PTO/SB/16 (12-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 1 of 2

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

Express Mail Label No. _____

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)

Additional inventors are being named on the _____ *separately numbered sheets attached hereto.*

TITLE OF THE INVENTION (500 characters max):

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ The address corresponding to Customer Number:

OR

☐ Firm or Individual Name

Address

City	State	Zip
Country	Telephone	Email

ENCLOSED APPLICATION PARTS *(check all that apply)*

☐ Application Data Sheet. See 37 CFR 1.76

☐ CD(s), Number of CDs _____

☐ Drawing(s) *Number of Sheets* _____

☐ Other (specify) _____

☐ Specification (e.g. description of the invention) *Number of Pages* _____

Fees Due: Filing Fee of $220 ($110 for small entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is $270 ($135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order made payable to the *Director of the United States Patent and Trademark Office* is enclosed to cover the filing fee and application size fee (if applicable).

☐ Payment by credit card. Form PTO-2038 is attached.

TOTAL FEE AMOUNT ($)

☐ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: _____ .

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

PTO/SB/16 (12-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

☐ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

_____

WARNING:

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

SIGNATURE _____ Date_____

TYPED or PRINTED NAME _____ REGISTRATION NO. _____
(if appropriate)

TELEPHONE _____ Docket Number: _____

PTO/SB/05 (08-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	
First Inventor	
Title	
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ **Fee Transmittal Form** (e.g., PTO/SB/17)
2. ☐ **Applicant claims small entity status**. See 37 CFR 1.27.
3. ☐ **Specification** [*Total Pages*_____]
   Both the claims and abstract must start on a new page
   (For information on the preferred arrangement, see MPEP 608.01(a))
4. ☐ **Drawing(s)** (*35 U.S.C. 113*) [*Total Sheets* _____]
5. **Oath or Declaration** [*Total Sheets* _____]
   a. ☐ Newly executed (original or copy)
   b. ☐ A copy from a prior application (37 CFR 1.63(d))
   (for continuation/divisional with Box 18 completed)
   i. ☐ DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ **Application Data Sheet.** See 37 CFR 1.76
7. ☐ **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)*
   ☐ Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
   (if applicable, items a. – c. are required)
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria VA 22313-1450

ACCOMPANYING APPLICATION PARTS

9. ☐ **Assignment Papers** (cover sheet & document(s))
   Name of Assignee_____
   _____
10. ☐ **37 CFR 3.73(b) Statement** *(when there is an assignee)* ☐ **Power of Attorney**
11. ☐ **English Translation Document** *(if applicable)*
12. ☐ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    ☐ Copies of citations attached
13. ☐ **Preliminary Amendment**
14. ☐ **Return Receipt Postcard** (MPEP 503)
    (*Should be specifically itemized)*
15. ☐ **Certified Copy of Priority Document(s)**
    (if foreign priority is claimed)
16. ☐ **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. ☐ Other:_____
    _____

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: ……

Prior application information: *Examiner* _____ *Art Unit:* _____

19. CORRESPONDENCE ADDRESS

☐ The address associated with Customer Number: _____ ***OR*** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature		Date	
Name (Print/Type)		Registration No. (Attorney/Agent)	

Doc Code: WFEE

Document Description: Fee Worksheet (PTO-875)

PTO/SB/06 (10-07)
Approved for use through 06/30/2010. OMB 0651 0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X =		OR	X =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X =			X =	
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $260 ($130 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			N/A			N/A	
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDI-TIONAL FEE ($)		RATE ($)	ADDI-TIONAL FEE ($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	X =		OR	X =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X =		OR	X =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDI-TIONAL FEE ($)		RATE ($)	ADDI-TIONAL FEE ($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	X =		OR	X =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X =		OR	X =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'L FEE		OR	TOTAL ADD'L 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.

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

PTO/SB/17 (10-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2009

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($)

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	
Examiner Name	
Art Unit	
Attorney Docket No.	

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify):_____

☐ Deposit Account Deposit Account Number:_____ Deposit Account Name:_____

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☐ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	**Fee ($)**	**Small Entity Fee ($)**	**Fee ($)**	**Small Entity Fee ($)**	**Fee ($)**	**Small Entity Fee ($)**	**Fees Paid ($)**
Utility	330	165	540	270	220	110	
Design	220	110	100	50	140	70	
Plant	220	110	330	165	170	85	
Reissue	330	165	540	270	650	325	
Provisional	220	110	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	**Fee ($)**	**Small Entity Fee ($)**
Each claim over 20 (including Reissues)	52	26
Each independent claim over 3 (including Reissues)	220	110
Multiple dependent claims	390	195

Total Claims		**Extra Claims**	**Fee ($)**	**Fee Paid ($)**
_____	- 20 or HP =	_____	x _____	= _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims		**Extra Claims**	**Fee ($)**	**Fee Paid ($)**
_____	- 3 or HP =	_____	x _____	= _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	**Fee Paid ($)**
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $270 ($135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets		**Extra Sheets**		**Number of each additional 50 or fraction thereof**	**Fee ($)**	**Fee Paid ($)**
_____	- 100 =	_____	/ 50 =	_____ (round **up** to a whole number)	x _____	= _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	_____
Other (e.g., late filing surcharge):_____	_____

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	Telephone
Name (Print/Type)			Date

PTO/SB/01A (01-09)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	

As the below named inventor(s), I/we declare that:

This declaration is directed to:

☐ The attached application, or

☐ Application No. _____ filed on _____

☐ As amended on _____ (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

WARNING:

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

All statements made herein of my/our own knowledge are true, 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 are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)

Inventor one: _____ Date: _____

Signature: _____ Citizen of: _____

Inventor two: _____ Date: _____

Signature: _____ Citizen of: _____

☐ Additional inventors or a legal representative are being named on _____ additional form(s) attached hereto.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651 0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet | | of | |

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]–Number[4]–Kind Code[5] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference 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 applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. OMB 0651 0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet | | of | |

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference 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 applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. 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 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

PTO/SB/14 (11-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention		

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

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

Applicant Information:

Applicant 1

Applicant Authority ◉ Inventor ◯ Legal Representative under 35 U.S.C. 117 ◯ Party of Interest under 35 U.S.C. 118

Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**

Residence Information (Select One) ◉ US Residency ◯ Non US Residency ◯ Active US Military Service

City		**State/Province**		**Country of Residence**	

Citizenship under 37 CFR 1.41(b)	

Mailing Address of Applicant:

Address 1	
Address 2	

City		**State/Province**	
Postal Code		**Country**	

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

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number		
Email Address		Add Email Remove Email

Application Information:

Title of the Invention			
Attorney Docket Number		**Small Entity Status Claimed**	☐
Application Type			
Subject Matter			
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		**Suggested Figure for Publication (if any)**	

PTO/SB/14 (11-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention		

Publication Information:

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

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number			

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

			Remove
Application Number	Country	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			◉ Yes ○ No

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

Assignee Information:

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

Assignee 1

PTO/SB/14 (11-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention		

If the Assignee is an Organization check here. ☐				
Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information:			
Address 1			
Address 2			
City		**State/Province**	
Country		Postal Code	
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the **Add** button.			

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.					
Signature				Date (YYYY-MM-DD)	
First Name		Last Name		Registration Number	

This collection of information is required by 37 CFR 1.76. 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 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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.**

PTO/SB/35 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U. S. DEPARTMENT OF COMMERCE

NONPUBLICATION REQUEST UNDER 35 U.S.C. 122(b)(2)(B)(i)

First Named Inventor	
Title	
Attorney Docket Number	

I hereby certify that the invention disclosed in the attached application **has not and will not be** the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

I hereby request that the attached application not be published under 35 U.S.C. 122(b).

_____ _____
Signature Date

_____ _____
Typed or printed name Registration Number, if applicable

_____
Telephone Number

This request must be signed in compliance with 37 CFR 1.33(b) and submitted with the application **upon filing.**

Applicant may rescind this nonpublication request at any time. If applicant rescinds a request that an application not be published under 35 U.S.C. 122(b), the application will be scheduled for publication at eighteen months from the earliest claimed filing date for which a benefit is claimed.

If applicant subsequently files an application directed to the invention disclosed in the attached application in another country, or under a multilateral international agreement, that requires publication of applications eighteen months after filing, the applicant **must** notify the United States Patent and Trademark Office of such filing within forty-five (45) days after the date of the filing of such foreign or international application. **Failure to do so will result in abandonment of this application (35 U.S.C. 122(b)(2)(B)(iii)).**

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

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☐ Responsive to communication(s) filed on _____

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) ____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) ____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/31/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Notice of References Cited	Application/Control No.	Applicant(s)/Patent Under Reexamination	
	Examiner	Art Unit	Page of

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification	
	A	US-				
	B	US-				
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification	
	N						
	O						
	P						
	Q						
	R						
	S						
	T						

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

U.S. Patent and Trademark Office
PTO-892 (Rev. 01-2001) **Notice of References Cited** Part of Paper No.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

111111 7590 06/28/2002

DOE & DOW
2100 PENNSYLVANIA AVENUE NW
WASHINGTON, DC 20037-3202

EXAMINER
BROWN, PETER

ART UNIT	CLASS-SUBCLASS
1799	111-999000

DATE MAILED: 06/28/2002

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
02/022,222	05/29/2000	JOHN RON	Q-49699	9999

TITLE OF INVENTION: TRANSITION METAL DEVICE OF UNKNOWN COMPOSITION

TOTAL CLAIMS	APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
4	nonprovisional	NO	$1240.00	?	?	09/28/2002

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

PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) 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. SEE 35 U.S.C. 151.

HOW TO REPLY 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 the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above and notify the United States Patent and Trademark Office of the change in status, or

B. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check the box below and enclose the PUBLICATION FEE and 1/2 the ISSUE FEE shown above.

- ☐ Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

II. PART B - FEE(S) TRANSMITTAL should be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). Even if the fee(s) have already been paid, Part B - Fee(s) Transmittal should be completed and returned. If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give the application 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.

PART B - FEE(S) TRANSMITTAL

Complete and mail this form, together with applicable fee(s), to: **Box ISSUE FEE**
Assistant Commissioner for Patents
Washington, D.C. 20231

MAILING INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 4 should be completed where appropriate. All further correspondence including 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)

111111 7590 06/28/2002

DOE & DOW
2100 PENNSYLVANIA AVENUE NW
WASHINGTON, DC 20037-3202

Note: The certificate of mailing below can only be used for domestic mailings of the Fee(s) 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 Fee(s) 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.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
02/022,222	05/29/2000	JOHN RON	Q-49699	9999

TITLE OF INVENTION: TRANSITION METAL DEVICE OF UNKNOWN COMPOSITION

TOTAL CLAIMS	APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
4	nonprovisional	NO	$1240.00	?	?	09/28/2002

EXAMINER	ART UNIT	CLASS-SUBCLASS
BROWN, PETER	1799	111-999000

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 Correspondence 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_____

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 appropriate when an assignment has been previously submitted to the USPTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) ❑ individual ❑ corporation or other private group entity ❑ government

4a. The following fee(s) are enclosed:

❑ Issue Fee

❑ Publication Fee

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s):

❑ A check in the amount of the fee(s) is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Commissioner is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number _____(enclose an extra copy of this form).

The COMMISSIONER OF PATENTS AND TRADEMARKS is requested to apply the Issue Fee and Publication Fee (if any) to the application identified above.

(Authorized Signature) (Date)

NOTE; The Issue Fee and Publication Fee (if required) 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 United States 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, United States 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.

TRANSMIT THIS FORM WITH FEE(S)

PTOL-85 (REV. 07-01) Approved for use through 01/31/2004. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
02/022,222	05/29/2000	JOHN RON	Q-49699	9999

111111 7590 06/28/2002

DOE & DOW
2100 PENNSYLVANIA AVENUE NW
WASHINGTON, DC 20037-3202

EXAMINER	
BROWN, PETER	
ART UNIT	**PAPER NUMBER**
1799	

DATE MAILED: 06/28/2002

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The patent term adjustment to date is 37 days. If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the term adjustment will be 37 days.

If a continued prosecution application (CPA) was filed in the above-identified application, the filing date that determines patent term adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) system. (http://pair.uspto.gov)

PTOL-85 (REV. 07-01) Approved for use through 01/31/2004.

Doc Code: TRAN.LET

Document Description: Transmittal Letter

PTO/SB/21 (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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	
Filing Date	
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	

Total Number of Pages in This Submission

ENCLOSURES (*Check all that apply*)

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature			
Printed name			
Date		Reg. No.	

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. 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 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **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/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Request for Continued Examination (RCE) Transmittal

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

Application Number	
Filing Date	
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☐ Enclosed

      i. ☐ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☐ Information Disclosure Statement (IDS)

      iv. ☐ Other _____

2. Miscellaneous

   a. ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

   a. ☐ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. _____.

      i. ☐ RCE fee required under 37 CFR 1.17(e)

      ii. ☐ Extension of time fee (37 CFR 1.136 and 1.17)

      iii. ☐ Other _____

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature		Date	
Name (Print/Type)		Registration No.	

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

Instruction Sheet for RCEs

(not to be submitted to the USPTO)

NOTES:

An RCE is not a new application, and filing an RCE will not result in an application being accorded a new filing date.

Filing Qualifications:

The application must be a utility or plant application filed on or after June 8, 1995. The application cannot be a provisional application, a utility or plant application filed before June 8, 1995, a design application, or a patent under reexamination. See 37 CFR 1.114(e).

Filing Requirements:

Prosecution in the application must be closed. Prosecution is closed if the application is under appeal, or the last Office action is a final action, a notice of allowance, or an action that otherwise closes prosecution in the application (e.g., an Office action under *Ex parte Quayle*). See 37 CFR 1.114(b).

A submission and a fee are required at the time the RCE is filed. If reply to an Office action under 35 U.S.C. 132 is outstanding (e.g., the application is under final rejection), the submission must meet the reply requirements of 37 CFR 1.111. If there is no outstanding Office action, the submission can be an information disclosure statement, an amendment, new arguments, or new evidence. See 37 CFR 1.114(c). The submission may be a previously filed amendment (e.g., an amendment after final rejection).

WARNINGS:

Request for Suspension of Action:

All RCE filing requirements must be met before suspension of action is granted. A request for a suspension of action under 37 CFR 1.103(c) does not satisfy the submission requirement and does not permit the filing of the required submission to be suspended.

Improper RCE will NOT toll Any Time Period:

Before Appeal **-** If the RCE is improper (e.g., prosecution in the application is not closed or the submission or fee has not been filed) and the application is not under appeal, the time period set forth in the last Office action will continue to run and the application will be abandoned after the statutory time period has expired if a reply to the Office action is not timely filed. No additional time will be given to correct the improper RCE.

Under Appeal **-** If the RCE is improper (e.g., the submission or the fee has not been filed) and the application is under appeal, the improper RCE is effective to withdraw the appeal. Withdrawal of the appeal results in the allowance or abandonment of the application depending on the status of the claims. If there are no allowed claims, the application is abandoned. If there is at least one allowed claim, the application will be passed to issue on the allowed claim(s). See MPEP 1215.01.

See MPEP 706.07(h) for further information on the RCE practice.

PTO/SB/36 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U. S. DEPARTMENT OF COMMERCE

RESCISSION OF PREVIOUS NONPUBLICATION REQUEST
(35 U.S.C. 122(b)(2)(B)(ii))
AND, IF APPLICABLE,
NOTICE OF FOREIGN FILING
(35 U.S.C. 122(b)(2)(B)(iii))

Send completed form to:
Mail Stop PG Pub
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
FAX: (571) 273-8300

Application Number	
Filing Date	
First Named Inventor	
Title	
Atty Docket Number	
Art Unit	
Examiner	

A request that the above-identified application not be published under 35 U.S.C. 122(b) (nonpublication request) was included with the above-identified application on filing pursuant to 35 U.S.C. 122(b)(2)(B)(i).
I hereby **rescind** the previous nonpublication request.

If a notice of foreign or international filing is or will be required by 35 U.S.C. 122(b)(2)(B)(iii) and 37 CFR 1.213(c), I hereby provide such notice. This notice is being provided no later than forty-five (**45**) days after the date of such foreign or international filing.

*If a notice of subsequent foreign or international filing required by 35 U.S.C. 122(b)(2)(B)(iii) and 37 CFR 1.213(c) was not filed within forty-five (**45**) days after the date of filing of the foreign or international application, the application is ABANDONED, and a petition to revive under 37 CFR 1.137(b) is required. See 37 CFR 1.137(f).*

Signature _____ Date _____

Typed or printed name _____ Registration Number, if applicable _____

Telephone Number _____

This request must be signed in compliance with 37 CFR 1.33(b).

If information or assistance is needed in completing this form, please contact the Pre-Grant Publication Division at (703)605-4283 or by e-mail at PGPub@USPTO.gov.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop PG Pub, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature

Name (Print/Type) Date

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

US 20060108362A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2006/0108362 A1

Lalancette (43) Pub. Date: May 25, 2006

(54) ADJUSTABLE ELECTRICAL OUTLET BOX

(75) Inventor: **Daniel Lalancette**, L'Acadie (CA)

Correspondence Address:
HOFFMAN & BARON, LLP
6900 JERICHO TURNPIKE
SYOSSET, NY 11791 (US)

(73) Assignee: **Thomas & Betts International, Inc.**

(21) Appl. No.: **11/263,688**

(22) Filed: **Nov. 1, 2005**

Related U.S. Application Data

(60) Provisional application No. 60/630,005, filed on Nov. 22, 2004.

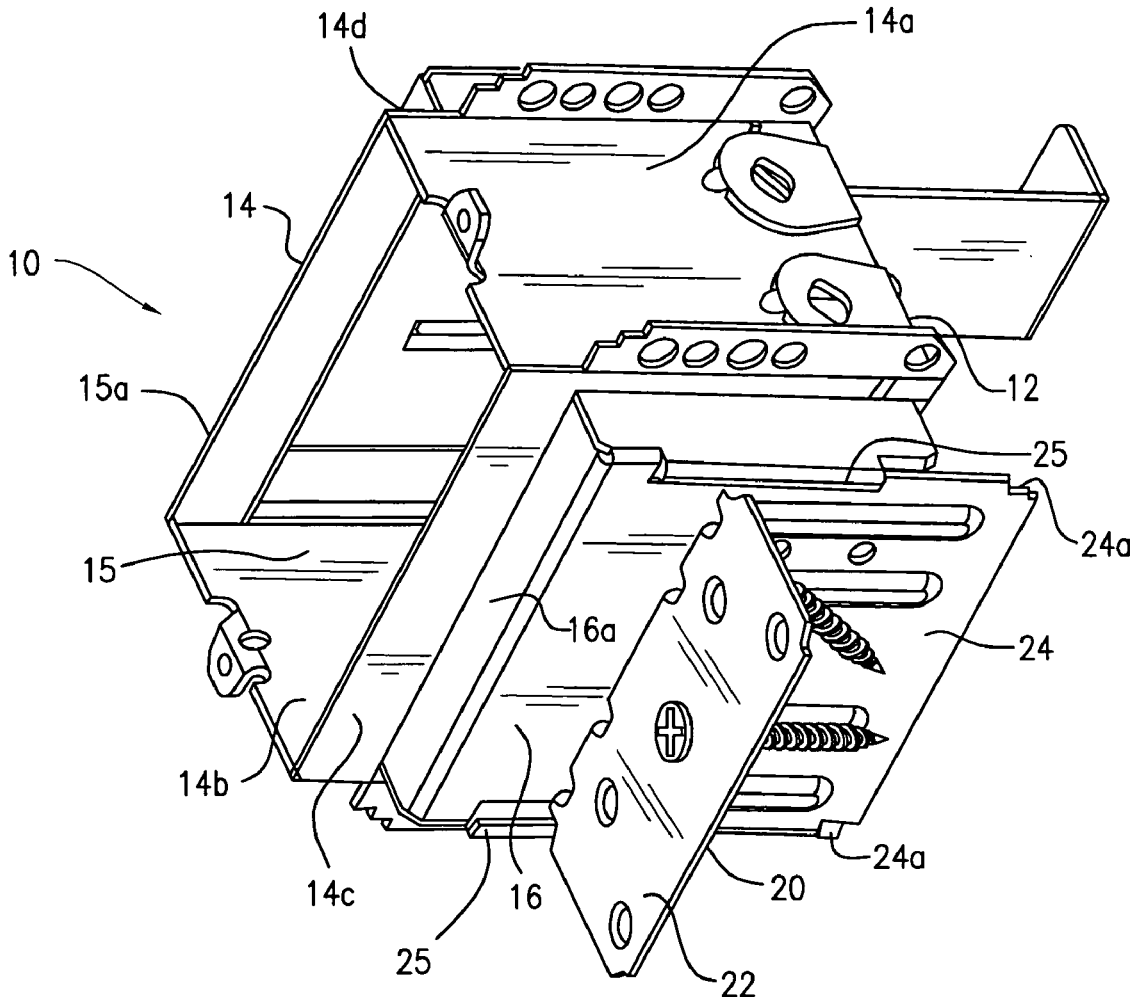
Publication Classification

(51) **Int. Cl.**
H02G 3/08 (2006.01)

(52) **U.S. Cl.** **220/3.7**

(57) **ABSTRACT**

The present invention is directed to an electrical outlet box assembly for adjustable positioning with respect to a wall stud. An electrical outlet box includes plural side walls defining a box interior having an open front face. A box locator is adjustably positioned on one of the side walls so as to adjust the location of the front face with respect to the stud to which the box locator is mounted. A support bracket is adjustably attached to another of the side walls for supporting the adjustably positioned box with respect to the back wall board.



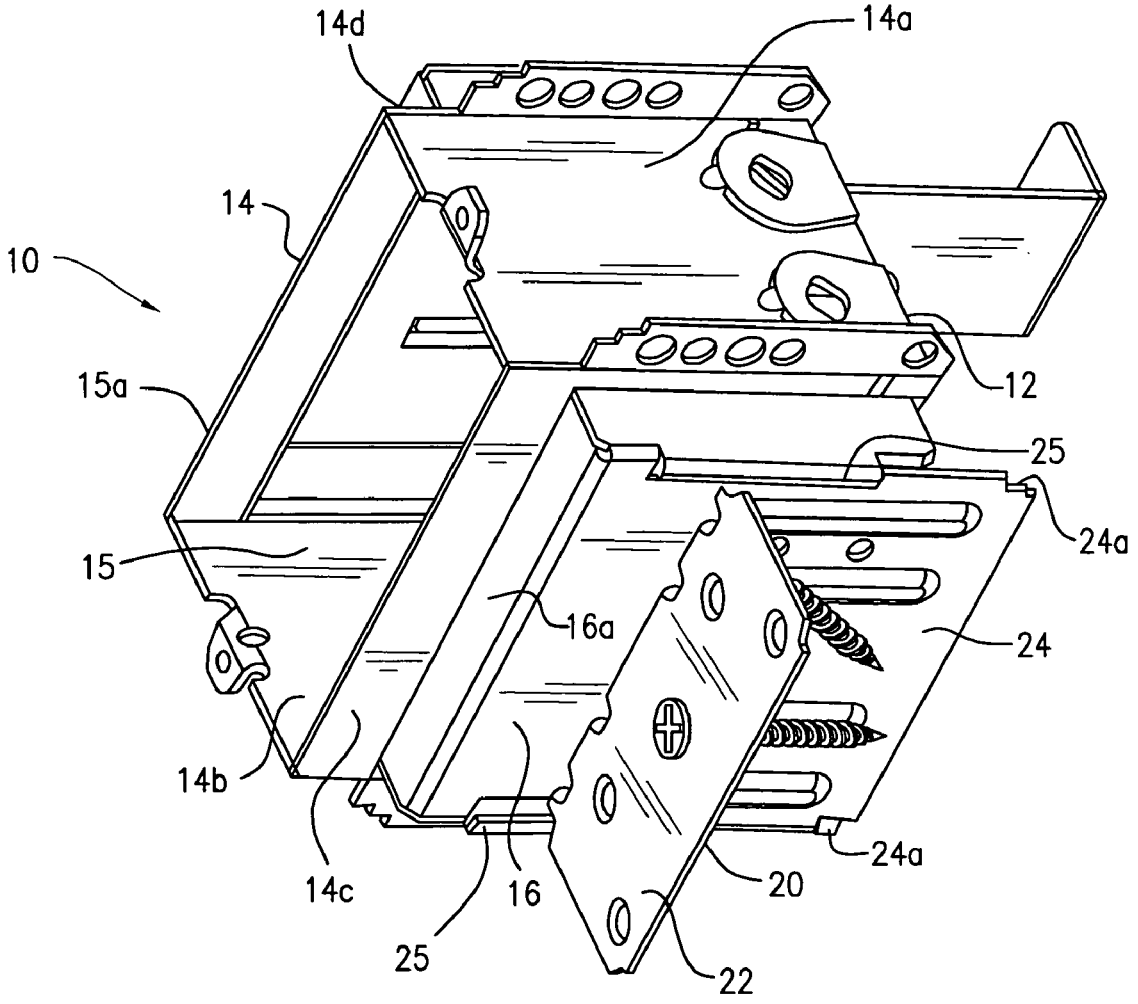


FIG. 1

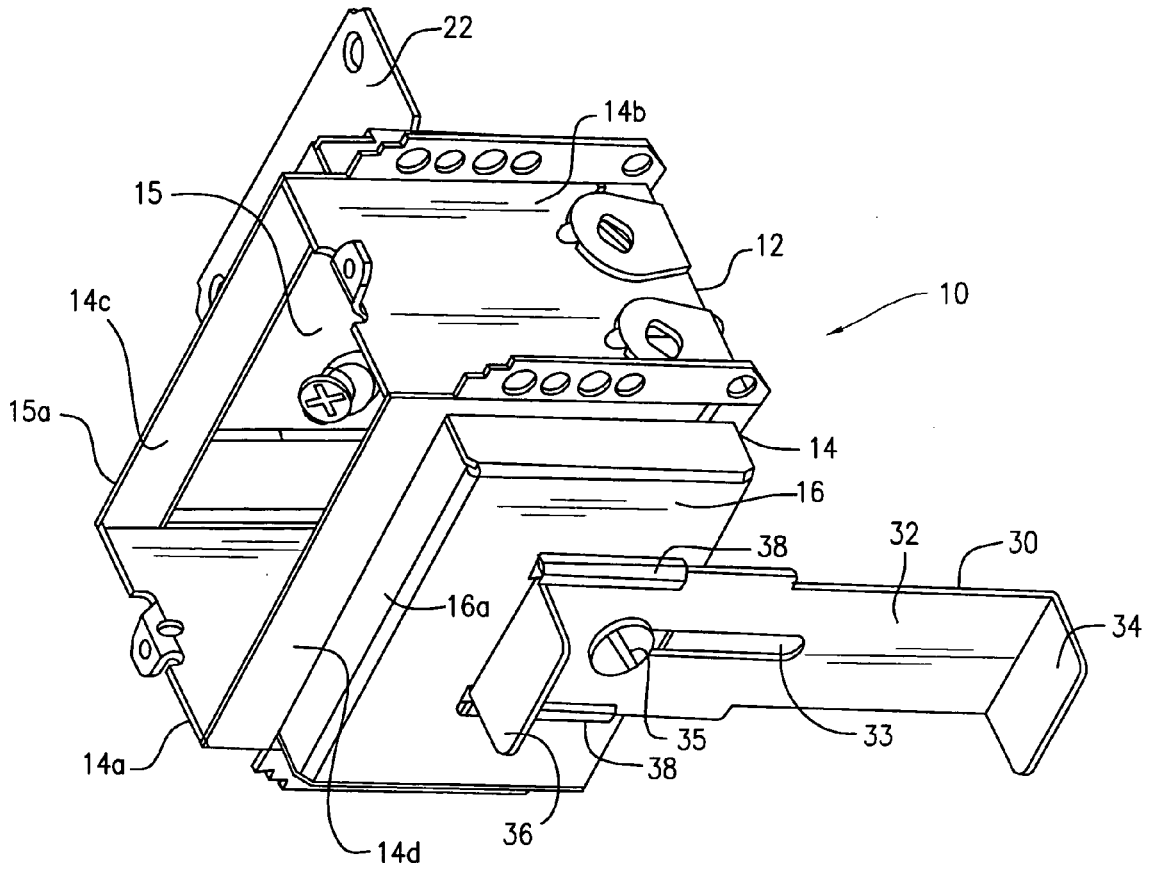


FIG. 2

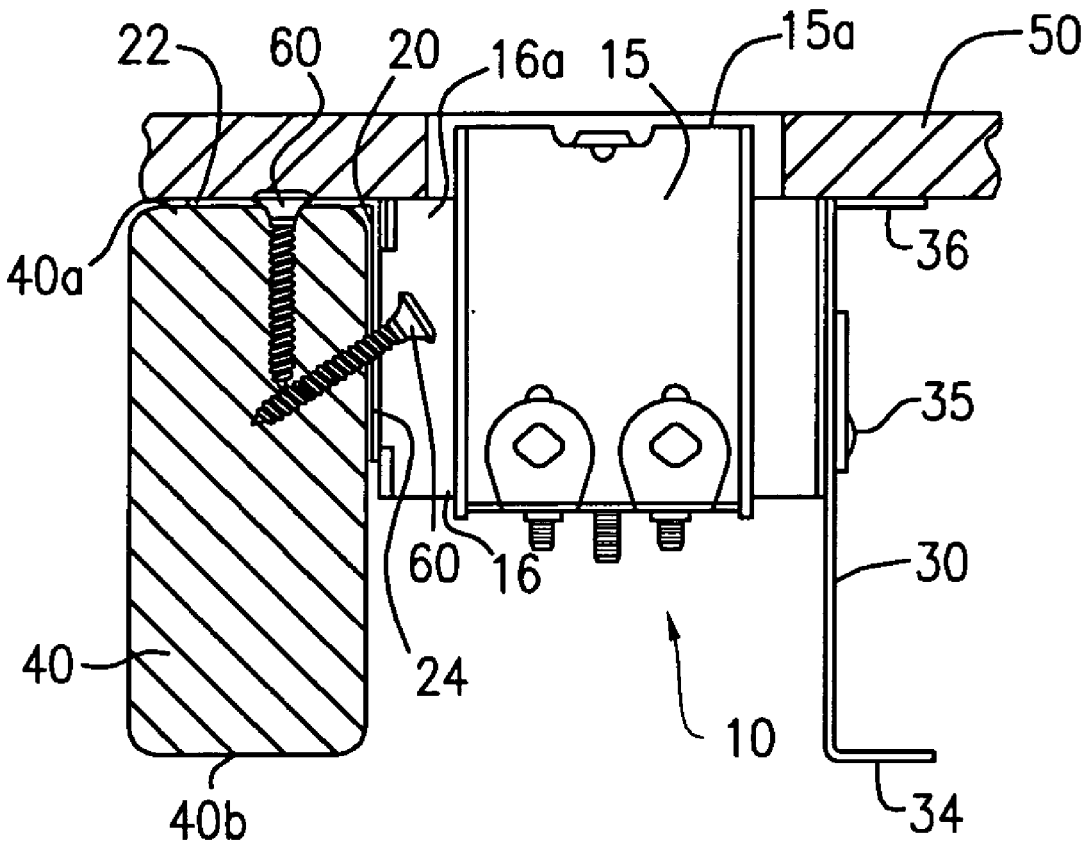


FIG. 3

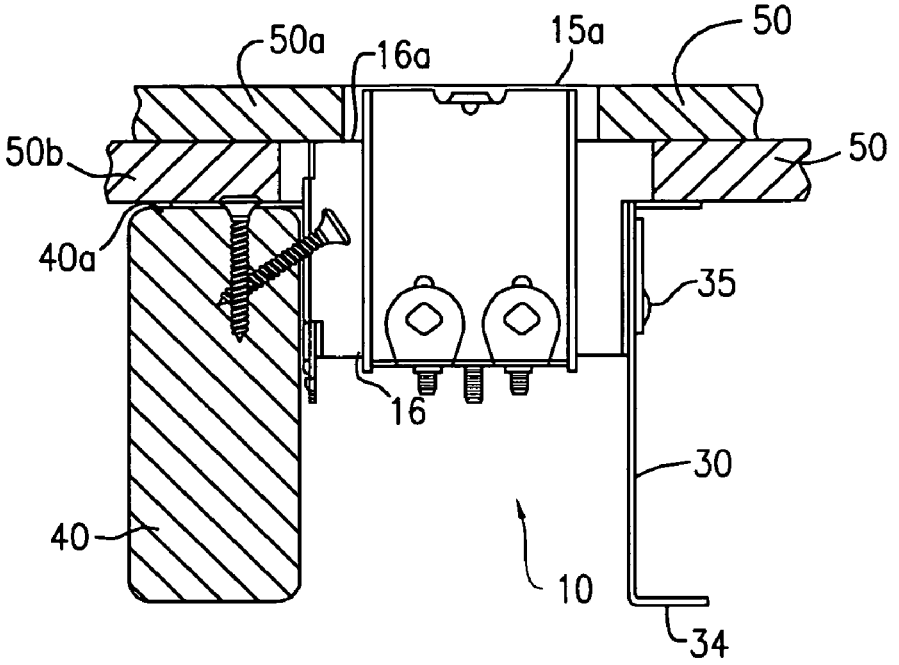

50a
16a
15a
50
50b
50
40a
35
16
30
40
10
34

FIG. 4

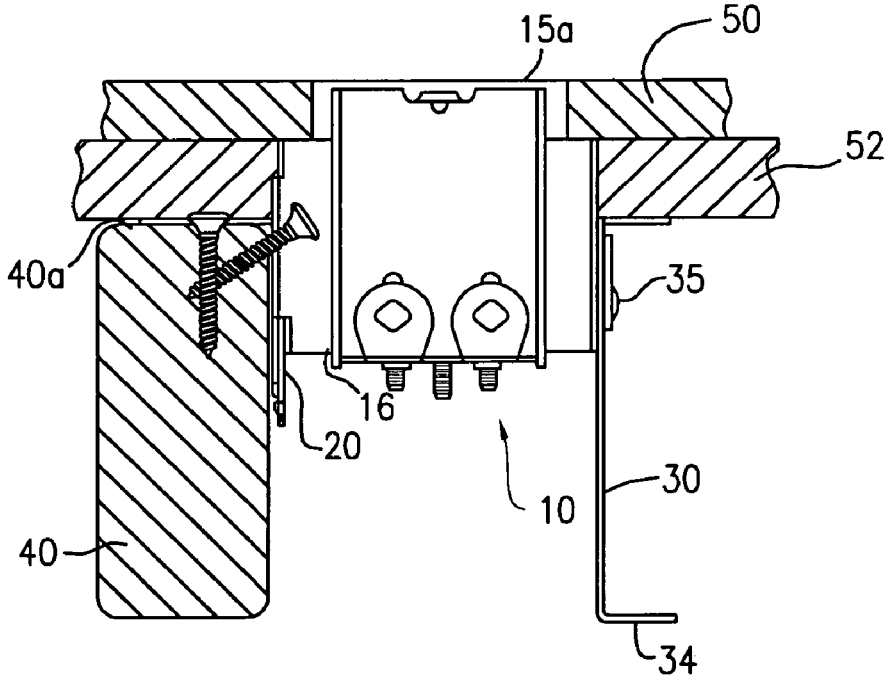

15a
50
52
40a
35
16
20
30
10
40
34

FIG. 5

ADJUSTABLE ELECTRICAL OUTLET BOX

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Application No. 60/630,005 filed Nov. 22, 2004.

FIELD OF THE INVENTION

[0002] The present invention relates generally to an electrical outlet box mounted to a wall stud. More particularly the present invention relates to an electrical outlet box which may be adjustably mounted to the wall stud so as to accurately position the outlet box with respect to the wall stud.

BACKGROUND OF THE INVENTION

[0003] Electrical outlet boxes are widely used to house electrical components such as switches and receptacles for termination of electrical wires run through the wall of a structure. Typically, these electrical outlet boxes are mounted to a wall stud supporting structural wall board. In new construction, the outlet box is mounted to the wall stud prior to attachment of the wall board. Thus, the outlet box must be properly positioned with respect to the stud so that the front face of the outlet box is aligned with the front of the wall board once it is placed against the stud. Such positioning of the box must be taken into consideration for the various thickness and layers of wall board.

[0004] In addition to such accurate mounting, subsequent electrical termination of the switches and receptacles in the box may cause the box to be moved or displaced once secured. In certain situations, there may be a tendency for the electrical installer to push the box inwardly into the wall cavity rendering the box useless.

[0005] The art has seen a number of brackets which are used in combination with stud mounted electrical boxes to both accurately align the front face of the outlet box with respect to the wall board and to prevent the box from being pushed into the wall cavity.

[0006] U.S. Pat. No. 4,978,092 shows an adjustable support bracket that prevents the box from being pushed into the wall cavity.

[0007] U.S. Pat. No. 2,473,051 also shows a box having an adjustable support preventing the box from being pushed into the cavity.

[0008] U.S. Pat. Nos. 5,289,934; 5,253,831 and 3,384,658 show adjustable stud mounted brackets which allow the box to be adjustably positioned with respect to the wall stud.

[0009] None of the prior art devices, however, allow both for adjustment of the box once the box is attached to the wall stud, as well as providing separate independent structure to prevent the adjusted box from being pushed into the wall cavity.

SUMMARY OF THE INVENTION

[0010] The present invention provides an electrical outlet box assembly for adjustable positioning with respect to a wall stud. An electrical outlet box includes plural side walls defining a box interior having an open front face. A box locator is adjustably positioned on one of the side walls. The box locator includes a mounting surface parallel to the open front face of the box and an attachment surface perpendicular thereto. The attachment surface is adjustably positioned along one of the side walls so as to adjust the location of the front face with respect to the stud to which the box locator is mounted. The attachment surface is fixable to the side wall upon adjustable positioning of the front face of the box. A support bracket is provided. The support bracket is adjustably attached to another of the side walls for supporting the adjustably positioned box with respect to the back wall board.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] **FIGS. 1 and 2** are perspective opposite side showings of adjustable electrical outlet box of the present invention.

[0012] **FIGS. 3-5** show the adjustable electrical outlet box of **FIG. 1** accommodating various thicknesses and numbers of wall board.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0013] The present invention provides an electrical outlet box for supporting electrical components such as switches and receptacles (not shown). In conventional fashion, the stripped ends of insulated wires (not shown) are run into the box so as to be terminated to the components mounted within the box. The box itself is designed to be secured to a wall stud such that when wall board is placed over the wall stud, the front face of the box is positioned generally flush thereto.

[0014] Referring now to **FIGS. 1 and 2**, the electrical outlet box **10** of the present invention is shown. Box **10** includes a back wall **12**, perimetrical side **14** including top and bottom walls **14***a* and **14***b* and opposed lateral side walls **14***c* and **14***d*. The box defines a box interior **15** where the components are terminated and supported. Each of the side walls **14***c* and **14***d* includes an extending compartment **16** so as to increase the interior volume of box **10**.

[0015] The extending compartments **16** define extending forward surfaces **16***a* which are generally parallel to the open front face **15***a* of box **10**. As will be described in further detail herein below, the surfaces **16***a* are used to support wall board so that the front face **15***a* of the box may be positioned flush thereto.

[0016] Referring specifically to **FIG. 1**, box **10** includes an adjustable box locator **20** which is slidably attached to the side of compartment **16**. The box locator **20** is generally a right angled member having a mounting surface **22** positioned generally parallel to front face **15***a* and an attachment surface **24** perpendicular thereto. The attachment surface **24** is held to compartment **16** by a pair of rails **25** which slidably accommodate attachment surface **24**. The distal edges of attachment surface **24** may include protrusions **24***a* to prevent dislodgement of the locator from the box. The box locator **20** allows the box **10** to be adjustably positioned with respect to a wall stud as will be described in further detail herein below.

[0017] Referring now to **FIG. 2**, a support bracket **30** is adjustably attached to compartment **16** on the opposite side wall **14***d* of box **10**. Support bracket **30** includes an elongate

body **32** having right angled stop members **34** and **36** extending from the ends thereof. Body **32** has a central elongate slot **33** through which an attachment screw **35** extends so as to attach the support bracket to the compartment **16**. The box is slidably coupled to compartment **16** by a pair of rails **38** so that the support bracket **30** can be slidably adjustably positioned along compartment **16**. As will be described in further detail herein below, the support bracket **30** is adjustably positioned so that stop **36** abuts against the inside of wall board and stop **34** is positioned adjacent the opposed wall board to prevent the box from being pushed into the wall during use.

[**0018**] Having described the components of the adjustable box of the present invention, it use may be described with respect to the **FIGS. 3-5**.

[**0019**] As shown in **FIG. 3**, the box **10** of the present invention may be supported to a wall stud **40** in such a manner that it accommodates a single thickness of ½" wall board **50**. The box is installed on the stud in the following manner. The mounting surface **22** of box locator **20** is secured to the face **40***a* of the stud using a conventional mounting screw **60**. The box **10** is then adjustably positioned by slidable movement of the box with respect to the locator **20** such that the front face **15***a* of the box extends approximately 7/16" from the face **40***a* of the stud. Once the box is properly positioned, a second screw **60** may be installed through the interior **15** of the box and through the attachment surface **24** to fix the position of the box with respect to the stud. The wall board **50** may now be attached to the stud **40**. A ledge **16***a* formed by compartment **16** serves to seat the wall board **50**. In this position, the front face **15***a* of the box is fixed at a position nearly flush with the wall board. Once the position of the front face of the box is fixed, support bracket **30** may be slidably positioned with respect to wall board **50**. The attachment screw **35** is loosened so that the support bracket **30** can be slidably adjustably positioned along the box. The bracket **30** is positioned such that stop **36** is slidably positioned against wall board **50**. The length of the support member is selected such that when properly positioned, the opposite stop **34** will be positioned next adjacent the wall board (not shown) which is attached to the opposite face **40***b* of stud **40**. In this manner, during use and installation, and subsequently upon reattachment of components to box **10**, the box will not be pushed into the wall.

[**0020**] **FIG. 4** shows a similar mounting technique for box **10** employed with two layers of ½" wall board **50**. In this embodiment, the box **10** is adjusted such that the front face **15***a* thereof is aligned substantially flush with the outer wall board surface at a distance of approximately 15/16" from face **40***a* of stud **40**. The wall boards **50***a* and **50***b* are attached to the stud **40** such that the outer wall board **50***a* is positioned over ledge **16***a* of compartment **16** while the inner wall board **50***b* is positioned rearwardly and to the side of compartment **16**. The bracket **30** is adjusted so that the stop **36** abuts against the inner surface of wall board **50***b*. In this position, opposed stop **34** abuts against the wall board attached to the face **40***b* of stud **40** to prevent the box from being inadvertently pushed into the wall during use.

[**0021**] As shown in **FIG. 5**, box **10** may also be used to accommodate multiple layers of different thicknesses of wall board. For example, in **FIG. 5**, wall board **50** which is ½" wall board is combined with wall board **52** which is ¾" wall board. In this embodiment, the front face **15***a* of box **15** is positioned approximately 15/16" from the face **40***a* of stud **40**. The adjustable positioning of both the box locator **20** and the support bracket **30** accommodate this combination by adjustment in a manner similar to that described with respect to **FIGS. 3 and 4**.

[**0022**] Furthermore, it is contemplated that the present invention can be used with a variety of wall board thicknesses as well as a variety of multiples of wall board layer. In each case, the box is adjustably positioned with respect to box locator **20** so as to position the front face **15***a* of box **10** substantially flush with the outer surface of the wall board. In the same manner, support bracket **30** can be adjustably positioned so as to prevent the box during use from being pushed into the wall.

What is claimed is:

1. An electrical outlet box assembly for adjustable positioning with respect to a wall stud comprising:

an electrical outlet box having plural side walls defining a box interior having an open front face;

a box locator adjustably positioned on one of said side walls, said box locator having a mounting surface portion parallel to said open front face of said box and an attachment surface perpendicular thereto, said attachment surface being adjustably positioned along said one side wall so as to adjust the location of said front face with respect to said stud, said attachment surface being fixable to said one side wall upon adjustable positioning of said front face of said box with regard to said stud; and

a support bracket being adjustably attached to another of said side walls for supporting said adjustably positioned box with respect to said stud.

2. An adjustable electrical outlet box of claim 1 wherein said box locator is screw attached to said side wall.

3. An adjustable electrical outlet box of claim 2 wherein said screw attachment is achieved through said box interior.

4. An electrical outlet box assembly for adjustable positioning with respect to a wall stud comprising:

an electrical outlet box having a back wall, a pair of opposed bottom walls and a pair of opposed side walls;

an extending compartment attached to each of said pair of opposed side walls defining first extending compartment and second extending compartment;

an adjustable box locator slidably attached to said first extending compartment; and

a support bracket adjustably attached to said second extending compartment.

5. An electrical outlet box assembly of claim 4, wherein said box locator is a right angled member having an attachment surface and a mounting surface perpendicular thereto, said attachment surface is slidably attached to said first extending compartment.

6. An electrical outlet box assembly of claim 5, wherein said first extending compartment further including a pair of

rails which slidably attaches said first extending compartment to said box locator.

7. An electrical outlet box assembly of claim 6, wherein said attachment surface of said box locator further includes protrusions to prevent dislodgment of the box locator from said pair of rails.

8. An electrical outlet box assembly of claim 7, wherein said support bracket includes a pair of opposed right angled stop members and an elongated body therebetween.

9. An electrical outlet box assembly of claim 8, wherein said elongate body having a central elongated slot and an attachment screw therethrough to attach said support bracket to said second extending compartment.

10. An electrical outlet box assembly for adjustable positioning with respect to a wall stud comprising:

an electrical outlet box having a back wall and a pair of opposed side walls;

an extending compartment attached to each of said pair of opposed side walls defining first extending compartment and second extending compartment;

an adjustable box locator having an attachment surface and a mounting surface perpendicular to said attachment surface, said attachment surface is slidably attached to said first extending compartment, said first extending compartment further including a pair of rails which slidably attaches said first extending compartment to said box locator, said attachment surface of said box locator further includes protrusions to prevent dislodgment of the box locator from said pair of rails; and

a support bracket includes a pair of opposed right angled stop members and an elongated body therebetween; said elongate body having a central elongated slot and an attachment screw therethrough to adjustably attach said support bracket to said second extending compartment, said second extending compartment further including a pair of rails to engage with said support bracket providing adjustable attachment thereto.

* * * * *

US007628286B2

(12) **United States Patent**
Lalancette

(10) **Patent No.: US 7,628,286 B2**
(45) **Date of Patent: Dec. 8, 2009**

(54) **ELECTRICAL OUTLET BOX ASSEMBLY FOR ADJUSTABLE POSITIONING WITH RESPECT TO A STUD**

(75) Inventor: **Daniel Lalancette**, L'Acadie (CA)

(73) Assignee: **Thomas & Betts International, Inc.**, Wilmington, DE (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 661 days.

(21) Appl. No.: **11/263,688**

(22) Filed: **Nov. 1, 2005**

(65) **Prior Publication Data**

US 2006/0108362 A1 May 25, 2006

Related U.S. Application Data

(60) Provisional application No. 60/630,005, filed on Nov. 22, 2004.

(51) **Int. Cl.**
H02G 3/08 (2006.01)
H02G 3/16 (2006.01)

(52) **U.S. Cl.** **220/3.7**; 220/3.92; 220/3.9; 220/3.6

(58) **Field of Classification Search** ..... 220/3.2–3.94; 174/17 R
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

876,187	A *	1/1908	Hornsby	220/3.5
1,113,092	A *	10/1914	Beugler	220/3.5
1,133,946	A *	3/1915	Farrell	220/3.4
1,275,692	A *	8/1918	Hubbell	220/3.7
1,275,725	A *	8/1918	Newton	220/3.7
1,774,934	A *	9/1930	Mangin	220/3.92
1,774,935	A *	9/1930	Mangin	174/63
1,814,449	A *	7/1931	Morgenstern	220/3.9
1,983,670	A *	12/1934	Knight	248/228.3
2,032,636	A *	3/1936	Seckinger	220/3.9
2,272,846	A *	2/1942	Lindstrom	220/3.6
2,286,898	A *	6/1942	Cover	220/3.6
2,374,622	A *	4/1945	Rugg	174/58
2,422,847	A *	6/1947	Peter	362/133
2,432,555	A	12/1947	Smith	
2,473,051	A	6/1949	Carlson	
2,512,188	A	6/1950	Wait et al.	
2,605,923	A *	8/1952	Bergquist	220/3.9
2,917,199	A *	12/1959	Appleton	220/3.7
3,115,265	A *	12/1963	Mulkey et. al.	220/3.5
3,148,698	A *	9/1964	Arnold	137/360
3,365,156	A *	1/1968	Beck	248/205.1
3,633,782	A	1/1972	Bellinger	
3,767,151	A	10/1973	Seal et al.	
3,834,658	A	9/1974	Theodorides	
4,057,164	A	11/1977	Maier	
4,062,470	A *	12/1977	Boteler	220/3.3
4,732,356	A	3/1988	Medlin, Sr.	

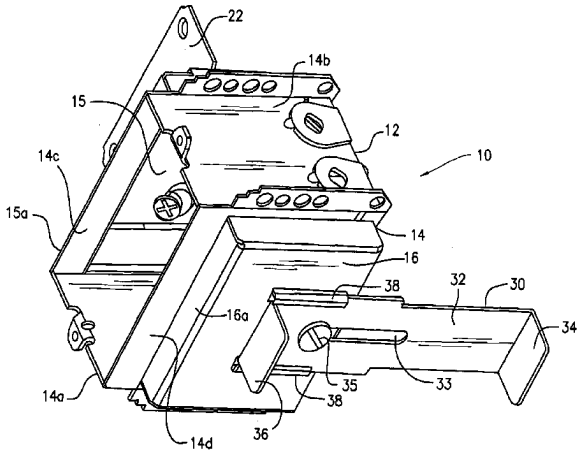
(Continued)

Primary Examiner—Anthony Stashick
Assistant Examiner—Ned A Walker
(74) *Attorney, Agent, or Firm*—Hoffmann & Baron, LLP

(57) **ABSTRACT**

The present invention is directed to an electrical outlet box assembly for adjustable positioning with respect to a wall stud. An electrical outlet box includes plural side walls defining a box interior having an open front face. A box locator is adjustably positioned on one of the side walls so as to adjust the location of the front face with respect to the stud to which the box locator is mounted. A support bracket is adjustably attached to another of the side walls for supporting the adjustably positioned box with respect to the back wall board.

7 Claims, 4 Drawing Sheets



U.S. PATENT DOCUMENTS

4,898,357	A		2/1990	Jorgensen et al.
4,964,525	A		10/1990	Coffey et al.
4,978,092	A		12/1990	Nattel
5,031,789	A		7/1991	Dauberger
5,253,831	A		10/1993	Theodorides
5,289,934	A		3/1994	Smith et al.
RE34,786	E		11/1994	Slough
5,378,854	A	*	1/1995	Hoover 174/53
5,596,174	A	*	1/1997	Sapienza 174/57
5,603,424	A	*	2/1997	Bordwell et al. 220/3.5
5,646,371	A		7/1997	Fabian
6,218,615	B1	*	4/2001	Canonico 174/50
6,749,162	B2	*	6/2004	Nicolides et al. 248/231.9
6,765,146	B1	*	7/2004	Gerardo 174/58
6,903,272	B2	*	6/2005	Dinh 174/58
6,956,172	B2	*	10/2005	Dinh 174/58
6,979,780	B1	*	12/2005	Lalancette 174/50
7,082,728	B1	*	8/2006	McConaughy et al. 52/220.1
7,141,736	B2	*	11/2006	Plankell 174/50
7,271,335	B2	*	9/2007	Dinh 174/58
2003/0024725	A1	*	2/2003	Lalancette et al. 174/58
2004/0045960	A1	*	3/2004	Rose 220/3.9

* cited by examiner

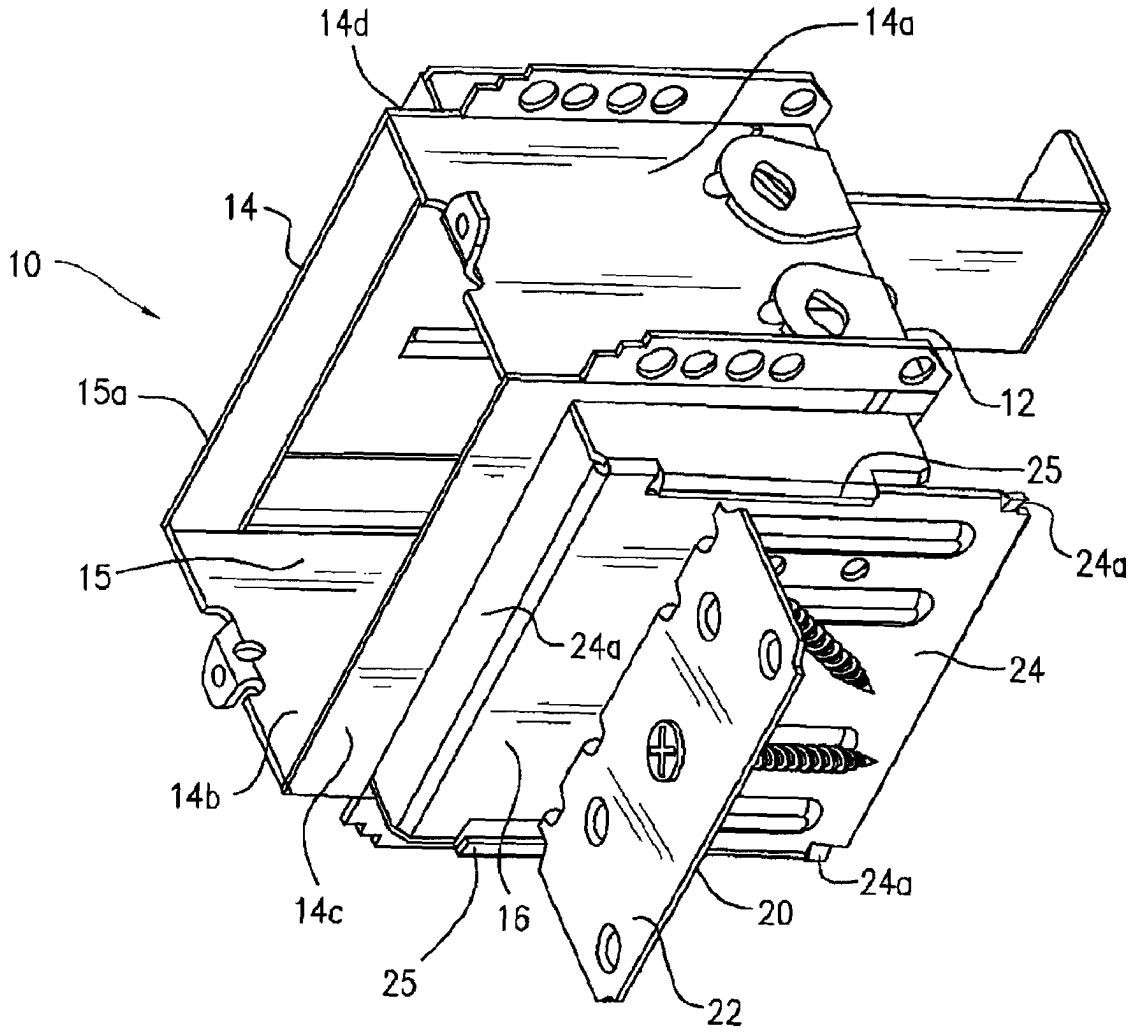


FIG. 1

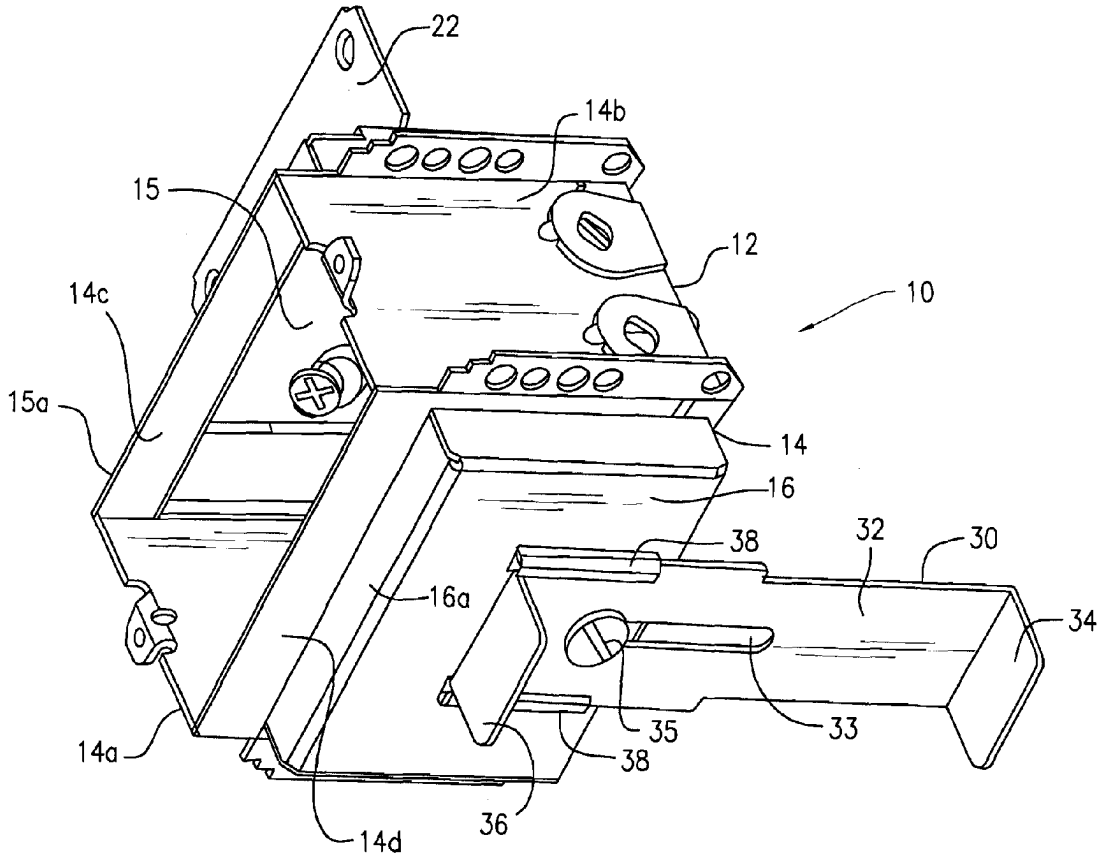


FIG. 2

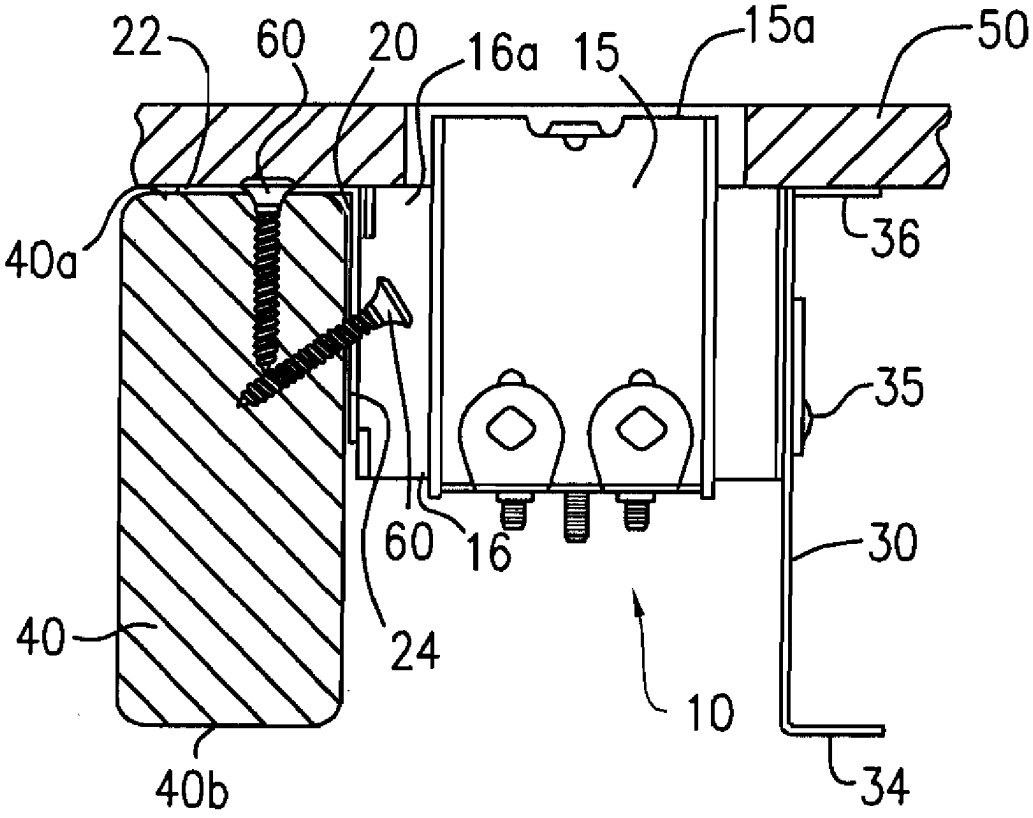


FIG. 3

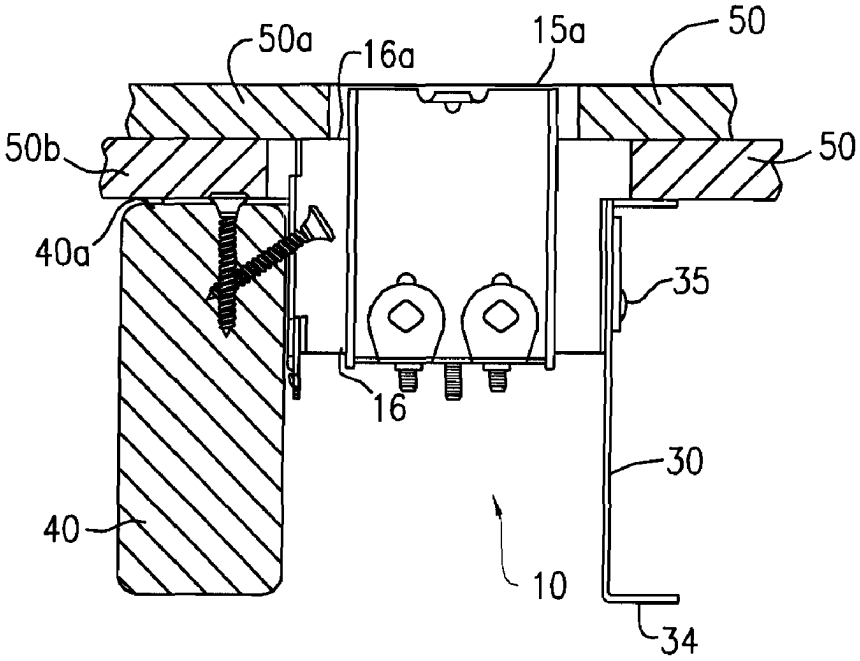

50a
16a
15a
50
50b
50
40a
35
16
30
40
10
34

FIG. 4

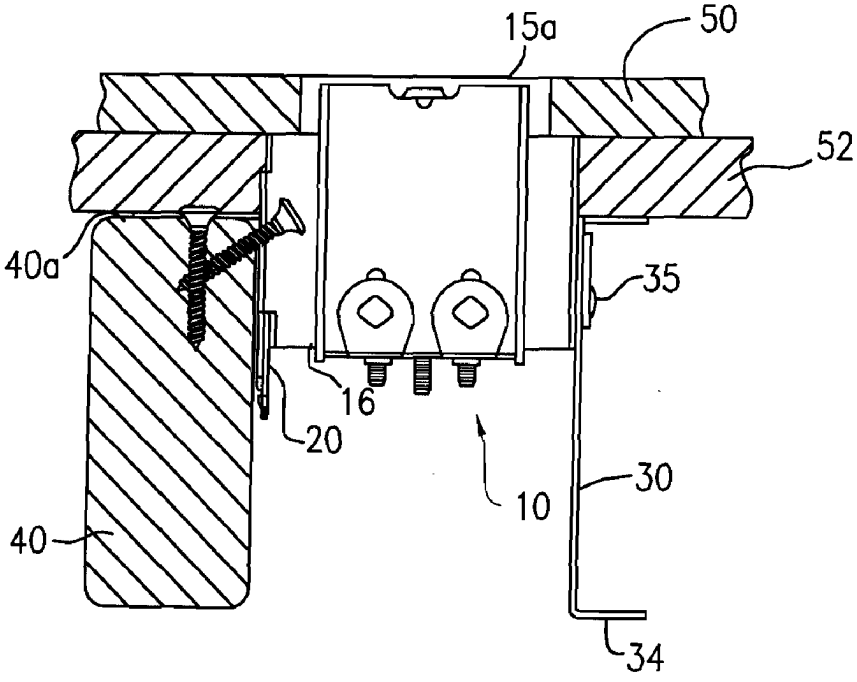

15a
50
52
40a
35
16
20
30
10
40
34

FIG. 5

ELECTRICAL OUTLET BOX ASSEMBLY FOR ADJUSTABLE POSITIONING WITH RESPECT TO A STUD

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. Provisional Application No. 60/630,005 filed Nov. 22, 2004.

FIELD OF THE INVENTION

The present invention relates generally to an electrical outlet box mounted to a wall stud. More particularly the present invention relates to an electrical outlet box which may be adjustably mounted to the wall stud so as to accurately position the outlet box with respect to the wall stud.

BACKGROUND OF THE INVENTION

Electrical outlet boxes are widely used to house electrical components such as switches and receptacles for termination of electrical wires run through the wall of a structure. Typically, these electrical outlet boxes are mounted to a wall stud supporting structural wall board. In new construction, the outlet box is mounted to the wall stud prior to attachment of the wall board. Thus, the outlet box must be properly positioned with respect to the stud so that the front face of the outlet box is aligned with the front of the wall board once it is placed against the stud. Such positioning of the box must be taken into consideration for the various thickness and layers of wall board.

In addition to such accurate mounting, subsequent electrical termination of the switches and receptacles in the box may cause the box to be moved or displaced once secured. In certain situations, there may be a tendency for the electrical installer to push the box inwardly into the wall cavity rendering the box useless.

The art has seen a number of brackets which are used in combination with stud mounted electrical boxes to both accurately align the front face of the outlet box with respect to the wall board and to prevent the box from being pushed into the wall cavity.

U.S. Pat. No. 4,978,092 shows an adjustable support bracket that prevents the box from being pushed into the wall cavity.

U.S. Pat. No. 2,473,051 also shows a box having an adjustable support preventing the box from being pushed into the cavity.

U.S. Pat. Nos. 5,289,934, 5,253,831 and 3,834,658 show adjustable stud mounted brackets which allow the box to be adjustably positioned with respect to the wall stud.

None of the prior art devices, however, allow both for adjustment of the box once the box is attached to the wall stud, as well as providing separate independent structure to prevent the adjusted box from being pushed into the wall cavity.

SUMMARY OF THE INVENTION

The present invention provides an electrical outlet box assembly for adjustable positioning with respect to a wall stud. An electrical outlet box includes plural side walls defining a box interior having an open front face. A box locator is adjustably positioned on one of the side walls. The box locator includes a mounting surface parallel to the open front face of the box and an attachment surface perpendicular thereto. The attachment surface is adjustably positioned along one of the side walls so as to adjust the location of the front face with respect to the stud to which the box locator is mounted. The attachment surface is fixable to the side wall upon adjustable positioning of the front face of the box. A support bracket is provided. The support bracket is adjustably attached to another of the side walls for supporting the adjustably positioned box with respect to the back wall board.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. **1** and **2** are perspective opposite side showings of adjustable electrical outlet box of the present invention.

FIGS. **3-5** show the adjustable electrical outlet box of FIG. **1** accommodating various thicknesses and numbers of wall board.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides an electrical outlet box for supporting electrical components such as switches and receptacles (not shown). In conventional fashion, the stripped ends of insulated wires (not shown) are run into the box so as to be terminated to the components mounted within the box. The box itself is designed to be secured to a wall stud such that when wall board is placed over the wall stud, the front face of the box is positioned generally flush thereto.

Referring now to FIGS. **1** and **2**, the electrical outlet box **10** of the present invention is shown. Box **10** includes a back wall **12**, perimetrical side **14** including top and bottom walls **14***a* and **14***b* and opposed lateral side walls **14***c* and **14***d*. The box defines a box interior **15** where the components are terminated and supported. Each of the side walls **14***c* and **14***d* includes an extending compartment **16** so as to increase the interior volume of box **10**.

The extending compartments **16** define extending forward surfaces **16***a* which are generally parallel to the open front face **15***a* of box **10**. As will be described in further detail herein below, the surfaces **16***a* are used to support wall board so that the front face **15***a* of the box may be positioned flush thereto.

Referring specifically to FIG. **1**, box **10** includes an adjustable box locator **20** which is slidably attached to the side of compartment **16**. The box locator **20** is generally a right angled member having a mounting surface **22** positioned generally parallel to front face **15***a* and an attachment surface **24** perpendicular thereto. The attachment surface **24** is held to compartment **16** by a pair of rails **25** which slidably accommodate attachment surface **24**. The distal edges of attachment surface **24** may include protrusions **24***a* to prevent dislodgement of the locator from the box. The box locator **20** allows the box **10** to be adjustably positioned with respect to a wall stud as will be described in further detail herein below.

Referring now to FIG. **2**, a support bracket **30** is adjustably attached to compartment **16** on the opposite side wall **14***d* of box **10**. Support bracket **30** includes an elongate body **32** having right angled stop members **34** and **36** extending from the ends thereof. Body **32** has a central elongate slot **33** through which an attachment screw **35** extends so as to attach the support bracket to the compartment **16**. The box is slidably coupled to compartment **16** by a pair of rails **38** so that the support bracket **30** can be slidably adjustably positioned along compartment **16**. As will be described in further detail herein below, the support bracket **30** is adjustably positioned so that stop **36** abuts against the inside of wall board and stop **34** is positioned adjacent the opposed wall board to prevent the box from being pushed into the wall during use.

Having described the components of the adjustable box of the present invention, its use may be described with respect to FIGS. **3-5**.

As shown in FIG. **3**, the box **10** of the present invention may be supported to a wall stud **40** in such a manner that it accommodates a single thickness of ½" wall board **50**. The box is installed on the stud in the following manner. The mounting surface **22** of box locator **20** is secured to the face **40***a* of the stud using a conventional mounting screw **60**. The box **10** is then adjustably positioned by slidable movement of the box with respect to the locator **20** such that the front face **15***a* of the box extends approximately 7/16" from the face **40***a* of the stud. Once the box is properly positioned, a second screw **60** may be installed through the interior **15** of the box and through the attachment surface **24** to fix the position of the box with respect to the stud. The wall board **50** may now be attached to the stud **40**. A ledge **16***a* formed by compartment **16** serves to seat the wall board **50**. In this position, the front face **15***a* of the box is fixed at a position nearly flush with the wall board. Once the position of the front face of the box is fixed, support bracket **30** may be slidably positioned with respect to wall board **50**. The attachment screw **35** is loosened so that the support bracket **30** can be slidably adjustably positioned along the box. The bracket **30** is positioned such that stop **36** is slidably positioned against wall board **50**. The length of the support member is selected such that when properly positioned, the opposite stop **34** will be positioned next adjacent the wall board (not shown) which is attached to the opposite face **40***b* of stud **40**. In this manner, during use and installation, and subsequently upon reattachment of components to box **10**, the box will not be pushed into the wall.

FIG. **4** shows a similar mounting technique for box **10** employed with two layers of ½" wall board **50**. In this embodiment, the box **10** is adjusted such that the front face **15***a* thereof is aligned substantially flush with the outer wall board surface at a distance of approximately 15/16" from face **40***a* of stud **40**. The wall boards **50***a* and **50***b* are attached to the stud **40** such that the outer wall board **50***a* is positioned over ledge **16***a* of compartment **16** while the inner wall board **50***b* is positioned rearwardly and to the side of compartment **16**. The bracket **30** is adjusted so that the stop **36** abuts against the inner surface of wall board **50***b*. In this position, opposed stop **34** abuts against the wall board attached to the face **40***b* of stud **40** to prevent the box from being inadvertently pushed into the wall during use.

As shown in FIG. **5**, box **10** may also be used to accommodate multiple layers of different thicknesses of wall board. For example, in FIG. **5**, wall board **50** which is ½" wall board is combined with wall board **52** which is ¾" wall board. In this embodiment, the front face **15***a* of box **15** is positioned approximately 15/16" from the face **40***a* of stud **40**. The adjustable positioning of both the box locator **20** and the support bracket **30** accommodate this combination by adjustment in a manner similar to that described with respect to FIGS. **3** and **4**.

Furthermore, it is contemplated that the present invention can be used with a variety of wall board thicknesses as well as a variety of multiples of wall board layer. In each case, the box is adjustably positioned with respect to box locator **20** so as to position the front face **15***a* of box **10** substantially flush with the outer surface of the wall board. In the same manner, support bracket **30** can be adjustably positioned so as to prevent the box during use from being pushed into the wall.

What is claimed is:

1. An electrical outlet box assembly for adjustable positioning with respect to a wall stud comprising:

an electrical outlet box having a back wall, a pair of opposed bottom walls and a pair of opposed side walls;

an extending compartment attached to each of said pair of opposed side walls defining first extending compartment and second extending compartment;

an adjustable box locator slidably attached to said first extending compartment, a mounting screw extending through said first extending compartment and said adjustable box locator for attachment of said electrical outlet box to said stud; and

a support bracket adjustably attached to said second extending compartment, said support bracket is U-shaped including one side adjacent to said second extending compartment and two sides extending perpendicular to said one side to provide support of said electrical box preventing said electrical box from being pushed into a wall.

2. An electrical outlet box assembly of claim **1** wherein said box locator is a right angled member having an attachment surface and a mounting surface perpendicular thereto, said attachment surface is slidably attached to said first extending compartment.

3. An electrical outlet box assembly of claim **2**, wherein said first extending compartment further including a pair of rails which slidably attaches said first extending compartment to said box locator.

4. An electrical outlet box assembly of claim **3**, wherein said attachment surface of said box locator further includes protrusions to prevent dislodgment of the box locator from said pair of rails.

5. An electrical outlet box assembly of claim **4**, wherein said support bracket includes a pair of opposed right angled stop members and an elongated body therebetween.

6. An electrical outlet box assembly of claim **5**, wherein said elongated body having a central elongated slot and an attachment screw therethrough to attach said support bracket to said second extending compartment.

7. An electrical outlet box assembly for adjustable positioning with respect to a wail stud comprising:

an electrical outlet box having a back wail and a pair of opposed side walls;

an extending compartment attached to each of said pair of opposed side walls defining first extending compartment and second extending compartment;

an adjustable box locator having an attachment surface and a mounting surface perpendicular to said attachment surface, said attachment surface is slidably attached to said first extending compartment, said first extending compartment further including a pair of rails which slidably attaches said first extending compartment to said box locator, said attachment surface of said box locator further includes protrusions to prevent dislodgment of the box locator from said pair of rails; and

a support bracket includes a pair of opposed right angled stop members and an elongated body therebetween; said elongate body having a central elongated slot and an attachment screw therethrough to adjustably attach said support bracket to said second extending compartment. said second extending compartment farther including a pair of rails to engage with said support bracket providing adjustable attachment thereto.

* * * * *

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2007 (06.12.2007)

PCT

(10) International Publication Number
WO 2007/140487 A2

(51) International Patent Classification:
G06F 7/04 (2006.01)

(21) International Application Number:
PCT/US2007/070244

(22) International Filing Date: 1 June 2007 (01.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/803,683 1 June 2006 (01.06.2006) US
11/756,824 1 June 2007 (01.06.2007) US

(71) Applicant *(for all designated States except US)*: **VERIFIDES TECHNOLOGY CORP.** [US/US]; 1221 Avenue Of the Americas, 26th Floor, New York, NY 10022 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **LACK, Michael** [US/US]; Arlington, VA (US). **STURTEVANT, Dan** [US/US]; Arlington, VA (US). **LALANCETTE, Chris** [US/US]; Arlington, VA (US).

(74) Agent: **OSTROW, Seth H.**; Dreier LLP, 499 Park Avenue, New York, NY 10022 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 2007/140487 A2

(54) Title: DATA ACCESS CONTROL SYSTEMS AND METHODS

(57) Abstract: Various hardware and software configurations are described herein which provide improved security and control over protected data. In some embodiments, a computer includes a main motherboard card coupled to all input/output devices connected to the computer, and a trusted operating system operates on the main motherboard which includes an access control module for controlling access to the protected data in accordance with rules. The trusted operating system stores the protected data in an unprotected form only on the memory devices on the main motherboard. The computer may also have a computer card coupled to the main motherboard via a PCI bus, on which is operating a guest operating system session for handling requests for data from software applications on the computer. A tamper detection mechanism is provided in the computer for protecting against attempts to copy the unprotected form of the protected data onto memory devices other than the one or more memory devices used by the motherboard or computer card.

DATA ACCESS CONTROL SYSTEMS AND METHODS

[0001] This application claims the benefit of provisional patent application No. 60/803,683, entitled "DATA ACCESS CONTROL," filed June 01, 2006, Attorney Docket No.12492.0290, which application is hereby incorporated herein by reference in its entirety.

FIELD OF INVENTION

[0002] The invention relates to methods and devices for controlling access to data.

BACKGROUND OF THE INVENTION

[0003] A computer system and associated methods and devices for distributing protected data and controlling access to and use of such data in accordance with rules are disclosed, for example, in U.S. Patent No. 5,933,498 to Schneck *et al.* entitled "System for Controlling Access and Distribution of Digital Property," which issued on August 3, 1999, the entire contents of which patent are incorporated herein by reference.

[0004] The ongoing advancement of computer hardware and software technologies, and the widespread use of networks such as the internet to distribute content in digital form, necessitate continued improvements in technologies for protecting digital content during distribution and use. The present inventions provide various improved configurations of hardware and/or software for controlling access to protected digital content.

SUMMARY OF THE INVENTION

[0005] Various hardware and software configurations are described herein which provide improved security and control over protected data. In some embodiments, a computer or computing system including multiple computers is provided. The computer includes a main motherboard card, having one or more first processors and one or more first memory devices such as RAM, being coupled to all input/output devices connected to the computer to input data into the computer or output data from the computer, such as hard or optical disk drives, USB ports, or network interfaces. A trusted operating system is programmed to operate on the main motherboard, and includes an access control module for controlling access to the protected data

in accordance with one or more rules. The rules may be specified in tickets received from a ticket server. The trusted operating system stores the protected data in an unprotected form, for example, when it has been decrypted, only on the first memory devices on the main motherboard.

[0006] In accordance with some embodiments, the computer may also have a computer card, having one or more second processors and one or more second memory devices, which is coupled to the main motherboard via a PCI bus. One or more guest operating system sessions may be running on the one or more computer cards for handling requests for data from one or more software applications on the computer. The software applications are usable to access and process the protected data in its unprotected form.

[0007] In some embodiments, a tamper detection mechanism is provided in the computer for protecting against attempts to copy the unprotected form of the protected data onto memory devices other than the one or more first or second memory devices. The tamper detection mechanism may further disable any further access to the protected data in its unprotected form by, for example, deleting any decryption keys used to decrypt and thus unprotect the protected data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The invention is illustrated in the figures of the accompanying drawings which are meant to be exemplary and not limiting, in which like references are intended to refer to like or corresponding parts, and in which:

[0009] FIG. 1 presents an exemplary embodiment of an architecture of a VeriFIDES client/server system;

[0010] FIG. 2 presents a preferred embodiment of an originator/recipient architecture implementing the VeriFIDES system;

[0011] FIG. 3 presents an alternative embodiment of the VeriFIDES system comprising a motherboard and communicatively coupled processing board;

[0012] FIG. 4 presents an alternative embodiment of the VeriFIDES system comprising VeriFIDES logic implemented as a PCI bridge.

[0013] FIG. 5 presents an alternative embodiment of the VeriFIDES system comprising the VeriFIDES system implemented as a co-processor;

[0014] FIG. 6 presents an exemplary system of the present invention comprising the VeriFIDES system residing on a separate peripheral card;

[0015] FIG. 7 presents a further embodiment of a guest operating system running on a card connected to a main computer;

[0016] FIG. 8 presents a taxonomy of ticket types on a machine;

[0017] FIG. 9 comprises a diagram illustrating how VeriFIDES can be used to limit the sphere of compromise of data;

[0018] FIG. 10 illustrates an alternative embodiment utilizing a remote desktop design for implementing the VeriFIDES system;

[0019] FIG. 11 provides an alternative embodiment for providing session connections to the VeriFIDES enabled PC;

[0020] FIG. 12 illustrates a method for monitoring incoming network packets in a preferred embodiment; and

[0021] FIG. 13 illustrates a method for monitoring outgoing network packets in a preferred embodiment.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0022] In the following description, reference is made to the accompanying drawings that form a part hereof, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

[0023] FIG. 1 illustrates an embodiment of an architecture of a client/server system according to the invention, which system shall be referred to herein as VeriFIDES™ in its

various embodiments described herein. As illustrated in FIG. 1, the VeriFIDES client/server architecture includes a VeriFIDES machine 101 and a VeriFIDES server 102. Within the VeriFIDES machine 101, a VeriFIDES operating system 103 runs separately from a plurality of user operating systems 104 and 105 running on the VeriFIDES machine 101. The VeriFIDES operating system 103 may contain an access control mechanism comprising a small footprint software component that executes on trusted hardware 106 underneath operating systems 104 and 105, as described further below.

[0024] The user operating systems 104 and 105 are the operating systems that control user interactions with the machine and which receive requests from the user to access information stored in the machine or elsewhere. In a preferred embodiment the VeriFIDES system never trusts operating systems 104 and 105. As a result, applications 107a-b, protocols/drivers 107c-d, and even the kernels themselves resident within the operating systems 104 and 105 may be compromised without loss of the security of the system. The compromise of applications, protocols, drivers or the kernels resident within the operating systems may lead to a denial of service, but a denial of service is preferable to leaking information.

[0025] The kernels for the user operating systems 104 and 105 and VeriFIDES operating system 103, although not illustrated, are resident within the operating systems operating between applications and hardware, or perceived hardware. The structure of an operating system is commonly understood in the art.

[0026] All input and output in the system comes from the access control mechanism resident in the VeriFIDES operating system 103. Input and output may include network, USB, CD-ROM and floppy traffic via the trusted hardware 106. This ensures that before any data ever makes it into the hands of the user, the VeriFIDES system has had time to examine it and to make decisions about whether this user has the right to see this information.

[0027] Sensitive information is protected by encryption. Data is always encrypted until it gets into the memory on the user's operating system 104 or 105. This ensures that even if hard

drives are lost, or data given to rogue users, the data cannot be examined unless access was specifically granted to that user. The VeriFIDES operating system 103 may encrypt data via any encryption means known in the art such as RSA, DSA, IDEA, etc.

[0028] Access to information is controlled through tickets. A ticket generally grants the user the right to access protected content protected by the VeriFIDES system. A ticket consists of the content decryption key and a set of access rights authorized for the end-user. In a preferred embodiment, particular permissions to that user may include how long they can see the document, whether or not they can print or perform other operations on the document, etc. This is how originator control is retained; the originator only grants the permissions that he or she wishes to. The use of tickets lets the originator pre-stage data; in particular, they may send out the document ahead of time, and then grant permissions to individuals as they require it. The concept of tickets is described more fully with respect to FIG. 8.

[0029] A VeriFIDES server 102 contains a ticket server 112 responsible for maintaining a list of the known VeriFIDES enabled computers, a list of protected data and their associated encryption keys. In addition, the ticket servers maintain the associations between access rights and protected content.

[0030] A VeriFIDES server 102 is further responsible for all of the administration of the (possibly many) VeriFIDES machines 101 it is in charge of. This includes granting tickets, revoking tickets, looking at access patterns, etc. A VeriFIDES server 102 has a working knowledge of what is going on with all of the machines it is in charge of, generally through the a plurality of audit logs.

[0031] Audit logs are located within and processed by the audit server 108. All actions on any VeriFIDES machine 101 are logged and sent over to the VeriFIDES audit server 108. These logs can then be viewed by the originator or administrator, and appropriate actions can be taken, such as revocation of tickets, disciplinary action, etc.

[0032] In one aspect, an application of the audit and logging functionality of the VeriFIDES server 102 is provided that can be used to drastically reduce the scope of questionable data in the event of a compromise. In another aspect, a modification to the way in which VeriFIDES processes tickets is provided that allows for 'state-based' access control over data.

[0033] Other audit and logging tools of the prior art can perform similar functions for narrowing the sphere of compromise. Technologies such as Apple's iPod perform 'state-based' access control. However, such other tools cannot guarantee the integrity or fidelity of their audit logs. Also, Apple's iPod only works on specific data formats and platforms.

[0034] In accordance with the present invention, to limit the sphere of compromise, the VeriFIDES audit logs indicate what particular files / data a user had a ticket for. Additionally, since all I/O in the computer goes through VeriFIDES, the logs indicate when and how particular files are accessed. Finally, since the logs are being generated beneath (and thus unaware of by) the operating system, much greater guarantees about the integrity of the logs can be provided. Thus, in the event of compromise, it is possible to know exactly what files a particular user had tickets or decryption keys for, when those files were accessed, and what type of access (view, copy, print, etc.) occurred.

[0035] In one embodiment, the VeriFIDES system involves running multiple instances of an operating system 104 and 105, such as Windows, (called the "guests") on a non-persistent disk in VMWare on Linux 103 (called the "host"). All of the VeriFIDES logic, decision making, and access control happens on the host, so that the user doesn't have any influence over these parameters. All of the services that the guests may need are served up through the host, including, but not limited to: NTP, DNS, USB connectivity, CDROM I/O, CD burning, hard drive, email, and internet/web. Embodiments utilizing multiple operating system sessions are described more fully with respect to FIGS. 10-11.

[0036] Returning to FIG. 1, the access control daemon, which is the heart of the VeriFIDES operating system 103, is a process that continually runs on the host system. All processes running on guest operating systems 104-105 come to access control to find out if they are allowed to do what they are currently doing, and if so, how to decrypt that data. Both of the preceding decisions are based on the tickets currently open and/or the tickets available to be opened. Without a ticket, access control will not allow any process to decrypt data from disk. With a proper ticket, however, access control will give the requesting process the key to decrypt the data, and that process will then go and decrypt it.

[0037] FIG. 8 presents a taxonomy of ticket types on a machine. In a preferred embodiment of the present invention, there are 2 classes of tickets: AUTHENTICATION and DATA. In addition, there are 4 types of tickets: user 304, file 302, host 303, and connection 301. In particular, AUTHENTICATION TICKETS may be user and host, while DATA TICKETS may be file and connection. Authentication tickets may allow users and other machines to authenticate themselves with the VeriFIDES machine. Data tickets may control access to protected content.

[0038] User Tickets 304 may define a user on the machine. They may contain a username and a domain that specify the user's identity. They also may contain userKey fields in the authentication section which will be compared against the data the user provides during authentication. These userKeys would contain a hash of a passphrase, a secret number in a smartcard, characteristics of a fingerprint, etc. User tickets 304 may also contain permissions indicating the usage restrictions for that user irregardless of any data accessed.

[0039] File Tickets 302 may be bound to a protected file or set of protected files. They may contain the symmetric key needed to decrypt the file. This type is used not only for files, but also for static web pages and emails. They may contain a permissions section which restricts the state of the session after the file has been accessed.

[0040] Host Tickets 303 are a special case in that they do not directly enable communication for the user. They may contain the public key of other VeriFIDES machines that this machine may want to talk to. This serves as a Public Key Infrastructure. This ticket is required to allow access control to communicate with other machines while sending audit logs, requesting tickets, or negotiating network connections with other VeriFIDES machines or gateways on behalf of the user of the guest machine. This ticket lacks information regarding authentication or permissions because it is used by access control rather than the user on the guest machine. A machine must be pre-staged with at least one Host ticket. This will be the host ticket of its trusted Ticket Server.

[0041] Connection Tickets 301 may define a connection that a guest machine can make to another VeriFIDES machine or gateway. Connection tickets 301 may contain a symmetric key to encrypt network traffic using that connection. In some embodiments, connection tickets 301 may not contain a key because the key may be negotiated with the other host by access control. The connection tickets 304 may define the machine, other machine, port, server vs. client access, and service that can be accessed. Wildcards may be used to allow this connection ticket to apply to any port or to allow it to apply to communication initiated by either end.

[0042] Each ticket contains a binding which is used to associate the ticket with a piece of protected data it is intended to grant access to. In a preferred embodiment, a ticket will contain a binding that will also be found in the footer of a protected file. VeriFIDES compares the binding in the file with the bindings in tickets to determine which ticket to decrypt the file with.

[0043] In any session, the set of open bindings defines the "context" of that session. This "context" describes who is accessing what protected data. This context will be used to support derivative works.

[0044] Tickets will also describe "permissions" that will be used to restrict the use of the data protected by that ticket. Each session will maintain an intersection of the permissions of all its open tickets/bindings. For example, accessed data is protected by Ticket A and Ticket B.

Ticket A's permissions require that your external media be read only. Ticket B's permissions shut off printing and require the session to end at 5:00 PM. The session is now in a state that combines all those restrictions.

[0045] The ticket identifier tells access control what and who this ticket is meant to be used for. It is one of the few fields that is dynamic depending on the ticket type. Tickets will either specify a user or use a wildcard that allows use by any user with the ability to log into the machine.

[0046] Tickets will only be able to be used to open documents while in a session at a specified classification level unless the ticket contains a wildcard that indicates that the ticket can be used to access data within any protected session on that machine.

[0047] The authentication methods of a ticket higher in FIG. 8 override the methods specified by ticket lower in FIG. 8 if they are more restrictive. For example, a user ticket may contain keys for fingerprint, smartcard, and passphrase but only require the passphrase for user login. A file ticket may require fingerprint authentication. The system would ask the user for a fingerprint when the user tried to access the file. In addition a higher level ticket may override the userKey required. A specific file might require a different smartcard than the one the user authenticated with or require a different password.

[0048] Appendix A at the end of this specification, and forming part hereof, contains a sample file structure for an XML file for storing and delivering tickets in accordance with embodiments of the present invention.

[0049] Returning to FIG. 1, in embodiments of the present invention, the VeriFIDES system incorporates hardware tamper detection/reaction 109, the scaled-down trusted Linux containing the VeriFIDES operating system 103 running on the main hardware, and the VeriFIDES access control mechanism running within the VeriFIDES operating system. The embodiment of FIG. 1 may be modified by adding an additional single board computer card containing the guest operating systems 104-105 and applications 107a-d. The VeriFIDES

operating system may remain resident on a main motherboard, separate but communicatively coupled to the single board computer card via a bus such as a PCI bus. In the discussion of this embodiment, references to the operating system are, unless otherwise specified, references to the guest sessions executing on the single board computer card, and references to the computer's RAM refer, unless otherwise specified, to RAM both on the motherboard and on the single board computer card.

[0050] All access control and encryption/decryption logic exists in the VeriFIDES operating system 103 (at least one user operating system 104-105) and is thus invisible to both the user operating system 104-105 and all application software 107a-b and protocols/drivers 107c-d. The VeriFIDES system operates at a level akin to a virtual machine from the perspective of the guest sessions 104-105, in that the guest sessions 104-105 are only aware of the hardware on the single board computer card and motherboard hardware that the VeriFIDES operating system 103 makes visible. Given that, the VeriFIDES system is transparent to the guest sessions 104-105 and applications 107a-b and protocols/drivers 107c-d running within them.

[0051] Protected data exist in decrypted form only in the RAM resident in the trusted motherboard hardware 106 of the VeriFIDES protected computers 101. Data are encrypted when at rest and while in transit. When an application in a guest session 104-105 attempts to access data, if the user is allowed to access that data, the VeriFIDES operating system 103 will decrypt that data inside the RAM on the motherboard, and then 'serve' the data up to the guest session via the PCI bus.

[0052] This decrypted data will exist in the RAM on the single board computer card as well, making them accessible to the guest sessions 104-105 and applications 104-105 running within the guest sessions 104-105. Thus, protected data exist in decrypted form only in the RAM and PCI bus of both the motherboard and the single board computer card.

[0053] Hardware tamper-detection 109 protects against attempts to copy the decrypted data from the system's RAM 106 or to load malicious software onto the VeriFIDES operating system 103. Given that the VeriFIDES operating system 103 resides at a level inaccessible to the guest sessions 104-105, it is secure from software attacks launched within these sessions, as will be described later. Thus, the only way to get information out of the machine would be via some sort of hardware-based attack such as probing the RAM or PCI bus on either the motherboard or the single board computer card.

[0054] In the architecture presented in FIG. 1, the entire contents of the computer's case would need to be protected, preventing probing of either PCI bus or RAM banks. VeriFIDES supports interaction with hardware tamper detection/reaction 109, but does not necessarily specify what type/strength of detection should be employed. Upon tamper detection, VeriFIDES can immediately zeroize the private key stored within private key storage 110, preventing the decryption of tickets, which in turn, prevents the decryption of protected data.

[0055] Data cannot leave a VeriFIDES protected operating system session 104-105 without being encrypted, unless the document originator gave specific permission to do so. All data leaving a guest session 104-105 executing on the single board computer card are intercepted by VeriFIDES access control 103 before they reach the computer's hardware 106 (hard disk, USB bus, network interface, CDRW drive, etc.). Permissions within a ticket specify what to do with this data. VeriFIDES access control 103 might encrypt the data with a specific symmetric key, prevent the data from reaching the hardware (providing a read-only capability), or, in special cases, allow the data to be written out un-encrypted.

[0056] All tickets are encrypted with a statistically-unique public/private key pair to prevent access to the data encryption key. Each VeriFIDES PC has a private key embedded in the hardware 110. Tickets are encrypted with the corresponding public key, ensuring that only the recipient host machine is able to decrypt the ticket. This mechanism relies on a public key

infrastructure. The cryptographic plug-in architecture of VeriFIDES system allows it to work with virtually any PKI technology.

[0057] The VeriFIDES system private key is stored in hardware 110 under the operating system, protected by tamper-detection/erasure circuitry 109, and thus is not accessible to the operating system 104-105, application software 107a-b or the end user, or a hacker.

[0058] As mentioned above, the guest sessions only have access to hardware exported by the VeriFIDES operating system 103. Thus, the private key is hidden and protected from the guest sessions. Because protection of this private key is critical to VeriFIDES security, tamper detection/reaction 109 can be employed in situations where physical attacks on the machine are a concern.

[0059] The data encryption key (protected by the encryption ticket) is only decrypted and visible in the VeriFIDES access control mechanism 103 and therefore cannot be used by the operating system, application software or the end user.

[0060] An embodiment of a single board card interacting with a motherboard card is described more with respect to FIGS. 10-11.

[0061] FIG. 2 illustrates a preferred embodiment of an originator/recipient architecture implementing the VeriFIDES system. As illustrated, an originator 2000 comprises at least one document application 2002, an operating system 2004, a VeriFIDES OS 2020 and trusted hardware 2006. The VeriFIDES OS 2020 further comprises a public key 2008, an encryption mechanism 2010, a secret key 2012, a secondary encryption mechanism 2016 and an original document 2014.

[0062] The VeriFIDES OS 2020 is operable to first encrypt a secret key 2012 via encryption mechanism 2010. This encrypted secret key is stored as a ticket allowing access to content protected by the originator. The secret key 2012 is also operable to encrypt a document 2014 via encryption mechanism 2016.

[0063] The generated ticket 2200 and cipher document 2300 are transmitted to a recipient machine 2100 containing an architecture similar to the originator machine 2000. As illustrated, a recipient machine 2100 comprises a document application 2102, an operating system 2104, a VeriFIDES operating system 2121 and trusted hardware 2106.

[0064] Upon receipt of the encrypted ticket 2200 and cipher doc 2300, the VeriFIDES OS 2121 is operable to decrypt the ticket 2200 with the same public key 2108 via decryption mechanism 2110. VeriFIDES OS 2121 is also operable to decrypt cipher doc 2300 via secret key 2112 through decryption mechanism 2116. The resulting document 2114 is provided to the user via operating system 2104 and document application 2102.

[0065] As mentioned above, the VeriFIDES operating system (including access control and encryption/decryption) exist at a level transparent to the guest sessions. Thus, the data encryption keys (which are stored in encrypted tickets) only exist in decrypted form in the RAM on the main motherboard. The RAM on the single board computer card never contains these keys.

[0066] In an alternative embodiment and as another layer of protection, a SunPCi card may be used in the system and running another version of Linux, which is then used to rdesktop into the guest. The user only ever interacts with this rdesktop session. Therefore, even if the user were malicious and attempted to break out of the rdesktop session, they would have two layers to get through to get to sensitive information; from rdesktop to the Linux on the card, and then from Linux on the card to Linux on the host. This provides a good layer of security.

[0067] FIG. 10 illustrates an alternative embodiment utilizing a remote desktop design for implementing the VeriFIDES system. As illustrated, a desktop PC running a version of Linux 1001 comprises a VeriFIDES access control module 1008, a plurality of Windows sessions executing in separate VMware processes 1009 and a plurality of output devices 1010. The desktop PC 1001 is communicatively coupled to a VeriFIDES card running another instance of Linux 1002. The VeriFIDES card comprises a non-transparent PCI bridge 1004, a plurality of

remote desktop client sessions 1003 and a plurality of input devices 1004. As illustrated, the remote desktop sessions 1003 are coupled to the desktop PC 1001 via remote desktop connection 1007 over the PCI bus. Furthermore, the non-transparent PCI bridge 1004 is connected to the VeriFIDES access control mechanism 1006 via the Linux hard disk 1006 and PCI bus.

[0068] A plurality of users may access the desktop PC via the remote sessions 1003. The VeriFIDES access control 1008 monitors the usage of users utilizing the desktop PC to ensure that malicious attempts are prevented as previous discussed. User input and output is routed from the remote sessions 1003 through the non-transparent PCI bridge 1004. Subsequently, any user input is routed from the non-transparent PCI bridge 1004 to the VeriFIDES access control 1008, thus eliminating the threat of misuse during input/output operations.

[0069] FIG. 11 provides an alternative embodiment for providing session connections to the VeriFIDES enabled PC. FIG. 11 provides two entities, the desktop PC running a scaled down trusted version of Linux 1102 and the VeriFIDES Card running a plurality of Microsoft Windows sessions 1101. A scaled down version of Linux would merely provide device drivers and minimal services required to interface with the hardware. A version of trusted Linux (SE, HP, etc.) could be used while stripping out components that are unnecessary for VeriFIDES, including X Windows, multi-user capability, network services, and others. "Userland" could be removed from Linux altogether and VeriFIDES code incorporated into the scaled-down kernel directly.

[0070] A user connects to the VeriFIDES PC via user devices 1107. The scaled-down Linux is only accessible from the guest sessions 1101 via the device drivers that are exported to the guest sessions. These drivers will interface over the PCI bus with the corresponding drivers running in the scaled-down Linux. The Linux device drivers need to be validated and trusted, to ensure that they do not provide a "back door" for the Windows sessions.

[0071] User input/output is handled by the non-transparent PCI bridge 1103. The non-transparent bridge 1103 handles all user interaction and handles the routing of protected data

1105 and Window sessions data 1106. As discussed previously, protected data 1105 and session data 1106 are all intercepted by the VeriFIDES access control 1104 resident on the desktop PC 1102. The VeriFIDES access control 1104 determines the authenticity and validity of each request for data devices 1108 made by a user connecting through the VeriFIDES card 1101, thus preventing invalid access.

[0072] In terms of external threats to Linux (via the network interface), the VeriFIDES infrastructure will be intercepting network packets immediately after they come off of the network interface before they are delivered to any guest sessions 104 and 105 or the VeriFIDES operating system 103. This mechanism will determine authenticity of the source, as well as enforce access control, preventing unauthorized hosts from connecting to the machine. The packet interceptor for example may be a small piece of code (under 10K lines of code) that can be hand verified to ensure that it is not susceptible to attacks.

[0073] FIG. 12 illustrates a method according to an embodiment of the invention for monitoring incoming network packets. As illustrated in FIG. 12, packets are received and queued, step 1201. A determination is first made whether the current packet is allowed within the VeriFIDES system, 1202. If the packet is restricted, it is dropped 1203. If the packet is allowed, it is checked for an IP security header, 1204. If the packet does not contain an IP security header, it is determined whether or not its destination is a VeriFIDES service port, 1208. If the destination is a service port, it is routed to the appropriate service, 1211 such as ticket requests or audit records. If not, the destination is rewritten, 1209 and the packet is placed back on the TCP/IP stack, 1210.

[0074] If the packet contains an IP security header, the header is stripped off the packet and the payload is decrypted as previously described, 1205. A final check is performed to determine if the destination is a VeriFIDES proxy port, 1206. If the destination is not a proxy port, the destination is again rewritten, 1209, and the packet is placed back on the TCP/IP stack,

1210. If the destination is, in fact, a proxy port, the packet is routed to the VeriFIDES proxy applications, 1207.

[0075] FIG. 13 illustrates a method in accordance with one embodiment for monitoring outgoing network packets. As illustrated in FIG. 13, a packet is first received and determined if it is destined for the external network, 1301. If the packet is not for an external network, it is routed to the appropriate VeriFIDES service, such as I/O, Tray, or Icon services, 1305. If the packet is destined for the external network, it is determined whether it is from an unclassified session, step 1302.

[0076] If the packet is not from an unclassified session, a check is made as to whether the packet is destined for a VeriFIDES proxy port, step 1303. If it is, it is forwarded to an appropriate proxy application 1304 and then added to the queue, 1308. If the packet is not destined for a proxy port, it is immediately added to the queue 1308. Furthermore, if the packet is from an unclassified section, it is added straight to the queue, 1308.

[0077] A check is then made as to whether the packet is allowed out of the system, 1309. If the packet is not allowed out, it is dropped, 1310. When the packet is allowed out of the system a check is made as to whether the packet originated locally, 1311. If the packet did not originate locally, the source address is rewritten, 1312 and a check is made to determine if the packet came from an unclassified section, 1315.

[0078] If the non-local packet is from an unclassified section it is placed on the TCP/IP stack, 1316. If it is from a classified section, IP security header information is added to the packed and the payload is encrypted, 1314. Subsequently the encrypted packet is added to the TCP/IP stack, 1316.

[0079] If a packet is determined to have originated locally, 1311, the packet is then checked to determine if its destination is a VeriFIDES proxy port, 1313. If the destination is a proxy port, IP security header information is attached, 1314 and the packet is added to the

TCP/IP stack, 1316. If the destination is not a proxy port, the packet is simply added to the TCP/IP stack, 1316.

[0080] The only I/O on the single board computer card may be keyboard, video, mouse, and the PCI interface to the main motherboard. That PCI interface consists of a non-transparent PCI bridge that is only programmable from the main motherboard's side. The card, designed to specifications, would be trusted hardware.

[0081] As explained earlier, references to RAM generally refer to the RAM on the motherboard (accessible only by Linux and VeriFIDES access control), as well as the RAM on the single board computer card (accessible only by the Windows sessions).

[0082] The previously mentioned private key would be stored on the motherboard, for example using something like Trusted Platform Module (TPM) technology.

[0083] The VeriFIDES system presented provides numerous advantages over the existing art. First, hackers are prevented from gaining access to data without a ticket or with a forged ticket. The data are encrypted, and the key needed to decrypt them is contained within the ticket. Without a ticket, the user is left with a hard drive full of encrypted gibberish.

[0084] Furthermore, tickets are bound to a particular machine via a public/private key pair as specified in the original patent. In some embodiments, VeriFIDES depends on a public key validation mechanism, similar to a trusted certificate authority such as Verisign. A hacker could generate a bogus ticket, but since it couldn't contain the decryption key, it would be useless. What could be spoofed is someone supplying a bogus public key to a ticket server to obtain a ticket allowing a user to decrypt a ticket.

[0085] In addition, there is a process for determining whether a particular user had the proper key to decrypt and access the data: All VeriFIDES protected data have a statistically unique random binding associated with the encrypted bytes. This binding is also contained in the ticket, ensuring a match between data and a ticket. The initial specification of a ticket includes the symmetric key to decrypt the data, a binding, and a set of permissions/access rights.

[0086] Retaining a ticket is analogous to going to a movie or sporting event. The ticket-taker rips the ticket in half and gives back a stub. When a user adds a VeriFIDES ticket, the access control mechanism keeps a permanent record of that ticket and returns a "stub" to the user. In this fashion, the user is prevented from "re-adding" that ticket since VeriFIDES knows that it was already used. Thus, if a ticket specifies that a user can only see a file 5 times, they cannot use that ticket twice to get 10 viewings.

[0087] To perform 'state-based' access control, when a ticket is used, the VeriFIDES access control mechanism retains a portion of the ticket. This section of the ticket will never be seen or accessed again by the user, and corresponds to a ticket collector at a movie theater or sporting event retaining half of a ticket and returning a ticket stub. This allows the access control mechanism to store state information (such as number of accesses, number of copies, number of hard copies, etc.) inside that portion of the ticket. When the user has reached whatever limits may have been specified within the original ticket, the access control mechanism will prevent further access to the data. If the access control mechanism does not retain a portion of the ticket, users could circumvent 'state-based' restrictions by making copies of their tickets. Thus, if a ticket specified that data could be accessed once, a user could make 10 copies of the ticket, allowing them to actually access the data 10 times.

[0088] FIG. 9 comprises a diagram illustrating how VeriFIDES can be used to limit the sphere of compromise of data. In the event of compromise, it can be known exactly what files a particular user had tickets (decryption keys) for, when those files were accessed, and what type of access (view, copy, print, etc.) occurred.

[0089] For limiting the sphere of compromise, with VeriFIDES, the audit and logging functions occurring below the operating system give a much higher degree of assurance and a higher fidelity of data. Additionally, as all data are encrypted and accessed with tickets, it can be known whether a particular user even had the key to decrypt and access protected data, giving greater confidence that data have not been compromised.

[0090] For 'state-based' access control, with VeriFIDES, we can provide a higher degree of assurance that 'state-based' permissions are being enforced since the state information is being stored in a location completely inaccessible to the user. Ticket Stubs allow the system to enforce "state-based" access control, such as controlling the number of times data are accessed, printed, copied, etc. This can have a huge benefit for entertainment content by enforcing the number of times a movie/game can be played. Limiting the sphere of compromise can also provide enormous financial benefits both to the government and the commercial worlds. In the event that data are compromised, VeriFIDES can drastically reduce the scope of data to be examined / concerned about.

[0091] FIG. 3 illustrates an alternative embodiment of the VeriFIDES system comprising a motherboard 301 and a communicatively coupled processing board 302. As illustrated in FIG. 3, the VeriFIDES system is implemented as a co-processor on a board. A board 302 containing a processor could be inserted into the computer. This board would contain dual I/O channels for every type of I/O controller present on the mother board (or peripheral cards) 301. All I/O would be re-routed from the motherboard / peripheral cards to inputs of the card containing the co-processor. The output ports of the card would be connected to the actual I/O devices. In this manner, all I/O would be routed through the access control software running on the processor on the board, thus implementing VeriFIDES functionality.

[0092] FIG. 4 illustrates an alternative embodiment of the VeriFIDES system comprising VeriFIDES logic implemented as a PCI bridge. As illustrated in FIG. 4, the VeriFIDES system is implemented as a PCI bridge 403. Elements 401-406 comprise a CPU, north bridge, random access memory, advanced graphics processor, PCI devices and south bridge, respectively. These elements are well known in the art and comprise a standard architecture for a computing device.

[0093] As illustrated, the VeriFIDES system is implemented within a PCI bridge 407 resident immediately after the north bridge 402. By incorporating additional processing capability into a PCI bridge, the access control mechanism can be executed within the bridge.

The access control software would be responsible for interpreting the PCI bus traffic, determining what to do with I/O data (encrypt, decrypt, block, etc.), and then re-forwarding the I/O data to the CPU and/or main memory.

[0094] FIG. 5 illustrates an alternative embodiment of the VeriFIDES system comprising the VeriFIDES system implemented as a co-processor. As illustrated in FIG. 5, the VeriFIDES system is implemented as a co-processor 402. In this dual processor architecture, the operating system executes on one processor 401 and the access control software executes on the second 402. The architecture defines a special bus 403 between the two processors for transferring interrupts, programmed I/O, and BIOS information from the access control CPU 402 to the operating system CPU 401. The access control CPU communicates with the rest of the computer hardware 404-408 in a traditional manner known to those in the art.

[0095] The architecture includes a dual port memory 405-406 with special address translation hardware 404 preventing the OS CPU 401 from accessing portions of memory containing the access control program, crypto keys, and other data that needs hiding 405.

[0096] It is known to use a co-Processor and hypervisor software. Also, Sun Microsystems has a product, the Sun PCI card, that is a full PC on a card that interacts with the Solaris Operating system via special Windows device drivers. The full PC functionality on the card would not be needed in the present embodiment nor new device drivers for Windows. The methods of the prior art require backing and support of computer manufacturers. In addition, Type I virtual machine software requires significant expertise and is difficult to write. A virtual machine does not provide many of the programming 'services' that a traditional OS does, making the implementation of VeriFIDES business logic much more difficult.

[0097] FIG. 6 illustrates an exemplary system of the present invention comprising the VeriFIDES system residing on a separate peripheral card. A card is installed containing its own memory 602, processor 601, and video out 608. This card will be responsible for running the 'guest' operating system (typically MS Windows). The main computer will run a modified

version of Linux that will export 'virtual' representations of all I/O devices attached to the computer. Linux will be responsible for intercepting all I/O and performing VeriFIDES business logic (encrypt, decrypt, block, watermark, etc.). The VeriFIDES card will also need to contain a special filter, that will prevent the CPU on the card from discovering the real I/O devices attached to the bus, and only allow data from our 'virtual' devices exported by Linux.

[0098] FIG. 7 illustrates a further embodiment of a guest operating system running on a card connected to a main computer. As illustrated, SunPCI card 702 is connected to a main board running Linux 701 via a network connection between NIC 704 and NIC 705. The SunPCI card 702 allows for user interaction via USB and VGA ports connected to user devices 703.

[0099] All user interaction is processed from NIC 704 to NIC 705 and is received by network bridge 706. Network bridge 706 forwards all requests to access control 709 which verifies the authenticity of the requests and forwards data to the session transition module 707 or the device driver 708. The host hard drive 710 is operable to receive request from the device driver 708 and return requested data to the SunPCI card 702 in accordance with the access control 709 policies. Access control 709 is further operable to receive external network requests from a network 712 through NIC 711 and network bridge 706. As described, network requests may be monitored and verified by access control 709 prior to their acceptance by the VeriFIDES system.

[00100] The previously presented embodiments allow PC's to be upgraded with VeriFIDES functionality, rather than having to incorporate VeriFIDES into newly manufactured PC's. Additionally, because VeriFIDES business logic would be running within an operating system such as Linux rather than a virtual machine, a large volume of software libraries and services are available for use that greatly simplify VeriFIDES development. This method provides a way to upgrade existing computers with VeriFIDES functionality by inserting a board and re-installing Windows. This method does not require the backing of computer/BIOS manufacturers to deploy VeriFIDES.

[00101] Notably, the figures and examples above are not meant to limit the scope of the present invention to a single embodiment, as other embodiments are possible by way of interchange of some or all of the described or illustrated elements. Moreover, where certain elements of the present invention can be partially or fully implemented using known components, only those portions of such known components that are necessary for an understanding of the present invention are described, and detailed descriptions of other portions of such known components are omitted so as not to obscure the invention. In the present specification, an embodiment showing a singular component should not necessarily be limited to other embodiments including a plurality of the same component, and vice-versa, unless explicitly stated otherwise herein. Moreover, applicants do not intend for any term in the specification or claims to be ascribed an uncommon or special meaning unless explicitly set forth as such. Further, the present invention encompasses present and future known equivalents to the known components referred to herein by way of illustration.

[00102] The foregoing description of the specific embodiments so fully reveals the general nature of the invention that others can, by applying knowledge within the skill of the relevant art(s) (including the contents of the documents cited and incorporated by reference herein), readily modify and/or adapt for various applications such specific embodiments, without undue experimentation, without departing from the general concept of the present invention. Such adaptations and modifications are therefore intended to be within the meaning and range of equivalents of the disclosed embodiments, based on the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the present specification is to be interpreted by the skilled artisan in light of the teachings and guidance presented herein, in combination with the knowledge of one skilled in the relevant art(s).

[00103] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example, and not

limitation. It would be apparent to one skilled in the relevant art(s) that various changes in form and detail could be made therein without departing from the spirit and scope of the invention. Thus, the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

Appendix A

```
<?xml version="1.0"?>
<ticket>
        <!-- options are user, file, host, connection -->
        <type/>
         <!-- see identifier section below -->
        <identifier> IDENTIFIER_XML </identifier>
        <!-- targetMachine is the machine this ticket is intended for. -->
        <targetMachine> string </targetMachine>
        <!-- The binding has different meanings depending on the ticket type.
                Last byte of all bindings indiciates what type of ticket the binding is associated
with: 0 = user, 1 = file, 2 = host, 4 = connection
                Binding is always 32 bytes
                User tickets: 31 bytes Random + 1 byte type
                File tickets: 31 bytes Random + 1 byte type
                Host tickets: 4 byte ip + 27 byte 0's + 1 byte type
                Connection tickets: 4 byte dst ip + 4 byte src ip + 2 byte dst port +
                                        2 byte connection type + 19 bytes random + 1 byte type
        -->
        <binding> base64(bytes) </binding>
        <!-- see below.  this is xml describing the security restrictions
             on a VeriFIDES machine using the ticket
            probably empty for a Host Ticket
        -->
        <permissions> PERMISSIONS_XML </permissions>
        <!-- this is the version of the ticket format. -->
        <version/>
        <!-- globally unique ticket id.  any ticket creator will generate a unique
             one of these for every ticket it produces -->
        <gutid> base64(bytes) </gutid>
        <!-- the machine where audit messages go -->
        <auditServer/>
        <!-- the machine that "owns" the data.  originator.  where you can go to
             get this ticket (may be a proxy for the owner) -->
        <ticketServer/>
        <!-- the machine that generated this ticket -->
        <ticketCreator/>
        <!-- in the preview section keys only contains the ticketMessageKey
             it contains the real keys in the authoritative section -->
        <keys>
                <!--  this is the symmetric key needed to decrypt the authoritative section
encrypted with the public key of the verifides machine it is intended for.
                -->
                <ticketMessageKey> base64(RSA(ticketKey:ticketIV)) </ticketMessageKey>
        </keys>
        <authoritative> base64(AES(
                <!-- authoritativeTicket is here just so that when we decrypt we have valid xml
with a top level tag.  Not needed in some embodiments -->
                <authoritativeTicket>
                        <type/>
                        <identifier/>  <!-- see structure above -->
                        <targetMachine/>
                        <binding> base64(bytes) </binding>
                        <permissions> PERMISSIONS_XML </permissions>
                        <version/>
                        <gutid> base64(bytes) </gutid>
                        <auditServer/>
                        <ticketServer/>
                        <ticketCreator/>
                        <-- these keys differ depending on the ticket type.  see "keys" below -->
                        <keys> KEYS_XML </keys>
                </authoritativeTicket>
        ))
        </authoritative>
</ticket>
<!--
  IDENTIFIER SECTION
  identifiers contain the things access control needs to look up the ticket.
  they don't change the state of the system.
-->
<identifier>
        <!-- For User, File, and Connection Tickets.
             For User Tickets this tells us which
             user is being defined by this ticket.  For File and Connection
             tickets this tells us which user may access this ticket.
             These may contain wildcards in File and Connection tickets
             to indicate that any user on the machine may use the ticket.
             These fields are empty in Host tickets.
        -->
        <domain/>
        <username/>
```

```
        <!-- For User, File, and Connection Tickets.
             May contain a wildcard if this ticket may be used
             in any session on the machine.
             This field is empty in Host tickets.
        -->
        <classification/> <!-- "Secret", "Top Secret", etc... -->
        <!-- For File Tickets -->
        <filename/> <!-- useful but not authoritative because names change -->
        <!-- For Host Tickets and Connection Tickets.
             This field contains the hostname of the machin> we may wish
             to communicate with.  This ticket contains this machine's public
             key.
        -->
        <remoteHostname/>
        <!-- For Connection Tickets.
             These fields describe the communication paths that this ticket
             enables.  Port, type, and resource may contain wildcards.
        -->
        <port/>
        <type/> <!-- Client, Server, Both -->
        <!-- for things such as web service
             url, jabber user, etc -->
        <resource/>
</identifier>
<!--
  KEYS
  all keys are now going to go in the "keys" section inside authoritative.
  we need a way to sign the ticket to ensure that the ticketCreator is who they
  say they are, otherwise we could spoof a ticket server and get network
  connections from malicious machines.  different types of tickets will implement
  different elements inside the keys section.
-->
<keys>
        <!-- required in ticket of type "file" -->
        <!-- used to decrypt files including local files, remote files,
             emails, web pages. -->
        <fileKey> base64(bytes) </fileKey>
        <!-- required in ticket of type "host" -->
        <!-- contains the certificate of another machine so that you can
             authenticatea remote machine.  VeriFIDES boxes may
             be prestaged with the host ticket for their ticket server and
             audit server.  the TS can also serve as your PKI by giving you
             other host tickets.
        -->
        <hostKey> base64(bytes) </hostKey>
        <!-- in ticket of type "connection."  not required.-->
        <!-in some embodiments this is not needed but it provides orthogonality.
             In some embodiments the symmetric key for communication with another host could be
put here instead of doing a negotiation once both sides have a host key.
        -->
        <connectionKey> base64(bytes) <connectionKey>
        <!-- required in ticket of type "user."  may be present in other types. -->
        <!-- These are keys or other info for authentication via various schemes.
               could include smartcard, fingerprint, passphrase etc.
               In user tickets these describe how a user gets in.
               In other types, they could set specific passwords, smartcards to
               access this data rather than just authenticating the user.
        -->
        <userKey type="TYPE1"> base64(bytes) </userKey>
        <userKey type="TYPE2"> base64(bytes) </userKey>
        <userKey type="TYPE3"> base64(bytes) </userKey>
        <!-- we need a way to ensure that this ticket came from who it said
             it came from otherwise it would be easy to get unauthorized
             network access.
        -->
        <ticketCreatorSignature> base64(hash of something in ticket)
</ticketCreatorSignature>
<keys>
<!--
  Permissions XML is xml inside a ticket which is used for the representation
  of permissions for the VeriFIDES file the ticket was issued for.  It tells
  the system how to behave and which system resources to restrict access to.
  This is what permissions look like.  They will be in all tickets except for
  "host" tickets.  As per prior convention, anything can be left empty.
  If it is empty, permissions default to permissions defined up the chain
  of ticket types.  If not defined anywhere, they default to system defaults
  which have been described in the permissions document.
  While the permissions section is a section inside the ticket XML, we can
  (and the permissions subsystem does) treat it as a standalone XML doc.
  Here is the basic structure of a permissions XML document:
```

```
-->
<permissions>
        <!--
            method will have an arbitrary type.
            AC matches type with the type in the userKey.   I sends type to a
            function registered for that type.  It sends the key gathered from the userKey
             section.
            The method returns true or false if access is allowed or not.
         -->
        <userAuthentication>
                <!-- required tells you if this method is required on data ticket open (yes),
                        or not (no), or if it is only required once per session (session).
                        if required is an integer, we are doing some kind of reauthentication
every [int] minutes.   Action is something like "golow" or "logout" or "destroy my machine."  It
is only used when int runs out. -->
                <method type="fingerprint"
                                required="yes|no|session|[int]"
                                action="-something-"/>
                <method type="smartcard">
                                required="yes|no|session|[int]"
                                action="-something-"/>
                <method type="passphrase">
                                required="yes|no|session|[int]"
                                action="-something-"/>
                <method type="[arbitrary]">
                                required="yes|no|session|[int]"
                                action="-something-"/>
        </userAuthentication>
        <!-- -filesystem
          the access attribute can be set to "disabled", "ro", or "rw".  If disabled,
          this device will be disabled for the rest of the session (meaning that no
          reads or writes are allowed).  If "ro", this device will only allow reads
          for the rest of the session if it previously allowed writes.  If "rw", access
          to this device is not restricted.  Default: rw.
          the "unclass" share is a special share which allows the user transfer
          unencrypted files from an Unclassified session to the Classified session.
          In some embodiments, put files in here while Classified because they
          will be encrypted and no tickets will be generated for them.
          the "verifides" share is the location of encypted verifides files on the
          system which will be automatically decrypted in a protected session provided
          the correct ticket is present.
          from a pure security perspective, treating external media I/O devices
           differently from each other makes no sense.
           further, disabled make no sense at all unless you disable everything
          from a usability perspective these are nice.  there may be some benefit
           to shutting off different kinds of busses.  especially removable busses.
           discussion for another day.
        -->
        <filesystem>
                <cdrom access="(disabled|ro|rw)"/>
                <cdrw access="(disabled|ro|rw)"/>
                <usb access="(disabled|ro|rw)"/>
                <verifides access="(disabled|ro|rw)"/>
                <unclass access="(disabled|ro|rw)"/>
        </filesystem>
        <!-- time is one of the most complex structures in a ticket.
             see the time section below for details -->
        <time>
                <NOT>|<INTERSECTION>|<UNION>
                        <timerange start="(INT)" stop="(INT)"/>
                        <timecycle scale="(min|hour|mday|wday|mon|yday)"
                           first="(INT)"
                           last="(INT)"
                        />
                </NOT>|</INTERSECTION>|</UNION>
        </time>
        <!-- This is a list of connections allowed while
             this ticket is in use we could just shut them when ticket is
             opened.  we could also not allow the ticket to be opened.
             Figure how to express each.
             It follows the
             hosts.allow/hosts.deny system with modifications.  To talk
             to an ip, that ip must pass this test as expressed in every
             open ticket. may contain wildcards.  see manpages for
             hosts.allow, hosts.options, tcp wrappers
        -->
        <connectionsAllowed>
                <connection> ip:[port-port]:[resource]:[ALLOW|DENY] </connection>
                ...
        </connectionsAllowed>
```

```
        <!-- List of bindings that can be in use at the same time
             as this ticket.
             go through the list.  if allowed, true, if denied false,
             if unlisted true.  wildcards (including ALL) used.
        -->
        <bindingsAllowed>
               <binding type="deny|allow"> base64(bytes) </binding>
               ...
        </bindingsAllowed>
        <!-- only allow concurrent access to tickets with the following originators
             or ticket servers.
        -->
        <ticketSourceAllowed>
               <ticketServer type="deny|allow"> ip:[ALLOW|DENY] </ticketServer>
               ...
        </ticketSourceAllowed>
        <!-- countdown -
          this is a value in minutes that indicates how long a document can be
          accessed before the system reverts to an Unclassified mode and destroys the
          session.  Default: infinite.
        -->
        <countdown minutes="(INT)"/>
        <!-- accesscount -
          this value indicates the number of Classified sessions in which
          this document can be accessed.  Note that this document doesn't decrement
          every time you open a file, but rather every time you open a file in a
          different session.  For example, if your access count is 2, then open the
          file in Classified, your access count will drop to 1.  Opening it again in
          that session will not affect the access count.  If you then say "Finished",
          then go back to the Classified session, and open the file again, your access
          count will drop to 0.  Default: infinite.
        -->
        <accesscount count="(INT)"/>
        <!-- printing -
          the printcount attribute tells how many times you may print a document on
          the system.  Warning: printcount will be decremented for every file that has
          been opened in a Classified session every time you print one document.
          Default: infinite.
                 the watermark attribute tells the printing subsystem to print a watermark
          containing the specified string on top of each printed page.  Default:
          no watermark.
          the allowed attribute is "true" or "false."  If true, printing is enabled.
          If false printing is disabled.  Default: true.
        -->
        <printing printcount="(INT)" watermark="(STRING)" allowed="(true|false)"/>
        <!-- phonehome
          By forcing the system to remain in contact with the ticket server, it allows
          the ticket server to revoke the ticket (or destroy private keys if the
          conops permit).  this prevents a user from unplugging from the network to
          avoid server initiated ticket revocation or destruction of private keys.
          the minutes attribute indicates the number of minutes between system
          initiated contacts with the ticket server for this particular ticket.
          Default: Infinite, no contact required.
          the timeout attribute indicates how long the system will give the user to
          re-establish communication with the ticket server after a system initiated
          contact failed.  Default: zero, action taken immediately.
          the action attribute determines what action will be taken if communication
          is not established with the ticket server within the allowed timeout period.
          "golow" will force the Classified session to exit and be destroyed.  "revoke"
          will destroy the session and revoke this ticket.  "bigred" will destroy the
          private keys on the system.
        -->
        <phonehome minutes="(INT)" timeout="(INT)" action="(golow|revoke|bigred)"/>
</permissions>
<!--
time -
                This is a subsystem all of its own.  The purpose of this system is to provide a
powerful and generic facility for specifying times at which this ticket  can or can not be used
to decrypt a file.
                all tags for this subsystem are contained inside the <time></time> tags.

Primitives
                There are 2 time permission primitives inside this section:
                These primitives are compared against a supplied time and reduce
                to a truth value (either "true" or "false")
                  1.  <timerange start="(INT)" stop="(INT)"/>
                  2.  <timecycle scale="(min|hour|mday|wday|mon|yday)"
                         first="(INT)"
                         last="(INT)"
                      />
```

The timerange tag describes a range of time between two integers whose values are seconds since the UNIX epoch (Jan 1 1970). Any time in this range (inclusive) will be considered "true" and anything outside will be considered "false".

The timecycle tag describes a cycle of time on the scale specified.

Example: <timecycle scale="hour" first="9" last="17"/> will be "true" between 9am and 5pm.

Example: <timecycle scale="mon" first="1" last="4"/> will be "true" during January through April of any year.

Operators

There are 3 time permissions operators inside this section:

When the operators are evaluated they reduce to permission primitives. ("true" or "false")

1. <NOT>(1 primitive)</NOT>
2. <INTERSECTION>(N primitive(s)) <INTERSECTION/>
3. <UNION>(N primitive(s)) <UNION/>

The NOT operator inverts the output of the primitive inside it.

Example:

```
<NOT>
     <timecycle scale="mon" first="1" last="4"/>
</NOT>
```

will evaluate to "true" during a time that is in May through December of any year.

The INTERSECTION operator operates on N primitives and evaluates to "true" if ALL primitives inside it evaluate to "true".

Example:

```
<INTERSECTION>
     <timecycle scale="hour" first="9" last="17"/>
     <timecycle scale="mon" first="1" last="4"/>
</INTERSECTION>
```

will evaluate to "true" during business hours in January through April of any year.

The UNION operator operates on N primitives and evaluates to "true" if ANY OF THE primitives inside it evaluate to "true".

Example:

```
<UNION>
     <timecycle scale="hour" first="9" last="11"/>
     <timecycle scale="hour" first="1" last="17"/>
<UNION>
```

This example evaluates to true during business hours but excludes a lunch hour between 12 and 1. Note that "11" on the scale of hours evaluates to true at "11:00" through "11:59" The "last" value is always inclusive.

Recursion

The operators can recursively contain other operators so long as they contain the correct number of primitives after all the operators and primitives inside them reduce to the correct number of truth values. There is no limit placed on the level of descent.

Example:

```
<time>
      <INTERSECTION>
      <timerange start="1072196405" stop="1072210999"/>
      <NOT>
          <UNION>
              <timecycle scale="mday" first="10" last="18"/>
              <INTERSECTION>
                      <timecycle scale="hour" first="10" last="20"/>
                      <timecycle scale="yday" first="12" last="40"/>
              </INTERSECTION>
          </UNION>
      </NOT>
      </INTERSECTION>
</time>
```

Here is an example demonstrating how to do business hours between 8:30am and 6:00pm:

```
<time>
     <UNION>
            <timecycle scale="hour" first="9" last="18"/>
            <INTERSECTION>
                   <timecycle scale="hour" first="8" last="8"/>
                   <timecycle scale="mins" first="30" last="60"/>
            </INTERSECTION>
     </UNION>
</time>
```

Computationally the processing of the time section in permissions is done using a Reverse Polish Notation (RPN) recursive descent scheme.

-->

We Claim:

1. A computing apparatus designed to control access to protected data, the computer comprising:

a main motherboard, having one or more first processors and one or more first memory devices, being coupled to all input/output devices connected to the computer to input data into the computer or output data from the computer;

a trusted operating system programmed to operate on the main motherboard, the trusted operating system including an access control module for controlling access to the protected data in accordance with one or more rules and for storing the protected data in an unprotected form only on the first memory devices on the main motherboard;

a computer card, having one or more second processors and one or more second memory devices, being coupled to the main motherboard via a PCI bus;

one or more guest operating systems, programmed to operate on the one or more computer cards, for running one or more software applications on the computer, the software applications being usable to access and process the protected data in its unprotected form; and

a tamper detection mechanism for protecting against attempts to copy the unprotected form of the protected data onto memory devices other than the one or more first or second memory devices.

2. The computing apparatus of claim 1, wherein the protected data is protected by being encrypted, and wherein the trusted operating system is programmed to use one or more decryption keys to decrypt the protected data in accordance with the one or more rules.

3. The computing apparatus of claim 2, wherein the trusted operating system is programmed to store the one or more decryption keys only on the main motherboard.

4. The computing apparatus of claim 2, wherein the tamper detection mechanism is programmed delete the one or more decryption keys in the event an attempt to tamper with the computer is detected.

5. The computing apparatus of claim 1, wherein the trusted operating system comprises a scaled down version of the Linux operating system.

6. The computing apparatus of claim 1, wherein the PCI bus comprises a non-transparent PCI bridge.

7. The computing apparatus of claim 1, comprising one or more tickets stored on the main motherboard and containing the one or more rules.

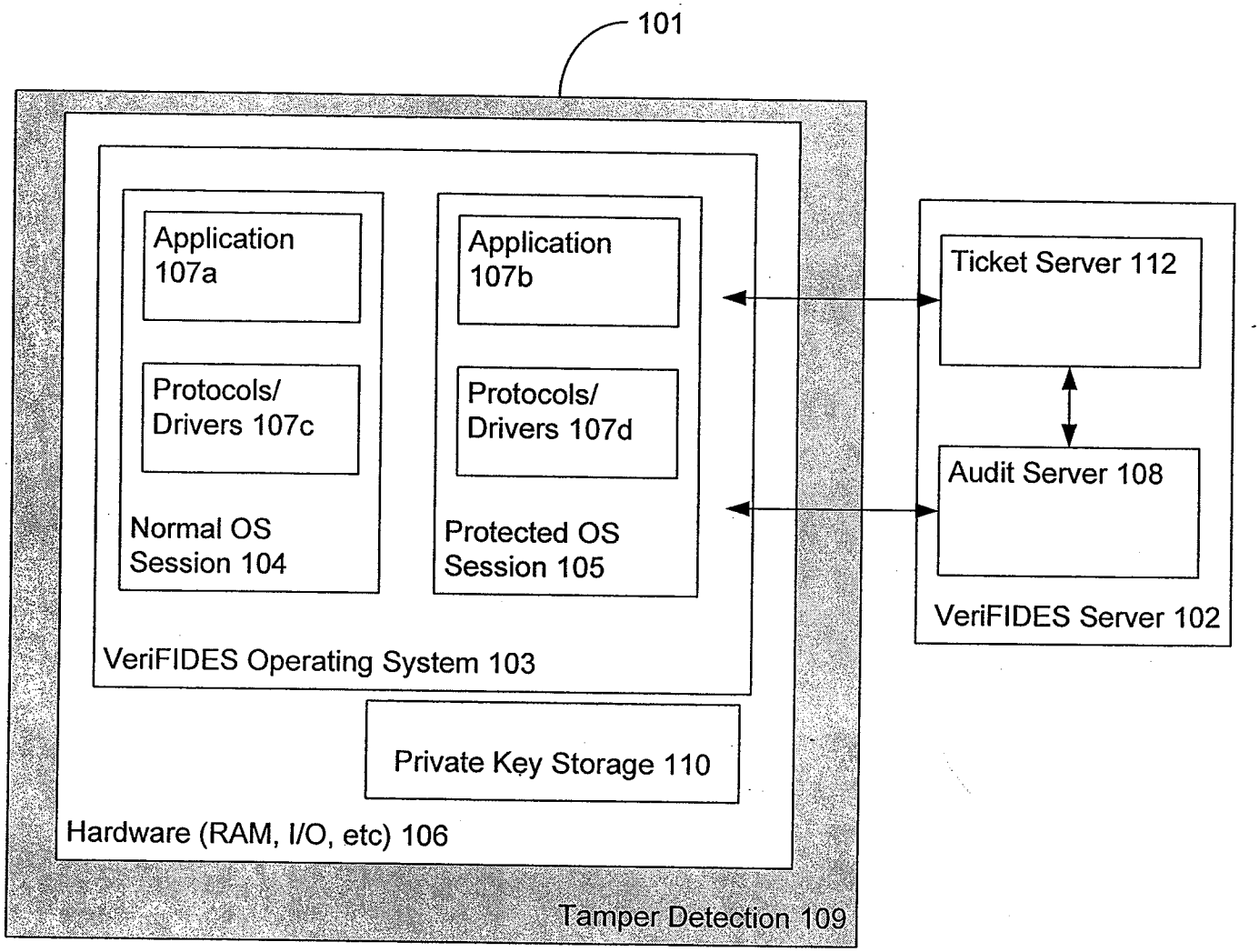

101
Application 107a
Protocols/ Drivers 107c
Normal OS Session 104
Application 107b
Protocols/ Drivers 107d
Protected OS Session 105
VeriFIDES Operating System 103
Private Key Storage 110
Hardware (RAM, I/O, etc) 106
Tamper Detection 109
Ticket Server 112
Audit Server 108
VeriFIDES Server 102

FIG. 1

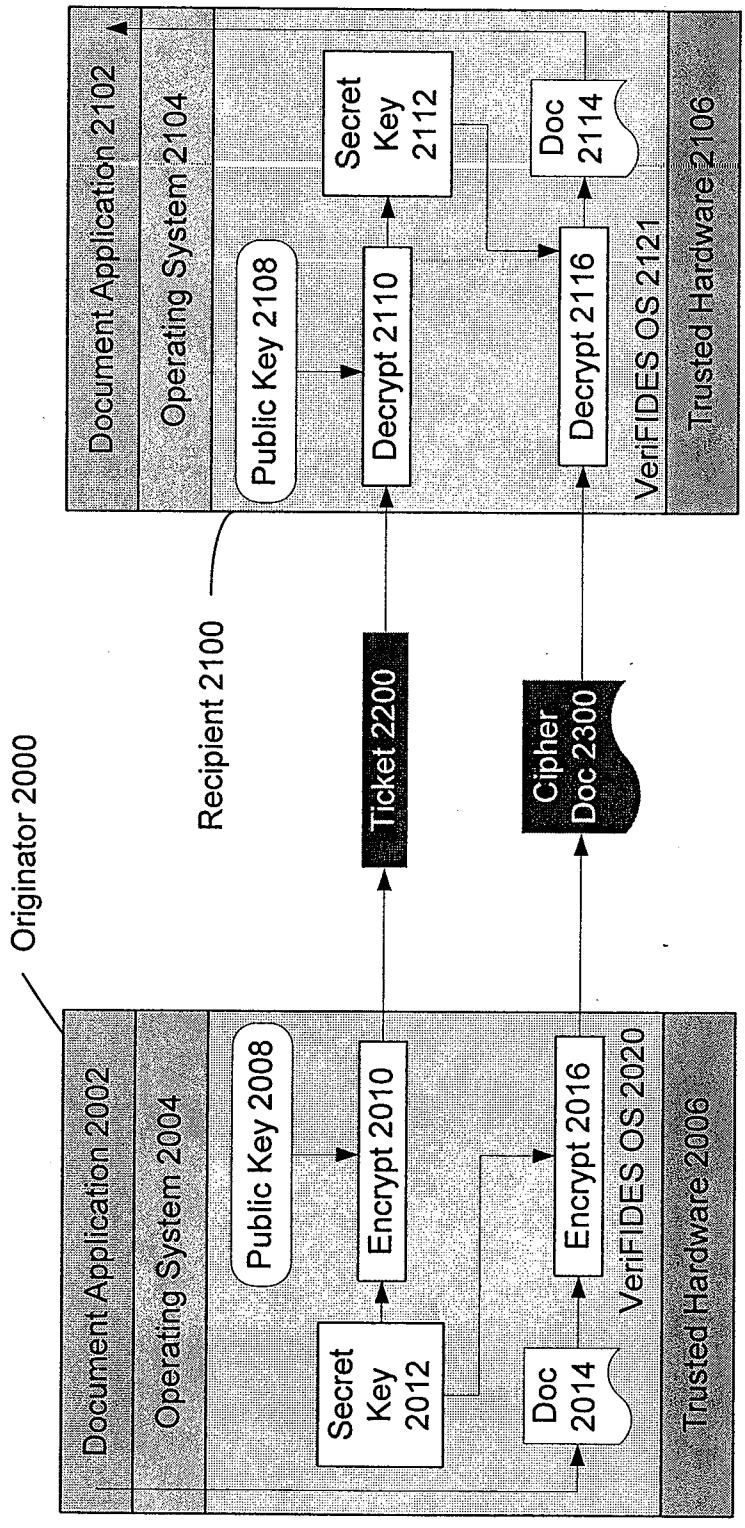

Originator 2000
Document Application 2002
Operating System 2004
Public Key 2008
Secret Key 2012
Encrypt 2010
Doc 2014
Encrypt 2016
VeriFIDES OS 2020
Trusted Hardware 2006
Ticket 2200
Cipher Doc 2300
Recipient 2100
Document Application 2102
Operating System 2104
Public Key 2108
Decrypt 2110
Secret Key 2112
Doc 2114
Decrypt 2116
VeriFIDES OS 2121
Trusted Hardware 2106

FIG. 2

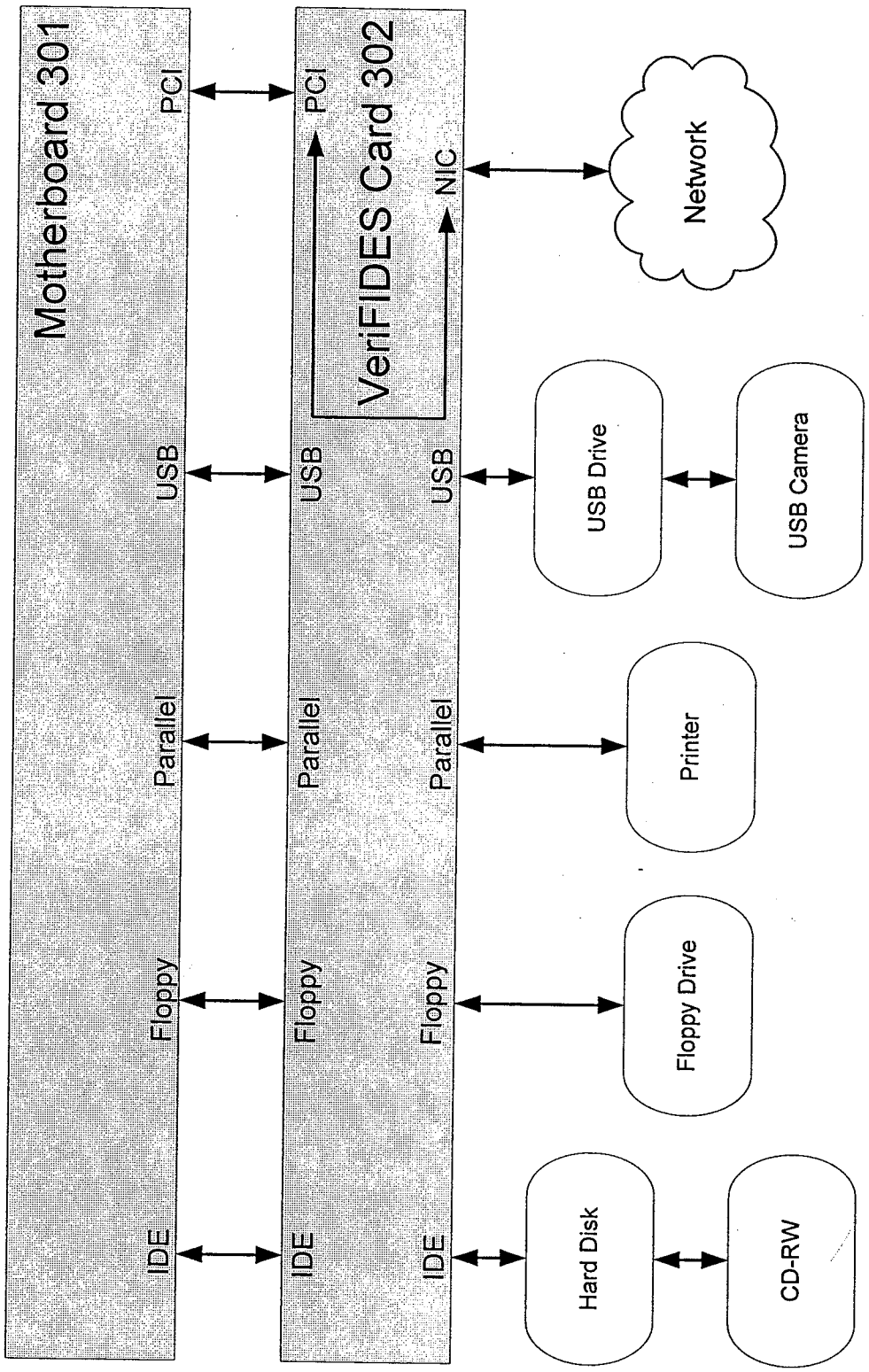

Motherboard 301
PCI
USB
Parallel
Floppy
IDE
VeriFIDES Card 302
PCI
USB
Parallel
Floppy
IDE
NIC
USB
Network
USB Drive
USB Camera
Printer
Floppy Drive
Hard Disk
CD-RW

FIG. 3

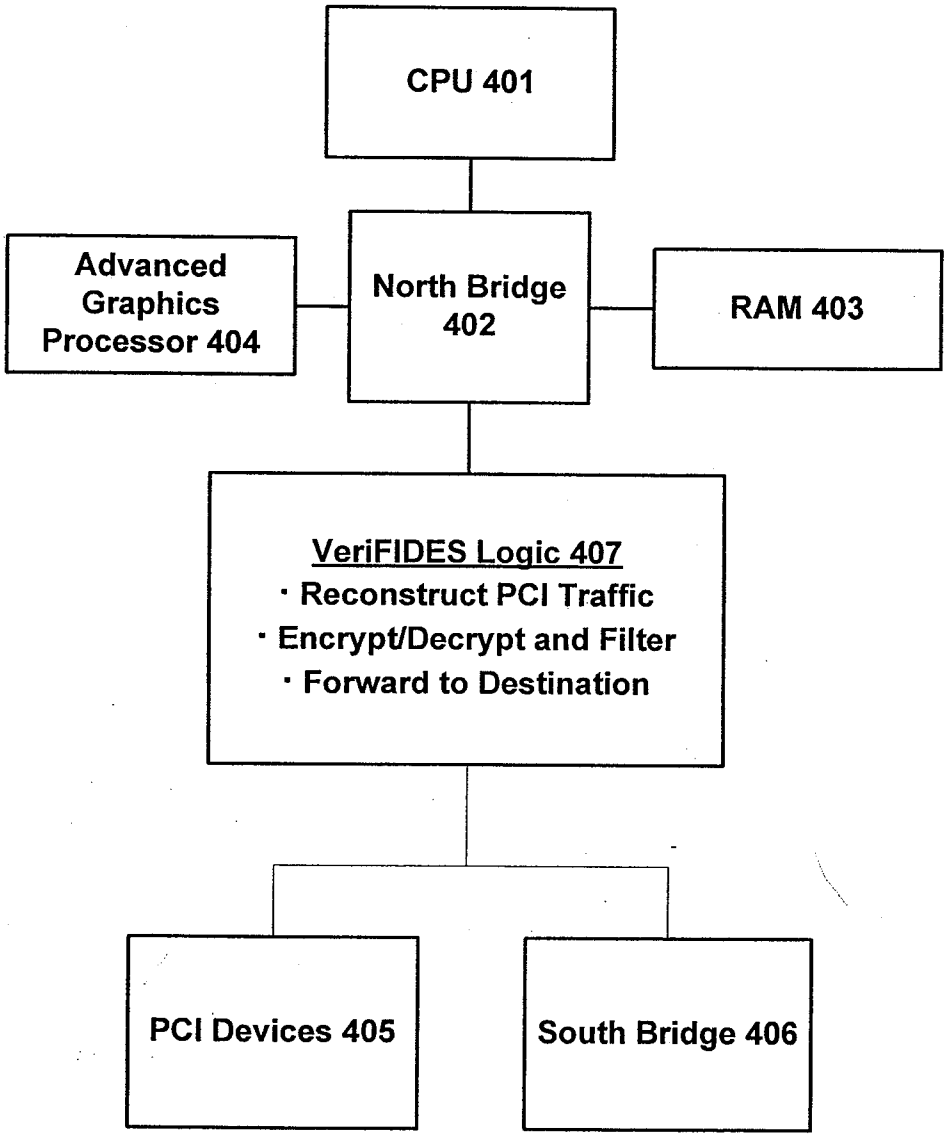

CPU 401
Advanced Graphics Processor 404
North Bridge 402
RAM 403
VeriFIDES Logic 407
· Reconstruct PCI Traffic
· Encrypt/Decrypt and Filter
· Forward to Destination
PCI Devices 405
South Bridge 406

FIG. 4

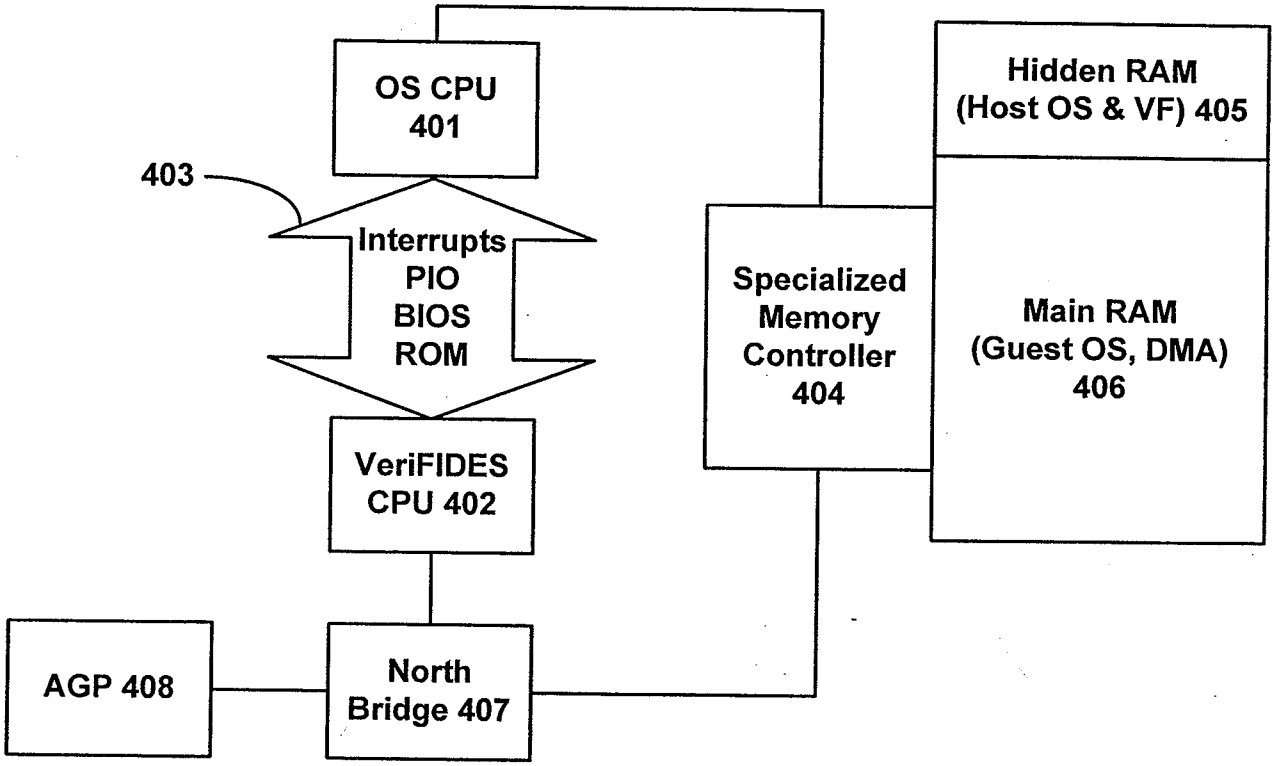

OS CPU
401
403
Interrupts
PIO
BIOS
ROM
VeriFIDES
CPU 402
AGP 408
North
Bridge 407
Specialized
Memory
Controller
404
Hidden RAM
(Host OS & VF) 405
Main RAM
(Guest OS, DMA)
406

FIG. 5

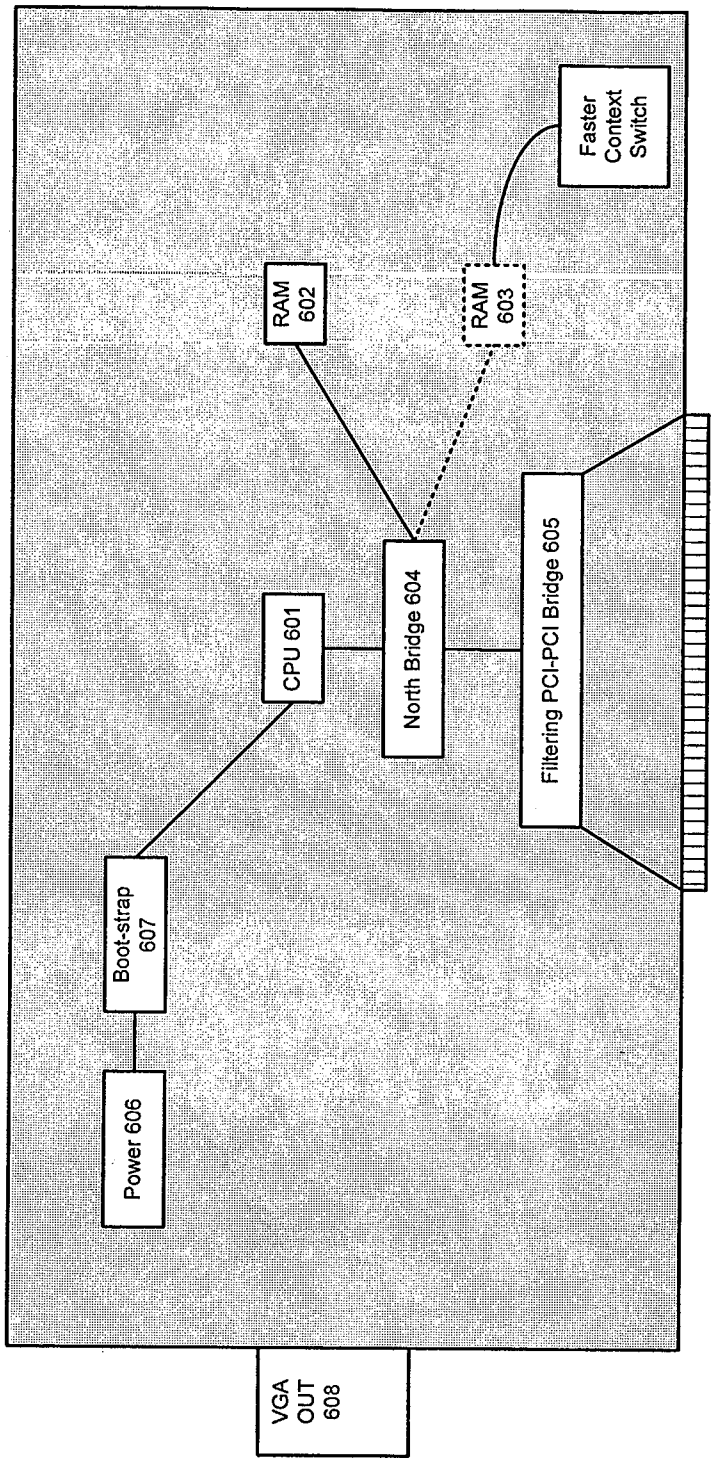

Faster Context Switch
RAM 602
RAM 603
CPU 601
North Bridge 604
Filtering PCI-PCI Bridge 605
Boot-strap 607
Power 606
VGA OUT 608

FIG. 6

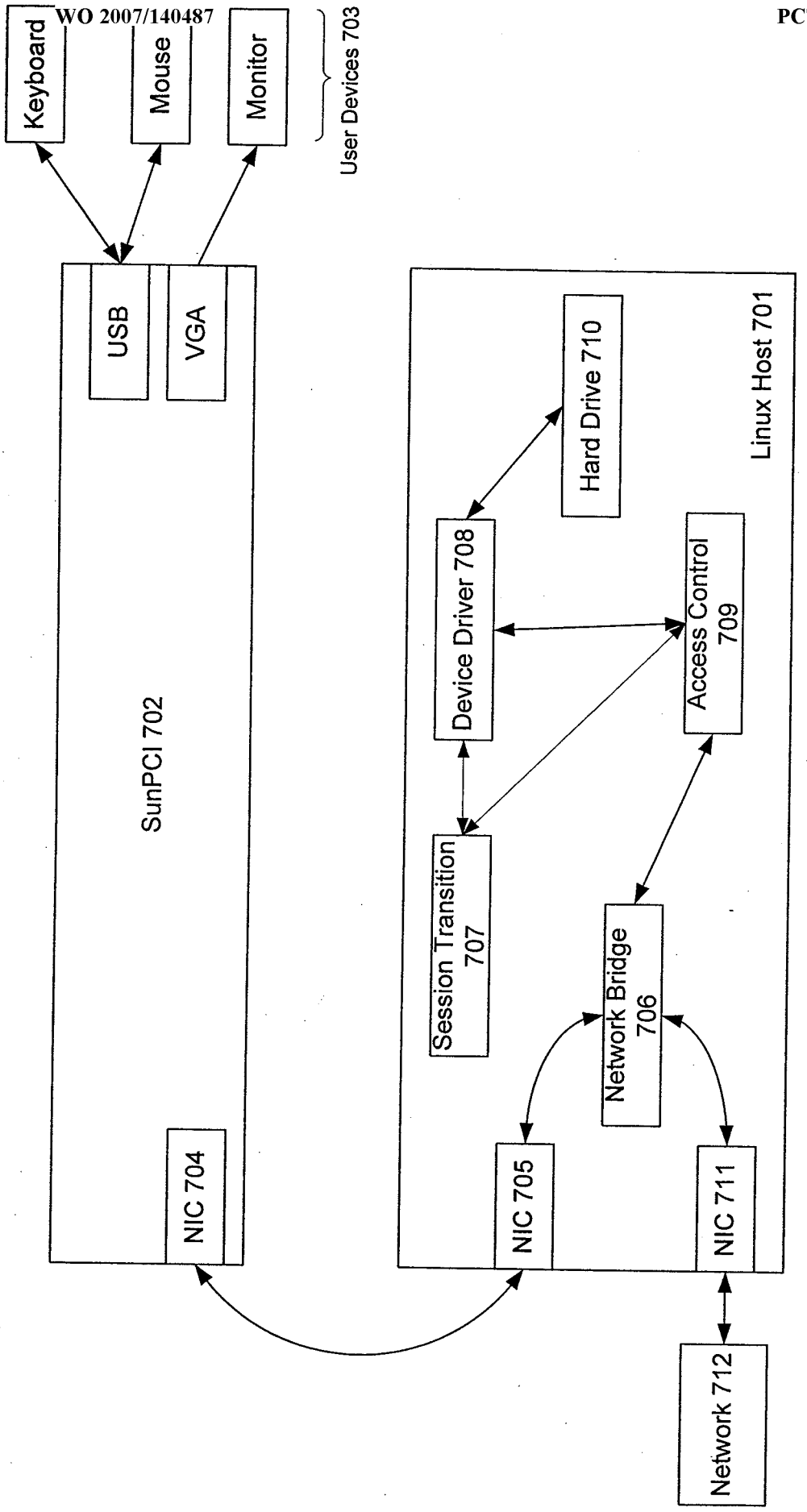

Keyboard
Mouse
Monitor
User Devices 703
USB
VGA
SunPCI 702
NIC 704
Linux Host 701
Hard Drive 710
Device Driver 708
Access Control 709
Session Transition 707
Network Bridge 706
NIC 705
NIC 711
Network 712

FIG. 7

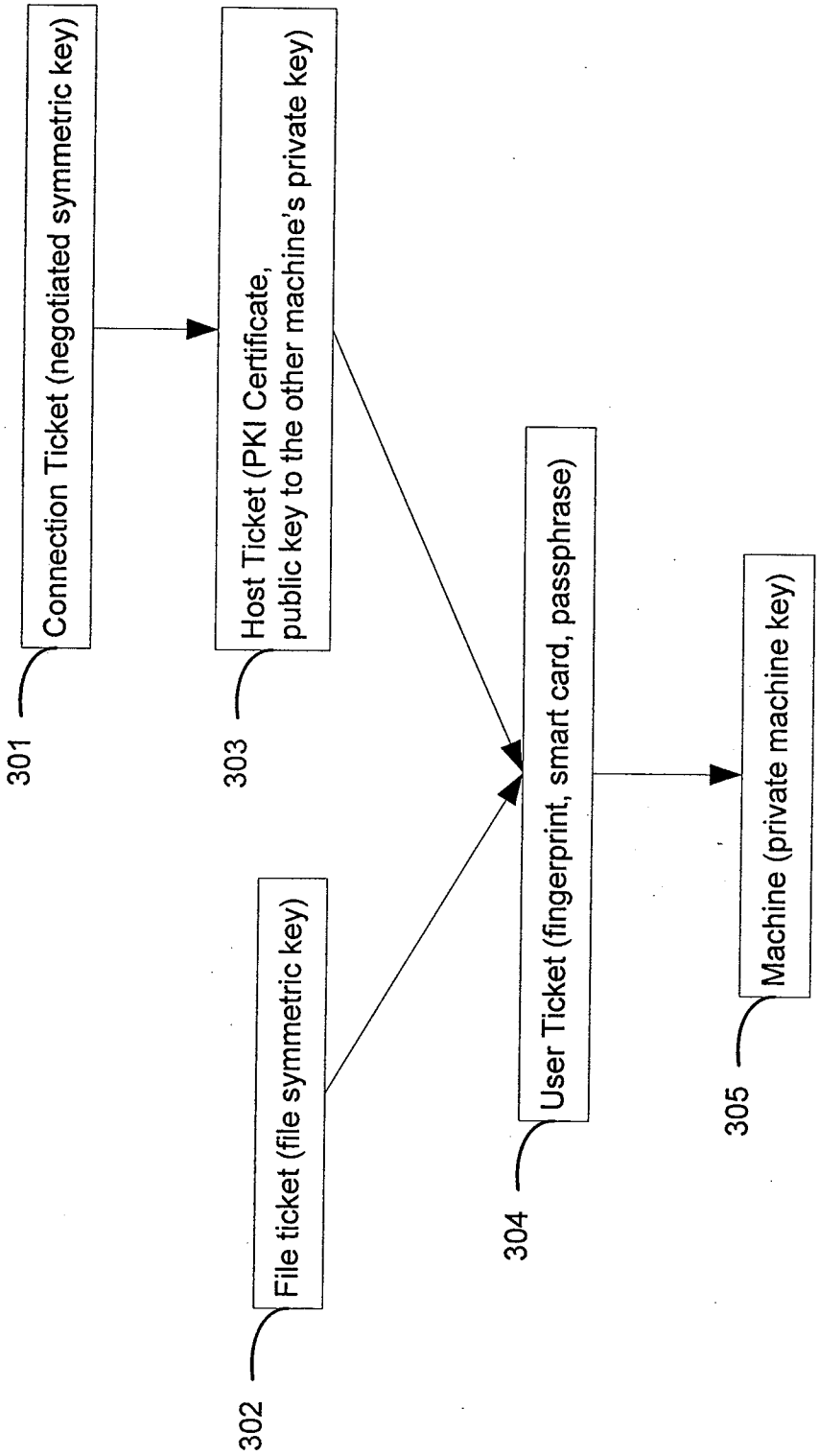

Connection Ticket (negotiated symmetric key)
Host Ticket (PKI Certificate, public key to the other machine's private key)
File ticket (file symmetric key)
User Ticket (fingerprint, smart card, passphrase)
Machine (private machine key)
301
303
302
304
305

FIG. 8

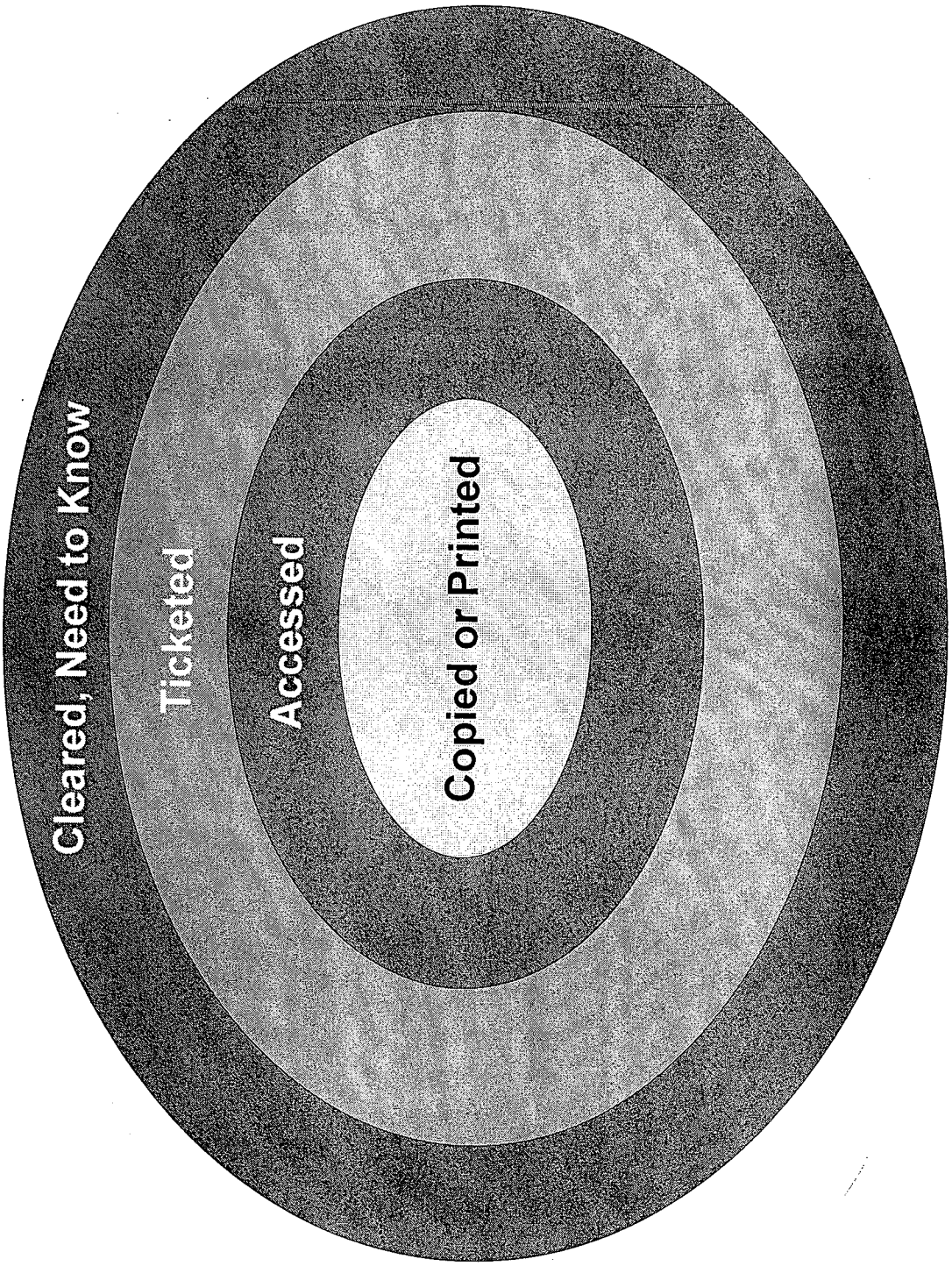


FIG. 9

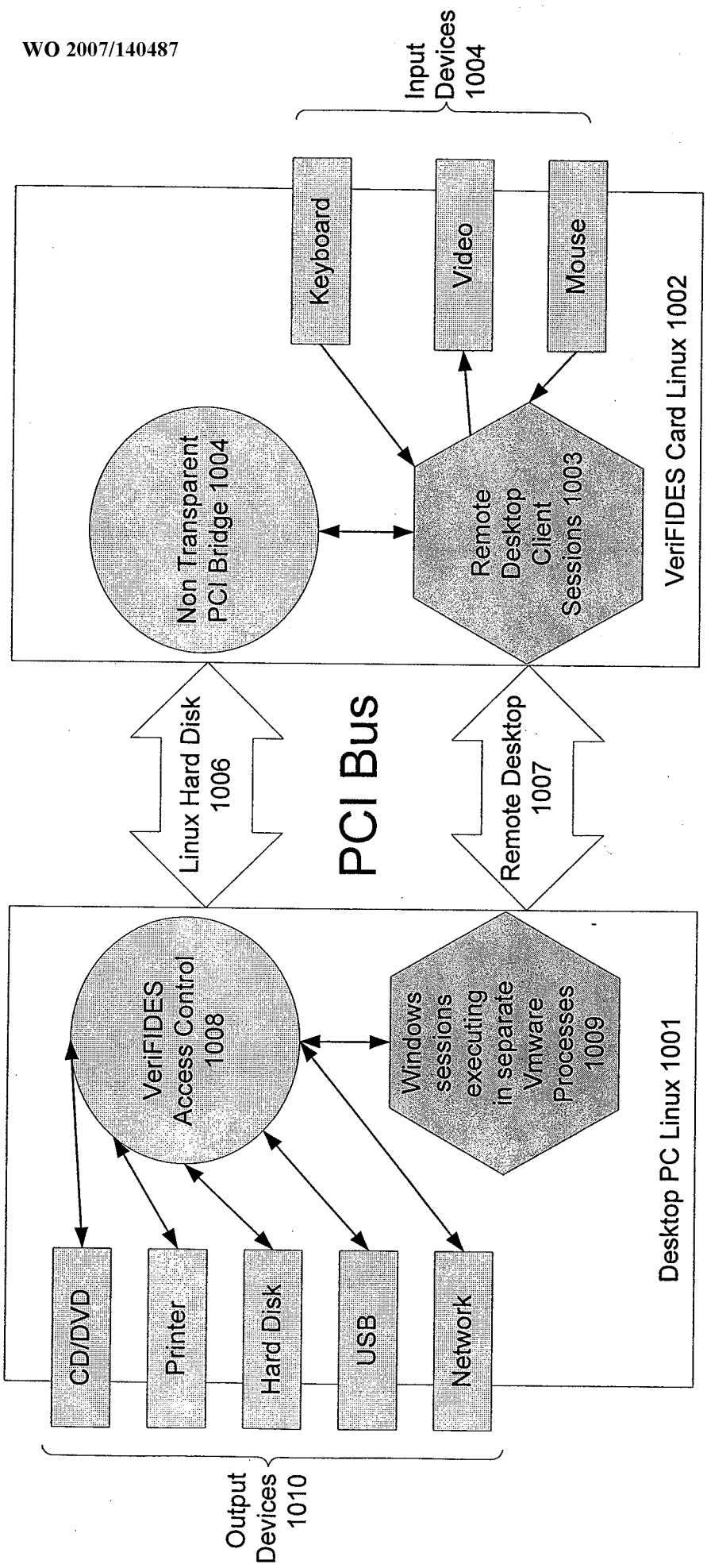

Input Devices 1004
Keyboard
Video
Mouse
VeriFIDES Card Linux 1002
Non Transparent PCI Bridge 1004
Remote Desktop Client Sessions 1003
Linux Hard Disk 1006
PCI Bus
Remote Desktop 1007
VeriFIDES Access Control 1008
Windows sessions executing in separate Vmware Processes 1009
Desktop PC Linux 1001
CD/DVD
Printer
Hard Disk
USB
Network
Output Devices 1010

FIG. 10

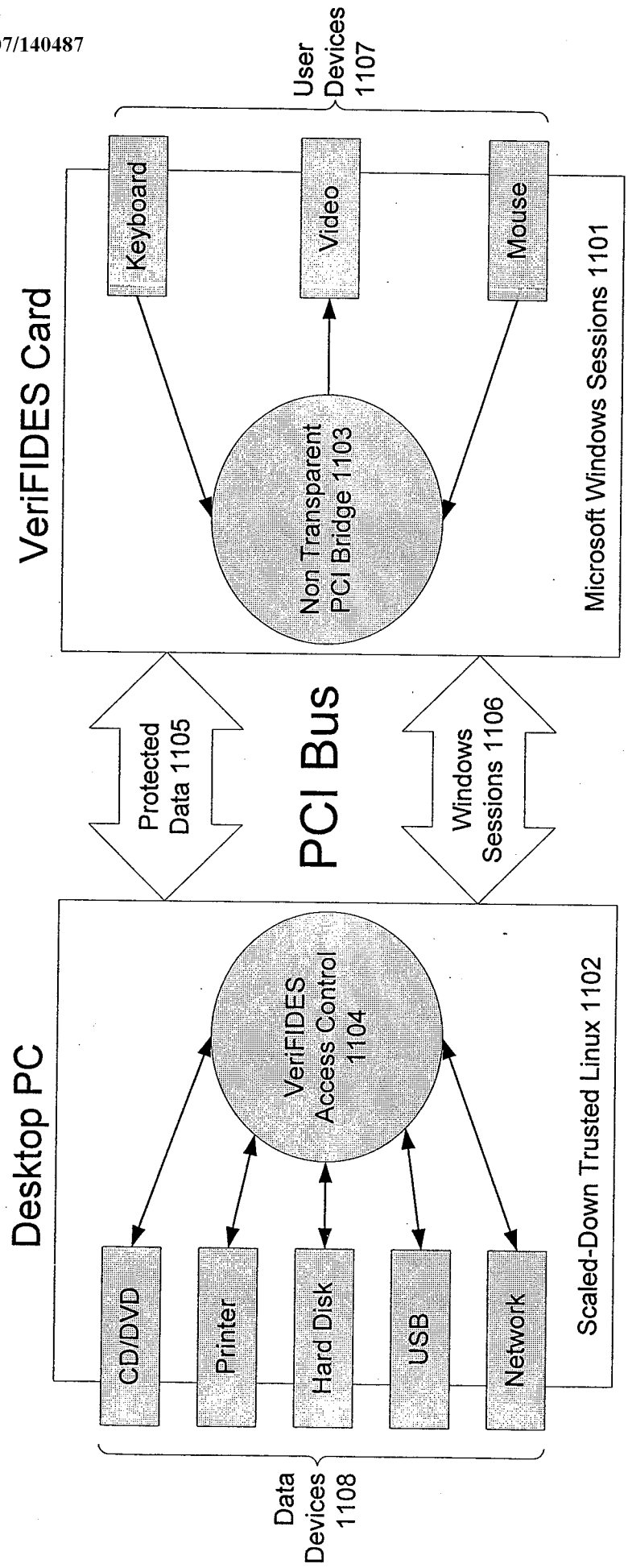

User Devices 1107
Keyboard
Video
Mouse
VeriFIDES Card
Non Transparent PCI Bridge 1103
Microsoft Windows Sessions 1101
Protected Data 1105
PCI Bus
Windows Sessions 1106
Desktop PC
VeriFIDES Access Control 1104
Scaled-Down Trusted Linux 1102
CD/DVD
Printer
Hard Disk
USB
Network
Data Devices 1108

FIG. 11

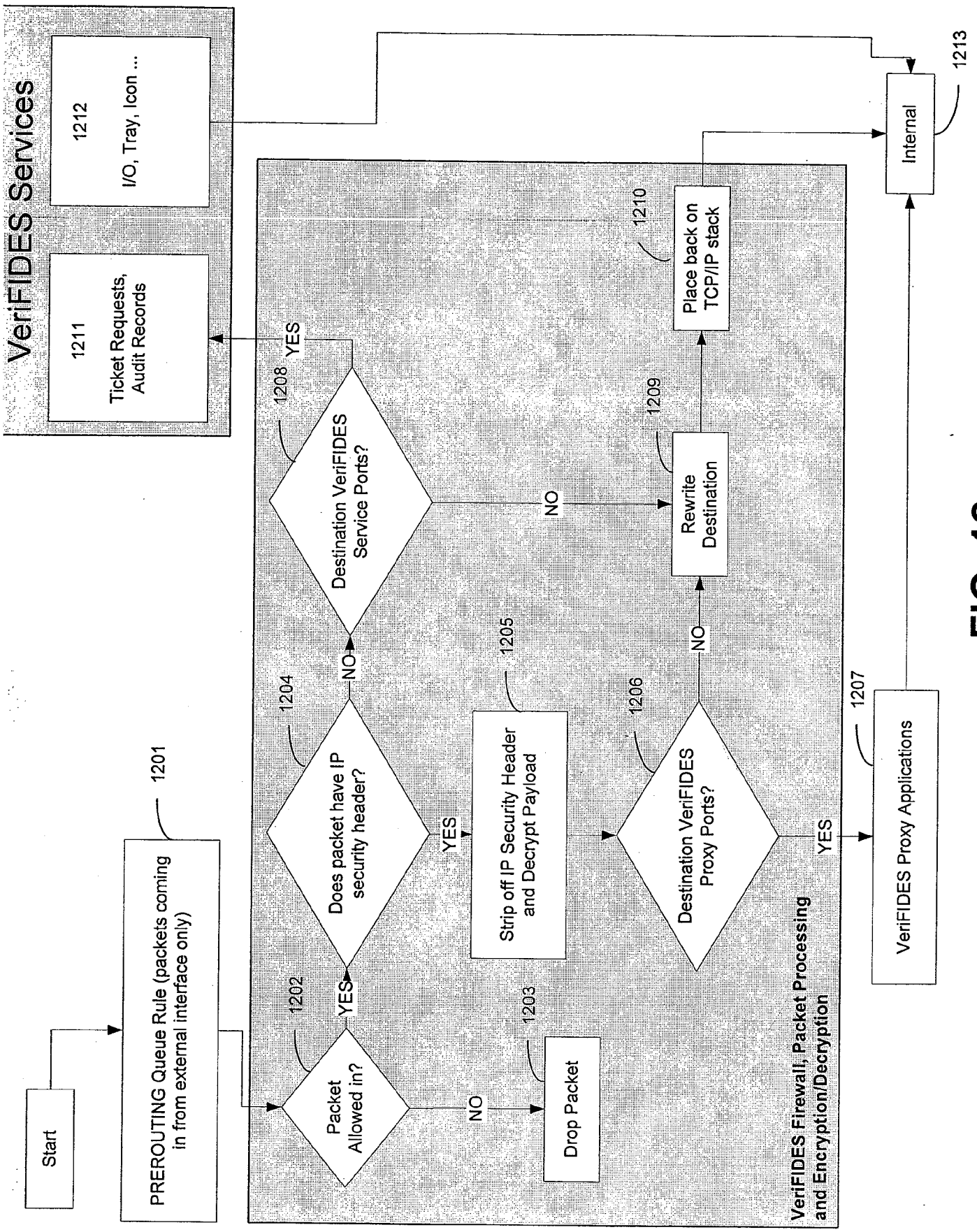

VeriFIDES Services
1212
I/O, Tray, Icon ...
1211
Ticket Requests, Audit Records
Start
PREROUTING Queue Rule (packets coming in from external interface only)
1201
Packet Allowed in?
1202
YES
NO
Drop Packet
1203
Does packet have IP security header?
1204
YES
NO
Strip off IP Security Header and Decrypt Payload
1205
Destination VeriFIDES Proxy Ports?
1206
YES
NO
Destination VeriFIDES Service Ports?
1208
YES
NO
Rewrite Destination
1209
Place back on TCP/IP stack
1210
VeriFIDES Proxy Applications
1207
Internal
1213
VeriFIDES Firewall, Packet Processing and Encryption/Decryption

FIG. 12

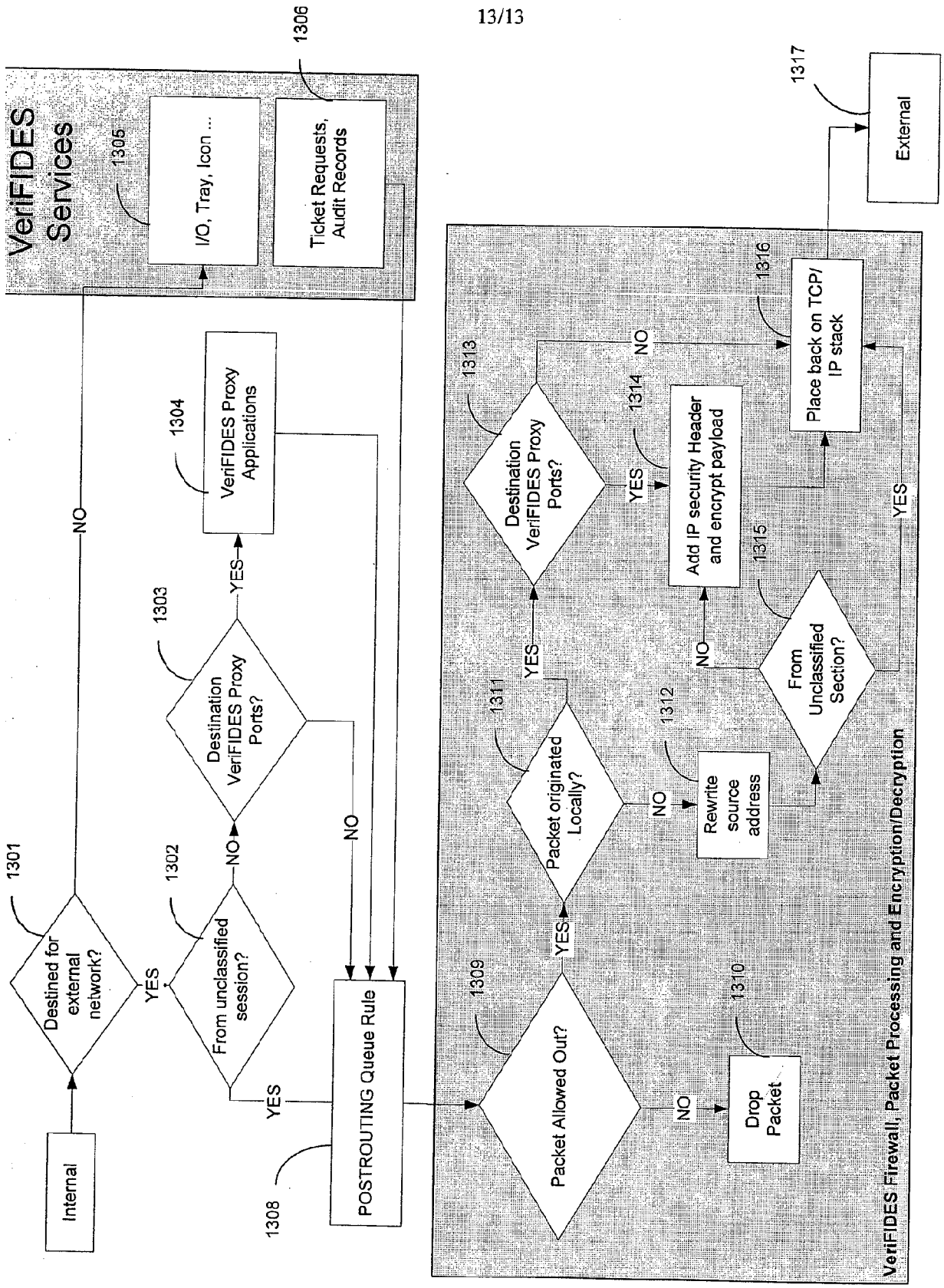

VeriFIDES Services
1306
1305
I/O, Tray, Icon ...
Ticket Requests, Audit Records
1304
VeriFIDES Proxy Applications
1303
Destination VeriFIDES Proxy Ports?
1302
From unclassified session?
1301
Destined for external network?
Internal
YES
NO
1308
POSTROUTING Queue Rule
VeriFIDES Firewall, Packet Processing and Encryption/Decryption
1309
Packet Allowed Out?
1310
Drop Packet
1311
Packet originated Locally?
1312
Rewrite source address
1313
Destination VeriFIDES Proxy Ports?
1314
Add IP security Header and encrypt payload
1315
From Unclassified Section?
1316
Place back on TCP/ IP stack
1317
External

FIG. 13