security operations on data, and a defined interaction with a host computing device that has not previously been integrated with security operations in a single integral device. The defined interactions can provide a variety of types of functionality (e.g., data storage, data communication, data input and output, user identification), as described further below. The peripheral device can also be implemented so that the security operations are performed in-line, i.e., the security operations are performed between the communication of data to or from the host computing device and the performance of the defined interaction. Moreover, the peripheral device can be implemented so that the security functionality of the peripheral device is transparent to the host computing device.

L'invention permet de faire communiquer un dispositif périphérique avec un ordinateur hôte et permet au dispositif périphérique d'effectuer une ou plusieurs opérations de sécurité: sur des données stockées dans l'ordinateur hôte, sur des données fournies par l'ordinateur hôte au dispositif périphérique (données qui peuvent par exemple être stockées ou être transférées sur un autre dispositif) ou sur des données récupérées par l'ordinateur hôte dans le dispositif périphérique (données qui peuvent par exemple avoir été stockées dans le dispositif périphérique ou y avoir été transférées depuis un autre dispositif). Le dispositif périphérique peut en particulier être adapté pour permettre d'assurer dans un unique périphérique monobloc l'exécution d'une ou plusieurs opérations de sécurité sur des données et permettre une interaction définie avec un ordinateur hôte n'ayant pas été intégré antérieurement aux opérations de sécurité d'un unique périphérique monobloc. Les interactions définies peuvent porter sur différents types de fonctions (par exemple stockage de données, entrée et sortie de données, identification de l'utilisateur)

telles que présentées plus loin. Le dispositif périphérique peut également être réalisé pour que les opérations de sécurité s'effectuent en ligne c.-à-d. entre la communication de données à destination ou en provenance de l'ordinateur hôte et l'exécution de l'interaction définie. De plus, le dispositif périphérique peut être réalisé pour que ses fonctions de sécurité soient transparentes vis à vis de l'ordinateur hôte.

Language of Publication: EN

INPADOC Legal Status Table:

<table>
<tr><th>Gazette Date</th><th>Code</th><th>INPADOC Legal Status Impact</th></tr>
<tr><td>2001-09-26</td><td>WWW</td><td>-</td></tr>
<tr><td colspan="3"><b>Description:</b> WIPO INFORMATION: WITHDRAWN IN NATIONAL OFFICE EP 1998926135</td></tr>
<tr><td>2000-12-04</td><td>NENP</td><td>-</td></tr>
<tr><td colspan="3"><b>Description:</b> NON-ENTRY INTO THE NATIONAL PHASE IN: CA</td></tr>
<tr><td>2000-04-06</td><td>REG</td><td>-</td></tr>
<tr><td colspan="3"><b>Description:</b> REFERENCE TO NATIONAL CODE DE 8642 IMPACT ABOLISHED FOR DE - I.E. PCT APPL. NOT ENT. GERMAN PHASE</td></tr>
<tr><td>2000-03-22</td><td>WWP</td><td>+</td></tr>
<tr><td colspan="3"><b>Description:</b> WIPO INFORMATION: PUBLISHED IN NATIONAL OFFICE EP 1998926135</td></tr>
<tr><td>2000-03-03</td><td>NENP</td><td>-</td></tr>
<tr><td colspan="3"><b>Description:</b> NON-ENTRY INTO THE NATIONAL PHASE IN: JP 1999502623</td></tr>
<tr><td>1999-12-24</td><td>WWE</td><td>+</td></tr>
<tr><td colspan="3"><b>Description:</b> WIPO INFORMATION: ENTRY INTO NATIONAL PHASE EP 1998926135</td></tr>
<tr><td>1999-04-21</td><td>121</td><td>-</td></tr>
<tr><td colspan="3"><b>Description:</b> EP: THE EPO HAS BEEN INFORMED BY WIPO THAT EP WAS DESIGNATED IN THIS APPLICATION</td></tr>
<tr><td>1999-03-04</td><td>DFPE</td><td>-</td></tr>
<tr><td colspan="3"><b>Description:</b> REQUEST FOR PRELIMINARY EXAMINATION FILED PRIOR TO EXPIRATION OF 19TH MONTH FROM PRIORITY DATE (PCT APPLICATION FILED BEFORE 20040101)</td></tr>
<tr><td>1998-12-10</td><td>AL</td><td>+</td></tr>
<tr><td colspan="3"></td></tr>
</table>

Description: DESIGNATED COUNTRIES FOR REGIONAL PATENTS WO 9855911 A1 GH; GM; KE; LS; MW; SD; SZ; UG; ZW; AM; AZ; BY; KG; KZ; MD; RU; TJ; TM; AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LU; MC; NL; PT; SE; BF; BJ; CF; CG; CI; CM; GA; GN; ML; MR; NE; SN; TD; TG		
1998-12-10	AK	+
Description: DESIGNATED STATES WO 9855911 A1 AL; AM; AT; AU; AZ; BA; BB; BG; BR; BY; CA; CH; CN; CU; CZ; DE; DK; EE; ES; FI; GB; GE; GH; GM; GW; HU; ID; IL; IS; JP; KE; KG; KP; KR; KZ; LC; LK; LR; LS; LT; LU; LV; MD; MG; MK; MN; MW; MX; NO; NZ; PL; PT; RO; RU; SD; SE; SG; SI; SK; SL; TJ; TM; TR; TT; UA; UG; UZ; VN; YU; ZW		

Post-Issuance (US):

Reassignment (US) Table:

Maintenance Status (US):

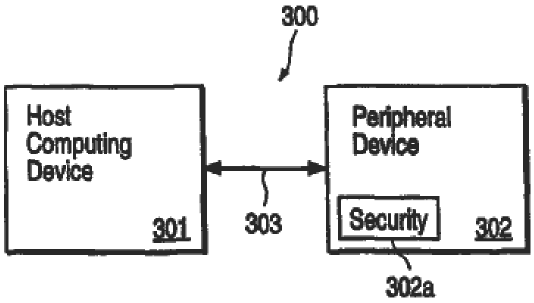
Litigation (US):

Opposition (EP):

License (EP):

EPO Procedural Status:

Front Page Drawing:



Assignee - Current US:

Record 2/4 AU199878042A Peripheral device with integrated security functionality

Publication Number: AU199878042A 19981221

Title: Peripheral device with integrated security functionality
Title - DWPI: Peripheral device with integrated security functionality in which portable computing module communicates with host device, and includes security functionality which enables security operations to be performed on data stored in host computer
Priority Number: US1997869305A | WO1998US11052A
Priority Date: 1997-06-04 | 1998-06-01
Application Number: AU199878042D
Application Date: 1998-06-01
Publication Date: 1998-12-21
IPC Class Table:

IPC	Section	Class	Subclass	Class Group	Subgroup
G06F002100	G	G06	G06F	G06F0021	G06F002100

IPC Class Table - DWPI:

IPC - DWPI	Section - DWPI	Class - DWPI	Subclass - DWPI	Class Group - DWPI	Subgroup - DWPI
G06F000100	G	G06	G06F	G06F0001	G06F000100
G06K001467	G	G06	G06K	G06K0014	G06K001467

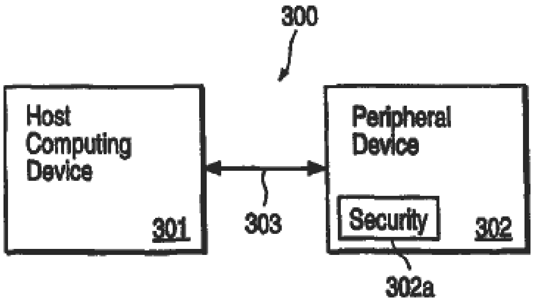
Assignee/Applicant: SPYRUS INC
JP F Terms:
JP FI Codes:
Assignee - Original:
Any CPC Table:

Type	Invention	Additional	Version	Office
Current	**G06F 21/34**	-	20130101	EP

ECLA: G06F002134
Abstract:
Language of Publication: EN
INPADOC Legal Status Table:

Gazette Date	Code	INPADOC Legal Status Impact
2000-02-17	MK6	-
Description: APPLICATION LAPSED SECTION 142(2)(F)/REG. 8.3(3) - PCT APPLIC. NOT ENTERING NATIONAL PHASE		

Post-Issuance (US):
Reassignment (US) Table:
Maintenance Status (US):
Litigation (US):
Opposition (EP):
License (EP):
EPO Procedural Status:
Front Page Drawing:



Assignee - Current US:

Record 3/4 EP986780A1 PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY | PERIPHERIEGERÄT MIT INTEGRIERTER SICHERHEITSFUNKTIONSFÄHIGKEIT | DISPOSITIF PERIPHERIQUE A FONCTIONS DE SECURITE INTEGREES

Publication Number: EP986780A1 20000322

Title: PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY | PERIPHERIEGERÄT MIT INTEGRIERTER SICHERHEITSFUNKTIONSFÄHIGKEIT | DISPOSITIF PERIPHERIQUE A FONCTIONS DE SECURITE INTEGREES
Title - DWPI: Peripheral device with integrated security functionality in which portable computing module communicates with host device, and includes security functionality which enables security operations to be performed on data stored in host computer
Priority Number: US1997869305A | WO1998US11052A
Priority Date: 1997-06-04 | 1998-06-01
Application Number: EP1998926135A
Application Date: 1998-06-01
Publication Date: 2000-03-22
IPC Class Table:

IPC	Section	Class	Subclass	Class Group	Subgroup
G06F002100	G	G06	G06F	G06F0021	G06F002100

IPC Class Table - DWPI:

IPC - DWPI	Section - DWPI	Class - DWPI	Subclass - DWPI	Class Group - DWPI	Subgroup - DWPI
G06F000100	G	G06	G06F	G06F0001	G06F000100
G06K001467	G	G06	G06K	G06K0014	G06K001467

Assignee/Applicant: Spyrus Inc.,San Jose, CA 95131,US,01935471
JP F Terms:
JP FI Codes:
Assignee - Original: Spyrus Inc.
Any CPC Table:

Type	Invention	Additional	Version	Office
Current	**G06F 21/34**	-	20130101	EP

ECLA: G06F002134
Abstract:

The invention enables a peripheral device to communicate with a host computing device to enable one or more security operations to be performed by the peripheral device on data stored within the

host computing device, data provided from the host computing device to the peripheral device (which can then be, for example, stored in the peripheral device or transmitted to yet another device), or data retrieved by the host computing device from the peripheral device (e.g., data that has been stored in the peripheral device or transmitted to the peripheral device from another device). In particular, the peripheral device can be adapted to enable, in a single integral peripheral device, performance of one or more security operations on data, and a defined interaction with a host computing device that has not previously been integrated with security operations in a single integral device. The defined interactions can provide a variety of types of functionality (e.g. , data storage, data communication, data input and output, user identification), as described further below. The peripheral device can also be implemented so that the security operations are performed in-line, i.e., the security operations are performed between the communication of data to or from the host computing device and the performance of the defined interaction. Moreover, the peripheral device can be implemented so that the security functionality of the peripheral device is transparent to the host computing device.

L'invention permet de faire communiquer un dispositif périphérique avec un ordinateur hôte et permet au dispositif périphérique d'effectuer une ou plusieurs opérations de sécurité: sur des données stockées dans l'ordinateur hôte, sur des données fournies par l'ordinateur hôte au dispositif périphérique (données qui peuvent par exemple être stockées ou être transférées sur un autre dispositif) ou sur des données récupérées par l'ordinateur hôte dans le dispositif périphérique (données qui peuvent par exemple avoir été stockées dans le dispositif périphérique ou y avoir été transférées depuis un autre dispositif). Le dispositif périphérique peut en particulier être adapté pour permettre d'assurer dans un unique périphérique monobloc l'exécution d'une ou plusieurs opérations de sécurité sur des données et permettre une interaction définie avec un ordinateur hôte n'ayant pas été intégré antérieurement aux opérations de sécurité d'un unique périphérique monobloc. Les interactions définies peuvent porter sur différents types de fonctions (par exemple stockage de données, entrée et sortie de données, identification de l'utilisateur) telles que présentées plus loin. Le dispositif périphérique peut également être réalisé pour que les opérations de sécurité s'effectuent en ligne c.-à-d. entre la communication de données à destination ou en provenance de l'ordinateur hôte et l'exécution de l'interaction définie. De plus, le dispositif périphérique peut être réalisé pour que ses fonctions de sécurité soient transparentes vis à vis de l'ordinateur hôte.

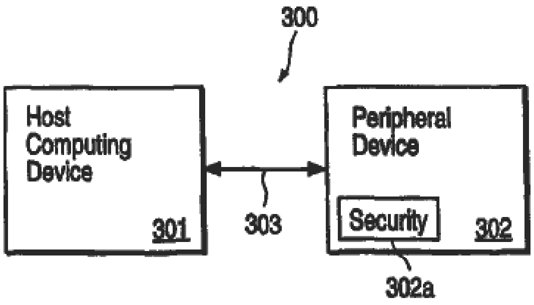
Language of Publication: EN

INPADOC Legal Status Table:

Gazette Date	Code	INPADOC Legal Status Impact
2002-06-05	18D	-
Description: DEEMED TO BE WITHDRAWN 2001-09-26		
2001-06-27	17Q	+
Description: FIRST EXAMINATION REPORT 2001-05-15		
2000-03-22	AK	+
Description: DESIGNATED CONTRACTING STATES: EP 0986780 A1 AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR;		

IE; IT; LI; LU; MC; NL; PT; SE		
2000-03-22	17P	+
Description: REQUEST FOR EXAMINATION FILED 1999-12-24		

Post-Issuance (US):
Reassignment (US) Table:
Maintenance Status (US):
Litigation (US):
Opposition (EP):
License (EP):
EPO Procedural Status: EX-REPORT 2001-05-15 2001 Dispatch of 1st examination report **|** RJ-DWDRAW 2001-09-26 2001 Deemed to be withdrawn **|** EX-RQ 1999-12-24 1999 Request for examination
Front Page Drawing:



Assignee - Current US:

Record 4/4 US6088802A Peripheral device with integrated security functionality

Publication Number: US6088802A 20000711

Title: Peripheral device with integrated security functionality
Title - DWPI: Peripheral device with integrated security functionality in which portable computing module communicates with host device, and includes security functionality which enables security operations to be performed on data stored in host computer
Priority Number: US1997869305A
Priority Date: 1997-06-04
Application Number: US1997869305A
Application Date: 1997-06-04
Publication Date: 2000-07-11
IPC Class Table:

IPC	Section	Class	Subclass	Class Group	Subgroup
G06F002100	G	G06	G06F	G06F0021	G06F002100

IPC Class Table - DWPI:

IPC - DWPI	Section - DWPI	Class - DWPI	Subclass - DWPI	Class Group - DWPI	Subgroup - DWPI
G06F000100	G	G06	G06F	G06F0001	G06F000100
G06K001467	G	G06	G06K	G06K0014	G06K001467

Assignee/Applicant: Spyrus Inc.,Santa Clara,CA,US
JP F Terms:
JP FI Codes:
Assignee - Original: Spyrus Inc.
Any CPC Table:

Type	Invention	Additional	Version	Office
Current	**G06F 21/34**	-	20130101	EP

ECLA: G06F002134
Abstract:

The invention enables a peripheral device to communicate with a host computing device to enable one or more security operations to be performed by the peripheral device on data stored within the host computing device, data provided from the host computing device to the peripheral device (which can then be, for example, stored in the peripheral device or transmitted to yet another device), or data retrieved by the host computing device from the peripheral device (e.g., data that has been stored in the peripheral device, transmitted to the peripheral device from another device or input to the peripheral device by a person). In particular, the peripheral device can be adapted

to enable, in a single integral peripheral device, performance of one or more security operations on data, and a defined interaction with a host computing device that has not previously been integrated with security operations in a single integral device. The defined interactions can provide a variety of types of functionality (e.g., data storage, data communication, data input and output, user identification). The peripheral device can also be implemented so that the security operations are performed in-line, i.e., the security operations are performed between the communication of data to or from the host computing device and the performance of the defined interaction. Moreover, the peripheral device can be implemented so that the security functionality of the peripheral device is transparent to the host computing device.

Language of Publication: EN

INPADOC Legal Status Table:

Gazette Date	Code	INPADOC Legal Status Impact
2015-02-17	AS	-
Description: ASSIGNMENT SPEX TECHNOLOGIES, INC., CALIFORNIA ASSIGNMENT OF ASSIGNORS INTEREST; ASSIGNOR:SPYRUS, INC.; REEL/FRAME:034971/0298 2015-02-12		
2012-01-10	FPAY	+
Description: FEE PAYMENT		
2008-06-06	SULP	+
Description: SURCHARGE FOR LATE PAYMENT		
2008-06-06	FPAY	+
Description: FEE PAYMENT		
2008-01-21	REMI	-
Description: MAINTENANCE FEE REMINDER MAILED		
2004-07-07	SULP	+
Description: SURCHARGE FOR LATE PAYMENT		
2004-07-07	FPAY	+
Description: FEE PAYMENT		
2004-01-28	REMI	-
Description: MAINTENANCE FEE REMINDER MAILED		
1998-01-20	AS	-

Description: ASSIGNMENT SPYRUS, INC., CALIFORNIA ASSIGNMENT OF ASSIGNORS INTEREST; ASSIGNORS:BIALICK, WILLIAM P.; SUTHERLAND, MARK J.; DOLPHIN-PETERSON, JANET L.; AND OTHERS; REEL/FRAME:008942/0204; SIGNING DATES FROM 19971218 TO 19971223

Post-Issuance (US):

Reassignment (US) Table:

Assignee	Assignor	Date Signed	Reel/Frame	Date
SPEX TECHNOLOGIES INC.,SAN JOSE,CA,US	SPYRUS, INC.	2015-02-12	034971/0298	2015-02-17
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).				
Corresponent: ROBERT J. ROSE PO BOX 4341 DIAMOND BAR, CA 91765				
SPYRUS INC.,SAN JOSE,CA,US	BIALICK, WILLIAM P.	1997-12-19	008942/0204	1998-01-20
	SUTHERLAND, MARK J.	1997-12-18		
	DOLPHIN-PETERSON, JANET L.	1997-12-20		
	ROWLAND, THOMAS K.	1997-12-18		
	SKEBA, KIRK W.	1997-12-23		
	HOUSLEY, RUSSELL D.	1997-12-19		
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).				
Corresponent: DAVID R. GRAHAM 1337 CHEWPON AVE. MILPITAS, CALIFORNIA 95035				

Maintenance Status (US):

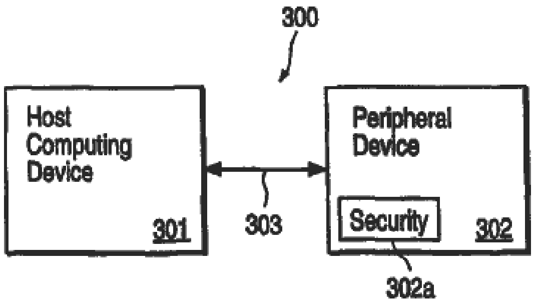
Litigation (US):

Opposition (EP):

License (EP):

EPO Procedural Status:

Front Page Drawing:



Assignee - Current US: SPEX TECHNOLOGIES INC.

THOMSON REUTERS

United States Patent and Trademark Office
Office of the Commissioner for Patents

PERIPHERAL DEVICE WITH INTEGRATED SECURITY FUNCTIONALITY

PATENT #	APPLICATION #	FILING DATE	ISSUE DATE
6088802	08869305	06/04/1997	07/11/2000

Payment Window Status

No maintenance fees are due.

WINDOW	STATUS	FEES
11.5 Year	Closed	Paid

Window	First Day to Pay	Surcharge Starts	Last Day to Pay	Status	Fees
3.5 Year	07/11/2003	01/13/2004	07/12/2004	Closed	Paid
7.5 Year	07/11/2007	01/12/2008	07/11/2008	Closed	Paid
11.5 Year	07/11/2011	01/12/2012	07/11/2012	Closed	Paid

Patent Holder Information

Customer #	23676
Entity Status	UNDISCOUNTED
Phone Number	6267964000
Address	Leech Tishman Fuscaldo & Lampl Jeffrey G. Sheldon 100 Corson Street Third Floor PASADENA, CA 91103-3842 UNITED STATES

Generated: 10/03/2016 01:46:37